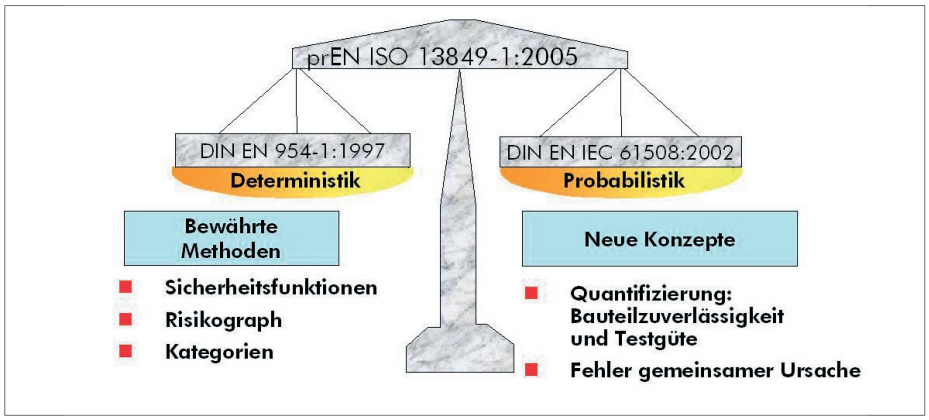
Sicherheitsnorm mit neuem Konzept

Revision der EN 954-1 (ISO 13849-1) vereinigt Kategorien mit Ausfallwahrscheinlichkeiten



1: Die Überarbeitung der EN ISO 13849-1 versucht den Balance-Akt zwischen bewährten Prinzipien der EN 954-1 und neuen Ansätzen der IEC 61508

Michael Hauke, Michael Schaefer

Seit 1996 werden sicherheitsrelevante Steuerungen von Maschinen, ob mechanisch, pneumatisch, hydraulisch oder elektrisch, nach EN 954-1 erfolgreich in fünf Kategorien eingeteilt. Mit dem Vormarsch programmierbar elektronischer Systeme ergab sich aber die Notwendigkeit einer grundlegenden Revision als prEN ISO 13849-1 mit gleichzeitiger Integration des in der elektrischen Sicherheits-Grundnorm IEC 61508 verankerten Bezugs auf Ausfallwahrscheinlichkeiten. Mit dem Anspruch, weiterhin alle Technologien angemessen und vor allem praktikabel zu klassifizieren, wurden die Kategorien in das größere Konzept des Performance Levels eingebettet.

Autoren: *Dipl.-Phys. Michael Hauke ist wissenschaftlicher Mitarbeiter des Fachbereichs 5 – Unfallverhütung und Produktsicherheit im BGIA – Berufsgenossenschaftliches Institut für Arbeitsschutz*
Dr. rer. nat. Michael Schaefer ist Leiter des Fachbereichs 5 – Unfallverhütung und Produktsicherheit im BGIA – Berufsgenossenschaftliches Institut für Arbeitsschutz

Das Beste aus zwei Welten

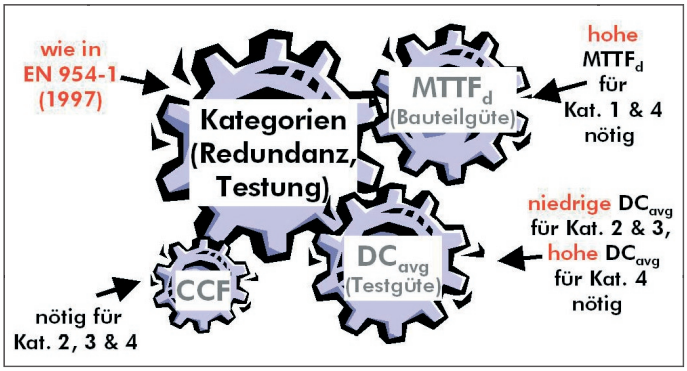
Wenn Sie die vier Grundrechenarten beherrschen lesen Sie bitte weiter!

Auch wenn sie längst noch nicht jeder kennt und anwenden kann, ist die EN 954-1 mit ihren Kategorien seit 1996 einer der meistgenutzten Standards, wenn es um Maschinensteuerungen mit Sicherheitsfunktionen geht. Mehr als 1000 Produktnormen, z.B. für Bearbeitungszentren, Pressen, Spritzguss- und Rotationsdruckmaschinen geben eine Kategorie vor und entscheiden damit darüber, ob eine Steuerung mit zusätzlichen internen Überwachungsmaßnahmen oder gar einem kompletten zweiten Kanal realisiert werden muss, abhängig vom zu erwartenden Risiko an der Maschine. Dies soll den Bediener schützen, auch wenn Teile der Hard- oder Software ausfallen. Die Kategorien beschreiben die Struktur einer Sicherheitssteuerung durch die Güte der verwendeten Bauteile, die Wirksamkeit von Tests und die Fehlertoleranz.

