SISTEMA: ein Tool zur einfachen Anwendung der Steuerungsnorm EN ISO 13849-1

Dr. Michael Huelke, BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Fachbereich 5: Unfallverhütung - Produktsicherheit
Michael Hauke, BGIA, Fachbereich 5: Unfallverhütung – Produktsicherheit
Jan Pilger, BGIA, Fachbereich 5: Unfallverhütung – Produktsicherheit

SISTEMA: a tool for the easy application of the control standard EN ISO 13849-1

The ISO 13849-1:2006, the revision of the standard formerly known as EN 954-1, gives guidelines to develop, validate and certify in a simple way safety-related control systems in the field of machinery. Deterministic and probabilistic requirements are combined in a practicable manner. The BGIA accompanies the application of these new simple methodologies by having launched a free software tool called "SISTEMA", which gives guidance through the different steps of the standard, even for large safety-related control systems. Moreover, it uses a more sophisticated calculation of the Performance Level than that proposed in the standard.

Functional safety, control systems, machinery, calculus of reliability, software tool

1. Hintergrund

Seit gut einem Jahrzehnt werden sicherheitsbezogene Teile von Maschinensteuerungen nach der Sicherheitsnorm DIN EN 954-1 konstruiert und bewertet. Um neue Technologien wie Elektronik und Software stärker zu berücksichtigen, wurde eine grundlegende Überarbeitung dieser Norm notwendig, wobei das BGIA intensiv mitgearbeitet hat. In der Revision DIN EN ISO 13849-1:2007 [1] werden bewährte deterministische Merkmale der Kategorien und neue Anforderungen zur Ausfallwahrscheinlichkeit (Lebensdauer der Bauteile, Güte der Testung) auf praktikable Weise miteinander kombiniert [2], [3], [4]. Das BGIA hatte schon seit Mitte der 90er Jahre, z.B. durch Mitarbeit im Europäischen Projekt STSARCES (Standards for Safety Related Complex Electronic Systems) [5], Kenntnisse und Erfahrungen mit der so genannten Quantifizierung sammeln und bei Prüfungen von Sicherheitskomponenten anwenden können. Dieses Know-how hat mit entscheidenden Impulsen und Grundlagenarbeiten zu den vereinfachten Berechnungsmethoden der Normenrevision beigetragen.

Diese Berechnungsmethoden und die Handhabung von Zuverlässigkeitsdaten sind im Maschinenbau noch relativ unbekannt und, trotz einfacher Ansätze, in der Praxis aufwändig. Aufgrund seines Präventionsauftrages und mit dem Hintergrundwissen zur Revision begleitet das BGIA daher die Einführung und Anwendung dieser neuen

Norm durch die Entwicklung und Bereitstellung von kostenfreien Hilfsmitteln. Eines davon ist das hier vorgestellte PC-Programm SISTEMA (Sichere Steuerungen von Maschinen). Im Wesentlichen soll mit SISTEMA die Ausfallwahrscheinlichkeit für geplante oder bereits realisierte Steuerungen einfach und schnell berechnet werden können. Neben der Erhöhung der Akzeptanz der neuen Methoden sollen durch strukturierte Bedienerführung die vollständige und fehlerfreie Anwendung der DIN EN ISO 13849-1 erreicht werden. Mit Plausibilitäts- und Konsistenzchecks sowie einem dreistufigen Meldungssystem hilft SISTEMA Anwendungsfehler zu vermeiden. Das Tool unterstützt Maschinenhersteller, Steuerungshersteller und Prüfstellen bei der Gestaltung, Integration und Bewertung von sicherheitsbezogenen Teilen von Maschinensteuerungen. Dabei werden alle relevanten Steuerungstechnologien berücksichtigt. Das Programm ist gefördert durch den Fachausschuss "Druck und Papierverarbeitung".

