Anforderungen an sichere Steuerungen nach der neuen EN 954–1

Michael Hauke, Michael Schaefer, Sankt Augustin

Anforderungen aus der Prozessindustrie haben dazu geführt, dass mit der IEC 61508 [1] die Bewertung der Ausfallwahrscheinlichkeit von elektrischen und elektronischen Sicherheitssteuerungen einen hohen Stellenwert erhält. Für vergleichsweise „kleine" Steuerungen des Maschinensektors erscheint dieses probabilistische Konzept in einigen Fällen, was den damit verbundenen Aufwand betrifft, überzogen. Für viele Maschinensteuerungen ist es nicht sinnvoll, Ausfallraten von Bauelementen ($MTTF_d$), Diagnose-Deckungsgrade von Tests (*DC*) und andere Wahrscheinlichkeitsgrößen durch komplexe mathematische Modelle in eine Ausfallwahrscheinlichkeit umzurechnen. Andererseits berücksichtigt die harmonisierte EN 954–1:1996 [2] durch ihren zentralen Begriff der „Kategorie" nur strukturelle Anforderungen. Die aktuelle Revision dieser Norm als prEN 13849–1 [2] tritt mit dem Anspruch an, den komplexen probabilistischen Ansatz der IEC 61508 mit dem allgemein akzeptierten Konzept der Kategorien aus EN 954–1:1996 zu vereinen. Der nachfolgende Beitrag stellt den pragmatischen Ansatz der prEN ISO 13849–1 vor.

Einige Konzepte der EN 954–1:1996 wurden leicht modifiziert, wie das Konzept der Sicherheitsfunktion, der Risikograph und der Begriff der Steuerungskategorien zur Beschreibung der Architektur (Redundanzen und Testung). Andere Konzepte wurden neu etabliert: die Beschreibung der Zuverlässigkeit von Bauelementen durch $MTTF_d$-Werte (Mean Time to Dangerous Failure), die Beschreibung von Fehleraufdeckungsgraden durch *DC*-Werte (Diagnostic Coverage) und die Beschreibung der Kanal-Unabhängigkeit durch Maßnahmen gegen Ausfälle gemeinsamer Ursache (*CCF* – Common Cause Failure). Zur besseren Handhabung wurden die $MTTF_d$- und *DC*-Werte in Klassen (z. B. niedrig, mittel und hoch) eingeteilt.

Die Kategorien bleiben in fünf Klassen unterteilt, welche mit Beispielarchitekturen hinterlegt werden. **Bild 1** zeigt die zentrale Idee, technologieunabhängig allen Teilen der Sicherheitskette gemäß ihrer inneren Struktur eine Kategorie zuzuordnen. Die zentrale Rolle in der EN 954–1:1996 müssen die Kategorien aber an eine neu eingeführte Größe, den „Performance Level" PL abtreten. Dieser wird in Analogie zum SIL (Safety Integrity Level) der IEC 61508 über Ausfallgrenzwerte in fünf Abstufungen (a, b, c, d und e) definiert, siehe **Tabelle 1**. Der PL ist abhängig von Kategorie, $MTTF_d$-, *DC*- und *CCF*-Werten der Steuerung, wobei in gewissen Grenzen Defizite bei einem dieser Parameter durch Mehrleistung bei einem anderen Parameter kompensiert werden können. Bild 1 bleibt also gültig, aber jetzt bestimmen mehr Parameter den PL jedes Teils der Sicherheitskette. Die Methoden zur Bestimmung der Einzelparameter werden im folgenden Text ebenso angerissen, wie der formale Ablauf zur Ablesung des erreichten Performance Levels und dessen Messung am geforderten Performance Level (Required Performance Level PL_r), wie er sich aus der Risikoanalyse ergibt.

