



Praktische Erfahrungen mit der DIN EN ISO 13849-1

Die mögliche Verlängerung der dreijährigen Übergangsfrist für die DIN EN 954-1 (alte ISO 13849-1) über das Jahresende hinaus hat in den letzten Wochen für viele Diskussionen gesorgt. Feedback aus der Praxis zeigt die Praktikabilität der neuen Norm ISO 13849-1:2006, offenbart aber auch, dass Anwender durchaus Detailfragen stellen.

Die in Europa eher als DIN EN 954-1 bekannte Norm ISO 13849-1 für sicherheitsbezogene Maschinensteuerungen wurde nach einer umfangreichen Revision Ende 2006 neu veröffentlicht. Dabei sind bewährte deterministische Anforderungen

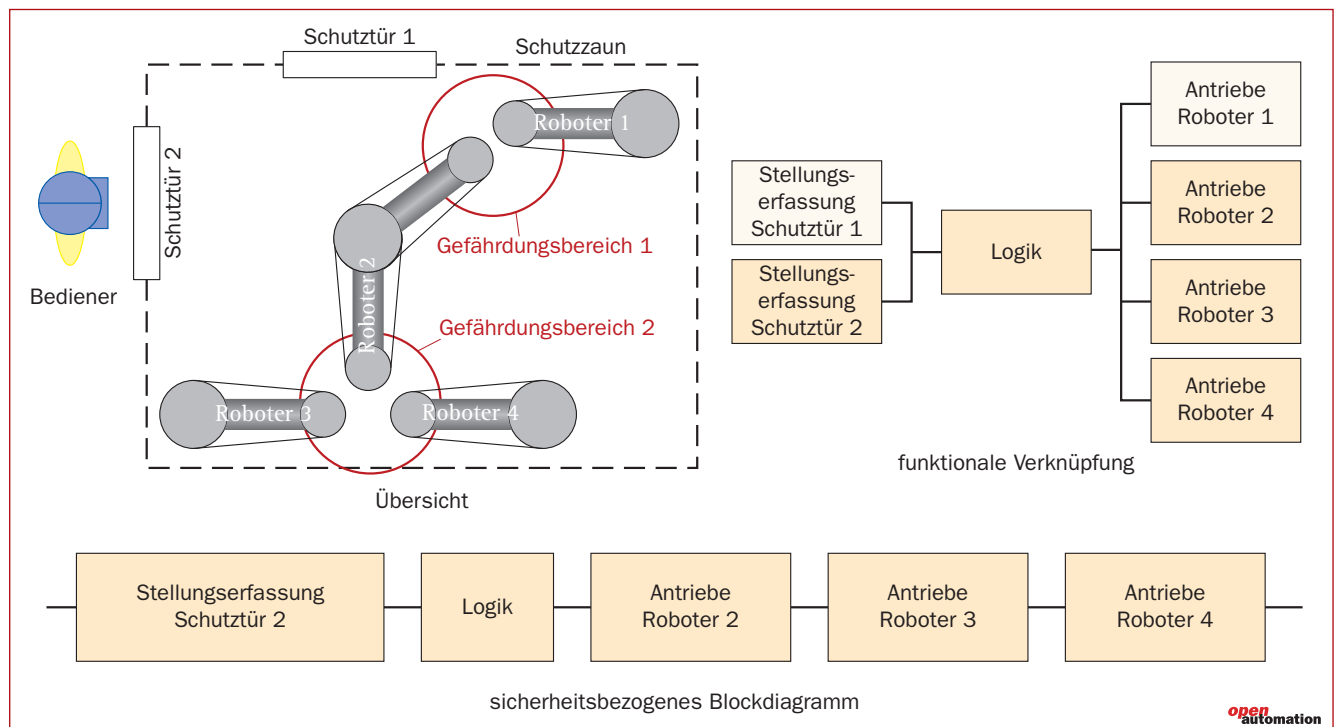
(Kategorien) zusammen mit einer Berechnung der Ausfallwahrscheinlichkeit (PFH-Wert, average probability of dangerous failure per hour) in das neue Konzept des Performance Level (PL) eingeflossen. Die dringend notwendige inhaltliche Modernisierung berücksichtigt auch neuere Technologien, wie Elektronik und Software. Das BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung unterstützt Industrie und Prüfstellen bei der Umsetzung der neuen Konzepte durch praktische Interpretations- und Anwendungshilfen, wie dem BGIA-Report 2/2008 und das Programm Sistema. In

der Anwendung der revidierten Normfassung haben sich einige Detailfragen ergeben. Die Autoren beantworten hier einige der Fragen, die vielen Anwendern derzeit „unter den Nägeln brennen“.

Ralf Apfeld, Thomas Bömer, Michael Hauke, Dr. Michael Huelke und Dr. Michael Schaefer sind Mitarbeiter des BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung.

Wie viele Sensoren und Aktoren sind an einer Sicherheitsfunktion beteiligt?

Als Sicherheitsfunktion im Sinn der Norm wird die sicherheitsgerichtete Reaktion auf ein auslösendes Ereignis verstanden, wenn die erforderliche Risikominderung von der Zuverlässigkeit einer sicherheitsbezogenen Steuerung abhängt. Beispielsweise soll das Öffnen jeder Schutz-



Die bei der Berechnung der PFH für eine Sicherheitsfunktion zu berücksichtigenden Sensoren und Aktoren hängen von der örtlichen und zeitlichen Überlagerung von Gefährdungen bezogen auf einen Bediener ab



MTTF _d jedes Kanals Jahre	PFH 1/h
100	2,47 × 10 ⁻⁸
110	2,23 × 10 ⁻⁸
120	2,03 × 10 ⁻⁸
130	1,87 × 10 ⁻⁸
150	1,61 × 10 ⁻⁸
160	1,50 × 10 ⁻⁸
180	1,33 × 10 ⁻⁸
200	1,19 × 10 ⁻⁸
220	1,08 × 10 ⁻⁸
240	9,81 × 10 ⁻⁹
270	8,67 × 10 ⁻⁹
300	7,76 × 10 ⁻⁹
330	7,04 × 10 ⁻⁹
360	6,44 × 10 ⁻⁹
390	5,94 × 10 ⁻⁹
430	5,38 × 10 ⁻⁹
470	4,91 × 10 ⁻⁹
510	4,52 × 10 ⁻⁹
560	4,11 × 10 ⁻⁹
620	3,70 × 10 ⁻⁹
680	3,37 × 10 ⁻⁹
750	3,05 × 10 ⁻⁹
820	2,79 × 10 ⁻⁹
910	2,51 × 10 ⁻⁹
1000	2,28 × 10 ⁻⁹
1100	2,07 × 10 ⁻⁹
1200	1,90 × 10 ⁻⁹
1300	1,75 × 10 ⁻⁹
1500	1,51 × 10 ⁻⁹
1600	1,42 × 10 ⁻⁹
1800	1,26 × 10 ⁻⁹
2000	1,13 × 10 ⁻⁹
2200	1,03 × 10 ⁻⁹
2300	9,85 × 10 ⁻¹⁰
2400	9,44 × 10 ⁻¹⁰
2500	9,06 × 10 ⁻¹⁰

Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH) in Kategorie 4 bei MTTF_d-Werten für jeden Kanal ab 100 Jahre (Erweiterung von Tabelle K.1 der Norm)

tür eines umzäunten Gefährdungsbereichs dazu führen, dass alle gefahrbringenden Bewegungen im Gefährdungsbereich stillgesetzt werden. Diese Situation ist im Bild dargestellt: Die Roboter führen gefahrbringende Bewegungen aus. Wie sind hier nun die Sicherheitsfunktionen zu gestalten? Müssen neben der zentralen Steuerungslogik auch die Stellungserfassung aller Schutztüren und alle mit einer Gefährdung verbundenen Antriebe zu einer einzigen Sicherheitsfunktion zusammengefasst werden oder beispielsweise immer nur eine Schutztür und ein Antrieb? Die Antwort ist bei hoch integrierten Anlagen oft entscheidend für den erreichbaren PL. Denn mit jedem Steuerungsteil erhöht sich die Gesamtausfallwahrscheinlichkeit, deren Zahlenwert den erreichten PL limitiert. Das BGIA schlägt eine Betrachtung nach drei Prinzipien vor:

- Sofern der Zutritt in einen Gefährdungsbereich regelmäßig nur durch eine Person erfolgt, bezieht sich eine Sicherheitsfunktion immer auf die Risikominderung für einen einzigen Bediener zu einem Zeitpunkt in einem Gefährdungsbereich.
- Bei örtlicher Überlagerung von Gefährdungen ist es unerheblich, wodurch der Bediener gefährdet wird, das heißt welcher Antrieb versagt. Schon wenn das Stillsetzen eines einzigen Antriebs im Gefährdungsbereich versagt, ist die zugehörige Sicherheitsfunktion gefährlich ausgefallen und ein Unfall möglich. Für die Definition einer Sicherheitsfunktion müssen daher alle Akteure, die gefahrbringende Bewegungen im betreffenden Gefährdungsbereich erzeugen, berücksichtigt werden.
- Bei ausgedehnten Gefährdungsbereichen kann es vorkommen, dass nicht alle Maschinenbewegungen eine Person an ihrem jeweiligen Standort gefährden können. In diesen Fällen ist es zulässig, eine Aufteilung in mehrere (Teil-) Gefährdungsbereiche vorzunehmen und für die Risikominderung jeweils eigene Sicherheitsfunktionen zu definieren.

Für das Beispiel im Bild folgt damit: Es wird der Zugang einer einzelnen Person (durch eine einzige Schutztür) zum Gefährdungsbereich angenommen. Der gesamte Gefährdungsbereich wird in mehrere Teilbereiche aufgeteilt. Im Bild sind die Gefährdungsbereiche 1 und 2 eingezeichnet, es kann jedoch noch weitere geben. Unter diesen Voraussetzungen reduziert sich die Anzahl der Bauteile, die die Sicherheitsfunktionen ausführen und damit auch die Anzahl der bei der Berechnung der Gesamt-PFH zu berücksichtigenden Komponenten. Neben der zentralen Steuerungslogik sind die Sensoren zur Stellungserfassung einer Schutztür beteiligt sowie die Roboter, deren gefahr-

bringende Bewegungen im jeweiligen Gefährdungsbereich auf den Bediener einwirken können.

Im Bild sind die für die Quantifizierung zu berücksichtigenden Blöcke dunkel hinterlegt. Zu den Gefährdungen gibt es in der Regel mehrere Sicherheitsfunktionen, die das Risiko mindern. Eine Sicherheitsfunktion für den Gefährdungsbereich 2 lautet beispielsweise „SF2“: Beim Öffnen der Schutztür 2 werden Roboter 2 bis 4 stillgesetzt.

Die Steuerungskette im sicherheitsbezogenen Blockdiagramm besteht demnach aus fünf Blöcken. Der gefährliche Ausfall jedes dieser fünf Blöcke kann allein zu einer Gefährdung des Bedieners führen. Sicherheitsfunktionen für den Gefährdungsbereich 2 werden voraussichtlich zu den höchsten PFH-Werten führen, da die Anzahl der beteiligten Komponenten hier am größten ist.

Das BGIA hat für die Überlagerung von Gefährdungen mit unterschiedlichen PL bereits Lösungsansätze gefunden, die in einer künftigen Veröffentlichung vorgestellt werden.

Kann mit langen Steuerungsketten überhaupt PL e erreicht werden?

Das genannte Beispiel lässt erahnen, dass Steuerungsketten in realen Systemen recht lang werden können. Die in Abschnitt 6.3 der Norm vorgeschlagene Methode zur Kombination von Subsystemen besteht darin, bei mehr als drei Subsystemen mit PL e das Ergebnis immer auf PL d herabzustufen. Diese einfache Regel ist aber oft nicht praktikabel. Hier ist es zweckmäßiger, das dahinterliegende Prinzip der Addition der PFH-Werte anzuwenden und aus dem Gesamt-PFH-Wert den Gesamt-PL einer Sicherheitsfunktion abzuleiten (Tabelle 3 der Norm). Doch auch bei dieser Vorgehensweise kann die generelle Beschränkung der „MTTF_d jedes Kanals“ auf 100 Jahre zu Schwierigkeiten führen. Diese Beschränkung wurde im Normengremium bewusst vereinbart, um die Gesamtausfallwahrscheinlichkeit einer sicherheitsbezogenen Steuerung nicht allein oder zu sehr von statistischen Kennwerten einzelner Bauteile abhängig zu machen. Für höhere PL sollte daneben eine höherwertige Struktur (Einfehlersicherheit, zum Beispiel durch Redundanz) und eine angemessene Diagnose erforderlich sein. Demnach ist es aber durchaus sinnvoll, die Kappungsgrenze der MTTF_d jedes Kanals für Steuerungen der Kategorie 4 anzuheben. Denn in Kategorie 4 ist Einfehlersicherheit, Sicherheit gegenüber Akkumulation unerkannter Fehler und eine hochwertige Diagnose schon umgesetzt. Das deutsche Normungsgremium zur DIN EN ISO

13849-1 hat daher den BGIA-Vorschlag zur Erhöhung der Kappungsgrenze nur für Kategorie 4 auf 2500 Jahre begrüßt. Das BGIA hat, in gleicher Weise wie in Anhang K für Kategorie 4, die PFH in Abhängigkeit von der $MTTF_d$ berechnet. Die Ergebnisse sind in der Tabelle dargestellt. Der PFH-Wert unterschreitet ab ca. 240 Jahren $MTTF_d$ formal die untere Grenze der Ausfallwahrscheinlichkeit pro Stunde (1×10^{-8}), die in der Norm für PL e angegeben wird. Im Sinn der Norm wird die PFH-Anforderung damit auf Subsystemebene übererfüllt. So können auch lange Steuerungsketten Sicherheitsfunktionen in PL e realisieren. Beispielsweise liefert die Kombination von zehn Kategorie-4-Subsystemen mit jeweils 1000 Jahren $MTTF_d$ (PFH: $2,28 \times 10^{-9}/h$) eine Gesamt-PFH von $2,28 \times 10^{-8}/h$ und erreicht damit mühelos PL e. In Sistema lässt sich ab Version 1.1.0 die Kappungsgrenze für Subsysteme der Kategorie 4 auf 2500 Jahre anheben (siehe Bearbeiten/Optionen/Experten Einstellungen).

Gibt es auch eine DIN EN ISO 13849-2?

Ja, bereits seit 2003. Dieser Normenteil beschreibt die Validierung der im Teil 1 gestellten Anforderungen und befindet sich momentan in Überarbeitung. Die vorgesehenen Änderungen beschränken sich auf Ergänzungen, kleinere Korrekturen und ein zusätzliches Beispiel.

Es wurde vorgeschlagen, die Gültigkeit der DIN EN 954-1 um drei weitere Jahre, also bis Ende 2012, zu verlängern. Ist schon eine Entscheidung gefallen?

Nein, ein scheinbar offizielles Schreiben von CEN berief sich auf eine vermeintliche Kommissionsentscheidung, die es aber nach einer Richtigstellung der Kommission nicht gegeben hat. Nun sollen zunächst Experten befragt und im Dezember 2009 eine Entscheidung getroffen werden. Es geht dabei um eine Verlängerung der EN 954-1 als harmonisierte und gelistete Norm und nicht – wie oft fälschlicherweise behauptet wird – um ein Zurückziehen der EN ISO 13849-1. Eine Verlängerung würde aber die notwendigen und häufig in der Industrie schon vollzogenen Innovationen nicht unerheblich ausbremsen. Es wäre mit weiterer Marktverzerrung und Verlust des derzeitigen Wettbewerbsvorteils vieler fortschrittlicher Unternehmen zu rechnen.

Sicherheitsbezogene Teile von Steuerungen mit integrierter Elektronik oder Software lassen sich mit dem deterministischen Ansatz der DIN EN 954-1 nicht ausreichend bewerten. In der Vergangenheit konnte dies nur unter Zuhilfenahme der Normen der Reihe IEC 61508 bzw. DIN EN 61508 (VDE 0803) bewerkstelligt werden,

die auch einen Wahrscheinlichkeitsansatz fordern und demnach gleichfalls Bauteildaten benötigen. Neuartige hydraulische und pneumatische Ventile können mit der bisherigen Norm konstruktiv gar nicht bewertet werden. Hier gibt es eine Vielzahl an innovativen Neuerungen, die ein hohes Maß an Sicherheit bei gleichzeitig guter Wirtschaftlichkeit ermöglichen.

Zuverlässigkeitswerte für Bauteile sind nach Aussage der Befürworter einer Verlängerung nur sehr langfristig zu ermitteln. Sind diese Werte schon auf dem Markt verfügbar?

Ja, zu einem großen Teil durch die Hersteller selbst. Auch die Norm hat diesem Punkt durch die dreijährige Übergangsfrist und die Listung sehr vieler Kennwerte typischer Bauteile Rechnung getragen. Wenn ein Komponentenhersteller die bereits seit der ersten Normfassung 1996 bekannten grundlegenden und bewährten Sicherheitsprinzipien anwendet, führt das einfache Verfahren guter ingenieurmäßiger Praxis zu fundierten Näherungen, zum Beispiel auf 150 Jahre $MTTF_d$ für ein hydraulisches Ventil.

Für elektronische Bauteile gibt es neben den Normanhängen auch umfassendere Datensammlungen, auf die Norm verweist. Zahlreiche Realisierungen nach der neuen Norm wurden dem BGIA im Rahmen von Beratungen und Prüfungen vorgestellt. Hier gab es im Einzelfall auch „exotische“ Bauteile, die bewertet werden konnten.

Weitere Fragen

Viele Fragen beantwortet der BGIA-Report 2/2008, der mittlerweile auch auf Englisch veröffentlicht wurde. Die Materie erscheint für Neueinsteiger zunächst umfangreich. Das Durcharbeiten praktischer Beispiele, wie sie in großer Zahl im Report beschrieben sind, erzeugt aber erfahrungsgemäß Sicherheit im Umgang mit den neuen Methoden. Das Sistema-Tool hilft bei einer der großen Neuerungen, nämlich der Berechnung der Ausfallwahrscheinlichkeit, und unterstützt zusätzlich die Erstellung der von der Maschinenrichtlinie geforderten Dokumentation. Die Akzeptanz von Sistema zeigt sich auch in der wachsenden Bereitschaft von Bauteilherstellern, ihre Zuverlässigkeitskennwerte als Sistema-Bibliotheken elektronisch zur Verfügung zu stellen. Unter „www.dguv.de/bgia/13849“ findet der Anwender der Norm alle bisher vom BGIA hierzu veröffentlichten Publikationen sowie praktische Hilfen.

**Ralf Apfeld, Thomas Bömer,
Michael Hauke, Dr. Michael Huelke,
Dr. Michael Schaefer**