IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Änderung der DIN EN ISO 13849-1

Die wesentlichen Neuerungen aus 2015 im Überblick

Übersicht

Fast zehn Jahre nach Erstveröffentlichung der revidierten Fassung als DIN EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze“ erscheint voraussichtlich Anfang 2016 die erste Änderung dieser Norm als konsolidierte Fassung. Da primär ihre Lesbarkeit und Anwendbarkeit verbessert werden sollten, sind keine umfassenden Änderungen enthalten. Trotzdem sind eine Reihe von Detailverbesserungen und Ergänzungen eingeflossen, die sich in der praktischen Anwendung bemerkbar machen werden. Dazu gehören u. a. die Berücksichtigung der Eintrittswahrscheinlichkeit eines Gefährdungsereignisses bei der Festlegung des erforderlichen Performance Levels (PL_r), ein neues vereinfachtes Verfahren zur PL-Bestimmung für den Ausgangsteil des sicherheitsbezogenen Steuerungsteils (SRP/CS[1]) und ein Vorschlag zum Umgang mit Anforderungen an SRESW (Sicherheitsbezogene Embedded Software) bei Verwendung von Standardkomponenten. Dieser Beitrag stellt die wesentlichen Änderungen vor. Wo der Text der Änderung 1 einer Interpretation bedarf, werden Empfehlungen gegeben.

1 Einleitung

Die bisherige Tabelle 1 der Norm „Empfohlene Anwendung der IEC 62061 und ISO 13849-1“ ist durch eine Referenz auf den in der Zwischenzeit erstellten Technischen Report DIN ISO/TR 23849 [1] ersetzt. Dort wird ausführlich auf die Unterschiede und Gemeinsamkeiten beider Normen eingegangen.

2 Anwendungsbereich

Hier wird klargestellt, dass die Norm nur für SRP/CS mit hoher Anforderungsrate oder kontinuierlicher Anforderung gilt. Nach Definition 3.1.38 erfolgt die Anforderung bei dieser Betriebsart häufiger als einmal pro Jahr.

3 Begriffe, Formelzeichen und Abkürzungen

Für die „durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde“ wird die Abkürzung „PFH_D“[2] eingeführt. Die Dimension dieser Größe ist 1/Zeit, ihre gebräuchliche Einheit 1/h.

Die „mittlere Zeit bis zum gefahrbringenden Ausfall“ wird nun mit einem Index in Großbuchstaben als „$MTTF_D$“[3] notiert (vorher „$MTTF_d$“). Ebenso ändert sich die Schreibweise des Index in B_{10D} und T_{10D}.

[1] SRP/CS = Safety related parts of a control system
[2] PFH_D = Probability of a dangerous failure per hour
[3] $MTTF_D$ = Mean time to dangerous failure

4 Abschnitt 4 Gestaltungsaspekte und Anhang K

Neben der Aktualisierung der Verweise auf ISO 12100:2010 (statt der Vorgängernorm ISO 12100-1:2003) wird erläutert, dass Subsysteme eines SRP/CS auch nach anderen Normen zur Funktionalen Sicherheit (z. B. IEC 62061, IEC 61508, IEC 61496) entworfen werden können. Sie können dann – ggf. nach „Übersetzung“ eines SILs[4] in einen PL nach Tabelle 4 der Norm – als Subsystem integriert werden, wobei die Regeln zur „Kombination von SRP/CS“ (Abschnitt 6.3 der Norm) anzuwenden sind. DIN ISO/TR 23849 [1] erläutert dies ebenfalls.

Die Begrenzung der $MTTF_D$ für jeden Kanal auf 100 Jahre wird für Subsysteme der Kategorie 4 auf 2500 Jahre angehoben. Im Anhang K der Norm wurden die zusätzlichen PFH_D- Werte ergänzt. Die Begrenzung auf 100 Jahre war ursprünglich eingeführt worden, damit hohe Performance Level nicht nur auf der Basis einer hohen statistischen Zuverlässigkeit der Einzelkomponenten erreicht werden können. Da in Kategorie 4 Redundanz und Fehleraufdeckung (DC, Diagnostic coverage) schon auf sehr hohem Niveau liegen, kann die $MTTF_D$-Begrenzung hier angehoben werden. Dadurch können bessere PFH_D-Werte erreicht werden und es kann eine größere Anzahl von PL-e-Subsystemen kombiniert werden, ohne dass das Gesamt-SRP/CS auf PL d „abrutscht“. Weitere Hinweise finden sich auch in [2].