Die Anforderungen an das Programm wurden nach systematischer Aufarbeitung der endgültigen Norminhalte und unter Berücksichtigung der Erfahrungen mit einem vorher entwickelten Softwareprotoypen definiert. Die verschiedenen Verfahren der Norm wurden in der Software so abgebildet, dass der Anwender nur noch seine Daten in übersichtlichen Eingabemasken eintragen muss und das Ergebnis ständig automatisch berechnet wird. Eine wichtige Anforderung war auch die Trennung zwischen der Benutzeroberfläche und der Datenbank für Projekte, Sicherheitsfunktionen und Bauteile. Neben robusten Rechenfunktionen wurden auch Komfortfunktionen implementiert, wie die Ergebnisprognose oder eine Datenbank für Standardbauteile und bereits berechnete Steuerungen. Die Gebrauchstauglichkeit der Software wird durch die Ergebnisdokumentation in einem Bericht und der Benutzereinweisung mit einem „Wizard“ erhöht.

SISTEMA ist derzeit mit deutscher und englischer Sprachversion verfügbar. Zukünftige weitere Sprachfassungen werden eine schnelle internationale Verbreitung ermöglichen. Die Erprobung des Programms erfolgte durch Prüfer im BGIA anhand der Bewertung von realen Steuerungen. Weiterhin wurden schon viele Schaltungsbeispiele berechnet, die in dem BGIA-Report 2/2008 veröffentlicht sind.

2. Funktion von SISTEMA

Mit dem Software-Assistenten SISTEMA steht den Entwicklern und Prüfern von sicherheitsbezogenen Maschinensteuerungen eine umfassende Hilfestellung bei der Bewertung der Sicherheit im Rahmen der DIN EN ISO 13849-1 zur Verfügung. Das Windows-Tool bietet dem Benutzer die Möglichkeit, die Struktur der sicherheitsbezogenen Steuerungsteile auf Basis der so genannten vorgesehenen Architekturen nachzubilden und erlaubt schließlich eine automatisierte Berechnung der Zuverlässigkeitswerte auf verschiedenen Detailebenen einschließlich des erreichten Performance Levels (PL) und der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH).

Über Eingabemasken werden relevante Parameter wie die Risikoparameter zur Bestimmung des erforderlichen Performance Level (PL_r), die Kategorie des Steuerungssystems, die Maßnahmen gegen Fehler gemeinsamer Ursache (common cause failure, CCF) bei mehrkanaligen Systemen, die mittlere Bauteilgüte (mean time to

dangerous failure, $MTTF_d$) und die mittlere Testqualität (average diagnostic coverage, DC_{avg}) von Bauelementen bzw. Blöcken Schritt für Schritt erfasst. Nachdem die geforderten Daten in SISTEMA eingetragen wurden, sind die berechneten Ergebnisse sogleich sichtbar. Praktisch für den Benutzer: Jede Parameteränderung wird in ihrer Auswirkung auf das Gesamtsystem über die Programmoberfläche direkt angezeigt. Das umständliche Nachschlagen in Tabellen und Ausrechnen von Formeln (Bestimmung der $MTTF_d$ nach dem „Parts Count"-Verfahren, Symmetrisierung der $MTTF_d$ für jeden Kanal, Abschätzung des DC_{avg}, Ermittlung von PFH und PL etc.) wird durch die Software übernommen und entfällt daher weitestgehend. Dies ermöglicht es dem Benutzer, Parameterwerte zu variieren, um so die Auswirkungen von Änderungen zu beurteilen, ohne dabei großen Aufwand zu treiben. Die Resultate werden schließlich in einem druckbaren Report zusammengefasst.

Dennoch bleiben auch mit der Berechnung durch ein Tool wie SISTEMA noch einige Herausforderungen für den Anwender, die nur durch Übung und Erfahrung zu meistern sind. Vor der Anwendung von SISTEMA stehen zunächst die Definition der Sicherheitsfunktionen sowie die Modellierung des Steuerungssystems, d.h. die Abbildung der realen Struktur einer sicherheitsbezogenen Steuerung auf ein Modell. Diese Darstellung nennt man „sicherheitsbezogenes Blockdiagramm". In der Praxis können die realen Strukturen nicht immer durch die in den Normen verwendeten Architekturen abgebildet werden. Nach dieser Modellierung bleibt als weitere Herausforderung, alle Daten über die Ausfallwahrscheinlichkeit von Bauteilen zu recherchieren. Mit zunehmender Anwendung der Norm werden aber die Hersteller alle relevanten Zuverlässigkeitskennwerte für ihre Komponenten oder Bauteile angeben können. Weiterhin gilt es auch die angemessene Testqualität (DC) einzelner Maßnahmen, vor allem bei sehr unterschiedlicher Wirksamkeit („Fehleraufdeckung durch den Prozess": DC = 0 – 99 %), richtig einzuschätzen.