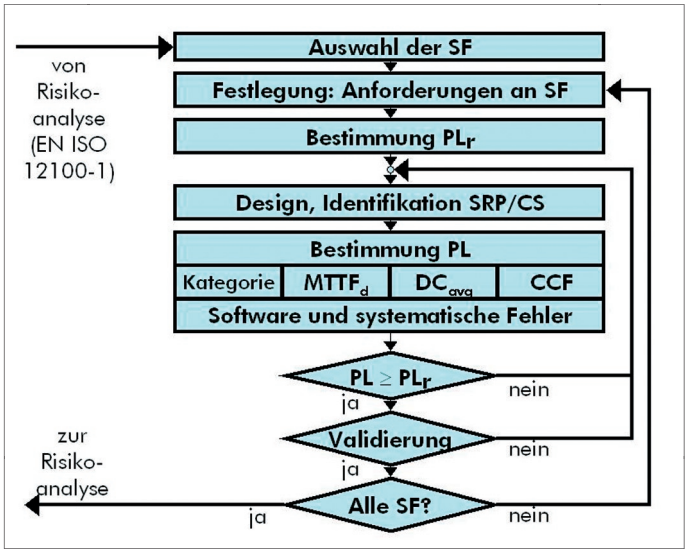
Alternative, aber relevante Normen im Bereich der funktionalen Sicherheit sind die IEC 61508 und ihre Sektornorm IEC 62061 für die Maschinen-Industrie, welche einen Sicherheits-Integitäts-Level (SIL) definieren. Beide gelten zunächst nur für elektrische, elektronische und programmierbar elektronische Systeme, auch wenn der grundlegende Ansatz, Ausfallwahrscheinlichkeiten und nicht Strukturen als charakteristische Kenngröße zu definieren, universeller ist. Sie sind seit kurzen auch inhaltsgleich als DIN EN 61508 (VDE 0803) bzw. EN 62061 (DIN IEC 62061/

prEN ISO 13849-1	IEC 62061	IEC 61508
deckt alle Technologien ab (Mechanik, Pneumatik, Hydraulik, Elektrik), nur gültig für Maschinen-Industrie	nur gültig für elektrische, elektronische und programmierbar elektronische Systeme; nur gültig für Maschinen-Industrie	nur gültig für elektrische, elektronische und programmierbar elektronische Systeme; gültig für Maschinen- und Prozess-Industrie
beschäftigt sich nur mit dem technischen Design von Sicherheits-Steuerungen, keine organisatorischen Anforderungen	beschäftigt sich mit allen Aspekten der funktionalen Sicherheit während des gesamten Lebenszyklus einer Maschine	beschäftigt sich mit allen Aspekten der funktionalen Sicherheit während des gesamten Lebenszyklus einer Maschine oder Anlage
harmonisiert bzw. harmonisierbar, d.h. Vermutungswirkung zur Maschinenrichtlinie	harmonisiert, d.h. Vermutungswirkung zur Maschinenrichtlinie	nicht harmonisierbar, d.h. keine Vermutungswirkung zur Maschinenrichtlinie
zwei Teile, ca. 100 und 60 Seiten	ein Teil, ca. 100 Seiten, praktisch nicht ohne IEC 61508 verwendbar	acht Teile, ca. 440 Seiten
Anwendungsnorm (Typ B1)	Sektornorm	Sicherheits-Grundnorm
praktikable, vereinfachte Methoden, basierend auf typischen Architekturen (Kategorien)	vereinfachte Methoden für die Zusammenschaltung von Subsystemen, sonst Verweis auf IEC 61508	Methoden werden meist offengelassen, um die Flexibilität bei der Methodenwahl nicht einzuschränken
EN seit 1997, Abschluss der Revision ca. 2006	EN seit 2005	EN seit 2001, laufende Überarbeitung

Tabelle 1



2 oben: Die Definition der Kategorien hat sich kaum geändert, aber es gibt zusätzliche Mindestanforderungen an $MTTF_d$, DC_{avg} und Maßnahmen gegen CCF



3: An die Ermittlung des erforderlichen Performance Levels (PL_r) schließt sich ein Vergleich mit dem erreichten Performance Level (PL) an – unter Umständen iterativ

VDE 0113-50) veröffentlicht. Durch die Zurückziehung der deutschen DIN V VDE 0801 für Rechner mit Sicherheitsaufgaben gibt es seit 2004 bei elektronischen Systemen keine echte Alternative zur IEC 61508. Daher war die anstehende Revision der EN 954-1, welche seit 1999 auch EN ISO 13849-1 heißt, ein willkommener Anlass, Software-Anforderungen zu integrieren, um weiterhin alle Technologien innerhalb eines Konzeptes bewerten zu können.