Bei den Annahmen für die vorgesehenen Architekturen, die die Basis für das vereinfachte Verfahren zur Abschätzung eines PL darstellen, gibt es zwei Änderungen:

- **Testhäufigkeit in Kategorie 2**
  Für Kategorie 2 galt bisher ausschließlich die Regel einer Anforderungsrate ≤ 1/100 der Testrate. Alternativ kann die Testung nun auch unmittelbar bei Anforderung der Sicherheitsfunktion erfolgen, wenn die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen sicheren Zustand (in der Regel wird die Maschine angehalten) kürzer ist als die Zeit zum Erreichen der Gefährdung. Hierzu erfolgt auch der Hinweis auf die Norm DIN EN ISO 13855 zur Berechnung von Sicherheitsabständen.

  Kapitel 4 des SISTEMA-Kochbuchs, Teil 4 [3] enthält weitere Ausführungen zur dieser Thematik.

- **$MTTF_D$ des Testkanals in Kategorie 2**
  Bisher wurde die $MTTF_{D,\,TE}$ der Testeinrichtung mit der $MTTF_{D,\,L}$ der Logik verglichen. Die neue Anforderung lautet: Für Kategorie 2 ist die $MTTF_D$ des gesamten Testkanals größer als die Hälfte der $MTTF_D$ des gesamten Funktionskanals. Diese neue Regel durfte bisher nur angewendet werden, wenn die Blöcke nicht aufgeteilt werden konnten.

Anhang K der Norm enthält zu diesem Thema ebenfalls eine neue Anmerkung, die auf das Verhältnis von Anforderungsrate zu Testrate eingeht:

- Wenn in Kategorie 2 die obige Bedingung an die Testrate (100-mal häufiger Testen als Anfordern) nicht eingehalten werden kann, aber die Anforderungsrate ≤ 1/25 der Testrate ist, dann können die PFH_D-Werte für Kategorie 2 aus Anhang K mit dem Faktor 1,1 multipliziert als Abschätzung zur sicheren Seite herangezogen werden.

In einer weiteren Anmerkung wird präzisiert, dass die PFH_D-Werte in Anhang K für alle Kategorien mit den diskreten DC_{avg}-Werten 60 %, 90 % und 99 % berechnet wurden.

[4] SIL = Safety integrity level

5 Neues vereinfachtes Verfahren für den Ausgangsteil des SRP/CS (Energieübertragungselemente) zur Bestimmung von PL und PFH_D ohne $MTTF_D$

Als Reaktion auf Forderungen aus der praktischen Anwendung wurde als neuer Abschnitt 4.5.5 der Norm ein zusätzliches und weiter vereinfachtes Verfahren aufgenommen zur Bestimmung von PFH_D und der quantifizierbaren Aspekte des PL für das Ausgangs-Subsystem. Die Bestimmung stützt sich hauptsächlich auf die realisierte Kategorie inklusive DC_{avg} und CCF (common cause failures). Eine Berechnung der (Kanal-)$MTTF_D$ entfällt, dafür müssen durchgängig bewährte (in Kategorien 1, 2, 3 und 4) oder betriebsbewährte („proven-in-use“) Bauteile (in Kategorien 2, 3 und 4) verwendet werden.

Betriebsbewährt ist eine neue Eigenschaft im Rahmen der Norm, nicht zu verwechseln mit bewährten Bauteilen. Der Nachweis der Betriebsbewährung basiert auf einer Analyse der betrieblichen Erfahrung für eine spezielle Konfiguration eines Bauteils in einer bestimmten Applikation. Die Analyse muss ergeben, dass die Wahrscheinlichkeit gefahrbringender systematischer Fehler niedrig genug ist, damit jede Sicherheitsfunktion, die das Bauteil verwendet, ihren erforderlichen Performance Level (PL_r) erreicht. Ein solcher Nachweis ist im Maschinenbau bisher unüblich. Es ist auch unklar, warum die Anforderung sich nur auf systematische Fehler bezieht und die zufälligen Bauteilfehler nicht berücksichtigt.