3. Anwendung von SISTEMA

SISTEMA verarbeitet so genannte Grundelemente aus insgesamt sechs verschiedenen Hierarchiestufen: das Projekt (PR), die Sicherheitsfunktion (SF), das Subsystem (SB), der Kanal (CH) / Testkanal (TE), der Block (BL) und das Element (EL). Deren Zusammenhang ist im Folgenden kurz dargestellt (Abbildung 1).

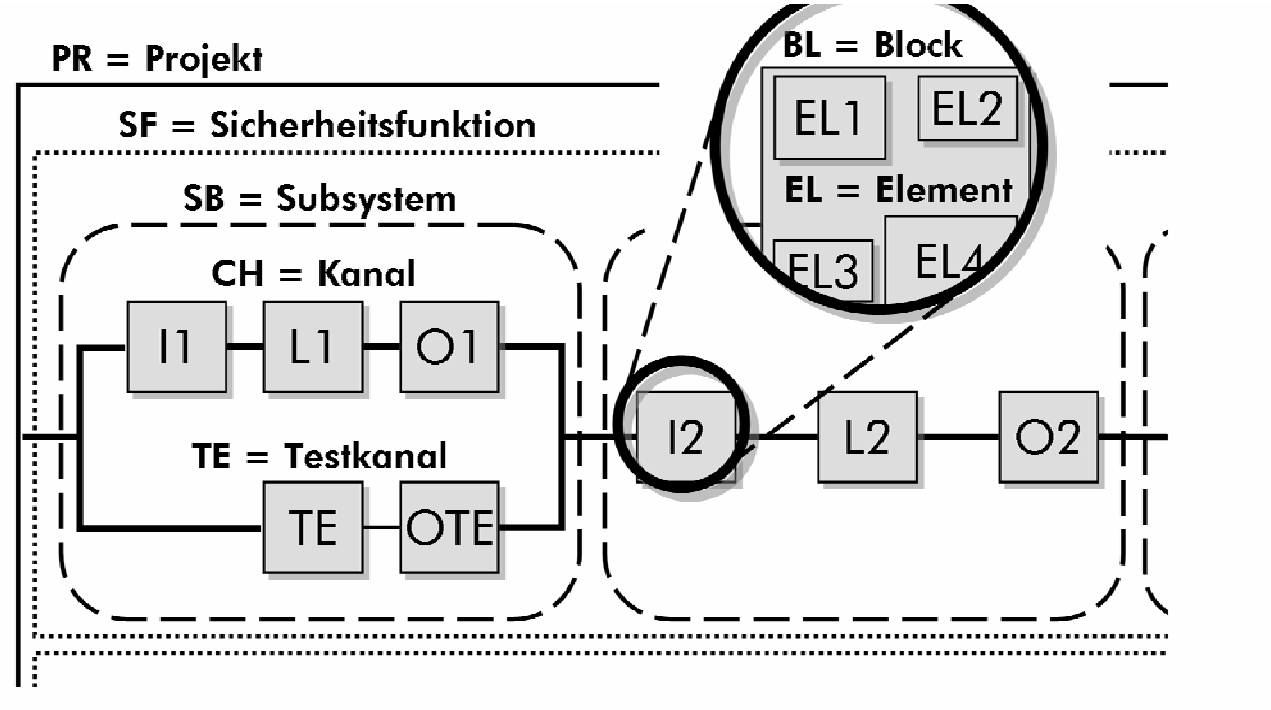

Abbildung 1: Die in SISTEMA betrachteten Hierarchieebenen

Der Benutzer eröffnet zunächst ein Projekt und kann darin die Maschine bzw. die Gefahrenstelle, die weiter betrachtet werden soll, definieren. Dem Projekt werden schließlich alle erforderlichen Sicherheitsfunktionen zugewiesen. Diese können durch den Benutzer festgelegt und dokumentiert, sowie mit einem PL_r belegt werden. Der tatsächlich erreichte Performance Level (PL) des parametrierten sicherheitsbezogenen Teils einer Steuerung (safety related part of a control system, SRP/CS) wird automatisch aus den Subsystemen ermittelt, die – in Serie geschaltet – die Sicherheitsfunktion ausführen. Den Subsystemen liegt jeweils – in Abhängigkeit zu der gewählten Kategorie – eine so genannte vorgesehene Architektur aus der Norm zugrunde. Aus der Architektur bestimmt sich unter anderem, ob die Steuerung einkanalig, einkanalig getestet oder redundant ausgelegt ist und ob bei der Auswertung ein spezieller Testkanal zu berücksichtigen ist. Jeder Kanal kann sich wiederum in beliebig viele Blöcke unterteilen, für die der Benutzer entweder direkt einen $MTTF_d$-Wert und einen DC-Wert einträgt, oder aber auf der niedrigsten Hierarchieebene die Werte für die einzelnen Bauelemente einträgt, aus denen sich der Block zusammensetzt.

4. Oberfläche von SISTEMA

Die Programmoberfläche von SISTEMA gliedert sich in vier Bereiche (Abbildung 2). Den größten Anteil der Fläche nimmt der Arbeitsbereich auf der rechten Seite ein. Er enthält je nach aktiver Sicht eine editierbare Eingabemaske oder einen Abschnitt aus dem Übersichtsdokument.