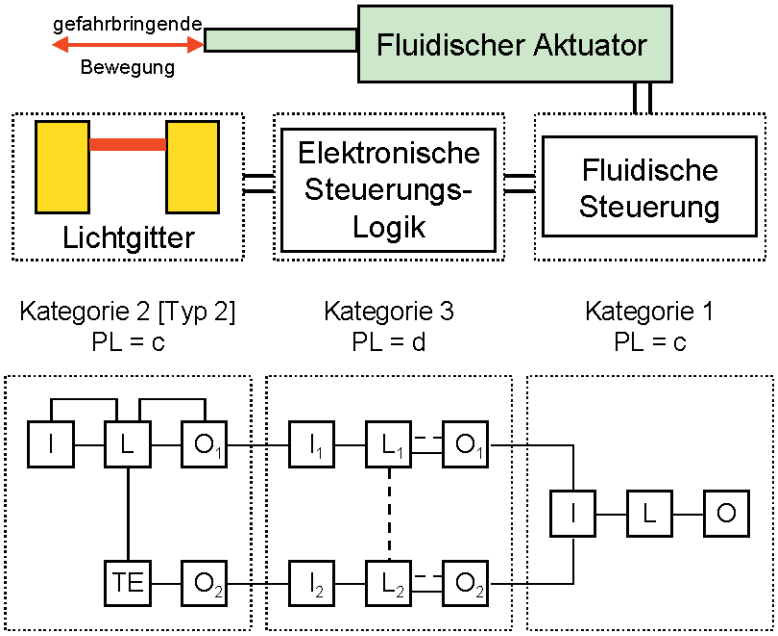


Bild 1 *Beispiel für die Zerlegung einer typischen Maschinensteuerung in vordefinierte Architekturklassen.*

Bei der Verwendung komplexer Technologien, wie z. B. programmierbarer Elektronik, unterliegt der Anwendungsbereich der Norm Einschränkungen, um den Ansatz für Systeme mit einfachen Sicherheitsfunktionen möglichst übersichtlich zu halten. Dieser Kompromiss führt allerdings zu Einschränkungen in der Flexibilität der Gestaltung. Der Anwender der Norm muss sich im Bereich der Architekturen an vorgegebenen Modellen orientieren. Dieser

Tabelle 1 *Beziehung zwischen PL, mittlerer Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde und SIL.*

Performance Level PL	Mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde in 1/h	SIL gemäß IEC 61508
a	$\geq 10^{-5}$ bis $< 10^{-4}$	keine besonderen Sicherheits-Anforderungen
b	$\geq 3 \cdot 10^{-6}$ bis $< 10^{-5}$	1
c	$\geq 10^{-6}$ bis $< 3 \cdot 10^{-6}$	1
d	$\geq 10^{-7}$ bis $< 10^{-6}$	2
e	$\geq 10^{-8}$ bis $< 10^{-7}$	3

scheinbare Nachteil wird aber sehr schnell durch die Vereinfachung der Berechnung der Zuverlässigkeit aufgewogen. Die mehr als 20-jährige Erfahrung des Berufsgenossenschaftlichen Instituts für Arbeitsschutz – BIA bei der Prüfung, Zertifizierung und Forschung sind bei der Gestaltung der vorgegebenen Architekturen vollständig eingeflossen. In Abhängigkeit von der Steuerungskategorie wurden diejenigen Architekturen ausgewählt, die mehr als 90 % der auf dem Markt realisierten Steuerungen abdecken, so dass diese Einschränkungen eher theoretischer Natur sind. Baut der Hersteller nach der Revision dieser Norm, so kann er davon ausgehen, alles Notwendige unternommen zu haben.

Entwicklungsbegleitender Prozess nach prEN ISO 13849–1

Die prEN ISO 13849–1 berücksichtigt nicht alle Phasen im Modell des sog. Lebenszyklus der IEC 61508. Dies liegt hauptsächlich an der Struktur des Europäischen Normenwerks. Hier sind zur Betrachtung des Gesamtlebenszyklus auch die Normen EN 292 [3] und EN 1050 [4] unbedingt und als erstes zu berücksichtigen. Dies bringt allerdings dem Entwickler den Vorteil, dass sich prEN 13849–1 auf den reinen Entwicklungsprozess sicherheitsbezogener Teile von Steuerungen beschränkt. In der allgemeinen Risikoanalyse gemäß EN 292 und EN 1050 werden diejenigen Aspekte der Gefährdung identifiziert, die von der Maschinensteuerung abhängen. Diese Herangehensweise findet ihren Niederschlag in der Notwendigkeit der Definition von Sicherheitsfunktionen, welche von der Maschinensteuerung auszuführen sind. Der Normvorschlag geht in seinem Abschnitt 5 dezidiert auf die Auswahl von Sicherheitsfunktionen und deren Charakteristiken ein. Ein Beispiel für eine Sicherheitsfunktion ist die Vermeidung des unerwarteten Anlaufs. Mit dieser Eingangsinformation der von der Maschinensteuerung zu leistenden Sicherheitsfunktionen wird der Geltungsbereich der prEN ISO 13849–1 betreten. In **Bild 2** ist die den Entwicklungsprozess begleitende Bewertung der Steuerung in ihren verschiedenen Phasen als Flussdiagramm dargestellt. In den folgenden Abschnitten werden die einzelnen Schritte zum Erreichen einer sicheren Steuerung beschrieben. Auf die bestehende EN 954–1:1996 wird hier Bezug genommen, diese aber nicht weiter erläutert. Einen Überblick dazu findet der Leser z. B. in [5].