Das neue Verfahren zur Bestimmung von PL und PFH_D ist nur in besonderen Fällen anwendbar, und zwar:

- für den Ausgangsteil des SRP/CS und
- wenn für mechanische, hydraulische oder pneumatische Bauteile (oder Bauteile gemischter Technologie, z. B. mechanische Bremse mit pneumatischer Ansteuerung) keine anwendungsspezifischen Zuverlässigkeitsdaten ($MTTF_D$, Ausfallrate, B_{10D} o. Ä.) verfügbar sind.

Tabelle 1 stellt – abhängig von der realisierten Kategorie und unter den an das Verfahren geknüpften Zusatzbedingungen – den abschätzbaren PFH_D-Wert und den damit erreichbaren PL dar.

Tabelle 1: PL und PFH_D als Abschätzung zur sicheren Seite basierend auf Kategorie, DC_{avg} und der Verwendung bewährter Bauteile (in Anlehnung an die Tabelle im neuen Abschnitt 4.5.5 der Norm).

	PFH_D in 1/h		Kat. B	Kat. 1	Kat. 2	Kat. 3	Kat. 4
PL b	$5{,}0 \cdot 10^{-6}$	⇦	●	○	○	○	○
PL c	$1{,}7 \cdot 10^{-6}$	⇦	-	●	●	○	○
PL d	$2{,}9 \cdot 10^{-7}$	⇦	-	-	-	●	○
PL e	$4{,}7 \cdot 10^{-8}$	⇦	-	-	-	-	●
●	Angewandte Kategorie wird empfohlen						
○	Angewandte Kategorie ist optional						
-	Kategorie ist nicht zulässig						

Dabei sind an das Verfahren folgende Zusatzbedingungen geknüpft:

- in Kategorie 1: Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien (wie bisher und in der Kategorie-1-Definition verankert)
- in Kategorie 2: $MTTF_D$ des Testkanals beträgt mindestens 10 Jahre
- in Kategorie 2, 3 und 4: Verwendung bewährter oder betriebsbewährter Bauteile, Verwendung bewährter Sicherheitsprinzipien. Bei Kategorie 2 gilt dies nach der Norm auch für den Testkanal.
- in Kategorie 2 und 3: ausreichende Maßnahmen gegen CCF und für jedes Bauteil DC mindestens „niedrig“
- in Kategorie 4: ausreichende Maßnahmen gegen CCF und für jedes Bauteil DC „hoch“

Ergänzend werden folgende Hinweise gegeben:

- Kategorie 1: Für sicherheitsbezogene Bauteile sollen vom Maschinenhersteller die T_{10D}-Werte auf der Basis von Daten zur Betriebsbewährung eines Bauteils bestimmt werden, es sei denn, deren Ausfall macht sich im technischen Prozess bemerkbar.
- Kategorie 2, 3 und 4: Da zur DC_{avg}-Berechnung wegen fehlender $MTTF_D$-Werte nicht auf die Formel E.1 der Norm zurückgegriffen werden kann, wird hier DC_{avg} einfach als arithmetischer Mittelwert der Einzel-DCs aller Komponenten in den Funktionskanälen des Ausgangsteils gebildet.

6 Umgang mit Anforderungen an SRESW (Sicherheitsbezogene Embedded Software) bei Verwendung von Standardkomponenten

Die Verwendung von zugekauften industriellen Standardkomponenten, die nicht speziell für den Einsatz in Sicherheitsfunktionen entwickelt wurden, aber Embedded Software enthalten, hat die Norm bisher nicht thematisiert. Es gibt aber in der Praxis viele SRP/CS-Beispiele, die solche Standardkomponenten wie speicherprogrammierbare Steuerungen (SPS), Frequenzumrichter oder Sensoren verwenden und die Sicherheit – z. B. durch diversitäre Redundanz mit Fehlererkennung – auf Systemebene realisieren. Ein solches Beispiel mit einer Standard-SPS und einem Standard-Frequenzumrichter ist in Anhang I der Norm dargestellt. Da Hersteller für solche Standardkomponenten die Einhaltung der SRESW-Anforderungen in der Regel nicht bestätigen und dies bei der Integration nicht nachträglich geleistet werden kann, wurde die Erfüllung der SRESW-Anforderungen bisher nicht nachgewiesen.