Die Überlappung des Regelungsanspruchs beider Normenwelten ist für Steuerungshersteller natürlich unbefriedigend und mit Mehraufwand verbunden. Zwar braucht sich die Fluidtechnik streng genommen nicht um SILs zu kümmern, aber einerseits wird auch dort zunehmend elektronische Technologie integriert und andererseits wird es im internationalen Geschäft üblich, auch für Ventile nach einem SIL zu fragen. Um die langfristige Zusammenlegung beider Normenwelten vorzubereiten und die Vorteile des Wahrscheinlichkeitsansatzes zu nutzen, ohne die bewährten Kategorien über Bord zu werfen, hat die Revision der EN ISO 13849-1 einen Balanceakt gewagt, siehe auch **Bild 1** und **Tabelle 1**. Dieser verlangt dem – vom neuen Konzept der Performance Level (PL) überraschten – Anwender zwar wie immer eine Einarbeitung ab (ein Tag Übung), bietet aber gleichzeitig ein längerfristig tragfähiges Konzept an, welches letztlich Doppelarbeit vermeidet. Mit der Vergleichbarkeit von PL und SIL und dem praktikablen, gut beschriebenen Ansatz der prEN ISO 13849-1 eröffnet sich nicht nur der Fluidtechnik die Chance eines sanften Übergangs auch in Anwendungsbereiche der Zuverlässigkeitsberechnungen. Die vier Grundrechenarten reichen!

Sicherheitsfunktionen und allgemeiner Ablauf

Als bewährtes Konzept steht die Definition der Sicherheitsfunktion (SF) am Anfang des Design- und Bewertungsprozesses nach prEN ISO 13849-1. Wie sieht der Beitrag der Sicherheits-Steuerung zur Risikoreduzierung an einer Maschine aus? Dies kann zum Beispiel der Schutz gegen unerwarteten Anlauf sein, wenn ein Bediener bei geöffneter Schutzeinrichtung einen Gefahrenraum betritt. Da es an einer Maschine durchaus mehrere Sicherheitsfunktionen geben kann (z.B. für Automatik- und Einrichtbetrieb), ist eine sorgfältige Betrachtung jeder Sicherheitsfunktion für sich sehr wichtig. Auch wenn durchaus dieselbe Hardware an verschiedenen Sicherheitsfunktionen beteiligt sein kann, ist die erforderliche Höhe der Risikoreduzierung u. U. unterschiedlich. **Bild 3** zeigt, wie es danach über die Ermittlung des geforderten (PL_r) und von einer Steuerung erreichten (PL) Performance Levels weitergeht im Ablaufplan der Norm.

Sollwert? Der erforderliche Performance Level PL_r

Das Risiko an einer Maschine kann neben der Steuerung auch z. B. durch trennende Schutzeinrichtungen (z. B. eine Schutztüre) oder persönliche Schutzausrüstung (z. B. eine Schutzbrille) verringert werden. Ist aber erst einmal festgelegt, was die Steuerung anteilig leisten muss, dann hilft der „Risikograph“ (siehe **Bild 4**) bei der schnellen und direkten Bestimmung des geforderten Performance Levels PL_r. Ist die Verletzung irreversibel (z. B. Tod, Verlust von Körperteilen) oder reversibel (z. B. Quetschungen), hält sich der Bediener häufig und lange im Gefahrenbereich auf (z. B. öfter als ein Mal pro Schicht) oder selten und kurz und hat er eine Möglichkeit den Unfall noch zu vermeiden (z. B. wegen langsamer Maschinenbewegung)? Diese drei Fragen entscheiden über den PL_r.

Konsequenzen	Se (Punkte)
Nicht reversibel: Tod, Verlust eines Auges oder Armes	4
Nicht reversibel: gebrochene Gliedmaßen, Verlust eines oder mehrerer Finger	3
Reversibel: Eingriff eines Arztes notwendig	2
Reversibel: Erste Hilfe notwendig	1

Tafel

Die Norm IEC 62061 bewertet das Risiko mit deutlich mehr Parametern. Beispielsweise wird die Schwere der Verletzung in vier Stufen eingeteilt (siehe unten stehende Tafel).

Dies sieht zunächst sehr praxisbezogen aus – ja scheint sogar Einsparpotenzial für die Sicherheit zu versprechen –, aber mal Hand aufs Herz: wer möchte über die obigen Verletzungen im Vorfeld ernsthaft verantwortlich entscheiden. Reicht es nicht aus zwischen schweren und leichten Verletzungen zu unterscheiden? Was sagt man später dem Opfer oder dem Richter, wenn statt dem Finger doch der Arm ab ist?

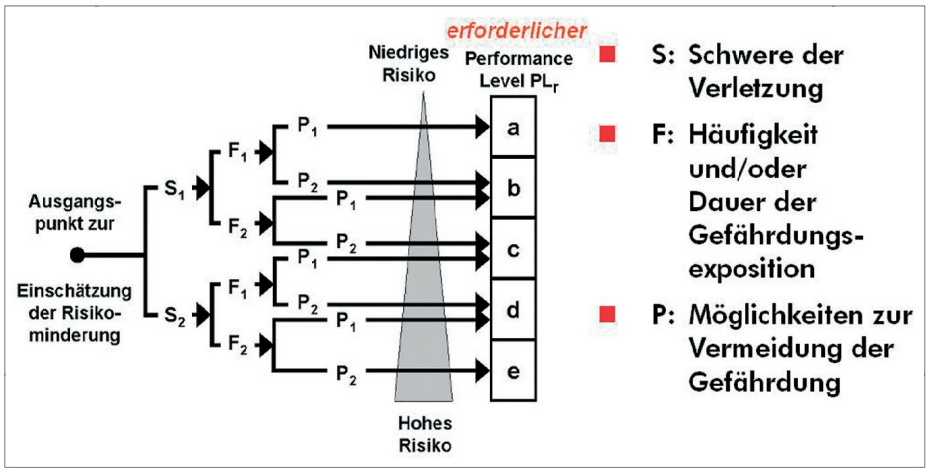
Istwert? Der erreichte Performance Level PL