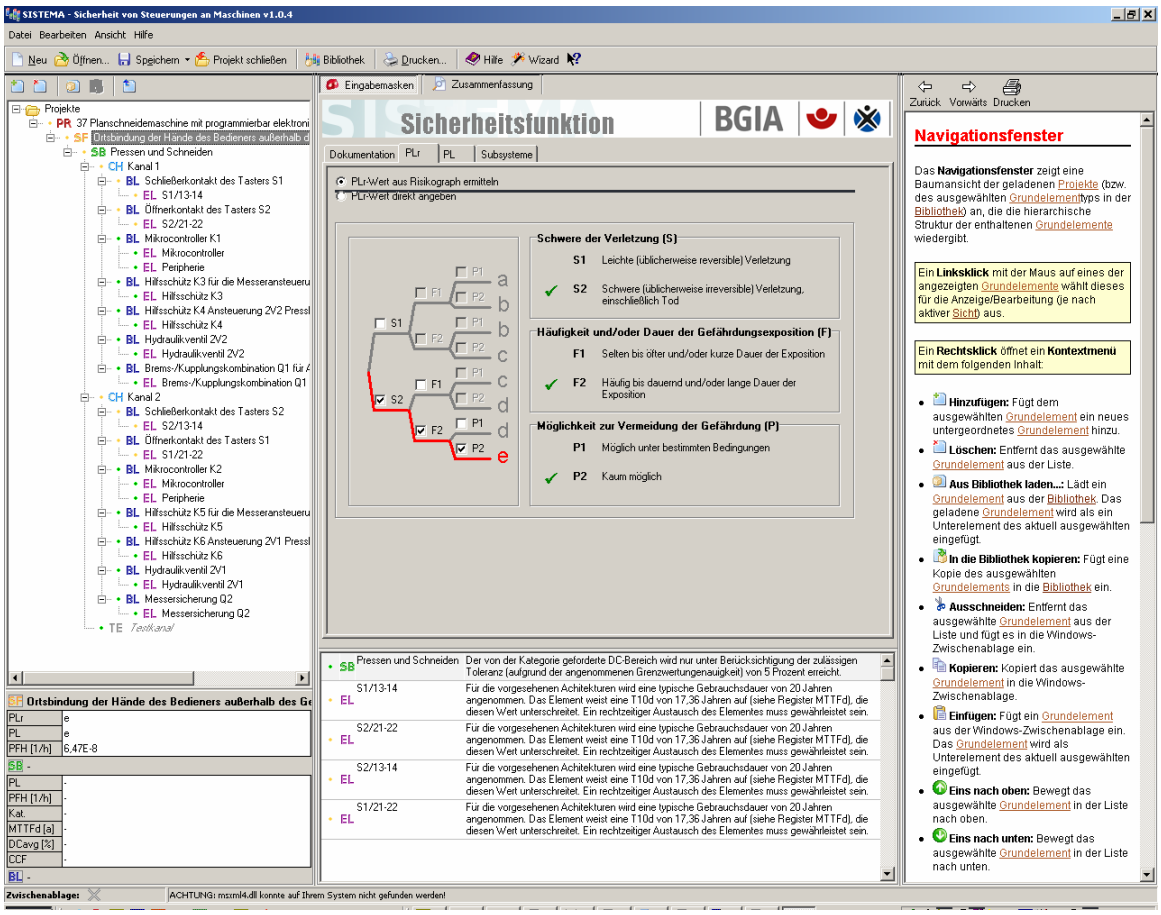

Abbildung 2: Die Programmoberfläche von SISTEMA

Der Inhalt der jeweiligen Sicht ist durch das ausgewählte Grundelement aus der oben genannten Hierarchie (Abbildung 1) bestimmt und wird über die Selektion in einer Baumansicht auf der linken Seite festgelegt. Jede Verzweigung in der Baumansicht steht für ein Grundelement. Über den Baum lassen sich auch Grundelemente auf den verschiedenen Ebenen neu erzeugen, entfernen, verschieben oder kopieren. Die Details des angewählten Grundelements werden in der Editieransicht über die Eingabemaske eingetragen. Jede Eingabemaske ist selbst über Register in verschiedene Bereiche untergliedert. Die jeweils letzte Registerkarte enthält eine Tabelle, die alle untergeordneten Verzweigungen zusammenfasst und die wichtigsten Informationen auflistet. Hat der Benutzer beispielsweise einen Block in der Baumansicht markiert, so zeigt diese Tabelle alle darin enthaltenen Elemente mit ihren $MTTF_d$- und DC-Werten an.

Ferner enthält die Baumansicht zu jedem Grundelement eine Statusinformation durch eine farbliche Markierung in Form eines Punktes neben der Verzweigung. Rot zeigt an, dass eine Bedingung der Norm nicht erfüllt ist, ein Grenzwert überschritten ist oder eine allgemeine Inkonsistenz vorliegt, durch die ein erforderlicher Wert nicht berechnet werden kann. In