In Änderung 1 wird für solche Standardkomponenten nun der Verzicht auf den Nachweis der SRESW-Anforderungen erlaubt unter folgenden Bedingungen:

- das SRP/CS ist auf PL a oder PL b begrenzt und verwendet Kategorie B, 2 oder 3;
- das SRP/CS ist auf PL c oder PL d begrenzt und darf mehrere Bauteile für zwei Kanäle in Kategorie 2 oder 3 verwenden. Die Bauteile dieser beiden Kanäle verwenden diversitäre Technologien. Die geforderten diversitären Technologien in beiden Kanälen führen dazu, dass die Wahrscheinlichkeit eines gefährlichen Ausfalls des SRP/CS durch einen Fehler in der SRESW stark verringert wird.

Neben den SRESW-Anforderungen sind nach Norm weitere, mehr hardwarebezogene Anforderungen zu beachten, z. B. hinsichtlich Vermeidung und Beherrschung systematischer Fehler oder Eig-

nung für die zu erwartenden Umweltbedingungen wie Klima, Vibration, elektromagnetische Verträglichkeit. Diese Anforderungen gelten unabhängig von der SRESW weiterhin. Dazu gehört auch, dass bereits ab Kategorie B grundlegende Sicherheitsprinzipien und ab Kategorie 1 bewährte Sicherheitsprinzipien verwendet werden müssen. Für alle Kategorien sind außerdem die Basisanforderungen der Kategorie B zu erfüllen: Das SRP/CS muss mindestens in Übereinstimmung mit den zutreffenden Normen gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert sein, also z. B. in Übereinstimmung mit DIN EN 61131-2 für SPS oder DIN EN 61800-1/-2 für Standard-Frequenzumrichter.

Die qualitätsgesicherte Entwicklung nach DIN EN ISO 900x wird in der Norm nicht explizit gefordert, stellt aber eine sinnvolle Anforderung dar, die sich in den sieben Basismaßnahmen für PL a und b aus Abschnitt 4.6.2 der Norm für selbstentwickelte SRP/CS mit Embedded Software (SRESW) widerspiegelt.

7 Abschnitt 5, Sicherheitsfunktionen

Hier wurde ein Hinweis ergänzt, dass es je nach Anwendung hilfreich ist, eine separate Sicherheitsfunktion für den Ausfall der Energie zu definieren. Ein Beispiel sind Vertikalachsen, deren Absinken durch die Schwerkraft auch im Fall des Energieverlustes verhindert werden soll. Bei vorhandener Energie wird die Achse z. B. durch einen elektrischen Antrieb hochgehalten, während bei Energieverlust eine mechanische Bremse zum Einsatz kommt (siehe [4] Abschnitte 4.3 und 6.4.2 sowie Beispiel 14).

8 Abschnitt 6, Kategorien

Wenn die Einleitung eines sicheren Zustands nach Erkennung eines Fehlers nicht möglich ist (z. B. durch Verschweißen des Kontakts eines Schaltglieds), war es bisher in Kategorie 2 erlaubt, „nur“ eine Warnung vor der Gefährdung bereitzustellen.

Nun wird – abhängig vom PL_r – genau festgelegt, wann eine Warnung in Frage kommt:

- Für PL_r a bis zu einschließlich PL_r c muss die Ausgabe (OTE) **wenn möglich** einen sicheren Zustand einleiten, der bis zur Behebung des Fehlers beibehalten wird. Wenn das Einleiten eines sicheren Zustands nicht möglich ist (z. B. durch Verschweißen des Kontakts eines Schaltglieds), kann es ausreichen, wenn der Ausgang der Testeinrichtung (OTE) nur eine Warnung bereitstellt.

- Für PL_r d **muss** der Ausgang (OTE) einen sicheren Zustand einleiten, der bis zur Behebung des Fehlers beibehalten wird. Eine Warnung ist in diesem Fall nicht mehr ausreichend.