Eine Sicherheitssteuerung ist voraussichtlich nur so gut wie die verwendeten Bauteile, ihr Zusammenspiel (Dimensionierung), die Wirksamkeit der Diagnose (z.B. Selbsttests) und die Fehlertoleranz (Fehlersicherheit) der Struktur. Dieses Prinzip gilt für die Kategorien genauso wie für den neu definierten PL, nur das der PL formell über Ausfallwahrscheinlichkeiten definiert ist. Kein Unterschied also zum SIL nach IEC 61508/62061 (siehe **Tabelle 2**). Die Revision der EN ISO 13849-1 lässt die zu verwendende Mathematik offen. So darf man durchaus die hoch komplexe Markov-Modellierung unter Berücksichtigung der oben genannten Parameter nutzen. Jedoch bricht nicht jeder Entwickler – die Autoren sprechen aus eigener Erfahrung – gerade in einen Freudentaumel aus, sich in das Feld der Zuverlässigkeitsstatistik einzuarbeiten (das kann schon einmal ein Jahr dauern). Daher musste ein Ansatz geschaffen werden, der die Mathematik nicht verbiegt, aber die

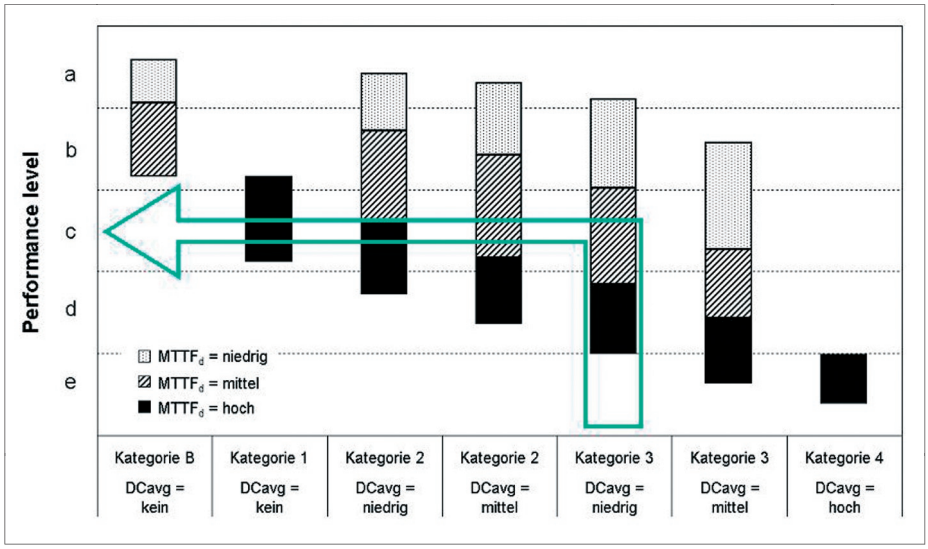
Performance Level (PL) nach prEN ISO 13849-1	Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde	Sicherheits-Integritäts-Level (SIL) nach IEC 61508
a	10^{-4} bis 10^{-5}	keine Entsprechung
b	10^{-5} bis $3{\cdot}10^{-6}$	1
c	$3{\cdot}10^{-6}$ bis 10^{-6}	1
d	10^{-6} bis 10^{-7}	2
e	10^{-7} bis 10^{-8}	3

Tabelle 2

Kenntnisse von Experten in einer Art Tabellenwerk widerspiegelt. Am liebsten unter Verwendung der vier Grundrechenarten. Deshalb gibt es ein empfohlenes Vorgehen, nämlich die Benutzung des Säulendiagramms (siehe **Bild 5**), in welchem diese Modellierung schon vorweggenommen ist. Nach Auswahl der realisierten Struktur (Kategorie) und der mittleren Testqualität (DC_{avg} englisch: **D**iagnostic **C**overage, avg steht für average) auf der waagerechten Achse ist die relevante Säule festgelegt. Die mittlere Bauteilgüte ($MTTF_d$ englisch: Mean Time To Failure, d steht für dangerous, siehe unten) entscheidet dann, welcher Abschnitt der Säule heranzuziehen ist, um auf der senkrechten Achse den erreichten PL abzulesen. Viel einfacher können vier Parameter fast nicht zu einem Ergebnis verknüpft werden. Aber vor dem Ablesen des PLs steht ja leider noch die Detailarbeit der Kategorie-, DC_{avg}- und $MTTF_d$-Ermittlung. Die Rechnung passt leider nicht auf einen Bierdeckel, aber lassen Sie sich nicht durch Formeln erschrecken. Die beinhalten nur die vier Grundrechenarten. Die Formeln sehen nur auf den ersten Blick scheußlich aus, aber am Besten rechnet man dann einmal ein kleines, dann ein größeres und schließlich ein noch größeres Bespiel durch. Danach kann man es, und es geht schnell – versprochen!