diesem Fall wird eine Warnung ausgegeben. Gelb bedeutet, dass ein unkritischer Hinweis vorliegt (z.B. wenn ein Grundelement noch unbenannt ist). Alle anderen Grundelemente werden grün gekennzeichnet. Eine Farbkennzeichnung vererbt sich immer auch auf die übergeordneten Verzweigungen, wobei rot die höchste und grün die niedrigste Priorität hat. Alle

Warnungen und Hinweise zu dem aktiven Grundelement werden im Meldungsfenster unterhalb des Arbeitsbereiches aufgeführt.

Der Bereich unterhalb der Baumansicht zeigt die wichtigsten Kontextinformationen des ausgewählten Grundelementes an. Diese bestehen aus PL, PFH, $MTTF_d$, DC_{avg} und CCF des übergeordneten Subsystems, sowie PL_r, PL und PFH der übergeordneten Sicherheitsfunktion (das gilt natürlich nur für Grundelemente, die in tieferen Hierarchieebenen liegen). So sieht der Benutzer laufend, wie sich seine Änderungen in den angezeigten Parametern bemerkbar machen.

Neben ihrer Flexibilität zeichnet sich die Programmoberfläche von SISTEMA durch eine komfortable und intuitive Bedienbarkeit aus. Kontextspezifische Hilfetexte sollen den Einstieg erleichtern. Zusätzliche Unterstützung bietet der mit der Anwendung ausgelieferte Wizard – ein Assistent, der den Einsteiger Schritt für Schritt bei der virtuellen Nachbildung seiner Steuerung begleitet und ihm einen schnellen Zugang gewährleistet.