Risikoanalyse der Steuerung – der Risikograph

Da derzeit ein einheitlicher Ansatz für die Risikoanalyse an Maschinen noch nicht besteht, hilft die Revision der Norm dem Maschinenhersteller durch ein einfaches informatives Tool, den sog. Risikographen, für jede Gefährdung und steuerungstechnische Sicherheitsfunktion eine

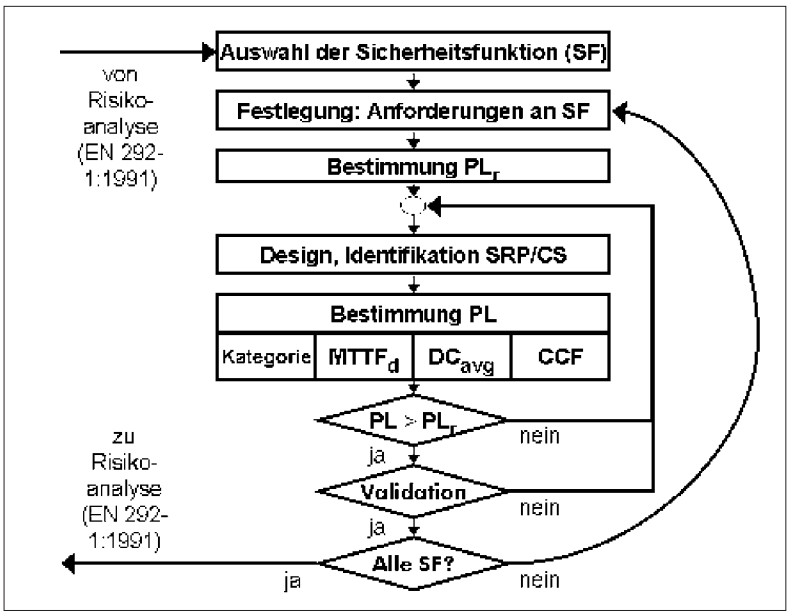


Bild 2 *Iterativer Prozess der Entwicklung von Sicherheitssteuerungen nach prEN ISO 13849–1:2003.*

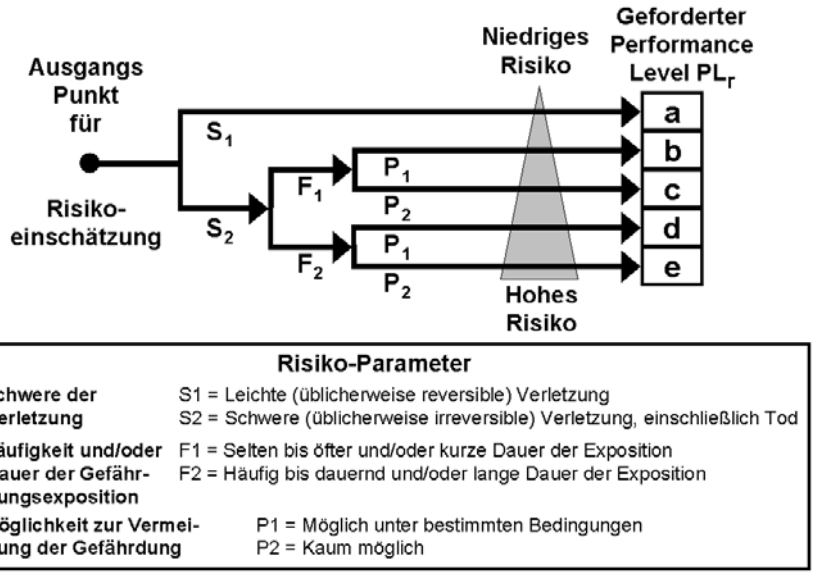


Bild 3 *Der Risikograph dient der Risikoeinschätzung des sicherheitsbezogenen Teils der Steuerung, indem für jede Sicherheitsfunktion der geforderte PL_r bestimmt wird.*

Risikobewertung für die Auswahl der sicherheitsbezogenen Teile von Steuerungen durchzuführen. **Bild 3** zeigt dieses Werkzeug für die Bestimmung des sog. geforderten (required) Performance Level PL_r. Für jede Sicherheitsfunktion muss dieser Graph durchlaufen werden. Dabei muss der Anwender die Schwere der Verletzung S, die Häufigkeit und/oder Aufenthaltsdauer im Gefahrenbereich F und die Möglichkeit der Gefahrenabwehr P abschätzen. Dies geschieht zunächst in rein qualitativer Form und fordert vom Anwender ein gewisses Augenmaß und Erfahrung bei der Beurteilung aus anderen Anwendungen. Für den F-Parameter gilt der Hinweis, dass dieser zu F2 gewählt werden sollte, wenn der Eingriff häufiger als einmal pro Schicht durchgeführt wird.

Das Ergebnis ist der für die einzelne Sicherheitsfunktion notwendige PL_r, der fünf Stufen zur Risikominderung vorschlägt: a, b, c, d und e. Hierbei ist zu beachten, dass diese Stufen hierarchisch sind und die Risikominderung von a nach e ansteigt.

Tabelle 1 zeigt den numerischen Zusammenhang zwischen dem PL, der Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion pro Stunde und dem SIL der IEC 61508. Diese Tabelle bildet im Übrigen die Brücke zwischen den verschiedenen Risikominderungsstufen der Normen prEN ISO 13849–1:2003 und IEC 61508.

Der durch die Risikoanalyse bestimmte geforderte PL_r ist sorgfältig zu unterscheiden von dem durch die Steuerung erreichten PL. Dieser wird im Wesentlichen von folgenden vier Einzelgrößen bestimmt und muss nach Abschluss des Entwicklungsprozesses größer als PL_r sein.

Bestimmung des PL von sicherheitsbezogenen Teilen von Steuerungen (Saftey-Related Part of a Control System, SRP/CS)

Kategorien – Strukturklassen

Eine Steuerung kann neben funktionalen Aufgaben u. U. mehrere Sicherheitsfunktionen ausführen. Die Gestaltung der sicherheitsbezogenen Teile der Steuerung, separat betrachtet für jede Sicherheitsfunktion, bestimmt den jeweiligen PL. Eine Steuerung kann also verschiedene Sicherheitsfunktionen mit unterschiedlichem PL ausführen. In der Regel handelt es sich bei Maschinensteuerungen um einfachste Sicherheitsfunktionen, die digitale Signale verarbeiten. Dazu wird rein funktional in 90 % aller Fälle ein Eingang (Input I), eine Logik (Logic L) und ein Ausgang (Output O) benötigt. Der Normvorschlag beschäftigt sich ausschließlich mit „Shut-Down"-Systemen, die im Fehlerfalle als sicheren Zustand ein Abschalten der gefahrbringenden Bewegung durchführen. Aus diesem Grunde sind, angelehnt an die Kategorien B, 1, 2, 3 und 4, vorgegebene Architekturen entstanden. Im Falle von Kategorie B und 1 sind die Architekturen zwar identisch, aber die Anforderungen an die Sicherheitsprinzipien unterschiedlich (**Bild 4**). Das gleiche gilt für die Kategorien 3 und 4: hier sind insbesondere die Anforderungen an die Fehlererkennung unterschiedlich (**Bild 5**). Die Architekturen erfüllen mit dem Zusatz der jeweiligen für die Kategorie notwendigen Sicherheitsprinzipien und Fehlererkennungen die Anforderungen der EN 954–1:1996, die zusammengefasst in **Tabelle 2** erläutert sind.

Die zusätzlichen Angaben im weiß hinterlegten Teil von Tabelle 2 sind die einzigen Änderungen am Kategorie-Begriff, welche durch die Revision eingeflossen sind. Neben den hier aufgeführten Änderungen sind die bisherigen Anforderungen an die Kategorien weiterhin zu erfüllen.

Ausfallraten ($MTTF_d$)

Die Ausfallraten der Bauelemente werden als $MTTF_d$ berücksichtigt. Diese Größe gibt den Mittelwert der Betriebsdauer ohne gefährlichen Fehler in einem einzelnen Kanal der Steuerung an. Dieser Bezug auf den einzelnen Kanal ist besonders bei den Kategorien 2, 3 und 4 zu beachten. Die Revision unterteilt die Zahlenwerte für $MTTF_d$ in die Bereiche niedrig, mittel und hoch, so dass hier nicht unbedingt mit exakten Zahlenwerten gearbeitet werden muss. **Tabelle 3** zeigt die drei Bereiche an. Um Missverständnissen vorzubeugen, sei hier klargestellt, dass jeder einzelne Kanal bei einer $MTTF_d$ von hoch nicht etwa grundsätzlich 100 Jahre fehlerfrei funktionieren muss; es handelt sich hier nur um einen mathematischen Mittelwert. Wie dieser mathematisch abgeleitet wird, ist z. B. in [6] beschrieben. Die in Tabelle 3 gezeigten Werte sind daneben noch einmal als Zeitverlauf aufgeführt, aus dem man z. B. bei der $MTTF_d$ von 100 Jahren herauslesen kann, dass schon im ersten Jahr von hundert Systemen ein System einen gefährlichen Ausfall haben kann. Insofern

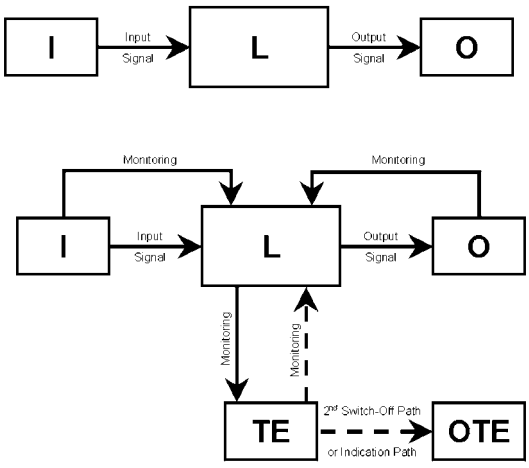


Bild 4 *Vorgegebene Architekturen für Kategorie B und 1 (oben), sowie Kategorie 2 (unten).*
I Eingang, z. B. Sensor, L Logik, O Ausgang, z. B. Hauptschütz, TE Testeinrichtung, OTE Ausgang der Testeinrichtung

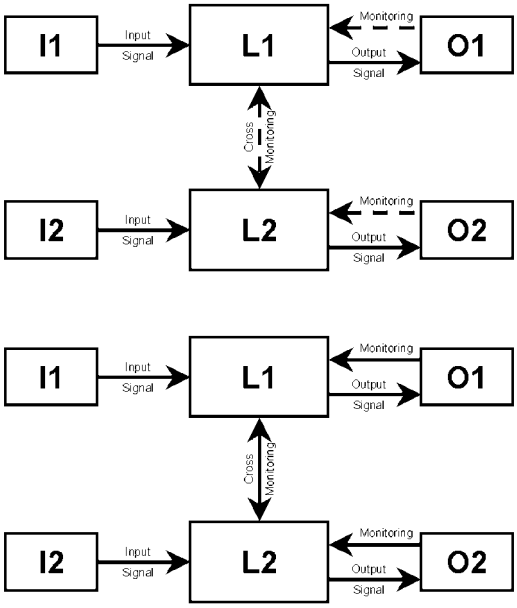


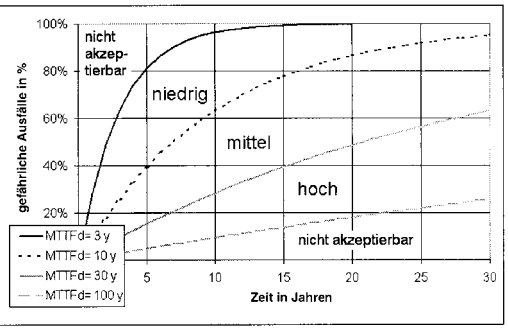
Bild 5 *Vorgegebene Architekturen für Kategorie 3 (oben) und Kategorie 4 (unten).*

Tabelle 2 *Anforderungen an Kategorien nach EN 954–1:1996 (blau hinterlegt) und Ergänzungen durch prEN 13849–1:2003 (weiß hinterlegt).*

Kategorie	Anforderungen (Kurzfassung)	$MTTF_d$	DC	CCF
B	Die sicherheitsbezogenen Teile von Steuerungen und/oder ihre Schutzeinrichtungen als auch ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt , zusammengestellt und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten.	niedrig bis mittel	keine	nicht relevant
1	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	hoch	keine	nicht relevant
2	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung geprüft werden.	niedrig bis hoch	niedrig bis mittel	muss beachtet werden
3	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet sein, dass 1. ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt und, 2. wann immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	niedrig bis hoch	niedrig bis mittel	muss beachtet werden
4	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet sein, dass 1. ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt und, 2. der einzelne Fehler bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt wird, oder, wenn dies nicht möglich ist, darf eine Anhäufung von Fehlern dann nicht zum Verlust der Sicherheitsfunktion führen.	hoch	hoch	muss beachtet werden

Tabelle 3 *Klassifizierung von $MTTF_d$ und Illustration des Anteils gefährlich ausgefallener Kanäle in Abhängigkeit von der Einsatzzeit bei niedriger, mittlerer und hoher $MTTF_d$.*

Bezeichnung	Wertebereich $MTTF_d$ in Jahren (y)
niedrig	$3\ y \le MTTF_d < 10\ y$
mittel	$10\ y \le MTTF_d < 30\ y$
hoch	$30\ y \le MTTF_d < 100\ y$



sind die Anforderungen hier mit Sicherheit nicht überzogen und aufgrund der weiten Intervalle, die im Normvorschlag definiert sind, ist hochgenaues Zahlenmaterial nicht notwendig.

Bei einer vorliegenden Schaltung wird die $MTTF_d$ relativ einfach durch die sog. Parts-Count-Methode bestimmt. Hierbei werden alle $MTTF_d$-Einzelwerte der sicherheitsrelevanten Komponenten eines Kanals reziprok addiert. Der Kehrwert des Ergebnisses bildet die $MTTF_d$. Bauelement-Ausfallraten können aus verschiedenen Datenbanken, z. B. [7], oder vom jeweiligen Komponentenhersteller bezogen werden, sofern es sich um elektronische Bauelemente handelt. Für mechanische Elemente wie z. B. fluidtechnische Ventile oder Schütze ist eine Untersuchung im BIA in Vorbereitung. Die Revision gibt im Anhang für eine Vielzahl von Bauelementen auch sog. Worst-Case-Werte an, die im Zweifel herangezogen werden können.

Da bei redundanten Systemen die Ermittlung der Ausfallwahrscheinlichkeit für das Gesamtsystem, d. h. beide Kanäle, gemacht werden muss, wird ein symmetrisierter Wert der beiden möglicherweise unterschiedlichen $MTTF_d$ der Einzelkanäle benötigt. Dazu wird einfach der kleinere der beiden Werte als endgültige $MTTF_d$ herangezogen oder die Symmetrisierung erfolgt über eine Gleichung, die aus den beiden $MTTF_d$-Werten der Kanäle einen Mittelwert bildet:

$$MTTF_d = \frac{2}{3}\left[MTTF_{d,1} + MTTF_{d,2} - \frac{1}{\frac{1}{MTTF_{d,1}} + \frac{1}{MTTF_{d,2}}}\right]$$

Diagnose-Deckungsgrade (DC)

Der Diagnose-Deckungsgrad *DC* ist ein Maß für die Fehlererkennung in einem sicherheitsrelevanten System. Der *DC* berechnet sich gemäß IEC 61508 als Verhältnis erkannter gefährlicher Ausfallraten zu allen gefährlichen Ausfallraten eines Systems. Hierzu ist i. Allg. eine Fehlerarten- und Auswirkungsanalyse (FMEA) durchzuführen. Die Revision geht hier den pragmatischen Weg, Testmaßnahmen im informativen Teil aufzuführen und diesen typische *DC*-Werte zuzuweisen. Hier wird auch auf die in IEC 61508 detailliert aufgeführten möglichen Maßnahmen zur Fehlererkennung verwiesen. Der für das Gesamtsystem maßgebliche mittlere Diagnose-Deckungsgrad DC_{avg} aller Teile (also im Gegensatz zur $MTTF_d$ nicht auf die Einzelkanäle bezogen) wird ebenfalls mit einer einfachen Mittelungsformel berechnet, bei der über alle *N* sicherheitsbezogenen Blöcke eines Systems aufsummiert wird:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d,1}} + \frac{DC_2}{MTTF_{d,2}} + \cdots + \frac{DC_N}{MTTF_{d,N}}}{\frac{1}{MTTF_{d,1}} + \frac{1}{MTTF_{d,2}} + \cdots + \frac{1}{MTTF_{d,N}}}$$

Die DC_{avg} ist neben der $MTTF_d$ ein weiterer Baustein, um den PL zu bestimmen.

Ausfälle gemeinsamer Ursache (CCF)

Ausfälle gemeinsamer Ursache treten naturgemäß nur bei redundanten Systemen auf, die durch die Kategorien 2, 3 und 4 repräsentiert werden. Externe Einflüsse, Entwurfsfehler usw. sind in der Hauptsache für solche Fehler verantwortlich. Unabhängig vom PL ist bei den Kategorien 2, 3 und 4 ein Bündel austauschbarer Maßnahmen notwendig, die in Form einer Tabelle maximal 100 Punkte erbringen. Mindestens 65 Punkte sind für das Erreichen der nötigen Sicherheit gegen Ausfälle gemeinsamer Ursache notwendig. Beispielhaft seien die folgenden Maßnahmen aufgeführt: Separation/Trennung, Diversität, Design/Applikation/Erfahrung, Beurteilung/Analyse, Kompetenz/Training und Tests unter Umgebungsbedingungen. Die komplette Tabelle befindet sich im Anhang F des Normvorschlags.

Dies ist der letzte Baustein neben Kategorie, $MTTF_d$ und DC_{avg}, der notwendig ist,

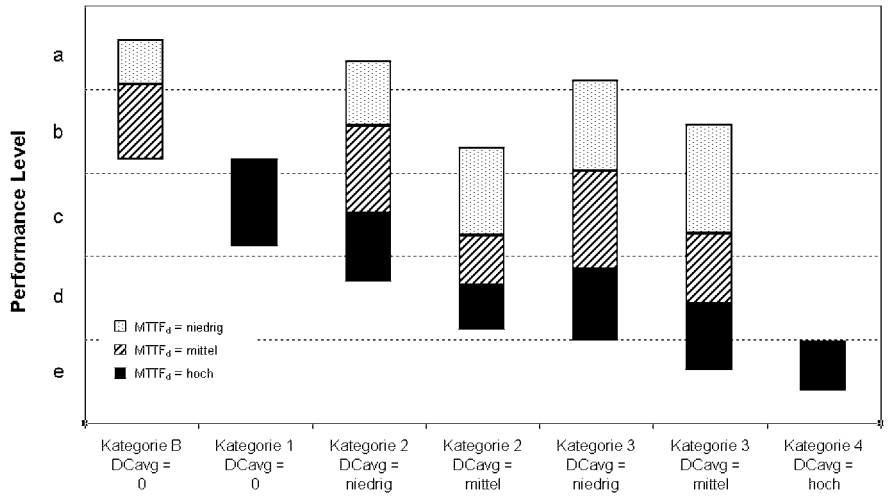


Bild 6 *Bestimmung des erreichten PL des sicherheitsbezogenen Teils einer Steuerung anhand der vier Eingangsparameter Kategorie, DC_{avg}, und $MTTF_d$ (CCF ist als Bestandteil der Kategorieanforderungen schon implizit berücksichtigt).*

um den PL des Systems zu ermitteln. **Bild 6** nimmt dem Anwender eine aufwändige Markov-Berechnung ab und stellt den PL der vorgegebenen Architekturen in Abhängigkeit von den Eingangsparametern dar. Für Details zur Technik der Markov-Modellierung zur Bestimmung der sicherheitsbezogenen Zuverlässigkeit von Steuerungen, mittels derer das Diagramm in Bild 6 entwickelt wurde, sei z. B. auf [8] verwiesen. Die oben ermittelten Eingangsparameter Kategorie und DC_{avg} werden auf der unteren Koordinate gesucht, gemäß der bestimmten $MTTF_d$ wird der passend schattierte Bereich des Balkens bestimmt, und aus dessen Lage lässt sich auf der linken Seite des Diagramms der PL ablesen. Dieser muss nun noch mindestens mit dem PL_r übereinstimmen, sonst muss das System einem Redesign unterworfen werden und die Prozedur der PL-Bestimmung neu durchlaufen werden.

Fazit

Die in der Revision der EN 954–1:1996 vorgeschlagenen Verfahren schlagen eine Brücke zwischen der gemäß IEC 61508 geforderten Berechnung der Ausfallwahrscheinlichkeit einer sicherheitsgerichteten Steuerung und dem bisherigen Ansatz, welcher sich primär auf die Systemstruktur stützt. Dieser Brückenschlag wird durch einen pragmatischen Ansatz erreicht, welcher den besonderen Verhältnissen im Maschinensektor gerecht wird. Dabei wird durch die Beibehaltung des Kategoriebegriffs und anderer zentraler Konzepte, wie der Sicherheitsfunktion und des Risikographs, die größtmögliche Kontinuität zur allgemein akzeptierten 1996er Fassung der EN 954–1 gewahrt. Durch Kombination der Kategorie eines Systems mit Zuverlässigkeitsparametern wie $MTTF_d$, DC und CCF ergibt sich als neue zentrale Bewertungsgröße für die Zuverlässigkeit einer Steuerung der PL. Obwohl dessen Bestimmung nun mehr Aufwand erfordert als allein die Bestimmung einer Steuerungskategorie, so ergibt sich dadurch gleichzeitig die Chance für den Entwickler, Defizite bei einem Parameter durch Mehrleistung bei einem anderen Parameter auszugleichen. Zur Bestimmung der Zuverlässigkeitsparameter $MTTF_d$, DC und CCF werden dem Steuerungsentwickler für Maschinen in der prEN ISO 13849–1 gegenüber der IEC 61508 stark vereinfachte Verfahren angeboten, die dennoch den wissenschaftlich abgesicherten Boden nicht verlassen. Diese Vereinfachungen tragen auch dem Anspruch der prEN ISO 13849–1 Rechnung, alle Technologien und auch Kombinationen von Technologien angemessen bewerten zu können. Der Revisionsentwurf liegt international abgestimmt seit August diesen Jahres in Brüssel bei CEN vor. Ende 2003 wird er als prEN ISO 13849–1 erhältlich sein. TÜ 419

Dipl.-Phys. **Michael Hauke** ist wissenschaftlicher Mitarbeiter in der Abt. 5 „Unfallverhütung – Produktsicherheit“ im Berufsgenossenschaftlichen Institut für Arbeitsschutz – BIA, Sankt Augustin.
Dr. rer. nat. **Michael Schaefer** leitet den Fachbereich „Unfallverhütung – Produktsicherheit“ im Berufsgenossenschaftlichen Institut für Arbeitsschutz – BIA, Sankt Augustin. Er ist im internationalen Arbeitskreis „CEN TC 114/ISO TC 199, WG6“ federführend mit der Revision der EN ISO 13849–1 betraut.

Quelle für alle Bilder und Tabellen dieses Beitrags ist die prEN ISO 13849–1:2003.

Literaturverzeichnis

[1] IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme. 7 Teile. Berlin: Beuth Verlag 2002.
[2] EN 954–1:1996: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze. Berlin: Beuth Verlag 1996. Identisch mit ISO 13849-1:1999.
[3] EN 292:1991: Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze. Berlin: Beuth Verlag 1991. Identisch mit ISO/FDIS 12100:2003.
[4] EN 1050:1996: Sicherheit von Maschinen – Leitsätze zur Risikobeurteilung. Berlin: Beuth Verlag 1996.Identisch mit ISO 14121:1999.
[5] *Kleinbreuer, W.; Kreutzkampf, F.; Meffert, K.; Reinert, D.*: Kategorien für sicherheitsbezogene Steuerungen nach EN 954–1. BIA-Report 6/97. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften Sankt Augustin 1997. Kostenlos als PDF vom Berufsgenossenschaftlichen Institut für Arbeitsschutz – BIA erhältlich unter www.hvbg.de/d/bia/ub/rep/rep02/bia0697.htm.
[6] *Goble, W. M.*: Control Systems – Safety Evaluation & Reliability. 2nd Ed. Hrsg.: Instrument Society of America (ISA). North Carolina: 1998.
[7] Siemens-Norm SN 29500: Ausfallraten Bauelemente. Siemens AG 1999.
[8] *Dorra, M.; Reinert, D.*: Quantitative Analysis of Complex Electronic Systems using Fault Tree Analysis and Markov Modeling. Annex 6 of the Final Report of the European Project STSARCES (Standards for Safety Related Complex Electronic Systems). European Commission – DG XII. Brüssel 2000.