4: Die Norm schlägt einen Risikographen zur Ermittlung des erforderlichen Performance Levels (PL_r) vor, welcher auf drei Parametern des Risikos basiert



5: Die Ermittlung des erreichten Performance Levels (PL) kann graphisch erfolgen. Die Markov-Modellierung hat der Normensetzer bereits in das Säulendiagramm investiert

Kategorien und Designated Architectures

Die Kategorien bleiben auch nach der Revision die Haupt-Säule bei der Bestimmung des PLs. An ihrer Definition hat sich im Wesentlichen nichts geändert, allerdings wurden Anforderungen an die Bauteilgüte als $MTTF_d$- Werte festgeschrieben und geforderte Testtiefen als DC_{avg}. Zusätzlich werden für Kategorie 2, 3 und 4 ausreichende Maßnahmen gegen Fehler gemeinsamer Ursache (CCF) gefordert. Einen Überblick über die Kategorien liefert **Tabelle 3**, deren drei rechte Spalten die Neuerungen darstellen. Ein wesentlicher Punkt bei der Verwendung der vorgeschlagenen einfachen Rechenmethoden ist die Darstellung der Kategorien als logische Blockschaltbilder, so genannte vorgesehene Architekturen (Designated Architectures). Diese logischen Prinzipschaltbilder sind in **Bild 6** dargestellt und sollten sich fast immer auf die konkreten technischen Realisierungen der entsprechenden Kategorie abbilden lassen. Die Einteilung in Eingangs- (I für Input), Verarbeitungs- (L für Logik) und Ausgangs- (O für Output) Gruppen, sowie Testeinrichtungen (TE) ist in aller Regel möglich. Die Blöcke sind durch funktionale Beziehungen (im für Interconnecting Means), z. B. in parallelen Steuerungskanälen und Überwachungsbeziehungen (m für Monitoring oder c für kreuzweise Überwachung) verbunden. Der Grad der Überwachung variiert mit der erforderlichen DC_{avg}, z. B. werden in Kategorie 3 aus den m- und c-Linien der Kategorie 4 gestrichelte Linien. Die nachfolgende Bestimmung von $MTTF_d$- und DC_{avg}-Werten basiert auf einem mehrstufigen Konzept: zunächst werden Werte für die Einzelkomponenten bestimmt, aus diesen werden Werte für die Blöcke errechnet und daraus schließlich repräsentative Mittelwerte für das gesamte System. Alle dazu nötigen Formeln und tabellierten Beispielwerte sind erfreulicherweise in den 100 Seiten der Norm schon enthalten.

Woher kommt die $MTTF_d$?

Eine der meistgestellten Fragen zur Ausfallwahrscheinlichkeit betrifft die Beschaffung zuverlässiger Ausfalldaten für die sicherheitsrelevanten Komponenten. Hier ist der Hersteller mit seinem technischen Datenblatt natürlich allen anderen Quellen vorzuziehen. Viele Komponentenhersteller (auch in der Pneumatik) haben hier bereits signalisiert, dass solche Daten künftig erhältlich sein werden. Aber auch, wenn es (noch) keine Herstellerangaben gibt, lassen sich typische Beispielwerte aus etablierten Datensammlungen (z. B. der SN 29500 oder der IEC/TR 62380) ermitteln. Sogar die prEN ISO 13849-1 selbst listet einige Werte. Je nach Technologie finden sich so Ausfallraten (z. B. λ in FIT), Lebensdauern (MTTF

in Jahren) oder Schaltspielzahlen (z. B. B_{10} in Schaltspielen), die nach klaren Regeln in der Norm in $MTTF_d$-Werte (für „Mean Time to Dangerous Failure“) umgerechnet werden können. Dabei sei betont, dass nur sicherheitsrelevante Bauteile in die Rechnung einbezogen werden müssen. Dieser Anteil wird nochmals dadurch reduziert, dass nur der Ausfall in die unsichere Richtung betrachtet werden muss. Bei einem Pneumatikventil, das eine Leckage aufweist, ist der Ausfall in der Regel nicht „dangerous“, aber ein Hängenbleiben des Ventils kann als „dangerous“ betrachtet werden (daher der Index d an $MTTF_d$). Weiterhin können begründete Fehlerausschlüsse herangezogen werden. Statt einer aufwändigen FMEA kann dann durch einfaches Aufsummieren (die so genannte „Parts-Count-Methode“) und die Annahme von 50 % gefährlichem Fehleranteil einfach die System-Kenngröße $MTTF_d$ berechnet werden, welche sich auf einen einzelnen Kanal der Steuerung bezieht. Um das Verfahren nicht zu rechenlastig zu gestalten, gibt es drei erlaubte Klassen für $MTTF_d$, die in **Tabelle 4** erläutert sind. Weniger als drei Jahre mittlere (nicht garantierte!) Lebensdauer wird sich bei Komponenten der Sicherheitstechnik kaum finden lassen, mehr als 100 Jahre dürfen nicht in Rechnung gestellt werden, um Systeme nicht künstlich gut zu rechnen. Auf die Besonderheiten der $MTTF_d$-Ermittlung für fluidtechnische Komponenten wird im nächsten Teil dieser dreiteiligen Artikelserie im Detail eingegangen.