5. Schnittstellen zu Anwender- und Herstellerdatenbanken

Komfortable Bibliotheksfunktionen runden den Leistungsumfang von SISTEMA ab. Die mitgelieferten Bibliotheken enthalten einige Standardelemente, Blöcke und komplette Subsysteme, lassen sich jedoch durch den Benutzer z.B. als Datenbank für seine häufig genutzten Bauteile, beliebig erweitern. Optional können weitere Bibliotheksmodule nachinstalliert werden, z.B. projekt- und maschinenspezifische Bibliotheken des Maschinenherstellers mit wieder verwendbaren Objekten. SISTEMA erlaubt dabei das Umschalten zwischen verschiedenen Bibliotheken. Der Anwender kann Bibliotheksdateien mit anderen SISTEMA-Anwendern austauschen und einbinden. Auch Komponentenhersteller können schreibgeschützte Bibliotheken mit Zuverlässigkeitsdaten ihrer Produkte erstellen und damit ihre Kunden unterstützen.

Auch die technischen und organisatorischen Maßnahmen, die zur Bewertung einer Steuerung notwendig sind, hält SISTEMA in verschiedenen Bibliotheken vor. Diese Bibliotheken enthalten zunächst die typischen und meist verwendeten Maßnahmen, wie sie auch in der DIN EN ISO 13849-1 enthalten sind. SISTEMA verwaltet dazu folgende Bibliotheken:

- Bibliothek „CCF-Maßnahmen“: Diese Bibliothek enthält eine Liste mit Maßnahmen gegen Fehler gemeinsamer Ursache inklusive deren Punktewert für die Quantifizierung der CCF nach Anhang F der DIN EN ISO 13849-1. Diese Liste kann durch den Benutzer beliebig erweitert werden.

- Bibliothek „DC-Maßnahmen“: Diese Bibliothek enthält eine Liste mit Diagnosemaßnahmen inklusive deren DC-Wert nach Anhang E der Norm. Diese Liste kann ebenfalls durch den Benutzer beliebig erweitert werden.

- Bibliothek „Verfahren guter ingenieurmäßiger Praxis“: Diese Bibliothek hält für diverse Arten von Elementen $MTTF_d$- bzw. $B10_d$-Werte bereit, die auf guter ingenieurmäßiger Praxis basieren, nach Anhang C der Norm. Änderungen, Löschungen oder Ergänzungen der Listeneinträge sind hier nicht möglich.

6. Verfeinerte Berechnungsverfahren für Performance Level

Mitunter kommt es vor, dass der für ein System ermittelte DC_{avg}-Wert nur geringfügig unterhalb einer der Schwellen „niedrig“ (60%), „mittel“ (90%) oder „hoch“ (99%) liegt. Wenn dann das vereinfachte Quantifizierungsverfahren aus DIN EN ISO 13849-1 angewendet wird, muss rein formal jeweils mit der nächst kleineren DC_{avg}-Stufe, also mit „kein“, „niedrig“ bzw. „mittel“ weitergearbeitet werden. Diese Vorgehensweise schätzt das System zur sicheren Seite ab. Wegen der wenigen Stufen der DC_{avg}-Skala kann jedoch manchmal eine nur kleine Systemänderung, die den Wert DC_{avg} eine der Schwellen gerade unterschreiten lässt, zu einer deutlichen Schlechterbewertung des Systems führen. Dies kann sogar passieren, wenn in einem Kanal hochwertig getestete Bauelemente (hoher DC) durch bessere Bauelemente (mit höherer $MTTF_d$) ersetzt werden. Die kleine Verbesserung der Kanal-$MTTF_d$ wird dann durch die formal vollzogene Herabstufung von DC_{avg} auf den nächst kleineren Wert überkompensiert, wodurch die ermittelte PFH schlechter (größer) wird. Dieser paradox erscheinende Effekt ist eine Folge der Grobstufigkeit der DC_{avg}-Skala, also letztlich eine Konsequenz der Einfachheit von Bild 5 (bzw. Tabelle K.1) der DIN EN ISO 13849-1.

Der beschriebene Effekt kann dadurch verhindert oder gemildert werden, dass an Stelle des Bildes 5 eine Grafik mit feinerer Abstufung der DC_{avg}-Werte benutzt wird. Sie ist unten in Abbildung 3 gezeigt. Mit Rücksicht auf die begrenzte Genauigkeit von DC_{avg}-Werten wurden für alle Kategorien auch die minimal möglichen DC_{avg}-Werte berücksichtigt. SISTEMA nutzt dieses verfeinerte Verfahren zur Bestimmung des PFH-Wertes und interpoliert dabei noch zwischen den in Abbildung 3 gezeigten Säulen. Generell kann dadurch eine starke Herabstufung von DC_{avg} vermieden und oft ein genauerer und zugleich besserer PFH-Wert ermittelt werden.

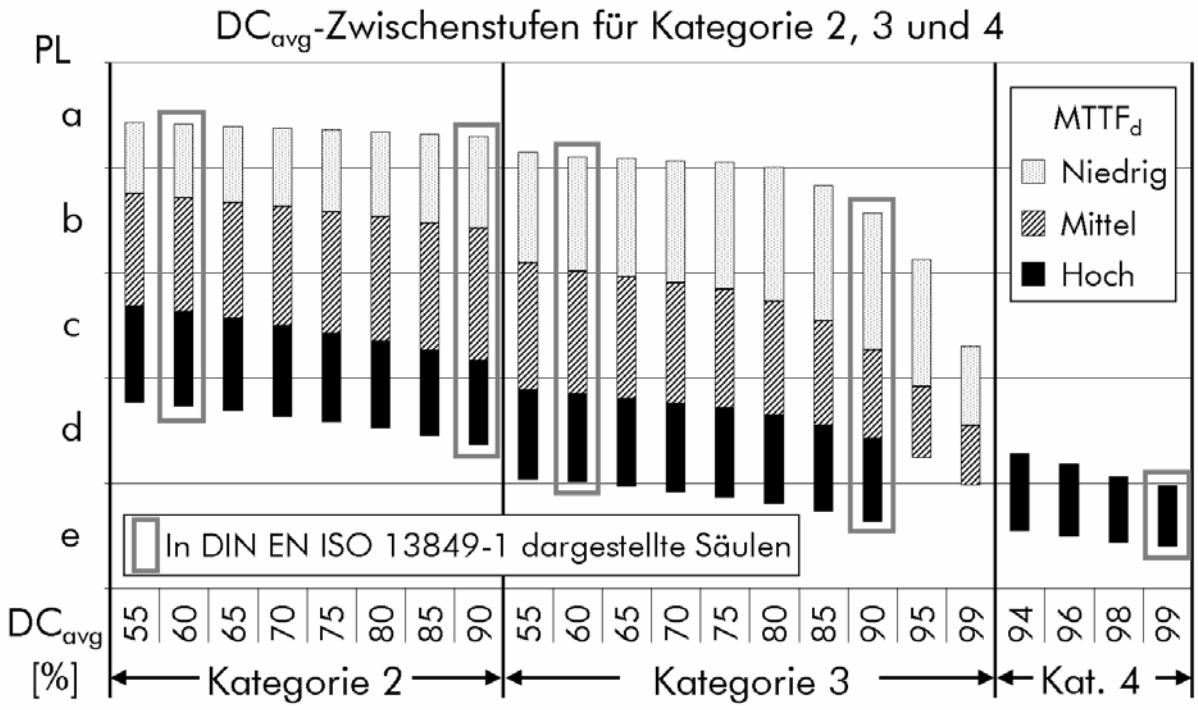

Abbildung 3: Verfeinertes Berechnungsverfahren für den Performance Level

7. Fazit und Ausblick

Die DIN EN ISO 13849-1:2007 zielt in hohem Maß auf Anwenderfreundlichkeit, Transparenz und Reproduzierbarkeit ab. Sie arbeitet vorwiegend mit der Quantifizierung von Bauteilezuverlässigkeiten, der Qualität der Fehlererkennung und fordert auch das Hinzurechnen von Fehlern gemeinsamer Ursache. Im Prinzip wurde bei der DIN EN ISO 13849-1 um den bewährten Kern der DIN EN 954-1 ein sorgfältig abgestimmter Überbau gebildet, der die überarbeitete Norm für alle heute relevanten Technologien rüstet. Daher ist für bisherige 954-Anwender eine schnelle Orientierung möglich. Auch setzt die DIN EN ISO 13849-1, anders als die IEC 61508, keine besonderen Mathematik-Kenntnisse voraus. Sie eignet sich übergreifend für Steuerungstechnologien, die auf Mechanik, Elektrik, Elektronik, Rechnertechnik, Pneumatik und Hydraulik basieren.

Mit SISTEMA steht den Entwicklern und Prüfern von sicherheitsbezogenen Maschinensteuerungen eine umfassende Hilfestellung bei der Bewertung der Sicherheit im Rahmen der DIN EN ISO 13849-1 zur Verfügung. Das Windows-Tool bietet dem Benutzer die Möglichkeit, die Struktur der sicherheitsbezogenen Steuerungsteile auf Basis der so genannten vorgesehenen Architekturen nachzubilden und erlaubt schließlich eine automatisierte Berechnung der Zuverlässigkeitswerte auf verschiedenen Detailebenen einschließlich des erreichten Performance Levels (PL).

Das BGIA begleitet die Einführung und Anwendung dieser neuen Methoden auch durch weitere Hilfsmittel und Publikationen, die kostenlos vom BGIA erhältlich sind. Zur einfachen Bestimmung des PL sicherheitsbezogener Maschinensteuerungen dient die PLC-Drehscheibe, verfügbar unter der Internetadresse http://www.dguv.de/bgia über den Webcode d3508. Die Methoden der Norm werden durch zwei gegeneinander verdrehbare Karton-Scheiben begreifbar gemacht. Sie wurde vom BGIA entwickelt mit Unterstützung durch den Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) - Fachverband Automation und den Verband Deutscher Maschinen- und Anlagenbau - VDMA. Mehrere Unternehmen in der Sicherheitstechnik nutzen diese Scheibe mit eigenem Corporate Design, um ihre Kunden zu unterstützen.

Der Steuerungsreport BGIA 6/97 wurde inzwischen komplett überarbeitet, um die Anwendung der DIN EN ISO 13849-1 und die neuen Anforderungen an Hardware und Software zu beschreiben. Es sind wieder viele Steuerungsbeispiele beschrieben, die mit dem hier vorgestellten Tool berechnet und als SISTEMA-Projektdateien auf den nachfolgend aufgeführten Internetseiten verfügbar sind. Dieser neue BGIA-Report 2/2008 ist unter dem Titel „Funktionale Sicherheit von Maschinensteuerungen - Anwendung der DIN EN ISO 13849-1“ (Webcode d18471) erschienen.

Die Software SISTEMA wird auf den Internetseiten des BGIA nach einer optionalen Registrierung zum Download bereitgestellt. SISTEMA ist mit deutscher und englicher Sprachversion erhältlich, Versionen für weitere Sprachen sind in Vorbereitung. Das Tool wird als Freeware zur kostenlosen Verwendung und Weitergabe an Dritte angeboten. Aktuelle Informationen sowie der Link zum Download sind verfügbar

unter der Internetadresse http://www.dguv.de/bgia über den Webcode d11223. Informationen zur Norm und allen Hilfsmittel finden sich unter der Adresse http://www.dguv.de/bgia/13849.

8. Literatur

[1] DIN EN ISO 13849-1:2007 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze“, Beuth, Berlin 2007

[2] Plüddemann, G.; Schaefer, M.; Hauke, M.: Im Wandel - Vergleich und Verkettung unterschiedlicher Sicherheitsnormen, Elektrotechnik 89 (2007) Nr. 2, S. 26-28

[3] Hauke, M.; Schaefer, M.: Sicherheitsnorm mit neuem Konzept, O + P Ölhydraulik und Pneumatik 50 (2006) Nr. 3, S. 142-147

[4] Plüddemann, G.: Sicherheitsgerichtete Funktionen im Maschinenbau - Neue Norm bietet Lichtblicke, Fachartikel aus IEE (2005) Nr. 8, S. 74-79

[5] Dorra, M.; Reinert, D.: Quantitative Analysis of Complex Electronic Systems using Fault Tree Analysis and Markov Modelling European Project STSARCES (Standards for Safety Related Complex Electronic Systems), Contract SMT 4CT97-2191, Final report of Work Package 2.1, Annex 6,European Commission - DG XII, Brussels 2000