9 Abschnitt 6, Kombination von SRP/CS

Mittlerweile geben Hersteller für fast alle auf dem Markt erhältlichen SRP/CS (gekapselte Subsysteme) neben dem PL (oder SIL) auch den PFH_D-Wert an. Bei selbst entwickelten SRP/CS sind diese Werte ohnehin vorhanden. Daher kann man bei der Kombination (Reihenschaltung) von SRP/CS, die zusammen eine Sicherheitsfunktion ausführen, folgendermaßen vorgehen:

- Begrenzung durch nicht quantifizierbare Aspekte: Der Gesamt-PL ist höchstens so groß wie der niedrigste PL aller kombinierten SRP/CS, und

- Begrenzung durch quantifizierbare Aspekte: Der Gesamt-PL ist höchstens so groß wie der PL, der – nach Tabelle 3 der Norm – der Summen-PFH_D entspricht. Die Summen-PFH_D wird gebildet als Summe der PFH_D-Werte aller kombinierten SRP/CS.

Das bisher in der Norm beschriebene Kombinationsverfahren nach Tabelle 11 ist nur noch als Ausnahme vorgesehen, falls für die kombinierten SRP/CS nur PL-Werte, aber keine PFH_D-Werte vorliegen.

10 Anhang A, PL_r-Bestimmung

In Anhang A gibt es mehrere Änderungen. Zunächst wird der informative Charakter des in Anhang A dargestellten Verfahrens zur PL_r-Bestimmung deutlicher hervorgehoben: Es ist nicht verbindlich und stellt nur eine Einschätzung der Risikominderung dar. Typ-C-Normen dürfen – aufgrund des im Expertenkreis getroffenen normativen Kompromisses unter Berücksichtigung von Gründen, die auch außerhalb der Parameter des Risikographen liegen können – in ihren PL_r-Festlegungen durchaus von dem PL_r abweichen, wie er sich nach dem Risikographen ergäbe.

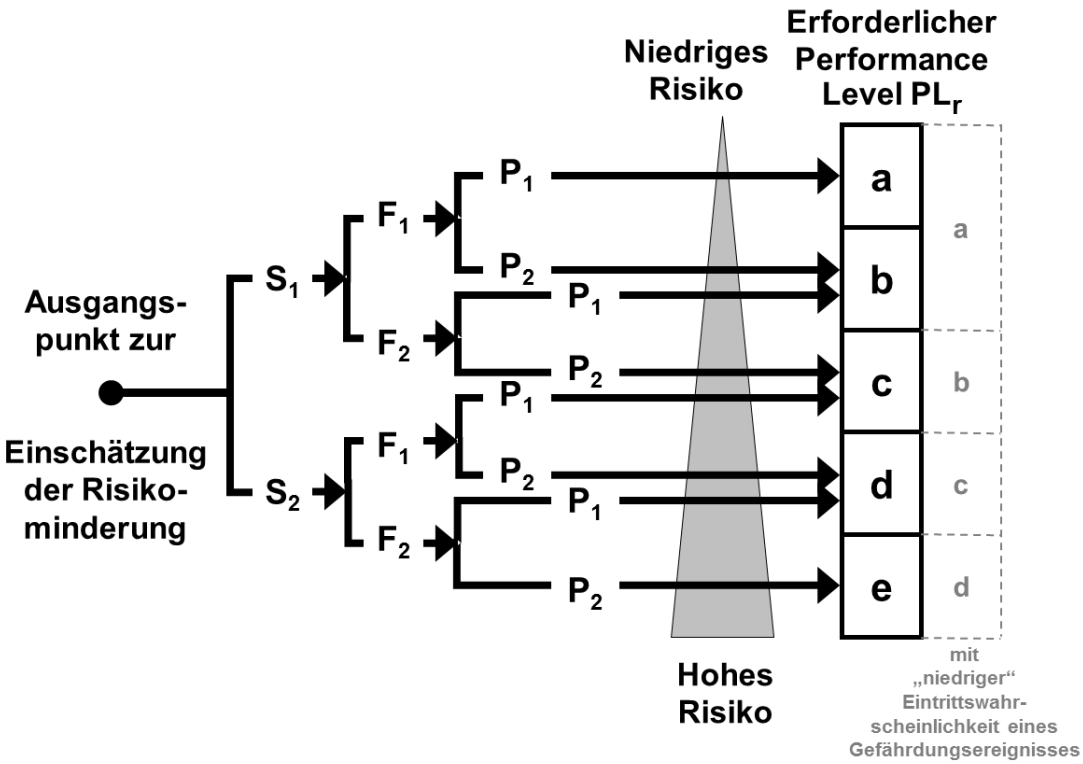
Die Anmerkung zur Unterscheidung von F1 und F2 ist nun folgendermaßen formuliert:

- Liegt keine andere Rechtfertigung vor, sollte F2 gewählt werden, wenn die Häufigkeit höher als einmal alle 15 Minuten ist.

- F1 darf gewählt werden, wenn die gesamte Expositionsdauer 1/20 der gesamten Betriebsdauer nicht überschreitet und die Häufigkeit nicht höher als einmal alle 15 Minuten ist.

Neu hinzu kommt nun die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses. Wenn sie als niedrig bewertet werden kann, darf der PL_r um einen Level verringert werden. Eine weitere Reduzierung von PL_r a ist dabei nicht vorgesehen, siehe Abbildung 1.

Abbildung 1: Ableitung des PL_r aus den Risikoparametern S, F und P mit zusätzlicher Möglichkeit zur Abstufung durch Berücksichtigung der Eintrittswahrscheinlichkeit eines Gefährdungsereignisses (in Anlehnung an den Graphen in Anhang A der Norm)



Die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses ist aus DIN EN ISO 12100 bekannt (dort „Eintritt eines Gefährdungsereignisses“) und in DIN ISO/TR 14121-2 als O-Parameter benannt (in DIN EN 62061: W-Parameter). Sie wird in der Norm im Zusammenhang mit dem P-Parameter genannt, aber unabhängig von diesem ermittelt. Ihre Bewertung hängt vom menschlichen Verhalten oder vom technischen Versagen ab und ist meist nur schwer mit der erforderlichen statistischen Verlässlichkeit abschätzbar. Zuverlässigkeitsdaten und die Unfallgeschichte an vergleichbaren Maschinen (mit denselben Risiken, gleichem Prozess, derselben Betätigung durch die Bedienperson und gleichen Technologien, die die Gefährdung verursachen) können die Einschätzung begründen. Bei der Unfallgeschichte ist jedoch zu beachten, dass diese in der Regel auf bereits installierten technischen Schutzmaßnahmen basiert und nicht auf der Situation vor Festlegung der beabsichtigten Sicherheitsfunktion (Startpunkt des Risikographen). Eine niedrige Zahl an Unfällen könnte also die bestehende PL_r-Einschätzung, auf der die Unfallgeschichte basiert, bestätigen. Sie ist aber nicht als Argument geeignet, den festzulegenden PL_r niedriger abzuschätzen als es dem aktuellen Stand entspricht.

Die Norm greift mit einem neuen Abschnitt A.3 nun auch das Thema „Überlagerte Gefährdungen“ auf und stellt klar, dass während der Risikobewertung jede Gefährdung getrennt bewertet werden kann. Die Sicherheitsfunktionen für getrennte Gefährdungen dürfen separiert werden, sodass als Ausgang des zugehörigen SRP/CS jeweils nur die Leistungssteuerungselemente für **eine** Gefährdung auftauchen (und in die PFH_D eingehen). In einer Fertigungszelle mit mehreren Robotern können die sicherheitsbezogenen Stoppfunktionen, z. B. als Reaktion auf das Öffnen einer Schutztür, folglich als separate Sicherheitsfunktionen für jeden Roboter einzeln definiert werden. Die gleiche Betrachtung gilt z. B. bei mehreren Klemmvorrichtungen an einem Drehtisch. Wenn aber in einem Maschinenteil mehrere Gefährdungen direkt miteinander verbunden sind, dann ist auch eine gemeinsame Betrachtung in einer kombinierten Sicherheitsfunktion angeraten. Ein Beispiel ist ein kontinuierlich arbeitender Schweißroboter, an dem eine Bedienperson gleichzeitig den vom Tool-Center-Point ausgehenden Gefährdungen „Quetschen durch Bewegen“ und „Verbrennen durch den Schweißvorgang“ ausgesetzt ist. Detailliertere Erläuterungen zur Bewertung von überlagerten Gefährdungen finden sich in [5, 6].