Bezeichnung der $MTTF_d$ jedes einzelnen Kanals	Bereich der $MTTF_d$ jedes einzelnen Kanals
niedrig	3 Jahre bis 10 Jahre
mittel	10 Jahre bis 30 Jahre
hoch	30 Jahre bis 100 Jahre

Tabelle 4

Man nehme: DC_{avg}

Die Ermittlung der DC_{avg} (für „average Diagnostic Coverage“) erfolgt sehr einfach: für jeden Block werden die Testmaßnahmen zusammengestellt, die diesen Block überwachen. Für jede dieser Testmaßnahmen wird einer von vier typischen DC-Werten aus einer Tabelle in der Norm ermittelt und schließlich errechnet eine Mittelungsformel daraus die Kenngröße DC_{avg}. Auch hier gibt es vier Klassen, siehe **Tabelle 5**.

Bezeichnung der DC	Bereich der DC
kein	unter 60 %
niedrig	60 % bis unter 90 %
mittel	90 % bis unter 99 %
hoch	99 % und darüber

Tabelle 5

Kategorie	Anforderungen (Kurzfassung)	$MTTF_d$	DC_{avg}	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. Grundlegende Sicherheitsprinzipien müssen verwendet werden.	niedrig bis mittel	kein	nicht relevant
1	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	hoch	kein	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. Wenn dies nicht möglich ist, darf eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen.	hoch	hoch	muss beachtet werden

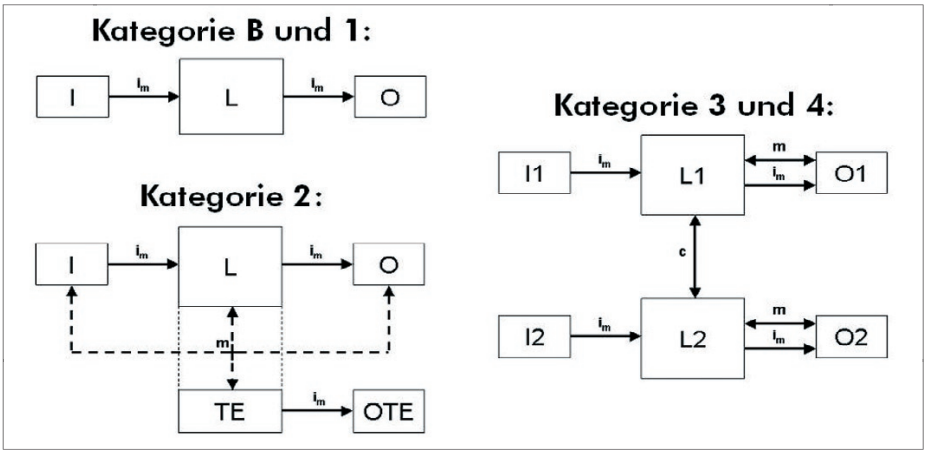
Tabelle 3

Aus Eins mach Zwei: CCF

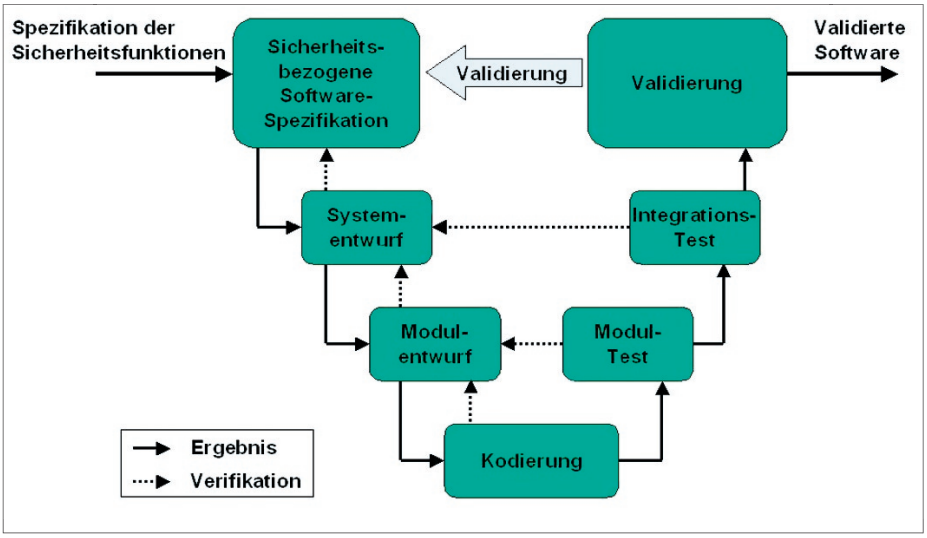
Ganz einfach wird es schließlich bei der letzten Kenngröße CCF (für Common Cause Failure). Hier wird unterstellt, dass eine Ursache (z. B. Verschmutzung, Übertemperatur, Kurzschluss) u. U. mehrere Folgefehler verursachen kann, die z. B. beide Steuerungskanäle gleichzeitig außer Kraft setzen kann. Zur Beherrschung dieser Gefahrenquelle muss für Systeme der Kategorie 2, 3 und 4 nachgewiesen werden, dass ausreichende Maßnahmen gegen CCF getroffen wurden. Dies geschieht anhand eines Punktesystems für acht typische Gegenmaßnahmen, bei dem mindestens 65 von 100 möglichen Punkten erreicht werden müssen.

Konstruktionsfehler, z.B. Software

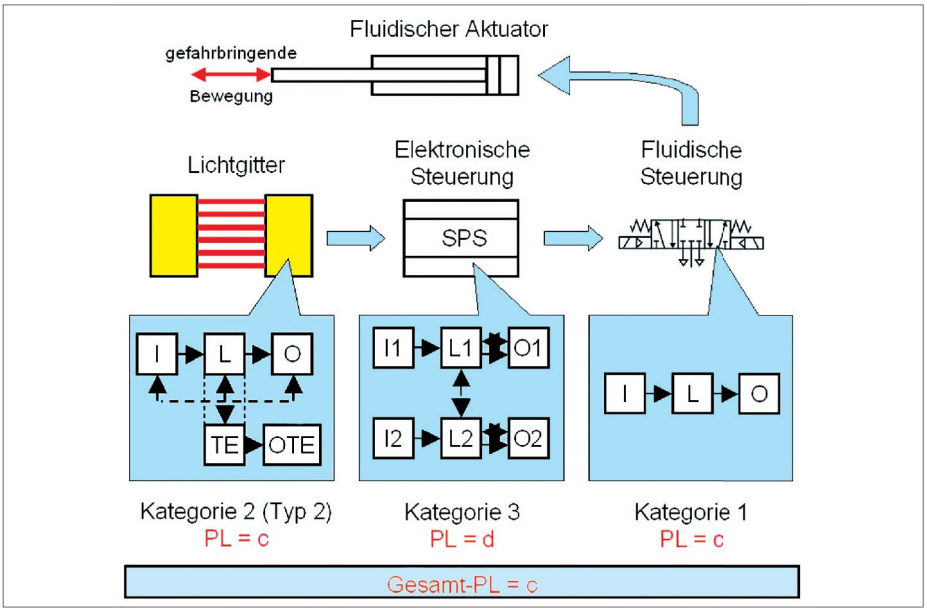
Neben den zufälligen Hardware-Ausfällen, die durch gute Struktur und geringe Ausfallwahrscheinlichkeit beherrscht werden können, gibt es noch das weite Feld der sogenannten systematischen Fehler (dem System bereits seit Konstruktion innewohnende Fehler wie z. B. Dimensionierungsfehler, Softwarefehler, logische Fehler), vor denen Maßnahmen zur Fehlervermeidung und



6: Die Kategorien werden in der prEN ISO 13849-1 durch typische Architekturen repräsentiert. Die meisten Steuerungen am Markt lassen sich hierauf abbilden.



7: Der Software-Lebenszyklus als V-Diagramm ist z.B. gegenüber IEC 61508 deutlich verkürzt und dient der Fehlervermeidung im Entwicklungsprozess



8: Gängige Praxis wird berechenbar: durch Umrechnung im Performance Level können unterschiedliche Kategorien in Serie vergleichbare Sicherheitsniveaus realisieren

Die Urheberrechte aller Bilder liegen beim BGIA

9: Kostenlose Unterstützung der Anwender durch das BGIA in Form von Literatur, dem SiSteMa-Hilfsprogramm und dem Performance Level Calculator als Drehscheibe

-beherrschung schützen sollen. Hier nehmen die Softwarefehler einen eigenen großen Bereich ein. Wie in der Einleitung schon gesagt, stellen Software-Anforderungen in der prEN ISO 13849-1 eine Neuerung dar, auch wenn die Maßnahmen im Einzelnen aus den einschlägigen Normen bereits bekannt sind. Die Norm unterscheidet dabei zwischen Embedded-SW (z. B. Firmware) und Anwender-SW (z. B. SPS-Anwen-

derprogrammen). Für beide Software-Arten wird zur Fehlervermeidung im Entwicklungsprozess die Anwendung eines vereinfachten V-Modells für den SW-Lebenszyklus empfohlen (siehe **Bild 7**). Die Maßnahmen zur Fehlerbeherrschung sind je nach gefordertem Performance Level abgestuft, nur bei Embedded-SW für PL e wird die Anwendung des Software-Teils der IEC 61508 empfohlen (wenn die Kanäle diversitär programmiert sind, dann hat man noch mal Glück gehabt und bleibt innerhalb der prEN ISO 13849-1). Bei allen Maßnahmen gegen systematische Fehler steht im Wesentlichen die sorgfältig geplante Konstruktion bzw. Gestaltung im Vordergrund. Es sollte selbstverständlich sein, dass hier das Design überschaubar, nachvollziehbar, änderungsfreundlich und wartbar ist. Dies dient natürlich auch dem Wohle der Maschinenfunktionen unabhängig von der Sicherheit. Dabei ist die Planung und die Überprüfung der Planung das A&O. Dies wird in Abhängigkeit von der Komplexität mehr oder weniger umfangreich, jedoch ist das System nachher beherrschbar und auch die Weiterentwicklung von Technologien lebt von der für den Entwickler erkennbaren Funktionalität. Nicht die Norm, sondern der Entwickler und Konstrukteur benötigt Dokumente, um die Arbeiten effektiv durchführen zu können.

Erreicht der Istwert den Sollwert? Prüfstein: PL $\geq$ PL_r

Ist die Bewertung eines Designs erst mal bis zur Ermittlung des realisierten PL fortgeschritten, stellt sich natürlich die bange Frage, ob dieser auch ausreicht. Dazu ist ein Vergleich mit dem vorher ermittelten PL_r nötig. Ist der PL schlechter als der PL_r, so sind mehr oder weniger große Nachbesserungen am Design (z.B. Verwendung anderer Bauteile mit besserer $MTTF_d$) nötig, bis der PL schließlich ausreichen gut ist. Ist diese Hürde genommen, so sind wie gehabt eine Reihe von Validierungsschritten zur Kategorie notwendig (siehe Bild 3), bei denen der Teil 2 der EN ISO 13849 ins Spiel kommt.

Zusammenspiel von Kategorien und Technologien

Für eine Sicherheitsfunktion werden häufig mehrere Steuerungselemente auch unterschiedlicher Technologie hintereinander geschaltet, wie z. B. im **Bild 8** skizziert: Lichtgitter, elektronische Steuerung und Pneumatikventil. Der Pneumatikzylinder selbst ist kein Steuerungsteil und daher nicht Gegenstand einer PL-Bewertung – kann aber durchaus auch durch die vorgestellte Methode bewertet werden. Eine Kette ist immer nur so stark wie ihr schwächstes Glied. Diese Weisheit gilt für die Verknüpfung von Steuerungsteilen sowohl unterschiedlicher Kategorien wie unterschiedlicher Performance Levels. Wie die Praxis in der Vergangenheit schon oft gezeigt hat, ist aber eine hydraulische Kategorie 1 wegen der hohen MTTFd der Komponenten u. U. vergleichbar sicher zu einer elektronischen Kategorie 3 mit mittlerer DC_{avg} und niedriger $MTTF_d$. Da Zu- und Abschläge zur Kategorie wegen $MTTF_d$ und DC_{avg} im PL bereits berücksichtigt sind, orientiert sich der PL für die Zusammenschaltung an der Häufigkeit des niedrigsten PLs in der Serienschaltung und nicht an der niedrigsten Einzel-Kategorie. „Wie durch ein Wunder“ zeigt sich dies auch tatsächlich in Bild 5. Das heißt die später aufgekommene vereinfachte Theorie passt ohne Lücken zur Praxis. Da mit der Anzahl der Steuerungselemente auch die Gesamt-Ausfallwahrscheinlichkeit steigt, kann der niedrigste PL noch um eine Stufe verringert sein, wenn z. B. davon mehr als drei Elemente hintereinander geschaltet werden.

Wie geht’s weiter?

Nach Erscheinen der überarbeiteten EN ISO 13849-1 voraussichtlich im Laufe des Jahres 2006 wird es zunächst eine dreijährige Übergangsfrist geben, in der die Vorgängerfassung parallel gültig bleibt. Damit ist einer der meistgenannten Kritikpunkt entkräftet, nämlich der Umfang der Neuerungen, welche erst ihren Weg in die Köpfe der Entwickler und Anwender finden müssen. Dieser Prozess soll vom BGIA auch durch frei verfügbare Anwendungshilfen unterstützt werden, sowohl in Form erklärender und mit Beispielen versehener Literatur als auch durch das Hilfsprogramm „SiSteMa“(**S**icherheit von **S**teuerungen an **M**aschinen), welches die Berechnung und Dokumentation von PL_r und PL unterstützt (**Bild 9**). Frisch verfügbar ist der „**P**erformance **L**evel **C**alculator“, welcher das Säulendiagramm in Form einer Drehscheibe darstellt, mit der der PL jederzeit einfach und genau ermittelt werden kann. Ob die überarbeitete Fassung ihren Anspruch erfüllt, durch einfache, praktikable Methoden und einen Technologieübergreifenden Ansatz die Brücke zwischen Kategorien und Ausfallwahrscheinlichkeit zu schlagen und ein solides Fundament für die Bewertung der nächsten Steuerungsgenerationen zu bieten, kann aber letztlich nur der Anwender (Autoren gehören zum Anwenderkreis!) entscheiden. In den nächsten beiden Teilen dieser Artikelserie werden dazu die fluidtechnischen Details genauer erläutert werden und die Bewertung anhand eines Schaltungsbeispiels vorgeführt werden.

Weiterführende Hilfen und Literatur finden sich auf der BGIA-Homepage (www.hvbg.de/bgia) unter dem Webcode 1674855. Dort kann u.a. die PLC-Drehscheibe kostenlos bestellt werden.