11 Anhänge C und D, $MTTF_D$-Werte

In Tabelle C.1 zum „Verfahren guter ingenieurmäßiger Praxis“ haben sich an mehreren Stellen Änderungen ergeben, die sich aus der praktischen Anwendung als notwendig erwiesen haben:

- Für hydraulische Bauteile (im Wesentlichen Ventile) können nun – abhängig von der mittleren Anzahl jährlicher Betätigungen n_{op} – auch höhere typische $MTTF_D$-Werte angesetzt werden. Der bisherige $MTTF_D$-Wert von 150 Jahren kann bei n_{op} kleiner als 1 000 000 Zyklen/Jahr auf 300 Jahre verdoppelt werden. Noch seltenere Betätigung (weniger als 500 000 oder weniger als 250 000 Zyklen/Jahr) führt zu weiteren Verdoppelungen auf 600 und 1200 Jahre. Die Betrachtung wurde damit derjenigen von pneumatischen Bauteilen angenähert.

- Der typische B_{10D}-Wert für Schütze mit nominaler Last wurde von 2 000 000 Zyklen auf 1 300 000 Zyklen reduziert. Dies ist in der Produktnorm für Schütze (DIN EN 60947-4-1) begründet, die einen Anteil gefährlicher Ausfälle von 74% angibt.

- Die beiden Zeilen für Not-Halt-Geräte wurden zusammengefasst. Not-Halt-Geräte und Zustimmungsschalter können je nach Anzahl der elektrischen Ausgangskontakte und der Fehlererkennung im nachgeordneten SRP/CS als Teilsysteme der Kategorie 1 oder Kategorie 3/4 abgeschätzt werden. Jedes Kontaktelement (einschließlich der Mechanik) kann als ein Kanal mit entsprechendem B_{10D}-Wert von 100 000 Zyklen betrachtet werden. Für Zustimmungsschalter umfasst dies beide Öffnungsfunktionen, das Durchdrücken oder Loslassen. Unabhängig davon

kann auch DIN EN ISO 13849-2, Tabelle D.8 angewendet werden, wonach unter bestimmten Bedingungen ein Fehlerausschluss erlaubt wird. Detaillierte Erläuterungen zur Modellierung von Not-Halt-Geräten, Zustimmungsschaltern, Positionsschaltern, Zuhaltungen und Drucktastern wird der überarbeitete BGIA-Report 2/2008 enthalten.

In den Tabellen C.2 bis C.7 für Halbleiter und passive Bauteile wurde die Spalte „$MTTF_D$ für Bauteile, ungünstigster Fall“ gelöscht. Die hier mit einem Sicherheitsfaktor von 10 gegenüber dem typischen Fall genannten Zahlen haben keine praktische Relevanz, da für die meisten Bauteile dieser Art besser geeignete Ausfalldaten direkt vom Hersteller erhältlich sind und sonst der „typische Fall“ als Abschätzung ausreichend ist.

Auch in Tabelle D.1 zum „Parts-Count-Verfahren“ werden für die elektrischen Bauteile nun typische Werte statt des ungünstigsten Falls angesetzt.

12 Anhang E, Diagnosedeckungsgrad

In Tabelle E.1 sind wegen mangelnder Praxisrelevanz zwei Maßnahmen gelöscht:

- Redundanter Abschaltpfad ohne Überwachung des Antriebselements (DC = 0 %)

- Redundanter Abschaltpfad mit Überwachung eines der Antriebselemente entweder durch die Logik oder durch eine Testeinrichtung (Der DC ist für jeden Abschaltpfad einzeln abzuschätzen, eine kombinierte Betrachtung ist nicht sinnvoll.).

Die DC-Maßnahme „Fehlererkennung durch den Prozess“ wird nun näher erläutert:

- Um den DC im angegebenen Bereich von 0 bis 99 % abzuschätzen, können zunächst alle relevanten gefahrbringenden Ausfälle identifiziert werden, um dann zu entscheiden, welche dieser Ausfälle im Prozess erkannt werden. Aus dem erkannten Anteil kann dann einer der Werte kein (0 %), niedrig (60 %), mittel (90 %) oder hoch (99 %) abgeschätzt werden.
  Dieser Hinweis gilt sinngemäß auch für andere Maßnahmen, für die eine DC-Spanne angegeben ist, z. B. „Indirekte Überwachung“.

- Diese Maßnahme darf für ein Bauteil selbstverständlich nur dann herangezogen werden, wenn gefahrbringende Ausfälle dieses Bauteils sich überhaupt im (Fertigungs-)Prozess offenbaren. Werden dagegen Bauteile nur durch die Anforderung der Sicherheitsfunktion betätigt, dann kann keine Fehlererkennung durch den Prozess beansprucht werden.

13 Anhang F, CCF

In Tabelle F.1 wurde an einigen Stellen die Lesbarkeit verbessert oder Informationen wurden ergänzt.

14 Anhang I, Beispiele

Im Anhang I (Beispiele) erfolgten einige Aktualisierungen, um die dargestellten Inhalte besser auf den Rest der Norm, besonders die Anhänge C bis F, abzustimmen. Beispielsweise werden die $MTTF_D$-Werte beider Schalter und des Schützes jetzt aus B_{10D}-Werten über n_{op} ermittelt.

15 Fazit

Die Normensetzung hat mit der nun vorliegenden Änderung 1 zur DIN EN ISO 13849-1 einen wichtigen Beitrag für eine bessere Anwendbarkeit geleistet und ist vielfach auf die Anregungen aus der Praxis eingegangen. Die Ergänzungen und Anpassungen führen aber im Allgemeinen nicht dazu, dass bestehende SRP/CS einer Neubewertung zu unterziehen sind. Eine teilweise von Expertenseite befürwortete grundlegende Überarbeitung der Anforderungen zur Gestaltung von sicherheitsbezogener Software konnte im Rahmen dieser Änderung allerdings nicht durchgeführt werden.

Die bekannten Anwendungshilfen des IFA zur DIN EN ISO 13849 werden sukzessive an die Änderung der Norm angepasst und unter www.dguv.de/ifa/13849 verfügbar gemacht. Die PLC-Drehscheibe [7] steht bereits in einer überarbeiteten Fassung zur Verfügung. Der Software-Assistent SISTEMA wird in einer Version 2.0 alle Änderungen enthalten und auch die Reports 2/2008 und 7/2013 inklusive der Schaltungsbeispiele werden an den neuen Stand der Norm angepasst.

16 Literatur

[1] DIN ISO/TR 23849; DIN SPEC 33883: Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen (12.14). Beuth, Berlin 2014

[2] 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/webcode/m199422

[3] Hauke, M.; Apfeld, R.: Das SISTEMA-Kochbuch – Teil 4: Wenn die vorgesehenen Architekturen nicht passen – Version 1.0 (DE). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2012 http://www.dguv.de/webcode/m207360

[4] Apfeld, R.; Zilligen, H.; Köhler, B.: Sichere Antriebssteuerungen mit Frequenzumrichtern (IFA Report 7/2013). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2013
http://www.dguv.de/webcode/d639540

[5] Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachausschuss-Informationsblatt Nr. 047, Ausgabe 5.2010. Hrsg: Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau, Mainz
http://www.bghm.de/fileadmin/user_upload/Arbeitsschuetzer/Praxishilfen/Fachbereichs-Informationsblaetter/047_MFS_A2010-05_ueberlagerteGefaehrdung.pdf

[6] Apfeld, R.; Schaefer, M.: Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2011
http://publikationen.dguv.de/dguv/pdf/10002/sicherheitsfunktionen.pdf

[7] Schaefer, M.; Hauke, M.: Performance Level Calculator – PLC. 5. Auflage. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2015
http://www.dguv.de/webcode/d3508

Autoren: Michael Hauke, Ralf Apfeld, Thomas Bömer, Michael Huelke, Paul Rempel, Björn Ostermann
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin