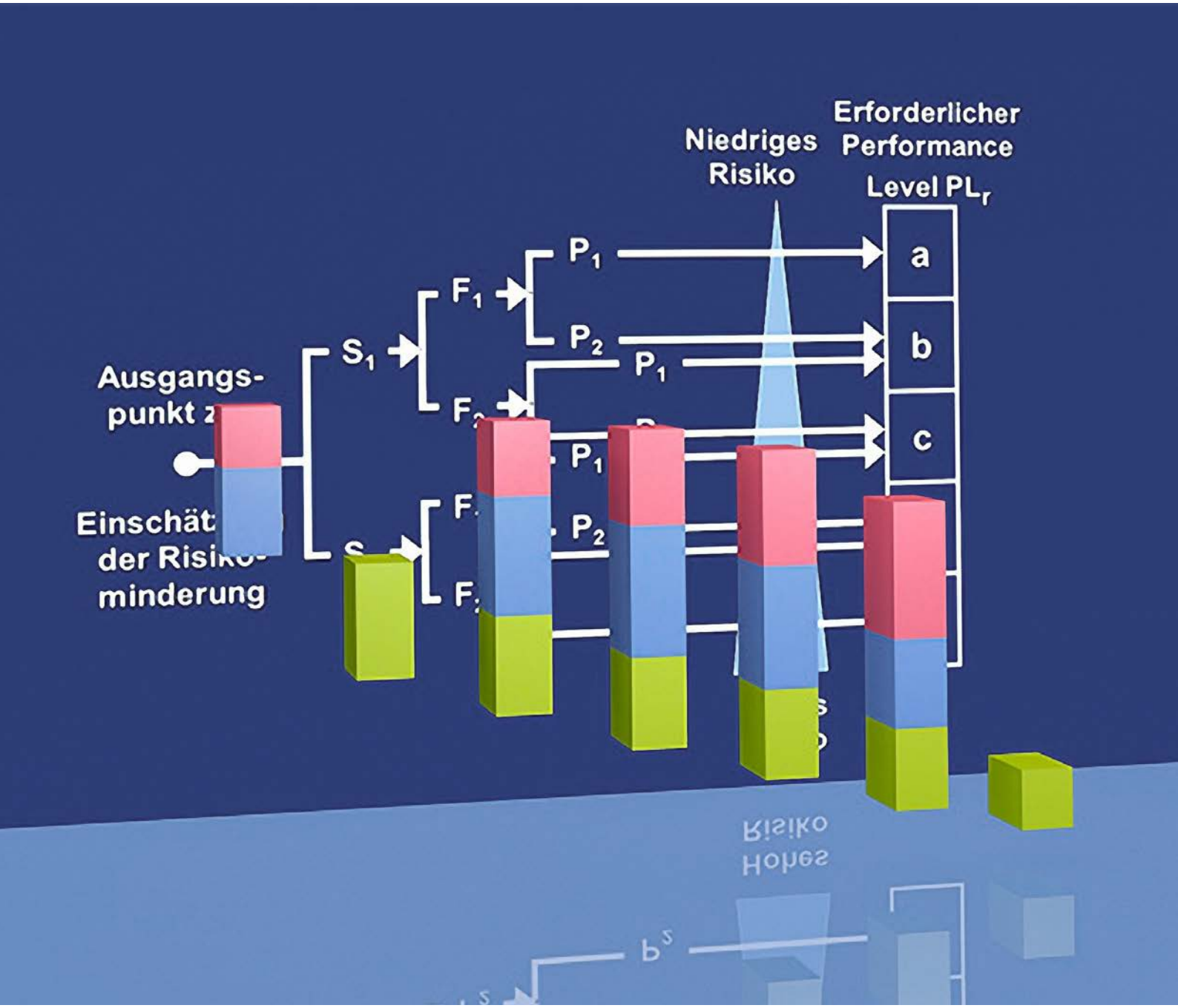
DGUV
Deutsche Gesetzliche
Unfallversicherung
Spitzenverband



IFA Report 2/2017

Funktionale Sicherheit von Maschinensteuerungen

– Anwendung der DIN EN ISO 13849 –

Impressum

Verfasst von:	Michael Hauke, Michael Schaefer, Ralf Apfeld, Thomas Bömer, Michael Huelke, Torsten Borowski, Karl-Heinz Büllesbach, Michael Dorra, Hans-Georg Foermer-Schaefer, Jürgen Uppenkamp, Oliver Lohmaier, Klaus-Dieter Heimann, Burkhard Köhler, Helmut Zilligen, Stefan Otto, Paul Rempel, Günter Reuß Abteilung 5, Unfallprävention: Digitalisierung – Technologien Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin
Redaktion:	Abteilung Fachübergreifende Aufgaben des IFA, Bereich Wissenschaftsmedien
Broschürenversand:	bestellung@dguv.de
Publikationsdatenbank:	www.dguv.de/publikationen
Herausgeber:	Deutsche Gesetzliche Unfallversicherung e.V. (DGUV) Glinkastraße 40, 10117 Berlin Tel.: 030 288763800 Fax: 030 288763808 E-Mail: info@dguv.de Internet: www.dguv.de 5., geänderte Auflage, zuletzt geändert: Juni 2021
Satz und Layout:	DGUV
ISBN (print)	978-3-86423-193-3
ISBN (online)	978-3-86423-194-0
ISSN:	0173-0387

Kurzfassung

Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849 –

Die Norm DIN EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ macht Vorgaben für die Gestaltung von sicherheitsbezogenen Teilen von Steuerungen. Dieser Report ist eine Aktualisierung des gleichnamigen BGIA-Reports 2/2008. Er stellt die wesentlichen Inhalte der Norm in ihrer dritten Ausgabe von 2016 vor und erläutert deren Anwendung an zahlreichen Beispielen aus den Bereichen Elektromechanik, Fluidtechnik, Elektronik und programmierbarer Elektronik, darunter auch Steuerungen gemischter Technologie. Der Zusammenhang der Norm mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie wird aufgezeigt und mögliche Verfahren zur Risikoabschätzung werden vorgestellt. Auf der Basis dieser Informationen erlaubt der Report die Auswahl des erforderlichen Performance Level PL_r für steuerungstechnische Sicherheitsfunktionen. Die Bestimmung des tatsächlich erreichten Performance Level PL wird detailliert erläutert. Auf die Anforderungen zum Erreichen des jeweiligen Performance Level und seine zugehörigen Kategorien, auf die Bauteilzuverlässigkeit, Diagnosedeckungsgrade, Softwaresicherheit und Maßnahmen gegen systematische Ausfälle sowie Fehler gemeinsamer Ursache wird im Detail eingegangen. Hintergrundinformationen zur Umsetzung der Anforderungen in die steuerungstechnische Praxis ergänzen das Angebot. Zahlreiche Schaltungsbeispiele zeigen bis auf die Ebene der Bauteile hinunter, wie die Performance Level a bis e mit den Kategorien B bis 4 in den jeweiligen Technologien technisch umgesetzt werden können. Sie geben dabei Hinweise auf die verwendeten Sicherheitsprinzipien und sicherheitstechnisch bewährte Bauteile. Zahlreiche Literaturhinweise dienen einem tieferen Verständnis der jeweiligen Beispiele. Der Report zeigt, wie die Anforderungen der DIN EN ISO 13849-1 in die technische Praxis umgesetzt werden können, und leistet damit einen Beitrag zur einheitlichen Anwendung und Interpretation der Norm auf nationaler und internationaler Ebene.

Abstract

Functional safety of machine controls – Application of EN ISO 13849 –

The EN ISO 13849-1 standard, "Safety of machinery – Safety-related parts of control systems", contains provisions governing the design of such parts. This report is an update of BGIA-Report 2/2008 of the same name. It describes the essential subject-matter of the standard in its third, revised 2016 edition, and explains its application with reference to numerous examples from the fields of electromechanics, fluidics, electronics and programmable electronics, including control systems employing mixed technologies. The standard is placed in its context of the essential safety requirements of the Machinery Directive, and possible methods for risk assessment are presented. Based upon this information, the report can be used to select the required Performance Level PL_r for safety functions in control systems. The Performance Level PL which is actually attained is explained in detail. The requirements for attainment of the relevant Performance Level and its associated Categories, component reliability, levels of diagnostic coverage, software safety and measures for the prevention of systematic and common-cause failures are all discussed comprehensively. Background information is also provided on implementation of the requirements in real-case control systems. Numerous example circuits show, down to component level, how Performance Levels a to e can be engineered in the selected technologies with Categories B to 4. The examples provide information on the safety principles employed and on components with well-tried safety functionality. Numerous literature references permit closer study of the examples provided. The report shows how the requirements of EN ISO 13849-1 can be implemented in engineering practice, and thus makes a contribution to consistent application and interpretation of the standard at national and international level.

Résumé

La sécurité fonctionnelle des systèmes de commande de machines – Application de la norme DIN EN ISO 13849 –

La norme DIN EN ISO 13849-1 « Sécurité des machines – Parties des systèmes de commande relatives à la sécurité » définit comment doivent être conçues les parties des systèmes de commande relatives à la sécurité. Le présent rapport est une version actualisée du rapport 2/2008 du même nom du BGIA. Il présente les principaux contenus de la norme dans sa troisième édition de 2016, et en explique l'application à partir de nombreux exemples pris dans les domaines de l'électromécanique, de la technique des fluides, de l'électronique et de l'électronique programmable, et notamment aussi des systèmes de commande de technologie mixte. Ce texte met en évidence le lien entre la norme et les exigences essentielles de sécurité de la directive Machines, et présente des procédures possibles permettant d'évaluer les risques. Sur la base de ces informations, le rapport permet de sélectionner le niveau de performance PL_r nécessaire pour les fonctions relatives à la sécurité des systèmes de commande. Il explique aussi en détail la manière de déterminer le niveau de performance PL effectivement atteint. Le rapport traite également en détail des exigences à satisfaire pour atteindre le niveau de performance donné et ses catégories correspondantes, de la fiabilité des composants, des taux de couverture de diagnostic, de la sécurité des logiciels et des mesures à prendre contre les défaillances systématiques, ainsi que contre les erreurs de cause commune. Cette offre est complétée par des informations générales concernant la mise en œuvre des exigences dans la pratique de la technique de commande. De nombreux exemples de circuits allant jusqu'au niveau des composants montrent comment les niveaux de performance 'a' à 'e' avec les catégories B à 4 peuvent être réalisés techniquement dans les technologies respectives. Ils fournissent des indications sur les principes de sécurité utilisés et sur les composants techniques qui ont fait leurs preuves en matière de sécurité. De nombreuses références bibliographiques permettent d'approfondir la compréhension des différents exemples. Montrant comment les exigences de la norme DIN EN ISO 13849-1 peuvent être mises en œuvre dans la pratique technique, le rapport contribue ainsi à ce que la norme soit utilisée et interprétée de manière identique, tant au niveau national qu'international.

Resumen

Seguridad funcional de los sistemas de mando de máquinas – Aplicación de la norma DIN EN ISO 13849 –

La norma DIN EN ISO 13849-1 «Seguridad de las máquinas: partes de los sistemas de mando relativas a la seguridad» establece reglas para el diseño de partes de sistemas de mando relativas a la seguridad. El presente informe es una actualización del informe del mismo nombre del BGIA 2/2008. En él se presentan los contenidos esenciales de la norma en su tercera edición de 2016 y se explica su aplicación con numerosos ejemplos de los ámbitos de la electromecánica, la tecnología de fluidos, la electrónica y la electrónica programable, incluidos los sistemas de mando de tecnologías mixtas. Se muestra la relación de la norma con los requisitos básicos de seguridad de la directiva de maquinaria y se presentan los posibles procedimientos de estimación del riesgo. Sobre la base de estas informaciones, el informe permite seleccionar el nivel de prestaciones requerido (required performance level PL_r) para las funciones de seguridad de los sistemas de mando. Se explica detalladamente cómo de determinar el nivel de prestaciones PL que se ha alcanzado realmente. Se tratan en detalle los requisitos para lograr el nivel de prestaciones en cuestión y sus categorías correspondientes, la fiabilidad de los componentes, los grados de cobertura del diagnóstico, la seguridad del software y las medidas contra fallos sistemáticos así como los errores de causa común. La oferta se completa con informaciones de trasfondo para implementar los requisitos en la práctica de la ingeniería de control. Numerosos ejemplos de circuitos que abarcan hasta el nivel de sus componentes muestran cómo implementar técnicamente los niveles de prestaciones «a» hasta «e» con las categorías B a 4 en las tecnologías correspondientes. Además, se dan indicaciones sobre los principios de seguridad aplicados y los componentes que han demostrado su valía en materia de seguridad. Las numerosas referencias bibliográficas tienen por objeto permitir entender en mayor profundidad los distintos ejemplos citados. El informe muestra cómo se pueden implementar los requisitos de la norma DIN EN ISO 13849-1 en la práctica técnica, contribuyendo así a la homogeneidad de aplicación y de interpretación de la norma a nivel nacional e internacional.

Inhaltsverzeichnis

1 Vorwort

2007 wurde die grundlegende Revision der Steuerungsnorm DIN EN ISO 13849-1 veröffentlicht. Kurz darauf erschien der BGIA-Report 2/2008 „Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849“, der sich wie sein Vorläuferreport 6/97 erneut zum Bestseller entwickelte. Mehr als 20 000 deutschsprachige gedruckte Exemplare wurden seitdem versendet, noch einmal höher ist die Zahl der Downloads auf den Internetseiten des Instituts für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA).

Mit dem Report und weiteren Hilfsmitteln zur Anwendung der Norm – der weitverbreiteten Software SISTEMA, den SISTEMA-Kochbüchern und der „Drehscheibe“ – hat das IFA einen wichtigen Beitrag zur erfolgreichen Einführung von neuen Ansätzen zur Beurteilung und Auslegung der Zuverlässigkeit von elektronischen und programmierbaren Steuerungen geleistet. Dieser Ansatz mit der Betrachtung von Ausfallwahrscheinlichkeiten von Bauteilen ist in der Sicherheits-Grundnormen-Reihe DIN EN 61508 verankert und mittlerweile in fast allen Industriesektoren etabliert – so auch im Maschinenbau.

Der Normensetzung ist es nicht zuletzt durch die intensive Mitwirkung erfahrener Experten des IFA gelungen, die DIN EN ISO 13849-1 so zu gestalten und weiterzuentwickeln, dass sie bei aller Komplexität der Materie praktisch anwendbar ist. Die Vorgängernorm EN 954 mit ihren rein deterministischen Anforderungen wurde endgültig abgelöst. Der Performance Level ist im Maschinenbau angekommen.

In den vergangenen Jahren hat sich die Norm ISO 13849-1 weltweit als der Standard für Maschinensteuerungen etabliert und es konnten weitere Praxiserfahrungen gesammelt werden. Die Experten des IFA haben die wesentlichen Umsetzungsfragen in eigenen Veröffentlichungen kommentiert und ihre Meinungen im Normungsgremium diskutiert. Das Ergebnis: 2016 war die dritte Ausgabe der DIN EN ISO 13849-1 fertiggestellt.

Danach war der richtige Zeitpunkt für einen überarbeiteten IFA Report zu sicherheitsrelevanten Steuerungen von Maschinen gekommen. Das Autorenteam hat den kompletten Report und alle Beispiele überarbeitet. Zusätzlich werden die Änderungen der Norm herausgestellt und interpretiert. Zudem erschi auch eine englische Sprachfassung erscheinen.

Der vorliegende Report und auch die mit SISTEMA ladbaren Steuerungsbeispiele bieten allen Interessierten einen einfachen Einstieg in die inzwischen bewährten normativen Methoden. Der Report ist als Lehrbuch und Nachschlagewerk gedacht. Hierbei ist er selbstverständlich kein Ersatz für die Norm, er enthält jedoch wertvolle Tipps und vor allem schon in der Praxis erarbeitete Erfahrungen und Hilfen.

Prof. Dr. *Dietmar Reinert*
Direktor des IFA

Dr. *Marc Wittlich*
Bereichsleiter

2 Einleitung

Seit dem 1. Januar 1995 müssen alle Maschinen, die innerhalb des europäischen Wirtschaftsraumes in Verkehr gebracht werden, den grundlegenden Anforderungen der Maschinenrichtlinie [1] genügen. Als Maschine gilt nach Artikel 2 dieser Richtlinie die Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist, sowie gegebenenfalls von Betätigungsgeräten, Steuer- und Energiekreisen, die für eine bestimmte Anwendung, z. B. Verarbeitung, Behandlung, Fortbewegung und Aufbereitung eines Werkstoffes, zusammengefügt sind. Mit der Novelle 2006/42/EG [2] der Maschinenrichtlinie werden auch Sicherheitsbauteile, die Hersteller mit dem Verwendungszweck der Gewährleistung einer Sicherheitsfunktion gesondert in Verkehr bringen und deren Ausfall und/oder Fehlfunktion die Sicherheit von Personen gefährdet und die für das Funktionieren der Maschine nicht erforderlich sind oder durch übliche Bauteile ersetzt werden können, unter den Begriff „Maschine“ im Sinne der Richtlinie gefasst. Die Formaldefinition der „Maschine“ erfüllen auch auswechselbare Ausrüstungen, bestimmte Lastaufnahmemittel, Ketten, Seile und Gurte. Detaillierte Ausführungen zu den einzelnen Punkten bietet der Leitfaden für die Anwendung der Maschinenrichtlinie 2006/42/EG [2]. Die Richtlinie gilt neu auch für unvollständige Maschinen.

Die grundlegenden Anforderungen der Maschinenrichtlinie an Konstruktion und Bau von Maschinen und Sicherheitsbauteilen finden sich im Anhang I der Richtlinie. Neben den allgemeinen Grundsätzen für die Integration der Sicherheit gibt es in diesem Anhang eigene Abschnitte zu Steuerungen und Befehlseinrichtungen von Maschinen und den Anforderungen an Schutzeinrichtungen. Die grundlegenden Sicherheitsanforderungen bei der Gestaltung von Maschinen und Sicherheitsbauteilen verpflichten Hersteller, eine Risikobeurteilung vorzunehmen, um alle mit der Maschine verbundenen Gefährdungen zu ermitteln. Drei Grundsätze werden genannt, um die mit den einzelnen Gefährdungen verbundenen Unfallrisiken auf ein akzeptables Maß zu reduzieren, und zwar in der angegebenen Reihenfolge:

- Beseitigung oder Minimierung der Risiken durch die inhärent sichere Konstruktion selbst,
- Ergreifen der notwendigen Schutzmaßnahmen gegen nicht zu beseitigende Risiken,
- Unterrichtung der Nutzenden über Restrisiken, spezielle Ausbildung, Einarbeitung und persönliche Schutzausrüstung.

Nach Artikel 7 lässt die Einhaltung harmonisierter europäischer Normen, deren Fundstelle im Amtsblatt der Europäischen Union (EU) veröffentlicht worden ist („Listung“), die Übereinstimmung mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie vermuten. Mehrere Hundert harmonisierte europäische Normen vertiefen bzw. konkretisieren die im Anhang I der Maschinenrichtlinie zugrunde gelegte Philosophie zur Erreichung der Arbeitssicherheit an Maschinen. Die nur noch einteilige Typ-A-Norm DIN EN ISO 12100 [3] behandelt z. B. Grundbegriffe und allgemeine Gestaltungsleitsätze für die Sicherheit von Maschinen. Inhalte der früheren DIN EN ISO 14121-1 – das gesamte Verfahren zur Identifizierung von Gefährdungen sowie zur Risikoeinschätzung und Risikobewertung der einzelnen Gefährdungen – wurden ebenfalls in die DIN EN ISO 12100 integriert. Daneben gibt es noch den technischen Bericht DIN ISO/TR 14121-2:2013 [4] als praktischen Leitfaden für die Risikobeurteilung mit Verfahrensbeispielen.
Auf der Basis dieser grundlegenden DIN EN ISO 12100 [3] beschreibt die aktualisierte Normenreihe DIN EN ISO 13849-1:2016 [5] und DIN EN ISO 13849-2:2013 [6] die erforderliche Risikominderung bei Gestaltung, Aufbau und Integration von sicherheitsbezogenen Teilen von Steuerungen und Schutzeinrichtungen, gleich ob elektrischer, elektronischer, hydraulischer, pneumatischer oder mechanischer Natur. Mit dieser Norm wird eine allgemein anwendbare Systematik für Steuerungen von Maschinen und/oder deren Schutzeinrichtungen vorgelegt. Die in der Norm beschriebenen Performance Level erweitern den aus DIN EN 954-1 bekannten Kategoriebegriff. Die sicherheitstechnischen Architekturen sind nun durchaus flexibler einsetzbar. Wesentlicher Pluspunkt der DIN EN ISO 13849-1 ist die oben bereits skizzierte technologieunabhängige Behandlung von sicherheitsbezogenen Teilen von Steuerungen. Über den Performance Level sind Kombinationen verschiedener Steuerungsstrukturen mit verschiedenen Technologien einfach realisierbar. Dabei bietet die Norm auf ca. 100 Seiten alles Notwendige in einem Guss. Die Methoden sind von der konkreten Anwendung oder Technologie unabhängig formuliert und werden deshalb von nahezu allen Produktnormen für die Sicherheit von Maschinen (in der Regel Typ-C-Normen) in Bezug genommen.

Die Norm erhielt als harmonisierte Norm nach Inkrafttreten der revidierten Maschinenrichtlinie 2006/42/EG [2] im Dezember 2009 ein stärkeres Gewicht. Dies wird im Wesentlichen auf die Neuerung zurückgeführt, dass sicherheitsrelevante Logiken – auch sicherheitsbezogene Teile von Steuerungen genannt – in den Anhang IV der Richtlinie aufgenommen wurden. Solche Anhang-IV-Produkte erfahren nach der Richtlinie eine besondere Behandlung, sofern sie nicht nach harmonisierten und im Amtsblatt veröffentlichten Normen hergestellt werden. Anhang-IV-Produkte sind zwar nicht prinzipiell EG-baumusterprüfpflichtig[1] – sie können u. a. auch unter einem von einer notifizierten Stelle

1 Neben der EG-Baumusterprüfung kann der Hersteller nach heute gültiger Maschinenrichtlinie bei Vorliegen von harmonisierten Normen auch eigenständig eine Konformitätsbewertung mit interner Fertigungskontrolle durchführen.

bewerteten umfassenden Qualitätssicherungssystem des Herstellers in den Markt eingeführt werden. Jedoch rückten Steuerungen mit der neuen Richtlinie verstärkt in den Mittelpunkt der Sicherheitsbetrachtung [7; 8].

Die DIN EN ISO 13849-1 mit ihrer dritten Ausgabe aus dem Jahr 2016 ist Nachfolgerin der DIN EN 954-1:1997 [9] und im EU-Amtsblatt gelistet. Die Konformitätsvermutung der Version 2008 lief zum 30. Juni 2016 aus. Der zweite Teil DIN EN ISO 13849-2 [6] wurde 2013 nach Überarbeitung veröffentlicht. Momentan befindet sich die DIN EN ISO 13849-1 bereits in der nächsten Revision und wird voraussichtlich 2023 in der vierten Ausgabe erscheinen. Dann wird auch dieser IFA Report wieder neu erscheinen.

Der vorliegende überarbeitete IFA Report hat zum Ziel, die Anwendung der DIN EN ISO 13849 zu erläutern und insbesondere anhand zahlreicher Lösungen die praktische Realisierung beispielhaft aufzuzeigen. Besonderes Augenmerk liegt auf der Darstellung und Interpretation der neuen oder überarbeiteten Anforderungen der dritten Ausgabe der DIN EN ISO 13849-1. Weder die Erläuterungen noch die Beispiele sind als offizieller nationaler oder europäischer Kommentar zu DIN EN ISO 13849-1 aufzufassen. Vielmehr sind in diesem Report die Erfahrungen des Instituts für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) aus 35 Jahren Praxis bei der Beurteilung von Schutz- und Steuereinrichtungen der unterschiedlichen Technologien und aus der langjährigen Mitwirkung in einschlägigen nationalen und internationalen Normungsgremien zusammengetragen.

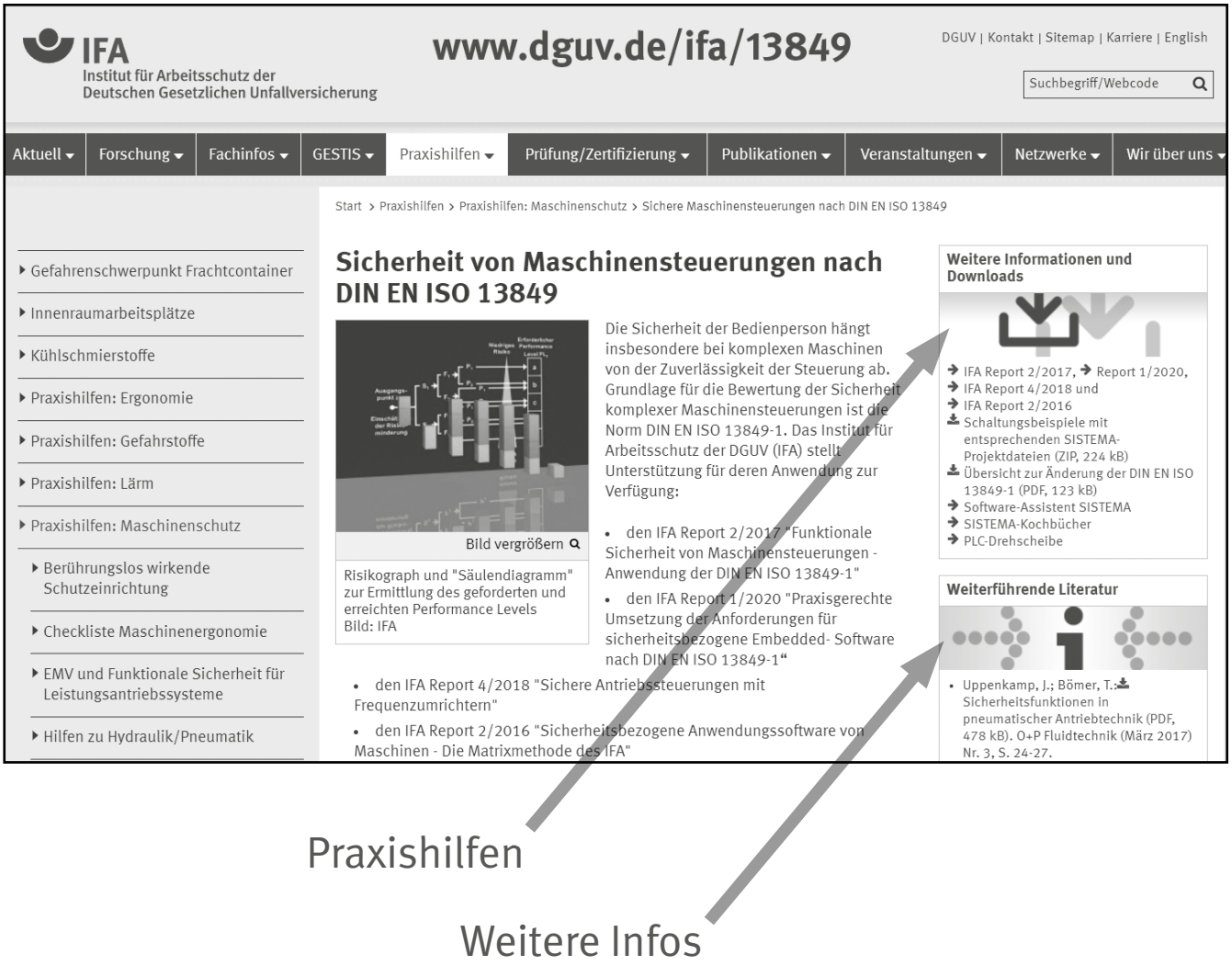
Kapitel 3 befasst sich mit den Basisnormen zur funktionalen Sicherheit an Maschinen und Maschinenanlagen, Kapitel 4 enthält eine Übersicht zur Gliederung dieses Reports bezüglich der Anwendung der DIN EN ISO 13849.

Die Autoren wünschen sich, dass dieser Report für die Konstruktion und den Betrieb sowie Fachleuten im Arbeitsschutz konkrete Hilfen für die Umsetzung der Anforderungen an sicherheitsbezogene Teile von Steuerungen gibt. Die vorliegende Interpretation der Norm ist in unterschiedlichen Anwendungen in der Praxis erprobt und die Grundideen der Beispiele sind in zahlreichen konkreten Anwendungen technisch umgesetzt worden.

Die Internetadresse www.dguv.de/ifa/13849 bietet einen zentralen Zugang zu allen Informationen und Hilfen des IFA zur funktionalen Sicherheit von Maschinensteuerungen (Abbildung 2.1). Neben der freien Software SISTEMA (Sicherheit von Steuerungen an Maschinen) können dort auch die SISTEMA-Projektdateien zu den Schaltungsbeispielen im Kapitel 8 heruntergeladen werden. Zukünftige Erweiterungen sollen stets aktuelle Hilfen zur Verfügung stellen.

Als Hilfe für die Leserinnen und Leser, die mit dem BGIA-Report 2/2008 bereits vertraut sind, sind am Anfang der Kapitel in diesem Report die wesentlichen Änderungen gegenüber dem BGIA-Report 2/2008 kurz zusammengefasst.

Abbildung 2.1:
Diese Internetseite bietet Links zu allen Praxishilfen zur Sicherheit von Maschinensteuerungen



3 Basisnormen zur funktionalen Sicherheit von Maschinensteuerungen

Neben der Norm DIN EN ISO 13849 – in diesem Report behandelt – gibt es alternative, aber relevante allgemeine Normen im Bereich der funktionalen Sicherheit[1]. Dies sind, wie in Abbildung 3.1 dargestellt, die Normen der Reihe DIN EN 61508 [10] und ihre Sektornorm DIN EN 62061 [11] für die Maschinenindustrie. Beide sind im Anwendungsbereich auf elektrische, elektronische und programmierbar elektronische Systeme beschränkt.

Als Klassifizierungsschema sind in DIN EN 61508 und DIN EN 62061 sogenannte Sicherheits-Integritätslevel (SIL) festgelegt. Diese sind ein Gradmesser für die sicherheitsgerichtete Zuverlässigkeit. Es handelt sich um Ausfallgrenzwerte, die jeweils eine Dekade umfassen[2]. DIN EN 61508 unterscheidet zwei verschiedene Anwendungen von Sicherheitsfunktionen:

- Sicherheitsfunktionen in einer Betriebsart mit niedriger Anforderungsrate (Häufigkeit von Anforderungen maximal einmal pro Jahr)
- Sicherheitsfunktionen in einer Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung

In der Betriebsart mit niedriger Anforderungsrate ist die Maßzahl für die Sicherheit die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls einer Sicherheitsfunktion zum Zeitpunkt der Anforderung PFD_{avg} (Average Probability of Failure on Demand). In der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung wird nach DIN EN 62061 die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde PFH_D[3] (Probability of a Dangerous Failure per Hour) bewertet (weitere Informationen siehe auch [12]). Im Maschinenbereich und damit in DIN EN 62061 ist bis auf Ausnahmen nur die zweite Definition relevant. Auch DIN EN ISO 13849-1 hat diese Definition der Betriebsart in der neuen Ausgabe übernommen und begrenzt den Anwendungsbereich der Norm entsprechend. SIL-4-Systeme mit höheren Risiken sind im Maschinenbereich nicht bekannt und werden daher in DIN EN 62061 nicht betrachtet (Abbildung 3.2, siehe Seite 18).

Der grundlegende Ansatz der von der International Electrotechnical Commission (IEC) erarbeiteten Normen zur funktionalen Sicherheit (DIN EN 61508 und DIN EN 62061), Ausfallwahrscheinlichkeiten und nicht speziell auch Strukturen als charakteristische Kenngröße zu definieren, erscheint zunächst

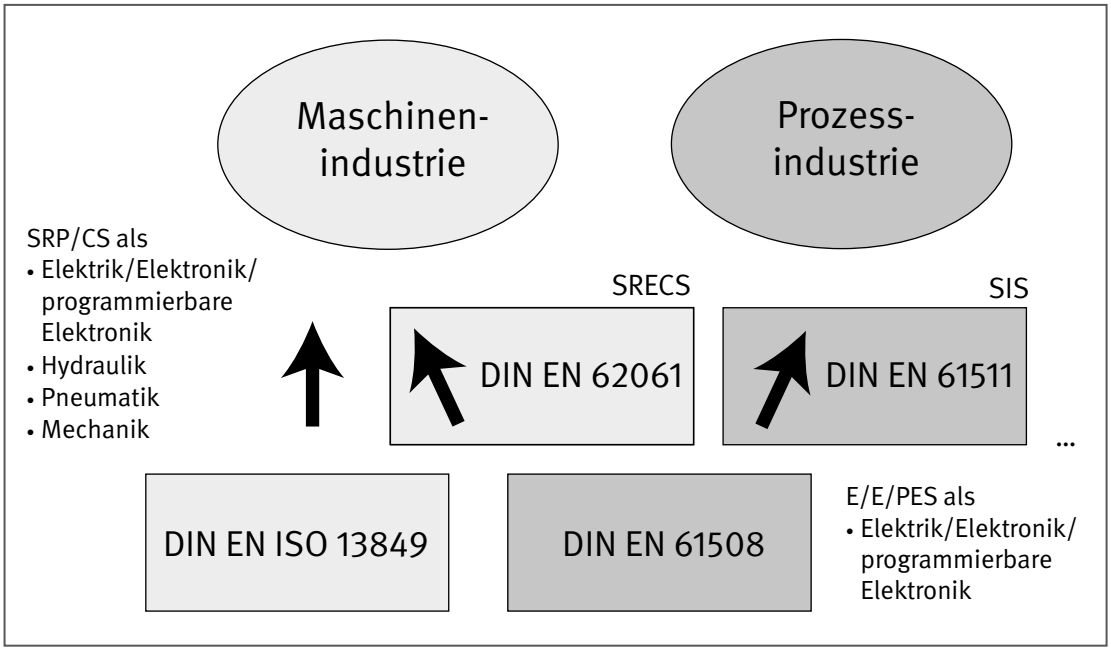


Abbildung 3.1: Anwendungsbereiche verschiedener Basisnormen zur funktionalen Sicherheit; SRP/CS: sicherheitsbezogene Teile einer Steuerung; SRECS: sicherheitsbezogenes elektrisches Steuerungssystem; SIS: sicherheitstechnisches System; E/E/PE-System: elektrisch/elektronisch/programmierbar elektronisches System

1 Funktionale Sicherheit bedeutet in diesem Zusammenhang, dass mögliche Gefährdungen behandelt werden, die durch Ausfälle eines Steuerungssystems bedingt sind, also von einer Fehlfunktion herrühren.

2 Daneben gibt es sogenannte deterministische Anforderungen, die im jeweiligen Level erfüllt werden müssen.

3 In der 2. Ausgabe der IEC 61508:2010 – nicht aber in ihrer Sektornorm IEC 62061 – wurde die verbale Umschreibung der PFH geändert in „Average frequency of a dangerous failure of the safety function“. Die ursprüngliche Abkürzung „PFH“ (in IEC 61508 ohne Index „D“) wurde jedoch beibehalten.

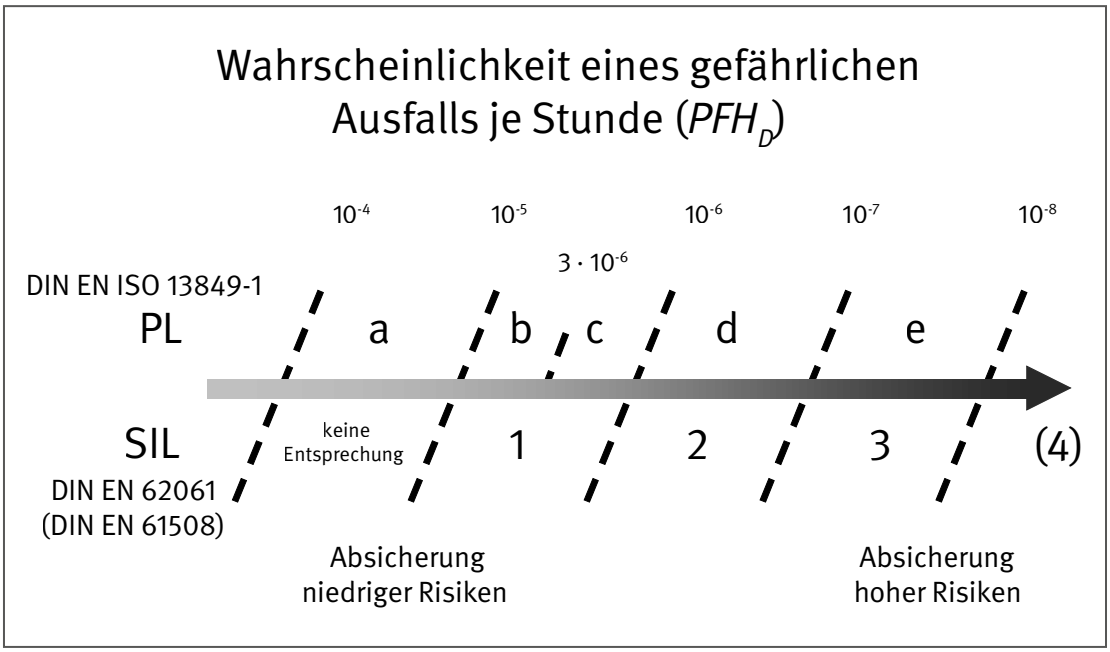


Abbildung 3.2: Performance Level (PL) und Sicherheits-Integritätslevel (SIL) als Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde

universeller. Der Ansatz der DIN EN ISO 13849-1 bietet Anwenderinnen und Anwendern jedoch die Möglichkeit, Sicherheitsfunktionen von einem Sensor bis hin zu einem Aktor (z. B. Ventil), auch wenn sie verschiedene Technologien umfassen, unter dem Dach einer Norm zu entwickeln und zu bewerten. Neben Teil 1 der DIN EN ISO 13849 existiert auch ein Teil 2 mit dem Titel „Validierung", der mit der vorliegenden Ausgabe aus dem Jahr 2013 auch die aktuellen Themen von Teil 1 berücksichtigt. Die Anhänge A bis D des Teils 2 enthalten umfangreiches Material zu den Themen „Grundlegende Sicherheitsprinzipien", „Bewährte Sicherheitsprinzipien", „Bewährte Bauteile" und „Fehlerlisten". Details hierzu sind im Anhang C dieses Reports dargestellt.

Die augenscheinliche Überlappung des Regelungsanspruchs beider Normenwelten kann für Steuerungshersteller und andere Normennutzende auf den ersten Blick nur unbefriedigend sein. Sowohl DIN EN ISO 13849-1 als auch DIN EN 62061 sind unter der Maschinenrichtlinie harmonisierte Normen. Die Teile 1 bis 4 der DIN EN 61508 haben zwar unter IEC-Aspekten den Status von Sicherheits-Grundnormen (Ausnahme: einfache Systeme), jedoch kann diese Normenreihe – auch als europäische Norm – nicht unter der Maschinenrichtlinie harmonisiert werden. In dieser Situation drängen sich zum Beispiel folgende Fragen auf:

- Welche Norm(en) sollte(n) zur Erfüllung der Maschinenrichtlinie angewendet werden?
- Liefern die Normen, soweit sich die Anwendungsbereiche überschneiden, gleichwertige Ergebnisse?
- Sind die Klassifizierungsschemata der Normen wie Kategorien, Performance Level (PL) und Sicherheits-Integritätslevel (SIL) kompatibel?
- Können Geräte, die unter Berücksichtigung einer der beiden Normen entwickelt wurden, im Rahmen der Realisierung einer Sicherheitsfunktion nach einer anderen Norm eingesetzt werden?

Um eine maximale Kompatibilität zur IEC-Welt zu erreichen sowie möglicherweise auf langfristige Sicht eine Zusammenlegung beider Normenwelten zu ermöglichen und außerdem die Vorteile des Wahrscheinlichkeitsansatzes zu nutzen, ohne die bewährten Kategorien über Bord zu werfen, hat DIN EN ISO 13849-1 als Nachfolgenorm der DIN EN 954-1 den Balanceakt gewagt, sowohl den deterministischen Ansatz der Kategorien als auch den Aspekt der sicherheitstechnischen Zuverlässigkeit mit der Definition des Performance Level (PL) zu vereinen (siehe auch [13]). Zahlenmäßig gibt es dabei korrespondierende Klassen (siehe Abbildung 3.2), die im praktischen Alltag schnell erste Abschätzungen erlauben.

Die vorgesehenen Architekturen im Sinne der Norm sind eher ein Angebot (vereinfachter Ansatz) als eine Verpflichtung. Sie sind jedoch als zentrales Element der Vereinfachung des in DIN EN ISO 13849 implementierten probabilistischen Ansatzes zu verstehen und ihre Anwendung ist einer der Hauptaspekte dieses Reports. In Bezug auf DIN EN 62061 legt der Anwendungsbereich der Norm nahe, dass auch komplexe, z. B. programmierbare Elektronik behandelt wird. Dies ist zwar korrekt, jedoch muss die Entwicklung von sogenannten SRECS (siehe Abbildung 3.1) dieser Technologie gemäß den Anforderungen der Norm nach DIN EN 61508 erfolgen. Die Möglichkeit der Verwendung von SRP/CS, die nach den von IEC stammenden Normen entwickelt wurden, betont DIN EN ISO 13849-1 mit ihrer neuen Ausgabe 1. Das heißt, solche SRP/CS können gleichwertig bei der Realisierung von Sicherheitsfunktionen unter DIN EN ISO 13849-1 eingesetzt werden.

Entscheidende Argumente für die Wahl von DIN EN ISO 13849 als Basis zur Realisierung funktionaler Sicherheit im Maschinenbereich können aus Sicht der Anwendung in der Praxis der technologieübergreifende Ansatz und der vereinfachte Quantifizierungsansatz unter Verwendung der vorgesehenen Architekturen sein. Dies schließt die detaillierte Betrachtung von nichtelektrischen und elektromechanischen Bauteilen ein. Natürlich werden insbesondere Firmen, die Sicherheitskomponenten, z. B.

eine speicherprogrammierbare Steuerung (SPS) für Sicherheitsanwendungen, in großer Zahl herstellen, weltweit auch andere Märkte als den Maschinenbereich bedienen wollen und daher neben DIN EN ISO 13849 auch DIN EN 61508 als Basis einer Entwicklung heranziehen.

Die früher in DIN EN ISO 13849-1 und DIN EN 62061 in den Einleitungen vorhandene gleichlautende Tabelle zur Auswahl der passenden Norm für den jeweiligen Anwendungsfall wurde inzwischen aus beiden Normen entfernt. Zu dem Thema existiert heute – wenig beachtet – ein Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen. DIN EN 62061 beschreibt als Sektornorm der DIN EN 61508 natürlich den Aspekt des „Managements der funktionalen Sicherheit“ sehr explizit. Entwicklung und Verifikation von Embedded-Software nach DIN EN ISO 13849-1 basieren auf heute gängigen und auch in DIN EN 61508 beschriebenen wesentlichen Anforderungen für sicherheitsrelevante Software. Weitgehende Einigkeit besteht aber darin, dass keine Mischung der Anforderungen aus beiden Normen vorgenommen werden soll. Der Leitfaden DIN ISO/TR 23849 [14] wurde von Mitgliedern beider Normenkreise erarbeitet und von ISO und IEC 2010 veröffentlicht. Seine Kernbotschaften lauten:

- Die Methoden der beiden Normen sind unterschiedlich, können aber eine vergleichbare Risikominderung erreichen,
- Aktivitäten, beide Normen zusammenzuführen, bedingen eine ausreichende Erfahrung mit der praktischen Anwendung.

Vonseiten der IEC wurde aber bereits 2011 der Vorschlag für eine Zusammenlegung beider Normen (auch als „Merging“ bezeichnet) zu einer ISO/IEC-Norm gemacht und 2012 mit dieser Arbeit begonnen. Das Ergebnis eines internationalen Fragebogens im Rahmen der Arbeiten zu ISO/IEC 17305 zeigt für die Bereiche Maschinenherstellung und Endanwendung eine klare Dominanz in der Anwendung der 13849-Normen. Abbildung 3.3 zeigt, dass ISO 13849-1 demnach mit ca. 90 % Verwendung bei einer großen Mehrheit der 715 Befragten zur Anwendung kommt. Unter Fachleuten wurde die Erstellung der geplanten ISO/IEC 17305 heftig diskutiert. Die langwierigen Diskussionen hatten dazu geführt, dass das Projekt gegenüber seinem ursprünglichen Zeitplan schon mindestens zwei Jahre zurücklag. Die Arbeitsgruppe war sich bewusst, dass sie zwingend die Abwärtskompatibilität zu den beiden Normen DIN EN ISO 13849-1 und DIN EN 62061 berücksichtigen musste. Erklärte Ziele waren eine einfache Anwendung der neuen Norm und Beibehaltung bisheriger Methoden. Die Frage, ob eine neue Norm diesen Zielen gerecht geworden wäre und ob sie die bestehenden Normen hätte ablösen können, kann nicht beantwortet werden. Auf Beschluss von ISO/TC 199 im Oktober 2015 wurden die Arbeiten an einer gemeinsamen Norm eingestellt und die Arbeitsgruppe in den Ruhemodus versetzt. Schon kurz nach der offiziellen Einstellung der Arbeiten lässt sich jedoch erkennen, dass das Thema an sich nicht ruht. Es sollen Empfehlungen dafür erarbeitet werden, ob und wenn ja wie ein zukünftiges Gemeinschaftsprojekt beider Normungsorganisationen zur funktionalen Sicherheit angegangen werden könnte. Beide Normen gehen im Rahmen ihrer „Maintenance“ zeitnah in die Überarbeitung. Ergebnisse der bisherigen Arbeiten zur ISO/IEC 17305 wird man in beiden Normen aufgreifen.

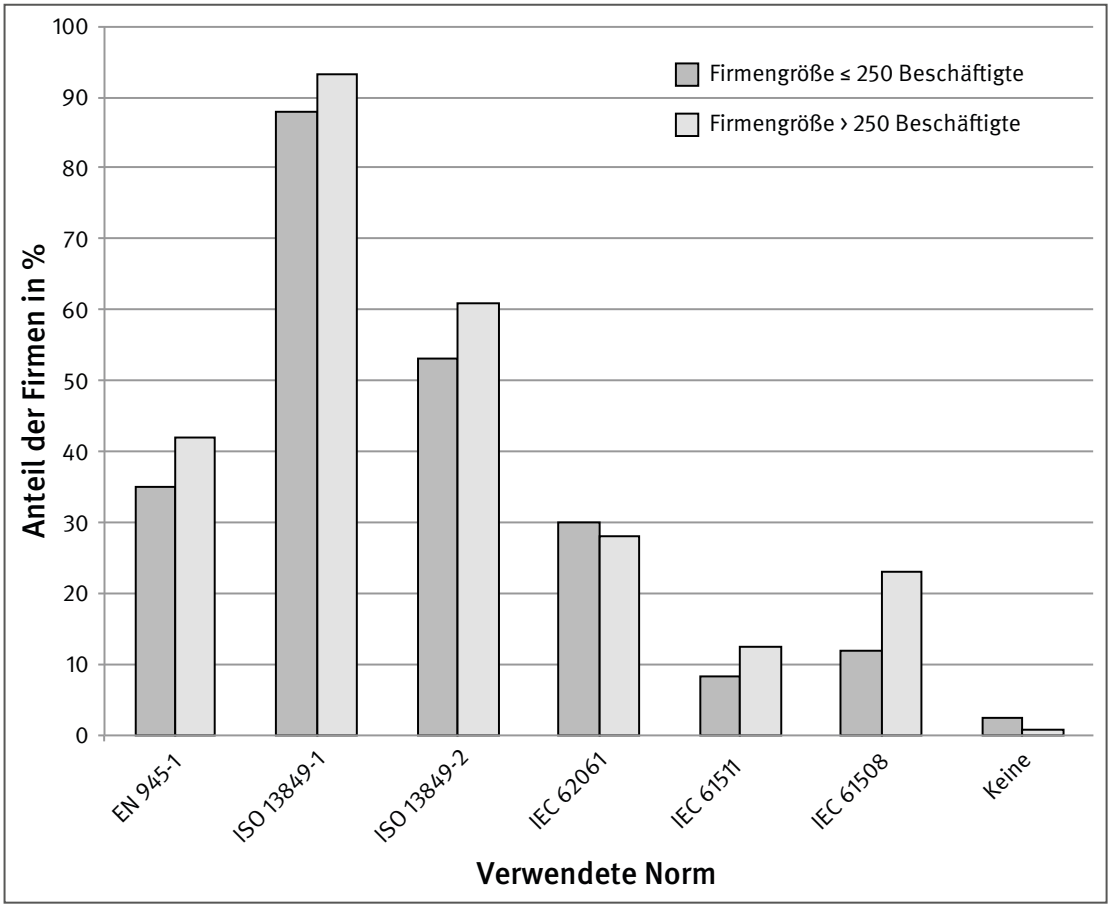


Abbildung 3.3: Vom Maschinenbau und in der Endanwendung verwendete Normen gemäß einer Umfrage von ISO und IEC aus den Jahren 2012/13 zum „Merging“ von ISO 13849-1 und IEC 62061

4 Report und Norm im Überblick

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Verweise aktualisiert
- Neuer Abschnitt 4.4 zu Änderungen durch die dritte Ausgabe der Norm 2016
- Abschnitt 4.5 (vorher 4.4) zur künftigen Entwicklung der Norm aktualisiert

Dieses Kapitel stellt die Querbezüge zwischen der Norm und den weiteren Kapiteln und Anhängen dieses Reports her. Gleichzeitig gibt es einen Überblick über den iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen und orientiert sich dabei an Abbildung 4.1, die Bild 3 der Norm entspricht. Am Ende des Kapitels werden die Änderungen von der zweiten zur dritten Ausgabe der Norm und ihre zukünftige Entwicklung angesprochen.

4.1 Identifikation von Sicherheitsfunktionen und ihren Eigenschaften

Als bewährtes Konzept steht die Definition einer oder mehrerer Sicherheitsfunktion(en) (SF) am Anfang des Gestaltungs- und Bewertungsprozesses. Dieses Vorgehen ist in Abbildung 4.1 durch die Blöcke 1 bis 3 dargestellt und wird im Kapitel 5 ausführlicher beschrieben. Die Frage lautet: Wie sieht der Beitrag der sicherheitsbezogenen Teile der Steuerung zur Reduzierung des Risikos einer Gefährdung an einer Maschine aus?

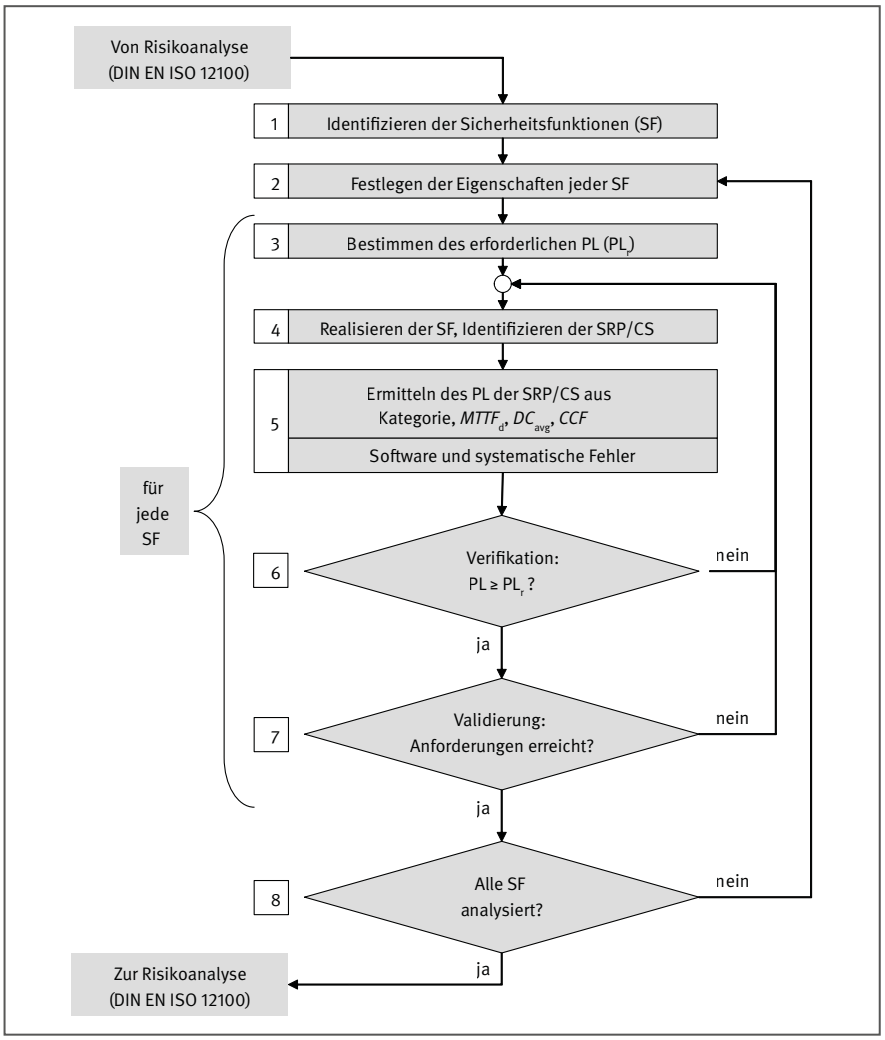


Abbildung 4.1:
Iterativer Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen:
SF = Sicherheitsfunktion;
PL = Performance Level;
PL_r = erforderlicher Performance Level;
SRP/CS = Safety-Related Part of a Control Systems (sicherheitsbezogenes Teil einer Steuerung);
$MTTF_D$ = Mean Time to Dangerous Failure (Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall);
DC_{avg} = average Diagnostic Coverage (mittlerer Diagnosedeckungsgrad);
CCF = Common Cause Failure (Ausfälle infolge gemeinsamer Ursache)

Eine Maschine soll zunächst derart konstruiert und gebaut sein, dass bei ihrer Nutzung keine Gefährdung mehr auftreten kann (inhärente Sicherheit). Zweiter Schritt ist anschließend, das Risiko für jede noch auftretende Gefährdung zu reduzieren. Dies kann man durch Schutzmaßnahmen erreichen, die oft aus der Kombination von Schutzeinrichtung und sicherer Steuerung bestehen. Damit diese Schutzmaßnahmen abhängig vom Risiko eine bestimmte Qualität erreichen, ist die Risikobeurteilung – von der Maschinenrichtlinie gefordert und beschrieben in DIN EN ISO 12100 – ein wesentlicher Schritt. Schutzeinrichtungen werden im Sinne der DIN EN ISO 13849-1 zusammen mit der sicheren Steuerung als sicherheitsbezogene Teile eines Steuerungssystems angesehen. Sie führen gemeinsam eine Sicherheitsfunktion aus; zum Beispiel können sie den unerwarteten Anlauf verhindern, wenn eine Bedienperson einen Gefahrenbereich betritt. Da es an einer Maschine durchaus mehrere Sicherheitsfunktionen geben kann (z. B. für Automatik- und Einrichtbetrieb), ist eine sorgfältige Betrachtung jeder einzelnen Gefährdung in jeder Betriebsart und der mit ihr verbundenen Sicherheitsfunktion sehr wichtig.

Die Sicherheitsfunktion kann von Teilen der Maschinensteuerung oder von zusätzlich notwendigen Komponenten übernommen werden. Beides sind in diesem Fall sicherheitsbezogene Teile von Steuerungen. Auch wenn durchaus dieselbe Hardware an verschiedenen Sicherheitsfunktionen beteiligt sein kann, kann die erforderliche Qualität der Risikoreduzierung für jede SF unterschiedlich sein. In der Norm wird die Qualität der Risikoreduzierung durch den Begriff „Performance Level“ (PL) definiert. Je nach Ergebnis der Risikobeurteilung wird für die Sicherheitsfunktionen ein mehr oder weniger hoher Wert für den PL gefordert. Diese Vorgabe für den Entwurf der Steuerung nennt man „erforderlicher Performance Level“ PL_r (der Index r steht für required). Wie kommt man nun zu diesem PL_r?

Das Risiko einer Gefährdung an einer Maschine kann außer durch die Steuerung z. B. auch durch trennende Schutzeinrichtungen, z. B. eine Schutztür, oder Persönliche Schutzausrüstung, z. B. eine Schutzbrille, verringert werden. Hat man einmal festgelegt, was die steuerungstechnischen Schutzmaßnahmen anteilig leisten müssen, dann hilft ein einfacher Entscheidungsbaum, der „Risikograph“, 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, die verheilen können)? Hält sich die Bedienperson häufig und lange im Gefahrenbereich auf (z. B. öfter als einmal pro 15 Minuten) oder selten und kurz? Hat sie eine Möglichkeit, den Unfall noch zu vermeiden (z. B. wegen langsamer Maschinenbewegung)? Diese drei Fragen entscheiden über den PL_r. Details findet man in Abschnitt 5.4, Beispiele im Anhang A.

4.2 Gestaltung und technische Realisierung der Sicherheitsfunktionen

Stehen die Anforderungen an die sicherheitsbezogenen Teile von Steuerungen fest, folgen zunächst der Entwurf und danach dessen Realisierung. Abschließend wird überprüft, ob durch die geplante Realisierung (Blöcke 4 und 5 in Abbildung 4.1) mit dem Istwert PL die erforderliche Risikominderung, der Sollwert PL_r, erreicht werden kann (Block 6 in Abbildung 4.1). Die Schritte der Blöcke 4 und 5 sind im Kapitel 6 ausführlich beschrieben. In der Tradition der bisherigen Steuerungs-Reports enthält auch dieser Report im Kapitel 8 viele ausgestaltete Schaltungsbeispiele für alle Steuerungstechnologien und jede Kategorie. Ein ausführlich beschriebenes Schaltungsbeispiel „Planschneidemaschine“ begleitet zusätzlich die allgemeinen Ausführungen in den Kapiteln 5, 6 und 7. Dadurch werden die nachfolgend beschriebenen Methoden und Parameter für die Entwicklung anschaulich vermittelt.

Sicherheitsbezogene Teile von Steuerungen können ihre risikomindernde Wirkung nur entfalten, wenn am Anfang die Sicherheitsfunktion korrekt definiert wurde. Bei der folgenden Realisierung fließen als Qualitätskriterien die Güte der verwendeten Bauteile (Lebensdauer), ihr Zusammenspiel (Dimensionierung), die Wirksamkeit der Diagnose (z. B. Selbsttests) und die Fehlertoleranz (Fehlersicherheit) der Struktur ein. Aus diesen Parametern bestimmt sich die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) und somit der erreichte PL. DIN EN ISO 13849-1 lässt die zu verwendenden Berechnungsmethoden offen. So darf man durchaus die hoch komplexe Markov-Modellierung unter Berücksichtigung der oben genannten Parameter nutzen. Die Norm beschreibt jedoch ein sehr vereinfachtes Vorgehen, nämlich die Verwendung von vorgesehenen Architekturen mit Anwendung eines Säulendiagramms (siehe Abbildung 6.10 auf Seite 61), in dem die Modellierung des PL schon vorweggenommen ist. Für Fachleute: Die Herleitung des Säulendiagramms findet sich in Anhang G.

Die Kategorien bleiben nach wie vor das Fundament bei der Bestimmung des PL. An ihrer Definition hat sich seit der ersten Ausgabe der Norm im Wesentlichen nichts geändert, allerdings werden seit der zweiten Ausgabe zusätzliche Anforderungen an die Bauteilgüte und an die Wirksamkeit der Diagnose gestellt. Ergänzend werden für die Kategorien 2, 3 und 4 ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache gefordert (siehe Tabelle 4.1).

Einen Überblick über die Kategorien liefert Tabelle 6.2 (Seite 51). Ein wesentlicher Aspekt bei der Verwendung der vorgeschlagenen einfachen Rechenmethoden ist die Darstellung der Kategorien als logische Blockschaltbilder, den sogenannten vorgesehenen Architekturen (Designated Architectures).

Da die Kategorien Fehlerbetrachtungen (Fehlervermeidung und -beherrschung) erfordern, kommen zusätzliche Aspekte hinzu, welche die Zuverlässigkeit der Einzelkomponenten, das Verhalten im Fehlerfall und die Fehlererkennung durch automatische Diagnosemaßnahmen betreffen. Die Grundlage hierzu liefern Fehlerlisten und Sicherheitsprinzipien (siehe Anhang C). Neben der „klassischen“ Failure Mode and Effects Analysis (FMEA, Ausfalleffektanalyse) bietet DIN EN ISO 13849-1 vereinfachte Rechenmethoden wie z. B. das „Parts Count“-Verfahren. Eine detaillierte Beschreibung dieser Thematik findet sich in Anhang B.

Eine der meistgestellten Fragen zur Ausfallwahrscheinlichkeit betrifft die Beschaffung zuverlässiger Ausfalldaten, der $MTTF_D$-Werte (*$MTTF_D$*: Mean Time to Dangerous Failure), für die sicherheitsbezogenen Komponenten. Hier ist der Bauteile- oder Komponentenhersteller mit seinem technischen Daten-

Tabelle 4.1:
Qualitative und quantifizierbare Aspekte der Kategorien; Ergänzungen zu den quantifizierbaren Aspekten nach der zweiten Ausgabe der Norm sind grau hinterlegt

Merkmal	Kategorie				
	B	1	2	3	4
Gestaltung gemäß zutreffender Normen, zu erwartenden Einflüssen standhalten	X	X	X	X	X
Grundlegende Sicherheitsprinzipien	X	X	X	X	X
Bewährte Sicherheitsprinzipien		X	X	X	X
Bewährte Bauteile		X			
Mean Time to Dangerous Failure – $MTTF_D$	niedrig bis mittel	hoch	niedrig bis hoch	niedrig bis hoch	hoch
Fehlererkennung (Tests)			X	X	X
Einfehlersicherheit				X	X
Berücksichtigung von Fehlerakkumulation					X
Mittlerer Diagnosedeckungsgrad – DC_{avg}	kein	kein	niedrig bis mittel	niedrig bis mittel	hoch
Maßnahmen gegen CCF			X	X	X
Hauptsächlich charakterisiert durch	Bauteilauswahl		Struktur		

blatt allen anderen Quellen vorzuziehen. Viele Komponentenhersteller stellen solche Daten bereits zur Verfügung. Aber auch wenn es keine Herstellerangabe gibt, lassen sich typische Beispielwerte aus etablierten Datensammlungen (z. B. SN 29500 oder IEC/TR 62380) ermitteln. Die Norm und Anhang D dieses Reports listen ebenfalls einige realistische Werte aus der Praxis auf und geben Hinweise zur Modellierung im sicherheitsbezogenen Blockdiagramm.

Die Wirksamkeit der Diagnose, als Wert des mittleren Diagnosedeckungsgrades DC_{avg} (average Diagnostic Coverage), ermittelt sich nach folgendem einfachem Prinzip: Für jeden Block werden die Testmaßnahmen zusammengestellt, die den Block überwachen. Für jede dieser Testmaßnahmen wird einer von vier typischen DC-Werten aus einer Tabelle in der Norm ermittelt. Eine nur scheinbar komplexe, aber im Kern einfache Mittelungsformel hilft, daraus die Kenngröße DC_{avg} zu berechnen. Weitere Informationen liefern Abschnitt 6.2.14 sowie Anhang E.

Ähnlich einfach wird es schließlich bei der letzten Kenngröße CCF (Common Cause Failure) (Abschnitt 6.2.15): Hier wird unterstellt, dass eine Ursache, z. B. Verschmutzung, Übertemperatur oder Kurzschluss, unter Umständen mehrere Folgefehler verursachen kann, die z. B. beide Steuerungskanäle gleichzeitig außer Kraft setzen können. Zur Beherrschung dieser Gefahrenquelle muss für Systeme der Kategorien 2, 3 und 4 nachgewiesen werden, dass ausreichende Maßnahmen gegen CCF getroffen wurden. Dies geschieht anhand eines Punktesystems für acht typische, meist technische Gegenmaßnahmen, mit denen mindestens 65 von 100 möglichen Punkten erreicht werden müssen (Details im Anhang F).

Neben den zufälligen Hardware-Ausfällen, die durch gute Struktur und geringe Ausfallwahrscheinlichkeit beherrscht werden können, gibt es das weite Feld der sogenannten systematischen Fehler – dem System bereits seit der Konstruktion innewohnenden Fehler wie z. B. Dimensionierungsfehler, Softwarefehler oder logische Fehler –, vor denen Maßnahmen zur Fehlervermeidung und -beherrschung schützen sollen. Hier nehmen die Softwarefehler einen großen Bereich ein. Die Anforderungen an die sicherheitsbezogene Software sind seit der zweiten Ausgabe in der Norm enthalten, aber im Einzelnen schon länger aus einschlägigen Normen bekannt. Die konkreten Maßnahmen sind je nach gefordertem PL abgestuft. Weitere Informationen geben Abschnitt 6.1.2 für systematische Ausfälle sowie Abschnitt 6.3 für Software.

4.3 Verifikation und Validierung der Steuerung für jede Sicherheitsfunktion

Ist das Design bis zur Ermittlung des realisierten PL fortgeschritten, stellt sich für jede durch die Steuerung ausgeführte Sicherheitsfunktion die Frage, ob dieser PL ausreicht. Dazu vergleicht man den PL mit dem geforderten PL_r (siehe Block 6, Abbildung 4.1). Ist der für eine Sicherheitsfunktion erreichte PL „schlechter“ als der geforderte 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 ausreichend gut ist. Ist diese Hürde genommen, so ist eine Reihe von Validierungsschritten notwendig, bei denen Teil 2 der DIN EN ISO 13849 ins Spiel kommt. Diese Validierung stellt systematisch sicher, dass alle funktionalen und leistungsbezogenen Anforderungen an die sicherheitsbezogenen Teile der Steuerung erreicht wurden (siehe Block 7, Abbildung 4.1). Weitere Details dazu finden sich im Kapitel 7.

4.4 Änderungen durch die dritte Ausgabe der Norm aus dem Jahr 2016

Durch ihre Änderung 1 wurde aus der zweiten die dritte Ausgabe der Norm. Die geänderten Passagen verbessern in erster Linie die Lesbarkeit und Anwendbarkeit. Einen detaillierten Überblick, konzentriert auf die Änderungen, hat das IFA bereits 2015 veröffentlicht [15]. Zu den wesentlichen Neuerungen 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) und ein Vorschlag zum Umgang mit Anforderungen an SRESW (Sicherheitsbezogene Embedded Software) bei Verwendung von Standardkomponenten.
Tabelle 4.2 zeigt, welche Hauptänderungen in welche Abschnitte der Norm und des vorliegenden Reports eingeflossen sind.

Die Schaltungsbeispiele in Kapitel 8 des Reports wurden auf der Basis der obigen Normänderungen gegenüber 2008 durchgängig aktualisiert.

Tabelle 4.2:
Wesentliche Änderungen in der dritten Ausgabe der Norm sowie die betroffenen Abschnitte der Norm und des vorliegenden Reports

Abschnitt der Norm	Änderung	Abschnitt des Reports
1 Einleitung	Ersatz der Tabelle 1 „Empfohlene Anwendung der IEC 62061 und ISO 13849-1“ durch einen Verweis auf DIN ISO/TR 23849	3 Basisnormen zur Funktionalen Sicherheit
2 Anwendungsbereich	Die Norm gilt für SRP/CS mit hoher Anforderungsrate oder kontinuierlicher Anforderung.	3 Basisnormen zur Funktionalen Sicherheit
3 Begriffe, Formelzeichen, Abkürzungen	Abkürzung PFH_D für die „durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde“	durchgängig
	$MTTF_D$, B_{10D}, T_{10D} und λ_D mit Index „D“ in Großbuchstaben	durchgängig
4 Gestaltungsaspekte (und Anhang K)	Aktualisierung der Verweise auf ISO 12100:2010	5 Sicherheitsfunktionen
	Kombination mit Subsystemen nach anderen Normen zur Funktionalen Sicherheit	6.4 Kombination von SRP/CS
	Anhebung der $MTTF_D$-Begrenzung für Kategorie 4 auf 2 500 Jahre	6.2.13 FMEA versus „Parts Count“-Verfahren
	Testhäufigkeit und $MTTF_D$ des Testkanals in Kategorie 2	6.2.5 Kategorie 2 und 6.2.14 Diagnosedeckungsgrad
	Alternative PFH_D-Bestimmung für den Ausgangsteil des SRP/CS nach Abschnitt 4.5.5 der Norm	6.2.17 PL-Bestimmung für den Ausgangsteil des SRP/CS
	Anforderungen an SRESW bei Verwendung von Standardkomponenten	6.3.10 Anforderungen an die Software von Standardkomponenten
5 Sicherheitsfunktionen	Berücksichtigung eines Energieausfalls mit möglicherweise separater Sicherheitsfunktion	5 Sicherheitsfunktionen
6.2 Kategorien	Warnung vor der Gefährdung als Alternative zur Einleitung eines sicheren Zustands in Kategorie 2 bis $PL_r = c$	6.2.5 Kategorie 2 und 6.2.14 Diagnosedeckungsgrad
6.3 Kombination	Kombination von SRP/CS: PFH_D-Addition als bevorzugtes Verfahren	6.4 Kombination von SRP/CS
Anhang A, Bestimmung des PL_r	Hervorhebung des informativen Charakters	5 Sicherheitsfunktionen, Anhang A, Beispiele
	Unterscheidung F1/F2	5.4.1 Risikograph
	Eintrittswahrscheinlichkeit eines Gefährdungsereignisses	5.4.1 Risikograph
	Überlagerte Gefährdungen	5.3.2 Beispiele, bei denen die Definition der Sicherheitsfunktion Einfluss auf die spätere Berechnung der PFH_D hat
Anhang C, $MTTF_D$	Änderungen einiger typischer Werte beim Verfahren guter ingenieurmäßiger Praxis	Anhang D, $MTTF_D$
Anhang E, DC	Zwei DC-Maßnahmen gelöscht „Fehlererkennung durch den Prozess“ näher erläutert	Anhang E, DC
Anhang I Beispiele	Aktualisierung	nicht relevant

4.5 Künftige Entwicklung von DIN EN ISO 13849-1

Die dritte Ausgabe der DIN EN ISO 13849-1 ersetzt die vorherige Ausgabe ohne eine besondere Übergangsfrist. Da die Änderungen – wie im vorherigen Abschnitt beschrieben – aber im Wesentlichen Ergänzungen, Aktualisierungen und Verbesserungen darstellen, ist der Übergang zwischen der zweiten und dritten Ausgabe der Norm meist unkritisch. Diesen Prozess unterstützt das IFA, wie schon seit Längerem gewohnt, durch frei verfügbare Anwendungshilfen. Dies erfolgt sowohl in Form erklärender und mit Beispielen versehener Literatur als auch durch das Freeware-Programm „SISTEMA“ (Sicherheit von Steuerungen an Maschinen), das die Berechnung und Dokumentation von PL_r und PL unterstützt (siehe Anhang H). Die fortlaufend ergänzte Reihe der SISTEMA-Kochbücher widmet sich speziellen Themen, die bei der Anwendung der Norm eine Rolle spielen: Diese betreffen nicht nur SISTEMA selbst (SISTEMA-Bibliotheken, Verwendung von Netzwerkbibliotheken, „Mehrere SISTEMA-Instanzen parallel ausführen“), sondern auch den gesamten Entwurfsprozess nach der Norm („Definition von Sicherheitsfunktionen“, „Vom Schaltbild zum Performance Level“, „Wenn die vorgesehenen Architekturen nicht passen“). Das Angebot wird abgerundet durch den vom IFA entworfenen „Performance Level Calculator“ [16], der das Säulendiagramm in Form einer Drehscheibe, mit der man PFH_D und PL jederzeit einfach und genau ermitteln kann, detailliert darstellt. Alle weiterführenden Hilfen und Literatur – darunter z. B. Hinweise auf die Prüfgrundlagen und Prüfgrundsätze [17] des DGUV Test, des Prüf- und Zertifizierungssystems der Deutschen Gesetzlichen Unfallversicherung – finden sich auf den Internetseiten des IFA unter der Adresse www.dguv.de/ifa/13849.

Bei den Arbeiten zur dritten Ausgabe der DIN EN ISO 13849-1 wurden einige größere Arbeitspakete identifiziert, die den Rahmen einer Änderung gesprengt hätten. Dazu gehört z. B. eine grundsätzliche Überarbeitung der Software-Anforderungen, um die praktische Anwendbarkeit zu verbessern, aber auch eine durchgängige Klarstellung, wann das „SRP/CS“ für die gesamte Steuerung, die eine Sicherheitsfunktion ausführt, steht und wann ein Subsystem, das nur einen Teil der Sicherheitsfunktion ausführt, gemeint ist. Um diese Vorschläge langfristig umsetzen zu können, hat das für die Norm zuständige Gremium beschlossen, im Anschluss an die Veröffentlichung der dritten Ausgabe schon 2016 mit einer Überarbeitung der Norm zu beginnen. Diese begleitet das IFA in bewährter Weise, um in einigen Jahren die zu erwartenden Ergebnisse (als vierte Ausgabe der Norm?) wieder wie oben beschrieben für die praktische Anwendung aufzubereiten.

5 Sicherheitsfunktionen und ihr Beitrag zur Risikominderung

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Normenreferenzen akualisiert
- „Überlagerte Gefährdungen“ wurden aufgenommen
- Hinweise zur Abgrenzung F1/F2 aktualisiert
- Berücksichtigung der „Wahrscheinlichkeit für den Eintritt eines Gefährdungsereignisses“ eingefügt
- Abschnitt 5.4.2 „Übergang von einer erforderlichen Kategorie nach DIN EN 954-1 zu einem PL_r“ gestrichen
- Beispiel Planschneidemaschine überarbeitet

Der vorliegende Report beschäftigt sich mit Sicherheitsfunktionen und ihrem Beitrag zur Risikominderung an Gefahrenstellen von Maschinen. Solche Sicherheitsfunktionen zu gestalten, ist Teil eines Prozesses zur Realisierung von sicheren Maschinen. Dieses Kapitel geht daher zunächst auf die Anforderungen der Maschinenrichtlinie ein, bevor die Festlegung von Sicherheitsfunktionen und ihrer Eigenschaften beschrieben wird. In Abschnitt 5.7 wird anschließend die Umsetzung am praktischen Beispiel einer Planschneidemaschinensteuerung gezeigt.

5.1 Anforderungen der EG-Maschinenrichtlinie

Die EG-Maschinenrichtlinie [2] ist in Deutschland im Rahmen des Produktsicherheitsgesetzes in nationales Recht umgesetzt und legt grundlegende Sicherheits- und Gesundheitsanforderungen für Maschinen fest. Der allgemeine Charakter der Maschinenrichtlinie wird durch Normen konkretisiert. Hierbei ist insbesondere die Norm DIN EN ISO 12100 [3] „Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze“ hervorzuheben. Für die Maschinenkonstruktion wird eine Methode vorgestellt, die für das Erreichen der Sicherheit von Maschinen geeignet ist. Diese Methode – Strategie zur Risikominderung – bezieht die Gestaltung der sicherheitsbezogenen Teile von Steuerungen[1] ein.

Sofern für die zu konstruierende Maschine eine harmonisierte produktspezifische Norm (Typ-C-Norm) vorliegt, die im Amtsblatt der EU veröffentlicht wurde [18], kann von einer Berücksichtigung der grundlegenden Sicherheits- und Gesundheitsanforderungen bereits ausgegangen werden. Man spricht in diesen Fällen von einer Norm mit Vermutungswirkung, denn bei Anwendung der Norm darf man die Übereinstimmung mit den Anforderungen der EG-Maschinenrichtlinie vermuten. Die Strategie zur Risikominderung ist aber immer dann anzuwenden, wenn keine Norm mit Vermutungswirkung existiert, wenn davon abgewichen wurde oder wenn zusätzliche Aspekte vorliegen, die von der Produktnorm nicht abgedeckt sind. Zur Feststellung der von einer Produktnorm nicht berücksichtigten Sachverhalte sind die ersten beiden Schritte der im Folgenden beschriebenen Strategie zur Risikominderung immer durchzuführen, also die Grenzen der Maschine festzulegen und die Gefährdungen zu identifizieren.

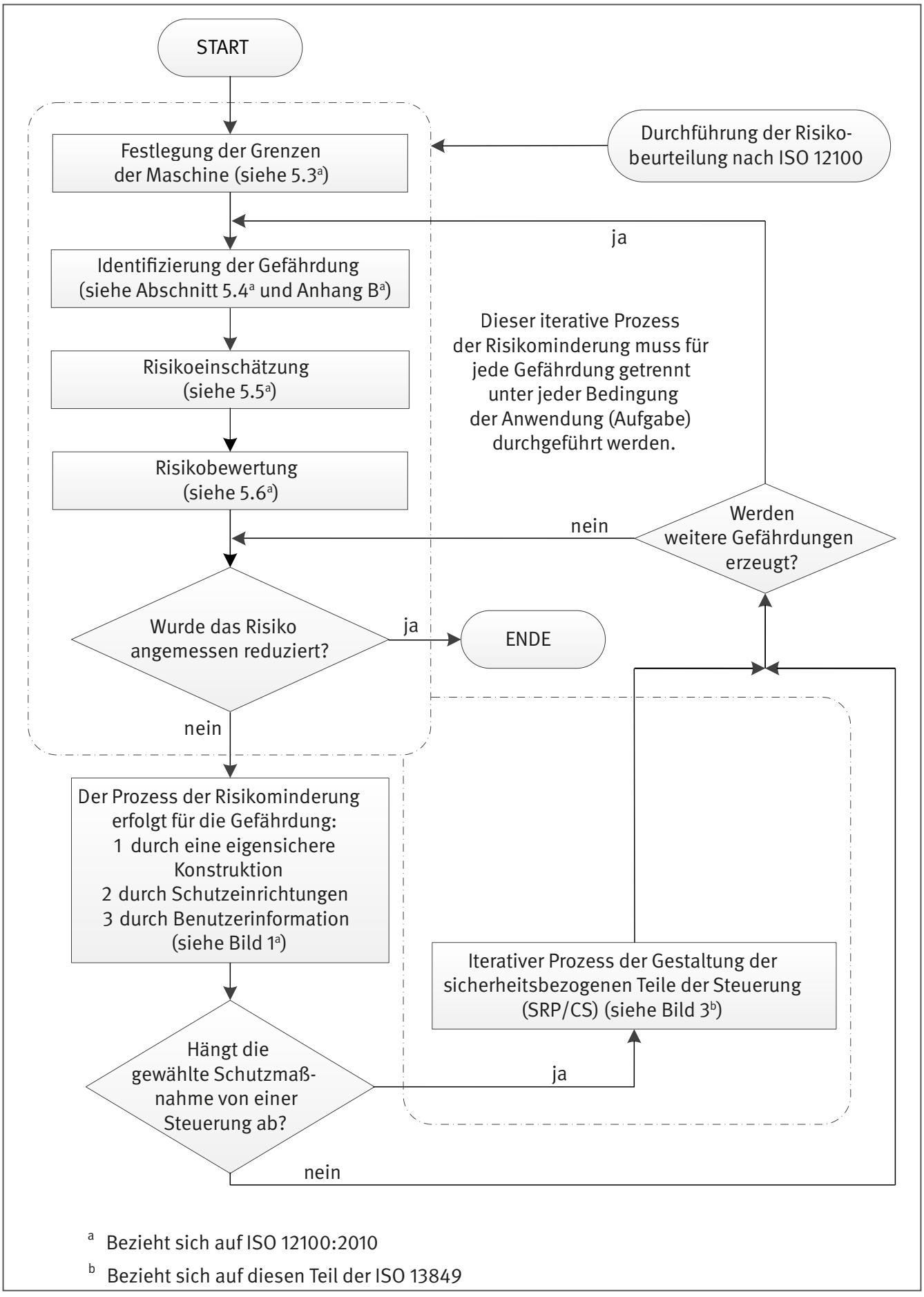
5.2 Strategie zur Risikominderung

Das in DIN EN ISO 12100 [3] vorgestellte Verfahren zur Risikominderung wurde in Bild 1 der DIN EN ISO 13849-1 übernommen und um die in dieser Norm konkretisierten Aspekte ergänzt (siehe Abbildung 5.1, siehe Seite 28). Als Erstes erfolgt eine Risikobeurteilung. Dabei ist es wichtig zu wissen, dass man bei den folgenden Schritten zunächst einmal von einer Maschine ausgeht, an der noch keine Schutzmaßnahmen getroffen wurden. Letztendlich dient der gesamte Prozess der Risikominderung dazu, die Art und auch die „Qualität“ der zu treffenden Schutzmaßnahme bzw. Schutzeinrichtung zu bestimmen.

Das Verfahren zur Risikominderung beginnt mit der Festlegung der Grenzen der Maschine. Neben den räumlichen Grenzen und der zeitlichen Nutzung einer Maschine sind insbesondere die Verwendungsgrenzen zu berücksichtigen. Dazu gehören die bestimmungsgemäße Verwendung (z. B. zulässige Materialien, die verarbeitet werden dürfen) der Maschine einschließlich aller Betriebsarten und der unterschiedlichen Eingriffsmöglichkeiten. Außerdem muss die vernünftigerweise vorhersehbare Fehlanwendung der Maschine berücksichtigt werden; damit wird u. a. die Manipulation von Schutzeinrichtungen berücksichtigt.

[1] Eine Sicherheitsfunktion wird u. a. mit sicherheitsbezogenen Teilen von Steuerungen realisiert. Diese beginnen mit der Erfassung sicherheitsbezogener Eingangssignale, z. B. mit der Detektion einer Schutztürstellung durch einen Positionsschalter der Bauart 2, bei dem der an der Tür befestigte getrennte Betätiger bereits ein sicherheitsbezogener Teil ist. Es schließt sich die Signalverarbeitung an, die ein Ausgangssignal erzeugt. Hier könnte es sich um ein Leistungsschütz handeln, das einen Motor mit dem Netz verbindet. Das Leistungsschütz ist ein sicherheitsbezogener Teil der Steuerung, während der Motor mit seiner Verkabelung in der Regel nicht mehr dazugehört.

Abbildung 5.1:
Iterativer Prozess zur Risikominderung



[a] Bezieht sich auf ISO 12100:2010

[b] Bezieht sich auf diesen Teil der ISO 13849

Anschließend folgt die Identifizierung der Gefährdungen, bei der sämtliche Phasen der Lebensdauer einer Maschine zu berücksichtigen sind, neben dem Automatikbetrieb insbesondere die Betriebsarten, die manuelle Eingriffe erfordern, z. B. für

- Einrichten,
- Prüfen,
- „Teachen“/Programmieren,
- Inbetriebnahme,
- Maschinenbeschickung,
- Produktentnahme,
- Fehlersuche und Fehlerbeseitigung,
- Reinigung,
- Instandhaltung.

Weitere Details zu diesem Prozessschritt sind zu finden in DIN EN ISO 12100 [3]. Für die systematische Identifizierung der Gefährdungen gibt es verschiedene Verfahren, Beispiele finden sich in DIN ISO/TR 14121-2 [4]. Darüber hinaus sind mögliche Gefährdungen ausführlich in DIN EN ISO 12100 [3] aufgelistet, einen Auszug zeigt Abbildung 5.2.

5.2.1 Risikoeinschätzung

Sind alle Gefährdungen ermittelt, die von einer Maschine ausgehen können, so muss für jede Gefährdung das Risiko eingeschätzt werden. Aus den folgenden Risikoelementen kann das mit einer bestimmten Gefährdungssituation zusammenhängende Risiko abgeleitet werden:

a) Schadensausmaß
b) Eintrittswahrscheinlichkeit dieses Schadens als Funktion
   - der Gefährdungsexposition einer Person/von Personen
   - des Eintritts eines Gefährdungsereignisses
   - der technischen und menschlichen Möglichkeiten zur Vermeidung oder Begrenzung des Schadens

Ziel des weiteren Vorgehens ist es, das Risiko auf ein akzeptables Maß zu reduzieren. Abbildung 5.3 (Seite 30) zeigt hierzu die Anteile der Risikoreduzierung mit und ohne sicherheitsrelevante Teile einer Steuerung. Weitere Informationen zum Thema Risiko enthält das IFA-Handbuch [19].

5.2.2 Risikobewertung

Im Anschluss an die Risikoeinschätzung wird eine Risikobewertung durchgeführt, um zu entscheiden, ob eine Risikominderung notwendig ist. Die Kriterien für eine hinreichende Risikominderung gibt DIN EN 12100 [3] vor:

- Wurden alle Betriebsbedingungen und alle Eingriffsmöglichkeiten berücksichtigt?
- Wurden die Gefährdungen durch angemessene Schutzmaßnahmen beseitigt oder die Risiken soweit vermindert, wie dies praktisch umsetzbar ist?
- Ist sichergestellt, dass die durchgeführten Maßnahmen nicht neue Gefährdungen schaffen?
- Sind die Benutzerinnen und Benutzer hinsichtlich der Restrisiken ausreichend informiert und gewarnt?
- Ist sichergestellt, dass die Arbeitsbedingungen der Bedienpersonen und die Benutzerfreundlichkeit der Maschine durch die ergriffenen Schutzmaßnahmen nicht konterkariert werden?
- Sind die durchgeführten Schutzmaßnahmen miteinander vereinbar?

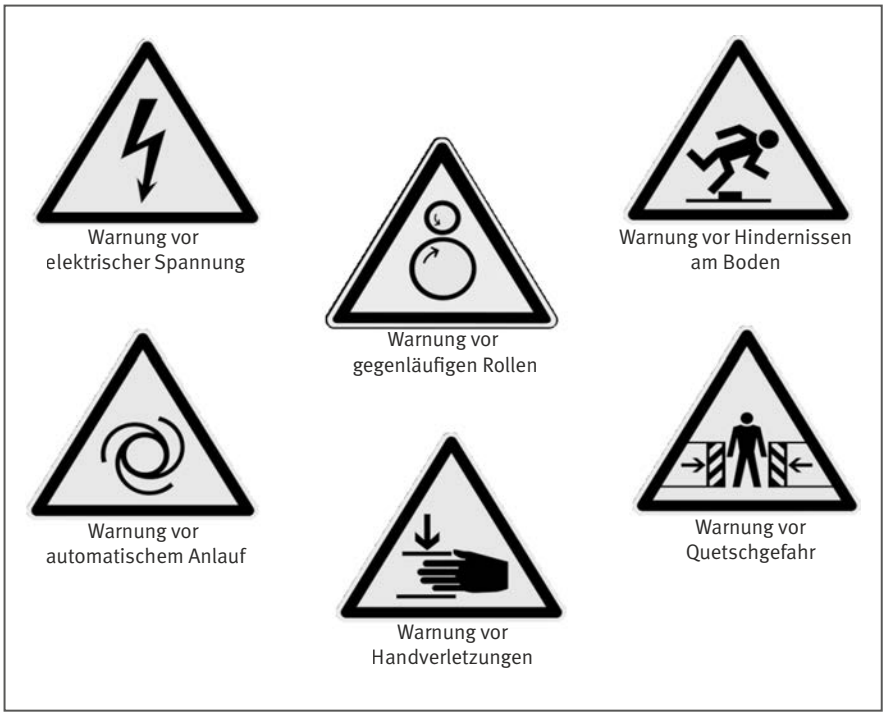


Abbildung 5.2:
Beispiele für Gefährdungen
(Quelle: DIN EN ISO 7010)

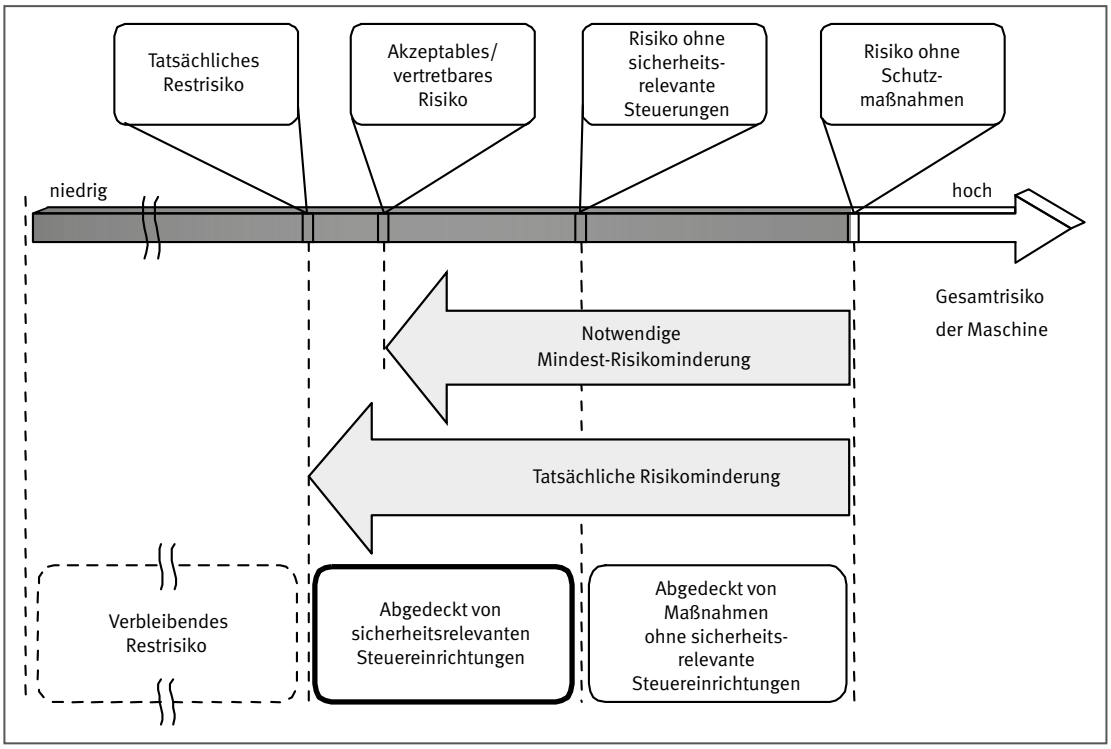


Abbildung 5.3:
Risikoeinschätzung und Risikominderung

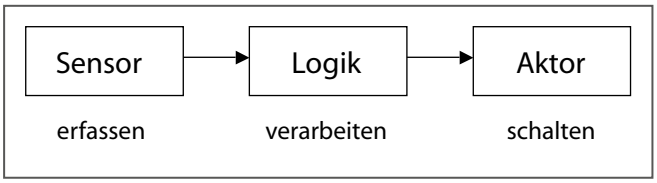
- Wurden die Folgen ausreichend berücksichtigt, die sich durch den Gebrauch einer für den gewerblichen/industriellen Einsatz konstruierten Maschine im nicht gewerblichen/nicht industriellen Bereich ergeben können?

5.3 Identifizierung der notwendigen Sicherheitsfunktionen und ihrer Eigenschaften

Kommt man zu der Bewertung, dass ein Risiko (noch) nicht akzeptabel ist, sind entsprechende Schutzeinrichtungen vorzusehen. Dem sind jedoch Bemühungen voranzustellen, die durch konstruktive Veränderungen der Maschine Gefährdungen vermeiden (inhärent sichere Konstruktion) oder zumindest weitestgehend reduzieren. Prinzipiell ist Risikominderung auch durch Benutzerinformation (einschließlich organisatorischer Maßnahmen) möglich. Letzteres ist jedoch nur in solchen Ausnahmefällen akzeptabel, bei denen durch technische Schutzmaßnahmen keine ökonomisch angemessene Risikoreduzierung möglich ist. In den meisten Fällen werden aber Schutzeinrichtungen erforderlich sein. In diesem Zusammenhang werden Sicherheitsfunktionen definiert, die von den SRP/CS (Safety Related Parts of Control Systems), den sicherheitsbezogenen Teilen von Steuerungen, ausgeführt werden (siehe Abbildung 5.4).

Für die Gestaltung der sicherheitsbezogenen Teile von Steuerungen ist nach [5] ein iterativer Prozess vorgesehen (siehe Abbildung 4.1). Abbildung 5.5 zeigt den für diesen Abschnitt des Reports relevanten Teil.

Abbildung 5.4:
Sicherheitsfunktionen werden von SRP/CS ausgeführt



5.3.1 Festlegung von Sicherheitsfunktionen

Die Festlegung der notwendigen Sicherheitsfunktionen hängt sowohl von der Anwendung als auch von der Gefährdung ab. Ist z. B. mit wegfliegenden Teilen zu rechnen, wird ein Lichtgitter ungeeignet sein und eine Fangvorrichtung (trennende Schutzeinrichtung) notwendig werden. Eine Sicherheitsfunktion ist also eine Funktion, die das Risiko, das bei einer bestimmten Gefährdung besteht, durch (auch steuerungstechnische) Maßnahmen auf ein akzeptables Maß mindert. Sofern nicht eine Typ-C-Norm hierzu Aussagen macht, werden die Sicherheitsfunktionen durch den Konstrukteur der Maschine festgelegt, z. B.:

a) gesteuertes Stillsetzen der Bewegung und Einfallen der Haltebremse im Stillstand
b) Verhindern einer Quetschstelle infolge der Absenkung von Maschinenteilen
c) Leistung des Schneidlasers bei direkter Exposition am Auge absenken
d) Absturz der Achse im Einrichtbetrieb verhindern
e) Ausweichen des Roboters bei Betreten seines Gefahrenbereiches
f) Einzug von Personen verhindern
g) Unterbrechung der durch Zwei-Hand-Bedienung gesteuerten Schließbewegung bei Eingriff einer zweiten Person in den Gefahrenbereich (Auslösung durch Lichtgitter)

Häufig verwendet man zusammengesetzte

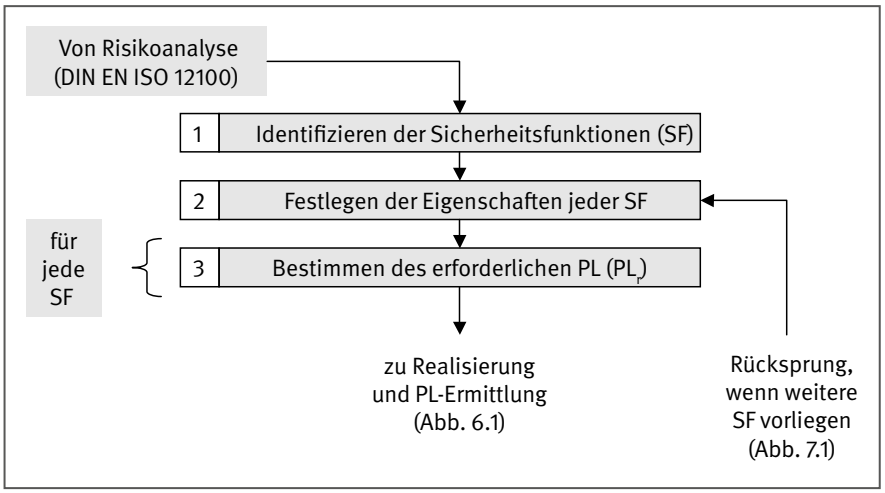


Abbildung 5.5:
Ausschnitt aus dem iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP/CS)

Sicherheitsfunktionen wie im Beispiel in Abschnitt 5.7. Durch die elektronische Ansteuerung wird die Bewegung zunächst bis zum Stillstand abgebremst und anschließend fällt eine mechanische Haltebremse ein. Hinweise zu möglichen Sicherheitsfunktionen geben die beiden folgenden Tabellen. In Tabelle 5.1 sind die Sicherheitsfunktionen nach Abschnitt 5.1 der DIN EN ISO 13849-1 zusammengefasst und um Beispiele für mögliche Anwendungen ergänzt. Hier ist auch die „Funktion zum Stillsetzen im Notfall" enthalten, die zwar kein Bestandteil einer Schutzeinrichtung ist, aber zur Realisierung einer ergänzenden Schutzmaßnahme verwendet wird (siehe Abschnitt 5.5). Tabelle 5.2 zeigt weitere Sicherheitsfunktionen für sichere Antriebssteuergeräte nach DIN EN 61800-5-2 – PDS(SR), Power Drive Systems(Safety Related)) [20]. Diese Norm enthält u. a. die häufig angewendeten Sicherheitsfunktionen zur Verhinderung eines unerwarteten Anlaufs STO (STO, Safe Torque Off), zum sicheren Stillsetzen SS1 und SS2 und zur sicheren Begrenzung einer Geschwindigkeit SLS (SLS, Safely-Limited Speed).

Für die pneumatische Antriebstechnik sind Sicherheitsfunktionen in dem VDMA-Einheitsblatt 24584 [21] beschrieben.

Tabelle 5.1:
Sicherheitsfunktionen aus DIN EN ISO 13849-1

Sicherheitsfunktion	Beispiel für mögliche Anwendung
Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung	Auslösen einer Schutzeinrichtung führt zu STO, SS1 oder SS2 (Tabelle 5.2)
Manuelle Rückstellfunktion	Quittierung beim Verlassen von hintertretbaren Bereichen
Start-/Wiederanlauffunktion	Nur zulässig bei steuernden trennenden Schutzeinrichtungen nach DIN EN ISO 12100
Lokale Steuerungsfunktion	Steuern von Maschinenbewegungen von einem Standort innerhalb des Gefahrenbereichs
Mutingfunktion	Zeitweises Unwirksammachen von Schutzeinrichtungen, z. B. beim Materialtransport
Einrichtung mit selbsttätiger Rückstellung (Tippschalter)	Maschinenbewegungen gesteuert von einem Standort innerhalb des Gefahrenbereichs, z. B. beim Einrichten
Zustimmfunktion	Maschinenbewegungen gesteuert von einem Standort innerhalb des Gefahrenbereichs, z. B. beim Einrichten
Verhinderung des unerwarteten Anlaufs	Manueller Eingriff in Gefahrenbereiche
Befreiung und Rettung eingeschlossener Personen	Auseinanderfahren von Walzen
Isolations- und Energieableitungsfunktion	Öffnung eines Hydraulikventils zum Druckabbau
Steuerungsfunktionen und Betriebsartenwahl	Aktivierung von Sicherheitsfunktionen durch Betriebsartenwahlschalter
Funktion zum Stillsetzen im Notfall	Reaktion auf die Betätigung eines Not-Halt-Geräts durch STO oder SS1 (Tabelle 5.2)

Tabelle 5.2:
Sicherheitsfunktionen aus DIN EN 61800-5-2; (Ausgabe 2017) [20]

Abkürzung	Bezeichnung englisch	Bezeichnung deutsch	Funktion
STO	Safe torque off	Sicher abgeschaltetes Moment	Motor erhält keine Energie, die eine Drehbewegung erzeugen kann; Stopp-Kategorie 0 nach DIN EN 60204-1
SS1-r SS1-t	Safe Stop 1	Sicherer Stopp 1	Motor verzögert; Überwachung Bremsrampe und STO nach Stillstand (SS1-r) oder STO nach Ablauf einer Verzögerungszeit (SS1-t); Stopp-Kategorie 1 nach DIN EN 60204-1
SS2-r SS2-t	Safe Stop 2	Sicherer Stopp 2	Motor verzögert; Überwachung Bremsrampe und SOS nach Stillstand (SS2-r) oder SOS nach Ablauf einer Verzögerungszeit (SS2-t); Stopp-Kategorie 2 nach DIN EN 60204-1
SOS	Safe Operating Stop	Sicherer Betriebshalt	Motor steht still und widersteht externen Kräften.
SLA	Safely-Limited Acceleration	Sicher begrenzte Beschleunigung	Das Überschreiten eines Beschleunigungsgrenzwerts wird verhindert.
SLS	Safely-Limited Speed	Sicher begrenzte Geschwindigkeit	Das Überschreiten eines Geschwindigkeitsgrenzwerts wird verhindert.
SLT	Safely-Limited Torque	Sicher begrenztes Moment	Das Überschreiten eines Drehmoment-/Kraftgrenzwerts wird verhindert.
SLP	Safely-Limited Position	Sicher begrenzte Position	Das Überschreiten eines Positionsgrenzwerts wird verhindert.
SLI	Safely-Limited Increment	Sicher begrenztes Schrittmaß	Der Motor wird um ein spezifiziertes Schrittmaß verfahren und stoppt anschließend.
SDI	Safe Direction	Sichere Bewegungsrichtung	Die nicht beabsichtigte Bewegungsrichtung des Motors wird verhindert.
SMT	Safe Motor Temperature	Sichere Motortemperatur	Das Überschreiten eines Motortemperaturgrenzwerts wird verhindert.
SBC	Safe Brake Control	Sichere Bremsenansteuerung	Sichere Ansteuerung einer externen Bremse
SCA	Safe Cam	Sicherer Nocken	Während sich die Motorposition in einem spezifizierten Bereich befindet, wird ein sicheres Ausgangssignal erzeugt.
SSM	Safe Speed Monitor	Sichere Geschwindigkeitsüberwachung	Während die Motordrehzahl niedriger als ein spezifizierter Wert ist, wird ein sicheres Ausgangssignal erzeugt.
SAR	Safe Acceleration Range	Sicherer Beschleunigungsbereich	Die Beschleunigung des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
SSR	Safe Speed Range	Sicherer Geschwindigkeitsbereich	Die Geschwindigkeit des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
STR	Safe Torque Range	Sicherer Momentenbereich	Das Drehmoment des Motors (die Kraft bei Linearmotoren) wird innerhalb spezifizierter Grenzwerte gehalten.

Die Art der Ausführung einer Sicherheitsfunktion kann sehr unterschiedlich sein. Daher sind zusammen mit der Auswahl einige Eigenschaften zu berücksichtigen und für jede Anwendung individuell festzulegen. Hierzu zählen

- Verwendung in unterschiedlichen Betriebsarten (z. B. Automatikbetrieb, Einrichtbetrieb, Störungsbeseitigung),
- Verwendung unterschiedlicher Sicherheitsfunktionen bei vorhandener bzw. ausgefallener Energieversorgung (siehe auch Abschnitt 4.3 in [22]),
- Reaktion(en) beim Ansprechen der Sicherheitsfunktion,
- Reaktion(en) beim Erkennen eines Fehlers der Sicherheitsfunktion,
- Ansprechzeit,
- Häufigkeit der Betätigung,
- ggf. eine Priorität, falls mehrere Sicherheitsfunktionen gleichzeitig aktiv sein können,
- Festlegung sicherheitsbezogener Parameter, z. B. der maximal zulässigen Geschwindigkeit,
- erforderlicher Performance Level PL_r.

Detaillierte Informationen zur Definition von Sicherheitsfunktionen sind im SISTEMA-Kochbuch 6 „Definition von Sicherheitsfunktionen – Was ist wichtig?“ [23] verfügbar.

5.3.2 Beispiele, bei denen die Definition der Sicherheitsfunktion Einfluss auf die spätere Berechnung der PFH_D hat

In späteren Kapiteln wird gezeigt, wie die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) für eine Sicherheitsfunktion berechnet werden kann. Die Grundlagen hierfür werden jedoch bereits hier bei der Definition der Sicherheitsfunktion festgelegt. Die technische Realisierung einer Sicherheitsfunktion bestimmt naturgemäß die Art und den Umfang der hierfür benötigten Komponenten. Die Definition der Sicherheitsfunktion hat daher erhebliche Auswirkungen auf die Bestimmung der sicherheitsgerichteten Zuverlässigkeit. In den folgenden Beispielen soll dieser Sachverhalt erläutert werden.

Beispiel 1:
Sicherheitsfunktion „Stillsetzen beim Öffnen der Schutztür"

Beim Öffnen der Schutztür hat eine Bedienperson Zugang zu einem Gefahrenbereich, in dem fünf Antriebe Bewegungen von Maschinenteilen steuern. Das Öffnen der Schutztür bewirkt ein schnellstmögliches Stillsetzen aller fünf Antriebe.

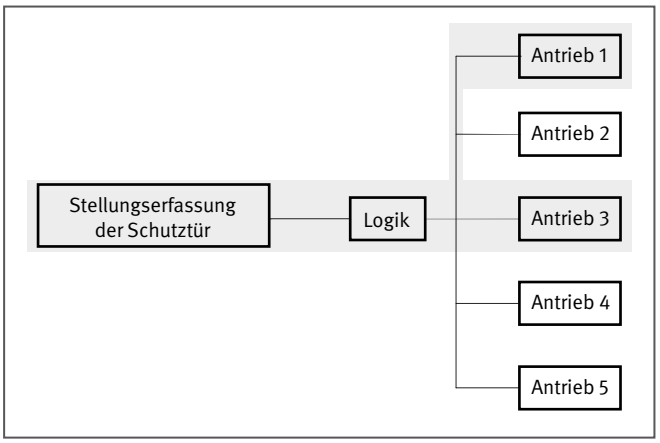
Bei der späteren Berechnung der PFH_D der Sicherheitsfunktion werden daher die PFH_D-Werte der folgenden Blöcke[2] addiert:

- Stellungsüberwachung der Schutztür einschließlich mechanischer Komponenten
- Logik
- Antrieb 1 bis 5

Das Resultat der Berechnung kann eine PFH_D sein, die für die Anwendung nicht mehr ausreichend ist, obwohl vielleicht nur die Antriebe 1 und 3 am momentanen Standort der Bedienperson gefahrbringende Bewegungen auslösen und die restlichen Antriebe rein „funktional" stillgesetzt werden. In diesem Fall empfiehlt es sich, für die Sicherheitsfunktion nur die Bewegungen zu berücksichtigen, die tatsächlich eine Gefährdung darstellen, und die Sicherheitsfunktion in Hinblick auf die für die Sicherheit der Bedienperson kritischen Antriebe umzuformulieren. Das zugehörige funktionale Schaltbild ist in Abbildung 5.6 dargestellt.

Sind an den gefahrbringenden Bewegungen in dem betrachteten Gefährdungsbereich mehrere Antriebe beteiligt, so spricht man von überlagerten Gefährdungen. Ist die Anzahl der zu berücksichtigenden Antriebe zu hoch, können sich auch hier die PFH_D-Werte der einzelnen Antriebe zu einer Gesamt-PFH_D summieren, die für den erforderlichen PL der Sicherheitsfunktion zu hoch ist. Die Überarbeitung der Norm sieht eine Berücksichtigung überlagerter Gefährdungen vor. Danach können unter Umständen die in der jeweiligen Sicherheitsfunktion betrachteten Gefährdungen auf Einzelgefährdungen bzw. die gefahrbringenden Maschinenbewegungen auf die Bewegungen einzelner Maschinenteile reduziert werden. Ob dies im Einzelfall möglich ist, muss während der Risikobeurteilung bestimmt werden. Eine Hilfestellung hierzu bieten Anhang J dieses Reports und [24].

Abbildung 5.6:
Stillsetzen der Antriebe 1 und 3 beim Öffnen der Schutztür



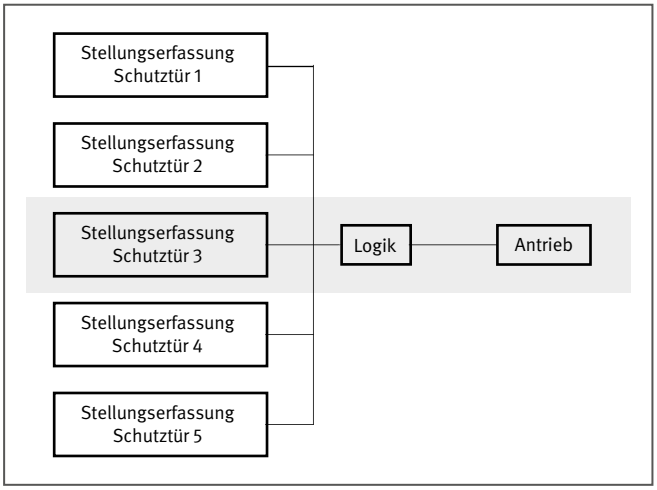
Beispiel 2:
Sicherheitsfunktion „Stillsetzen des Antriebs beim Öffnen einer Schutztür"

Eine gefahrbringende Bewegung ist durch einen Zaun abgesichert, der über fünf Schutztüren verfügt. Das Öffnen einer der Türen führt zum Stillsetzen. Da eine Person immer nur eine der Schutztüren zur gleichen Zeit öffnen wird, ist jede Tür Bestandteil einer eigenen Sicherheitsfunktion SF1 bis SF5, die sich aus folgenden Blöcken zusammensetzt:

- Stellungsüberwachung Schutztür x (x = 1, 2, ... 5), einschließlich mechanischer Komponenten
- Logik
- Antrieb

Abbildung 5.7 zeigt das funktionale Schaltbild und die Blöcke der Sicherheitsfunktion SF3.

Abbildung 5.7:
Stillsetzen des Antriebs beim Öffnen der Schutztür 3



[2] Fehlermöglichkeiten der elektrischen Installation werden den jeweiligen Blöcken zugeordnet.

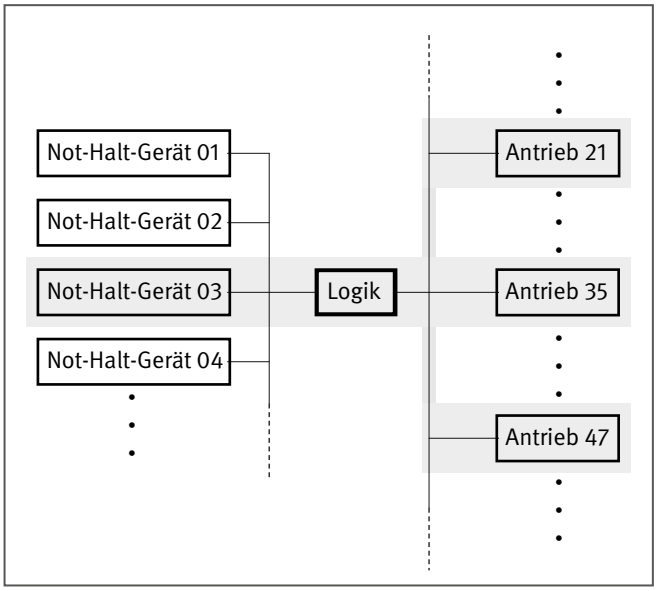
Beispiel 3:
Not-Halt-Funktion „Stillsetzen aller Antriebe bei Betätigung eines Not-Halt-Gerätes“ (siehe Abschnitt 5.5)

An einer größeren Maschine sind 20 Not-Halt-Geräte installiert, deren Betätigung alle 50 Antriebe schnellstmöglich stillsetzt. Welche Komponenten sind in diesem Fall bei der Realisierung der Not-Halt-Funktion zu berücksichtigen? Es ist nicht vorhersehbar, welches Not-Halt-Gerät zum Auslösen der Not-Halt-Funktion betätigt wird. Da der Bediener immer nur ein Not-Halt-Gerät betätigt, werden die Not-Halt-Funktionen SF1 bis SF20 definiert. Der jeweilige Standort einer gefährdeten Person beim Auslösen des Not-Halts ist nicht bekannt, aber wo auch immer sich diese Person befindet, stellen nicht alle 50 Antriebe eine Gefährdung dar. Daher sollte stellvertretend für alle denkbaren Situationen der ungünstigste Fall betrachtet werden. Dieser ist bestimmt durch die schlechteste PFH_D, ist also u. a. abhängig von der Anzahl der Antriebe in der Sicherheitskette, die am ungünstigsten Standort gefahrbringende Bewegungen erzeugen, sowie den jeweiligen einzelnen PFH_D-Werten. Das zugehörige Blockschaltbild ist in Abbildung 5.8 dargestellt.

Bei der späteren Bestimmung der PFH_D der Not-Halt-Funktion müssen die PFH_D-Werte der folgenden Blöcke berücksichtigt werden:

- Not-Halt-Gerät 03
- Logik
- Antrieb 21
- Antrieb 35
- Antrieb 47

Abbildung 5.8:
Not-Halt der Gesamtmaschine, ungünstigster Fall



Die Beispiele zeigen, dass sich bei der Definition einer Sicherheitsfunktion eine „lokale Sichtweise“ empfiehlt, bei der berücksichtigt wird:

- An welchem Ort befinden sich zum betrachteten Zeitpunkt Personen?
- Welche Bewegungen stellen am Standort der Person(en) Gefährdungen dar?
- Durch welche Schutzeinrichtungen wird zu dem betrachteten Zeitpunkt die Sicherheitsfunktion ausgelöst?

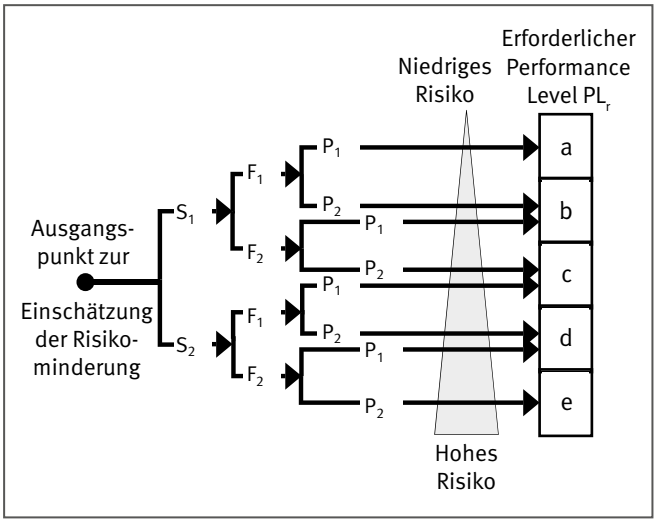
5.4 Bestimmung des erforderlichen Performance Level PL_r

Für jede vorgesehene Sicherheitsfunktion muss ein erforderlicher Performance Level PL_r[3] festgelegt werden – im technischen Sinne der Sollwert. Die Anforderungen ergeben sich aus der notwendigen Risikominderung, bei deren Festlegung u. a. ein ggf. unbekanntes Unfallgeschehen zu berücksichtigen ist. DIN ISO/TR 14121-2 [4] beschreibt Verfahren, um das erforderliche Maß der Risikominderung zu bestimmen. In DIN EN ISO 13849-1 wird hiervon die Methode des Risikographen angewendet.

5.4.1 Risikograph

Das Diagramm im Anhang A der Norm führt direkt zum erforderlichen Performance Level PL_r und wird im Folgenden erläutert (siehe Abbildung 5.9). Weitere Beispiele zur Bestimmung des PL_r finden sich in Anhang A.

Abbildung 5.9:
Risikograph zur Bestimmung des PL_r für jede Sicherheitsfunktion



[3] Mit der Kennzeichnung durch den Index r (required) wird darauf hingewiesen, dass es sich um den für die Sicherheitsfunktion erforderlichen Performance Level (Sollwert) handelt. In der späteren Validierung wird überprüft, ob der von der tatsächlichen Steuerung (Istwert) erreichte PL ≥ PL_r ist. „>“ bedeutet in diesem Zusammenhang: PL = e > PL = d > PL = c > PL = b > PL = a

Beginnend am Ausgangspunkt werden die Risikoparameter[4]

- S – Schwere der Verletzung,
- F – Häufigkeit und/oder Dauer der Gefährdungsexposition,
- P – Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens

bewertet. Der Risikograph führt dadurch zum erforderlichen PL_r. Diese Analyse ist für jede Sicherheitsfunktion und ohne Berücksichtigung der hierdurch erreichten Risikominderung durchzuführen. Sofern andere technische Maßnahmen bestehen, die unabhängig von der Steuerung realisiert sind, z. B. eine mechanisch trennende Schutzeinrichtung oder zusätzliche Sicherheitsfunktionen, so können diese bei der Bestimmung des PL_r als wirksam vorausgesetzt werden.

Schwere der Verletzung S1 und S2

Die Schwere der Verletzung (S-Parameter) an einer Gefahrenstelle wird in der Regel eine große Bandbreite einnehmen. Entscheidend für die Anforderung an die Steuerung ist jedoch nur die Unterscheidung zwischen:

- S1 – leicht (üblicherweise reversible Verletzung)
- S2 – ernst (üblicherweise irreversible Verletzung einschließlich Tod)

Bei der Entscheidung über S1 oder S2 sind die üblichen Auswirkungen von Unfällen und die normalerweise zu erwartenden Heilungsprozesse anzunehmen.

Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2 (F-Parameter)

Häufigkeit und Dauer der Gefährdungsexposition werden bewertet mit:

- F1 – selten bis weniger häufig und/oder die Dauer der Gefährdungsexposition ist kurz
- F2 – häufig bis dauernd und/oder die Dauer der Gefährdungsexposition ist lang

Es wird also sowohl die Anzahl der Eingriffe in den Gefahrenbereich in einem Zeitraum berücksichtigt als auch die Zeitdauer des Aufenthalts. Die Norm gibt eine Entscheidungshilfe dafür, dass bei Eingriffen, die häufiger als einmal alle 15 Minuten erfolgen, F2 gewählt werden sollte. In allen anderen Fällen ist F1 die richtige Wahl, sofern die Dauer der Gefährdungsexposition nicht 1/20 der gesamten Betriebsdauer der Maschine überschreitet. Bei der Bewertung ist ein durchschnittlicher Wert für die Dauer der Gefährdungsexposition im Verhältnis zur gesamten Nutzungszeit einer Maschine zu berücksichtigen.

Bei einer manuell beschickten Presse in der Metallbearbeitung, bei der zyklisch zwischen die Werkzeuge der Maschine gegriffen werden muss, ist sicherlich F2 zutreffend. Für ein Bearbeitungszentrum hingegen, das einmal jährlich eingerichtet wird und dann automatisch produziert, wird sicherlich F1 gewählt. Bei der Bewertung der Häufigkeit und Dauer ist es nicht zulässig zu unterscheiden, ob dieselbe oder unterschiedliche Personen der Gefährdung ausgesetzt werden.

Möglichkeit zur Vermeidung der Gefährdung P1 und P2 (P-Parameter)

An dieser Stelle soll bewertet werden, ob das Erkennen und die Vermeidung einer Gefährdungssituation

- P1 – möglich unter bestimmten Bedingungen,
- P2 – kaum möglich

ist. Bei der Festlegung dieses Parameters sind u. a. die physikalischen Eigenschaften einer Maschine, die Qualifikation des Bedienpersonals und dessen mögliche Reaktion von Bedeutung. Muss z. B. ein Einrichtbetrieb an laufender Maschine mit begrenzter Geschwindigkeit erfolgen, so wird bei geringen Beschleunigungswerten der Einrichtung der Parameter P1 die richtige Wahl sein: Die Bedienperson hat bei langsam auftretenden Gefährdungen die Möglichkeit, sich bei ausreichendem Bewegungsraum aus dem Gefahrenbereich zu entfernen. P2 ist zu wählen, wenn schnell größere Geschwindigkeiten erreicht werden können und die Chance, den Unfall durch Ausweichen der Bedienperson zu vermeiden, praktisch nicht gegeben ist. Bei dieser Bewertung ist nur die Begrenzung durch das physikalisch Mögliche und nicht die Begrenzung durch steuerungstechnische Komponenten zu berücksichtigen, denn diese könnten im Fehlerfall versagen. So ist beispielsweise bei Walzen, die sich in Richtung der Hand bewegen, im störungsfreien Betrieb ein Einzug nicht möglich. Im Fehlerfall der Steuerung kann sich die Drehrichtung allerdings ändern und die Hand würde im ungünstigsten Falle eingezogen.

Ein weiterer Einflussfaktor auf die Festlegung des PL_r ist die Wahrscheinlichkeit für den Eintritt eines Gefährdungsereignisses ([3], 5.5.2.3.2). Hierbei können menschliches Verhalten und technisches Versagen eine Rolle spielen. Beides lässt sich zahlenmäßig schwer abschätzen, die Norm nennt aber hierzu beispielhaft die Kriterien

- Zuverlässigkeitsdaten,
- Unfallgeschichte an vergleichbaren Maschinen.

Sofern Fakten vorliegen, mit denen die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses als „niedrig“ bewertet kann, darf der PL_r um einen Level verringert werden, jedoch PL a nicht unterschreiten.

[4] Die Wahrscheinlichkeit für den Eintritt eines Gefährdungsereignisses wird im Zusammenhang mit dem Risikoparameter P betrachtet.

Wie kann man nun ein „niedrig“ begründen? Die Berücksichtigung von Zuverlässigkeitsdaten bezieht sich u. a. auf die prozessbezogene (nicht sicherheitsbezogene) Steuerung. Der Maschinenhersteller muss also hierzu bewerten, ob eine gute Zuverlässigkeit der Bauteile (hohe *MTTF*, in diesem Fall ohne „D“) auch für seine Maschine angenommen werden kann. Wie groß ist also z. B. die Wahrscheinlichkeit, dass eine Standard-SPS zur funktionalen Steuerung einer Maschine fehlerhaft den unerwarteten Anlauf eines Antriebs auslöst? Wie sind neue Bauteile zu bewerten, die zwar mit guten Werten für die *MTTF* ausgestattet sind, für die aber noch keine Praxiserfahrungen vorliegen? Sind die Einsatzbedingungen von SPS & Co. (Sensoren, Frequenzumrichter, Netzteile usw.) vergleichbar mit den üblichen Applikationen? Wie sieht das Versorgungsnetz aus? Gibt es am zukünftigen Einsatzort der Maschine evtl. höhere elektromagnetische Imissionen? Welche Temperaturen herrschen? Usw. Auch wenn die Grenzdaten der eingesetzten Bauteile nicht verletzt werden, so kann dadurch doch die Wahrscheinlichkeit für einen Ausfall ansteigen. Hinzu kommen die Fehlermöglichkeiten in der Software, die natürlich ebenfalls für Gefährdungsereignisse sorgen können.

Falls das Unfallgeschehen aus dem Betrieb von vergleichbaren Maschinen mit identischen Risiken, gleichem Bedien- und Schutzkonzept und gleichen Schutzeinrichtungen bekannt ist und als gering angesehen wird, kann die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses ebenfalls als niedrig eingeschätzt werden.

Der durch diese Überlegungen reduzierte PL_r darf keinesfalls niedriger sein als bei den betrachteten Vergleichsmaschinen, denn aus geringem Unfallgeschehen lässt sich nicht ableiten, dass das sicherheitstechnische Niveau der implementierten Sicherheitsfunktionen höher als erforderlich ist. Niemand kann vorhersagen, ob eine Absenkung des aktuellen Niveaus nicht einen inakzeptablen Anstieg des Unfallgeschehens bewirken würde.

Auf die sich anschließende Gestaltung der Sicherheitsfunktionen geht Kapitel 6 ein.

5.5 Ergänzende Schutzmaßnahmen

Die Anforderungen an ergänzende Schutzmaßnahmen (i. d. R. Not-Halt) sind in DIN EN ISO 12100 [3], Abschnitt 6.3.5, enthalten. Im Hinblick auf die im vorliegenden Report behandelten steuerungstechnischen Fragestellungen sind hierunter insbesondere zu verstehen:

- Maßnahmen zum Stillsetzen im Notfall
- Umkehrung von Bewegungen
- Energietrennung und Energieableitung

Definitionsgemäß handelt es sich hierbei nicht um technische Schutzmaßnahmen oder Sicherheitsfunktionen im Sinne der DIN EN ISO 13849. Allerdings sollen diese ergänzenden Schutzmaßnahmen auch dann greifen, wenn technische Schutzmaßnahmen (trennende und/oder nicht trennende Schutzeinrichtungen) versagt haben bzw. durch Manipulation unwirksam gemacht wurden. Generell sind für ergänzende Schutzmaßnahmen zunächst die Anforderungen der DIN EN 60204-1 [25] an Steuerstromkreise und Steuerfunktionen von Maschinen zu berücksichtigen. Im Abschnitt 9.4 „Steuerfunktionen im Fehlerfall“ wird ein angemessenes Niveau der sicherheitstechnischen Leistungsfähigkeit verlangt, das durch die Risikobewertung der Maschine festzulegen ist. Insbesondere für die Not-Halt-Funktion gelten aber auch die Anforderungen der DIN EN ISO 13849. Dies schließt die Bestimmung eines Performance Levels mit ein. Dieser sollte für Not-Halt-Funktionen, wie in DIN EN ISO 13850 [13] festgelegt, mindestens PL c betragen. In jedem Falle dürfen ergänzende Schutzmaßnahmen nicht die Funktion und das Niveau von Schutzeinrichtungen beeinflussen.

5.6 Behandlung von Altmaschinen

Unter Altmaschinen sind solche Maschinen zu verstehen, die bereits vor Inkrafttreten der Maschinenrichtlinie in Verkehr gebracht wurden. Die Anforderungen der Richtlinie wurden auf diese Maschinen nicht angewendet. Werden Altmaschinen erweitert, verändert, modernisiert usw., kann dies jedoch erforderlich werden. In solchen Fällen ist zu bewerten, ob eine „wesentliche Veränderung“ vorliegt. Ist dies der Fall, gelten die Anforderungen der EG-Maschinenrichtlinie auch für „alte“ Maschinen, ebenso wie für neue. Dazu gehört u. a. die Anwendung der DIN EN ISO 13849. Bei der Entscheidung, ob eine „wesentliche Veränderung“ vorliegt, hilft ein Interpretationspapier des Bundesministeriums für Arbeit und Soziales [26].

5.7 Risikominderung am Beispiel einer Planschneidemaschine mit diversitärer Redundanz in der Logiksteuerung (Kategorie 4 – PL e)

Das Beispiel in diesem Abschnitt illustriert die Anwendung der DIN EN ISO 13849-1 an einer Planschneidemaschine. Dabei werden nur einzelne Aspekte näher dargestellt und nicht der gesamte Prozess.

Planschneidemaschinen (siehe Abbildung 5.10) dienen zum Schneiden von gestapelten Papierbögen oder ähnlichen Materialien mittels eines Messers. Das Schneidgut wird meist von Hand unter das Schneidmesser gelegt. Unmittelbar vor dem Schnitt wird ein Pressbalken mit hoher Kraft auf den Stapel abgesenkt, um diesen während des Schnittes zu fixieren. Messer und Pressbalken werden hydraulisch angetrieben.

5.7.1 Festlegung der Grenzen der Maschine

Räumliche Grenzen

Da die Planschneidemaschine von Hand beschickt wird, ist außer ausreichendem Bewegungsraum für die Bedienperson auch genügend Platz zur Bereitstellung von Schneidgut, Abfuhr und Lagerung der geschnittenen Papierstapel sowie Entsorgung von Abfallpapier erforderlich.

Zeitliche Grenzen

Je nach Anwendungsfall kann die Maschine über einen Zeitraum von ca. 20 Jahren eingesetzt werden. Durch die Abnutzung von Bauteilen kann sich die benötigte Zeit für das Stillsetzen einer

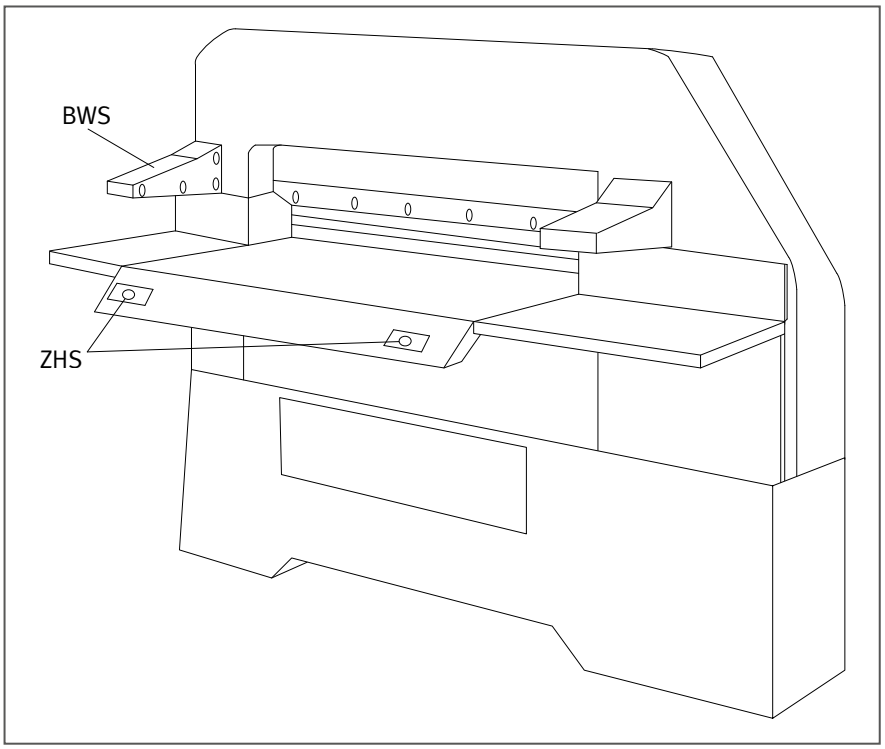


Abbildung 5.10:
Planschneidemaschine mit Zweihandschaltung (ZHS) und berührungslos wirkender Schutzeinrichtung (BWS)

Bewegung verlängern. Die daraus resultierende Überschreitung des Nachlaufwegs muss daher detektiert werden und zu einer Stillsetzung der Maschine führen.

Verwendungsgrenzen

Die bestimmungsgemäße Verwendung der Maschine besteht im Schneiden von gestapelten Papierbögen oder ähnlichen Materialien. Die Maschine wird manuell von einer einzelnen Person beschickt. Je nach Aufstellungsort und Maschinenbreite ist jedoch nicht auszuschließen, dass sich weitere Personen in der Umgebung aufhalten.

Folgende Betriebsarten sind vorgesehen:

1. Pressen
2. manuelles Schneiden (Einzelschnitt)
3. automatische Schnittfolge
   (automatischer Ablauf nach erstem manuellen Schnitt)
4. Messerwechsel

In den ersten drei Betriebsarten ist eine alleinige Bewegung des Pressbalkens möglich, um die Schnittlinie anzuzeigen (Schnitt andeuten). Hierzu betätigt die Bedienperson ein Fußpedal und kann dabei mit den Händen im Gefahrenbereich die Position des Papierstapels verändern.

5.7.2 Identifizierung der Gefährdungen

Folgende mechanische Gefährdungen sind für eine Planschneidemaschine signifikant:

- G1 – Quetschen durch den Pressbalken
- G2 – Schneiden durch das Schneidmesser während des Schnittvorgangs
- G3 – Schneiden durch das Schneidmesser im Ruhezustand

Risikoeinschätzung

Die dynamische Presskraft des Pressbalkens (Gefährdung G1) ist so groß, dass es nicht nur zu reversiblen Quetschungen, sondern auch zu Knochenbrüchen kommen kann. Für Gefährdung G2 muss von abgetrennten Gliedmaßen ausgegangen werden. Gefährdung G3 kann z. B. während der manuellen Positionierung der Papierstapel zu Verletzungen der Hände oder Unterarme am stillstehenden Schneidmesser führen, die in der Regel jedoch reversibel sind.

Die Gefährdungsexposition der bedienenden Personen ist sehr hoch, da sie betriebsmäßig regelmäßig (zyklisch) manuell in den Gefahrenbereich eingreifen.

Die Absenkgeschwindigkeit von Pressbalken und Messer (Gefährdungen G1 und G2) ist sehr hoch, sodass für die Bedienperson praktisch keine Möglichkeit besteht, die Gefahr abzuwenden. Bei stillstehendem Messer (Gefährdung G3) hat die Bedienperson die Möglichkeit, den Schaden zu vermeiden oder zu begrenzen.

Die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses aufgrund technischen Versagens ist nicht bekannt. Das Unfallgeschehen an vergleichbaren Maschinen ist jedoch gering, sodass die hier vorgesehenen Schutzeinrichtungen offensichtlich ausreichend sind. Sollte die Risikoanalyse für eine Sicherheitsfunktion einen höheren PL_r ergeben als an den vergleichbaren Maschinen tatsächlich realisiert, so darf prinzipiell eine Reduzierung des PL_r um einen Level erfolgen. Da die Sicherheitsfunktionen vergleichbarer Planschneidemaschinen jedoch mit dem höchsten PL realisiert werden, wird in diesem Fall eine Reduzierung des PL_r nicht möglich sein (siehe Abschnitt 5.7.4).

Risikobewertung

Unter Berücksichtigung aller Betriebsbedingungen und aller Eingriffsmöglichkeiten ist festzustellen, dass eine Risikominderung erforderlich ist.

Inhärent sichere Konstruktion

Die dynamische Presskraft des Pressbalkens und die Energie des Messers zu reduzieren, ist nicht möglich, da dies die Funktion der Maschine einschränken würde. Auch eine Anordnung und Gestaltung der Maschine, die verhindert, dass die bedienende Person in den Gefahrenbereich eingreifen kann, ist nicht möglich, da sie die Papierstapel genau dort ausrichten muss.

Folgende Maßnahmen können jedoch ergriffen werden:

1. Alle Zugänge zum Gefahrenbereich mit Ausnahme der Bedienseite verdecken.
2. Scharfe Kanten und Ecken vermeiden.
3. Für eine angemessene Arbeitsposition und Zugänglichkeit der Bedienteile sorgen.
4. Maschine ergonomisch gestalten.
5. Elektrische Gefährdungen verhindern.
6. Gefährdungen durch die hydraulische Ausrüstung vermeiden.
7. Die Mechanik zur Führung von Schneidmesser und Pressbalken wird derart verbunden, dass das Messer im oberen Totpunkt vom Pressbalken verdeckt wird.

5.7.3 Notwendige Sicherheitsfunktionen

Unter Berücksichtigung aller Betriebsarten und aller manuellen Eingriffe sind folgende Sicherheitsfunktionen erforderlich:

- SF1 – STO (Safe Torque Off), Sicher abgeschaltetes Moment zur Vermeidung eines unerwarteten Anlaufs
- SF2 – Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung
- SF3 – Erkennung eines Eingriffs weiterer Personen in den Gefahrenbereich durch eine BWS (berührungslos wirkende Schutzeinrichtung, z. B. ein Lichtgitter) und sofortige Schnittunterbrechung
- SF4 – Selbsttätiger Stopp aller Bewegungen nach jedem Einzelschnitt bzw. nach Beendigung der automatischen Schnittfolge
- SF5 – Reduzierung der dynamischen Presskraft für den Pressbalken bei der Funktion „Schnitt andeuten“
- SF6 – Selbsttätige Rückkehr von Pressbalken und Messer in ihre Ausgangslage bei Schnittunterbrechung

Anmerkung: Es wäre möglich, auf die Maschinenteile Schneidmesser und Pressbalken das Prinzip der überlagerten Gefährdungen anzuwenden (siehe Abschnitt 5.3.2). In diesem Fall würden SF1, SF3, SF4 und SF6 aufgeteilt werden, sodass für Schneidmesser und Pressbalken jeweils eigene Sicherheitsfunktionen definiert wären. Im vorliegenden Fall wird darauf jedoch verzichtet, da aufgrund der geringen Anzahl der Bauteile in SF1 bis SF6 die erforderliche PFH_D auch für diese zusammengefassten Sicherheitsfunktionen erreicht werden kann.

Eigenschaften der Sicherheitsfunktionen

Bei Eingriff in das Lichtgitter ist der Schnitt sofort zu unterbrechen. Die Sicherheitsfunktion SF3 hat daher Priorität gegenüber SF2. Für SF5 ist die maximal zulässige Kraft für den Pressbalken bei „Schnittlinie andeuten“ anzugeben (siehe [27]).

5.7.4 Bestimmung des erforderlichen Performance Level PL_r

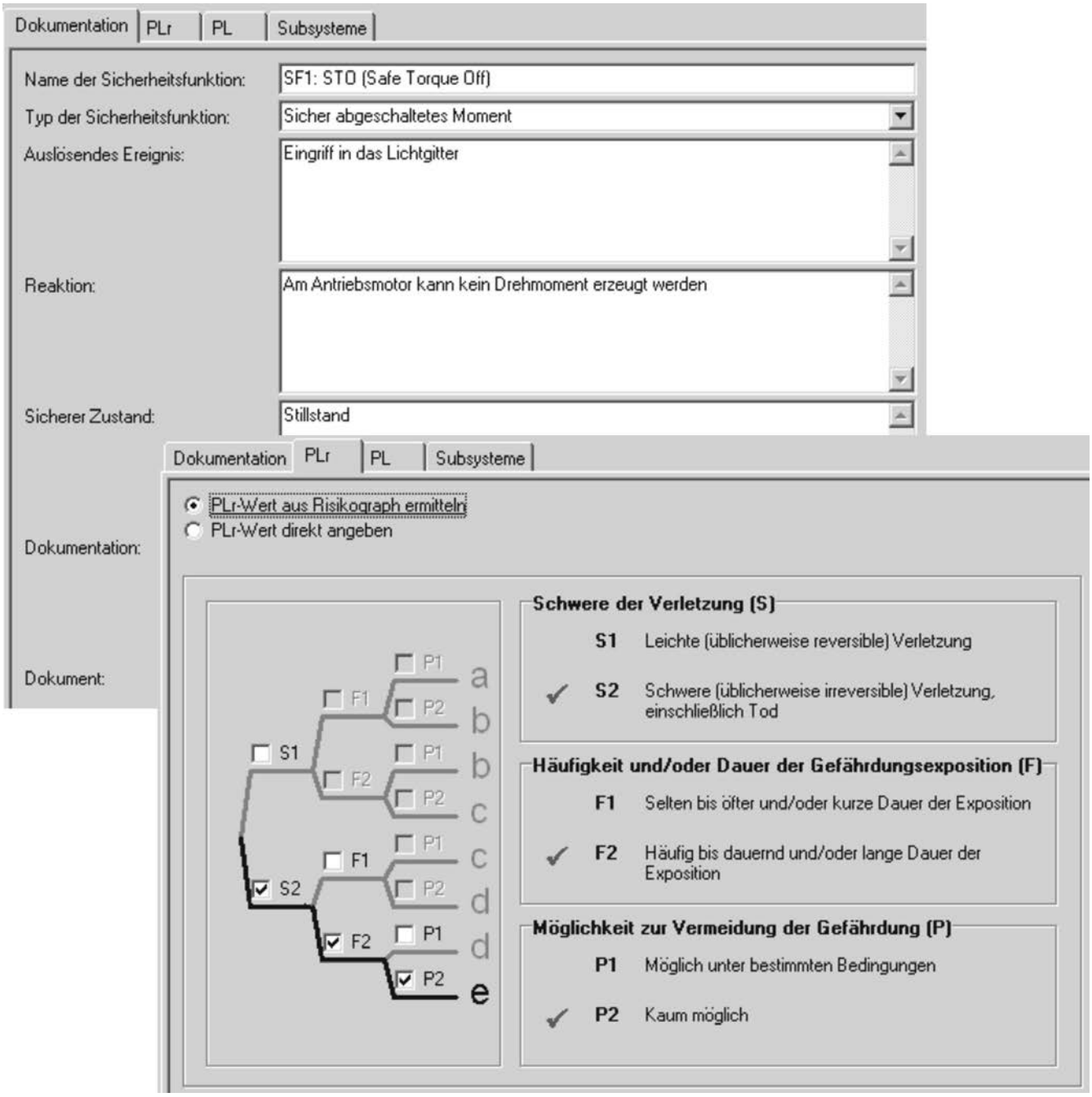
Der PL_r ist für jede Sicherheitsfunktion zu bestimmen. Analysiert man die Situationen, in denen die einzelnen Sicherheitsfunktionen benutzt werden, stellt man eine gleichartige Bewertung der Risikoparameter S, F und P für die Sicherheitsfunktionen SF1 bis SF6 fest:

- S2 – ernste, üblicherweise irreversible Verletzung
- F2 – dauernder Aufenthalt im Gefahrenbereich, die Häufigkeit ist also höher als einmal alle 15 Minuten
- P2 – Vermeidung einer Gefährdungssituation kaum möglich

Entsprechend dem Risikographen in Abbildung 5.9 ergibt sich aus dieser Bewertung ein erforderlicher Performance Level PL_r = e. An vergleichbaren Maschinen ist das Unfallgeschehen gering. Die hier betrachteten Sicherheitsfunktionen dieser Maschinen sind bereits mit PL e realisiert worden, wie es in [28] vorgegeben ist. Das Ergebnis der Risikoanalyse wird also durch die Praxis bestätigt, eine mögliche Reduzierung des PL_r ergibt sich hieraus nicht. Abbildung 5.11 zeigt Dokumentation und Risikograph in der Software SISTEMA für die Sicherheitsfunktion SF1.

Für die Gefährdung 3 „Schneiden durch das Schneidmesser im Ruhezustand“ ist eine ausreichende Risikominderung durch eine mechanische Kopplung von Schneidmesser und Pressbalken erreicht worden. Eine Sicherheitsfunktion ist nicht erforderlich.

Abbildung 5.11:
Dokumentation und Risikograph für SF1



5.7.5 Ergänzende Schutzmaßnahmen

Folgende Maßnahmen sind erforderlich:

1. Stillsetzen im Notfall
   In der Maschinensteuerung stehen bereits geeignete Sicherheitsfunktionen mit PL = e zur Verfügung, die für den Not-Halt verwendet werden. Bei zweikanaliger Verdrahtung des Not-Halt-Gerätes entspricht dann auch das Stillsetzen im Notfall einem PL = e.

2. Die Befreiung einer eingeklemmten Person erfordert eine rückläufige Bewegung von Messer und Pressbalken, die durch Federkraft ausgeführt wird.

6 Gestaltung sicherer Steuerungen

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- In Abschnitt 6.1.2 (systematische Ausfälle) wurden zusätzliche Hinweise zu anwendungsspezifischen integrierten Schaltungen (ASIC), feldprogrammierbaren Gate-Arrays (FPGA), programmierbaren Logikbausteinen und zu komplexen Standardbausteinen hinzugefügt. Abschnitt 6.1.3 (Ergonomie) wurde an die neue Maschinenrichtlinie 2006/42/EG angepasst.
- In Abschnitt 6.2.5 (Kategorie 2) wurden Empfehlungen zur Interpretation der Anforderungen an eine Kategorie 2 eingefügt.
- In den Abschnitten 6.2.5 (Kategorie 2) und 6.2.14 (DC) wurde klargestellt, dass eine Warnung statt der Einleitung eines sicheren Zustands nur bis PL_r = c eine unter bestimmten Bedingungen erlaubte Alternative sein kann. Außerdem wurde die Testung bei Anforderung der Sicherheitsfunktion als Alternative zum mindestens 100-mal häufigeren Testen als Anfordern der Sicherheitsfunktion hinzugefügt. Wird nur 25-mal häufiger getestet als angefordert, kann dies durch Multiplikation der PFH_D mit dem Faktor 1,1 zur sicheren Seite abgeschätzt werden. Ferner bezieht sich die Anforderung zur Qualität der Testeinrichtung in Kategorie 2 nun auf die $MTTF_D$ des Testkanals (statt nur des Blocks „TE“) in Relation zur $MTTF_D$ des Funktionskanals (statt nur des Blocks „L“).
- In den Abschnitten 6.2.9 und 6.4 wurde das „gekapselte Subsystem“ eingeführt.
- In Abschnitt 6.2.13 (FMEA versus „Parts Count“-Verfahren) wurde die Anhebung der $MTTF_D$-Kappung in Kategorie 4 auf 2 500 Jahre ergänzt.
- In Abschnitt 6.2.14 (Diagnosedeckungsgrad) wurden die Erläuterungen zur Testhäufigkeit überarbeitet und Hinweise zu Bauteilen mit DC < 60 % bis hinunter zu DC = 0 % hinzugefügt.
- Ein neuer Abschnitt 6.2.17 zur alternativen PFH_D-Bestimmung für den Ausgangsteil des SRP/CS nach Abschnitt 4.5.5 der Norm wurde eingefügt.
- Der alte Abschnitt 6.2.17 (Bussysteme als Verbindungsmittel) wird damit zum Abschnitt 6.2.18.
- Abschnitt 6.3.10 Anforderungen an SRESW für Standardkomponenten wurde an den neuen Abschnitt 4.6.2 der Norm angepasst. Außerdem wird auf den IFA Report 2/2016 „Sicherheitsbezogene Anwendungssoftware von Maschinen“ verwiesen.
- In Abschnitt 6.4 (Kombination von SRP/CS als Subsysteme) wurde die PFH_D-Addition als neues Regelverfahren genannt, das tabellarische Verfahren zur PL-Abstufung je nach Anzahl der Subsysteme wurde zur Alternativlösung degradiert, falls für Subsysteme keine PFH_D-Werte vorliegen.
- Das Beispiel der Planschneidemaschine in Abschnitt 6.5 wurde aktualisiert.
- Hinweise auf die weiterführenden SISTEMA-Kochbücher 1, 4 und 6 wurden ergänzt.

6.1 Einleitung

Wenn die genaue Sicherheitsfunktion und ihr geforderter Beitrag zur Risikominderung in Form des PL_r feststehen, schließt sich der konkrete Entwurf der sicherheitsbezogenen Teile der Steuerung (SRP/CS), die die Sicherheitsfunktion(en) ausführen sollen, an. Den entsprechenden Ausschnitt aus dem iterativen Gestaltungsprozess der DIN EN ISO 13849-1 zeigt Abbildung 6.1 (siehe Seite 42).

Die sicherheitstechnische Qualität der SRP/CS wird als einer von fünf Performance Level (PL) angegeben. Jedem dieser PL ist ein Bereich der Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde zugeordnet (Tabelle 6.1, siehe Seite 42). Neben der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde, auch als PFH_D (Probability of a Dangerous Failure per Hour) bezeichnet, sind weitere Maßnahmen, z. B. zur Ertüchtigung von Software oder gegen systematische Ausfälle, notwendig, um den entsprechenden PL zu erreichen.

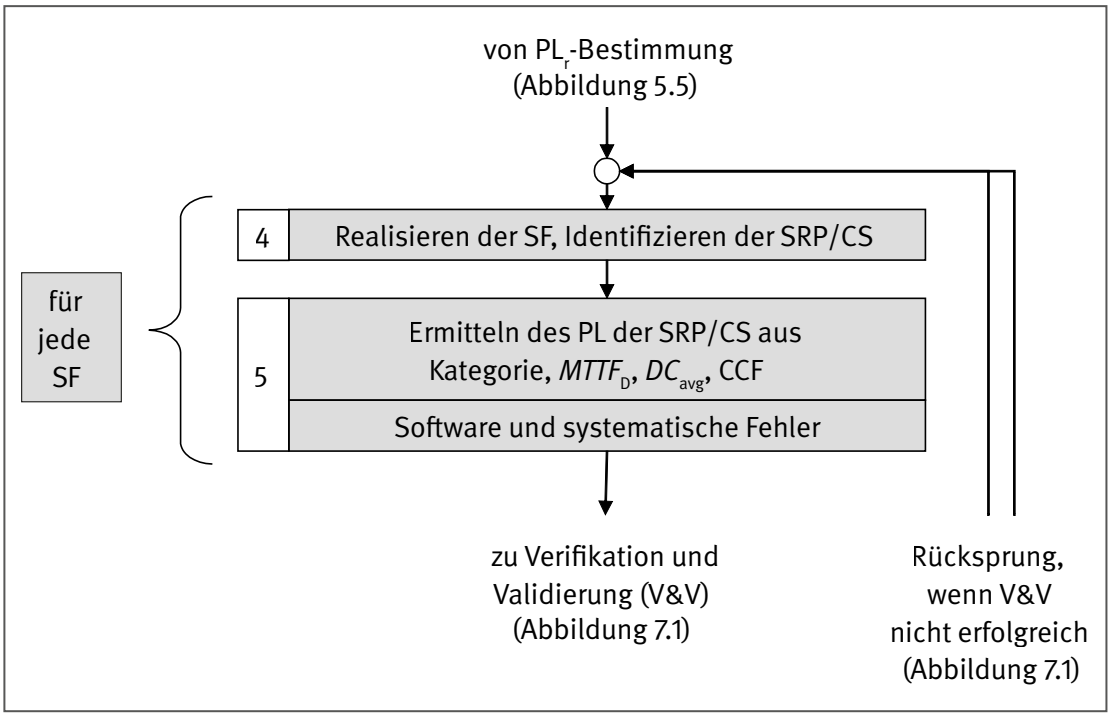


Abbildung 6.1:
Ermittlung des erreichten PL in der Realisierungsphase der SRP/CS als Ausschnitt aus dem iterativen Gestaltungsprozess, siehe Abbildung 4.1

Tabelle 6.1:
Zuordnung der Ausfallwahrscheinlichkeit zu den Performance Level

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) in h^{-1}
a	$\geq 10^{-5}$ bis $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ bis $< 10^{-5}$
c	$\geq 10^{-6}$ bis $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ bis $< 10^{-6}$
e	$\geq 10^{-8}$ bis $< 10^{-7}$

Die Auswahl des Verfahrens zum Nachweis der Ausfallwahrscheinlichkeit steht grundsätzlich frei (z. B. Markov-Berechnungen, Petri-Netz-Verfahren), es sollen aber immer folgende Kriterien berücksichtigt werden:

- quantifizierbare Aspekte (Struktur, Bauteilzuverlässigkeit, Diagnose in Form von Tests, Ausfälle infolge gemeinsamer Ursache) und

- nicht quantifizierbare, qualitative Aspekte, die das Verhalten der SRP/CS beeinflussen (Verhalten der Sicherheitsfunktion unter Fehlerbedingungen, sicherheitsbezogene Software, systematische Ausfälle und Umgebungsbedingungen)

Für beide Gruppen schlägt DIN EN ISO 13849-1 praxisorientierte Verfahren vor, die wissenschaftlich fundiert zu einer guten Abschätzung des erreichten PL führen. Für jeden Teilaspekt kann der Nachweis nach Bedarf vergröbert oder verfeinert werden, sodass neben einem schnellen Überschlag auch ein detaillierter Nachweis möglich ist.

Zunächst wird unter Abschnitt 6.1.1 der Entwicklungsablauf beschrieben: Dazu gehören z. B. Anforderungen an Spezifikation und Dokumentation innerhalb des SRP/CS-Lebenszyklus. Anschließend folgen notwendige Maßnahmen zur Beherrschung systematischer Ausfälle (Abschnitt 6.1.2) sowie ergonomische Gestaltungsaspekte (Abschnitt 6.1.3). In Abschnitt 6.2 werden die Kategorien und die darauf basierende vereinfachte Methode zur Bewertung der quantifizierbaren Aspekte beschrieben. Abschnitt 6.3 stellt anschließend Anforderungen an Software vor. Abschließend zeigt Abschnitt 6.4, welche quantifizierbaren Aspekte bei der Kombination von SRP/CS beachtet werden müssen. Abbildung 6.2 erläutert die Notwendigkeit dieses zusätzlichen Abschnitts. Die gesamte Maschinensteuerung CS (Control System) teilt sich in sicherheitsbezogene Teile (SRP/CS) und die meistens deutlich umfangreicheren, nicht sicherheitsbezogenen Teile auf, die alleine den normalen Betriebsfunktionen dienen. Die Kombination sicherheitsbezogener Teile einer Steuerung beginnt an dem Punkt, an dem sicherheitsbezogene Signale erzeugt werden (einschließlich z. B. Betätiger und Rolle eines Positionsschalters) und endet an den Ausgängen der Leistungssteuerungselemente (einschließlich z. B. Hauptkontakte eines Schützes). Treten im energielosen Zustand keine Gefährdungen auf (Ruhestromprinzip), so gelten Leistungselemente wie Motoren oder Zylinder nicht als SRP/CS. Wirken jedoch externe oder interne Fremdkräfte (z. B. an Vertikalachsen), so müssen die Leistungselemente zusätzlich sicherheitstechnisch ertüchtigt sein (z. B. Rückschlagventile an Zylindern, zusätzliche mechanische Bremse). Abschnitt 6.5 schließlich beschreibt – in Fortführung von Abschnitt 5.7 – die konkrete Umsetzung am praktischen Beispiel der Steuerung einer Planschneidemaschine.

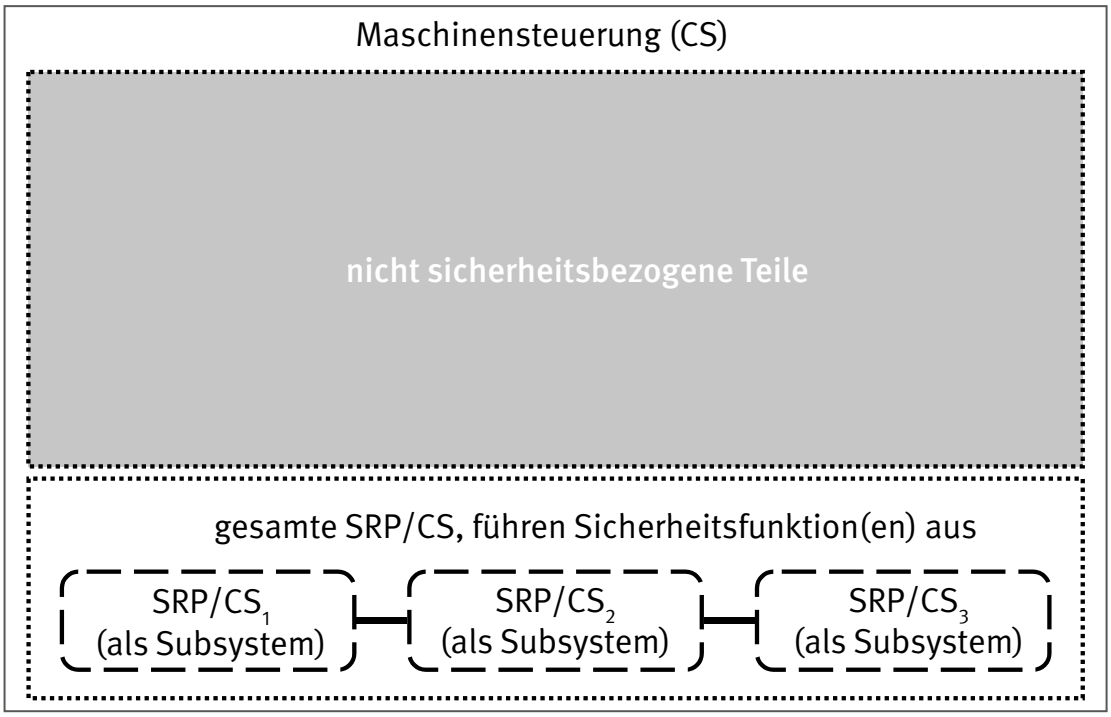


Abbildung 6.2: SRP/CS und Subsysteme innerhalb der Maschinensteuerung

6.1.1 Entwicklungsablauf

Jede Handlung bei der Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (Anwendungsbereich der Norm) muss daran orientiert sein, möglichst fehlerfreie, den Anforderungen entsprechende Produkte zu entwickeln und diese auch wie vorgesehen einzusetzen. Schließlich geht es um die Gesundheit von Menschen und die Vermeidung von Unfällen. Das Motto für den Entwicklungsablauf muss daher lauten: strukturiert und gut dokumentiert!

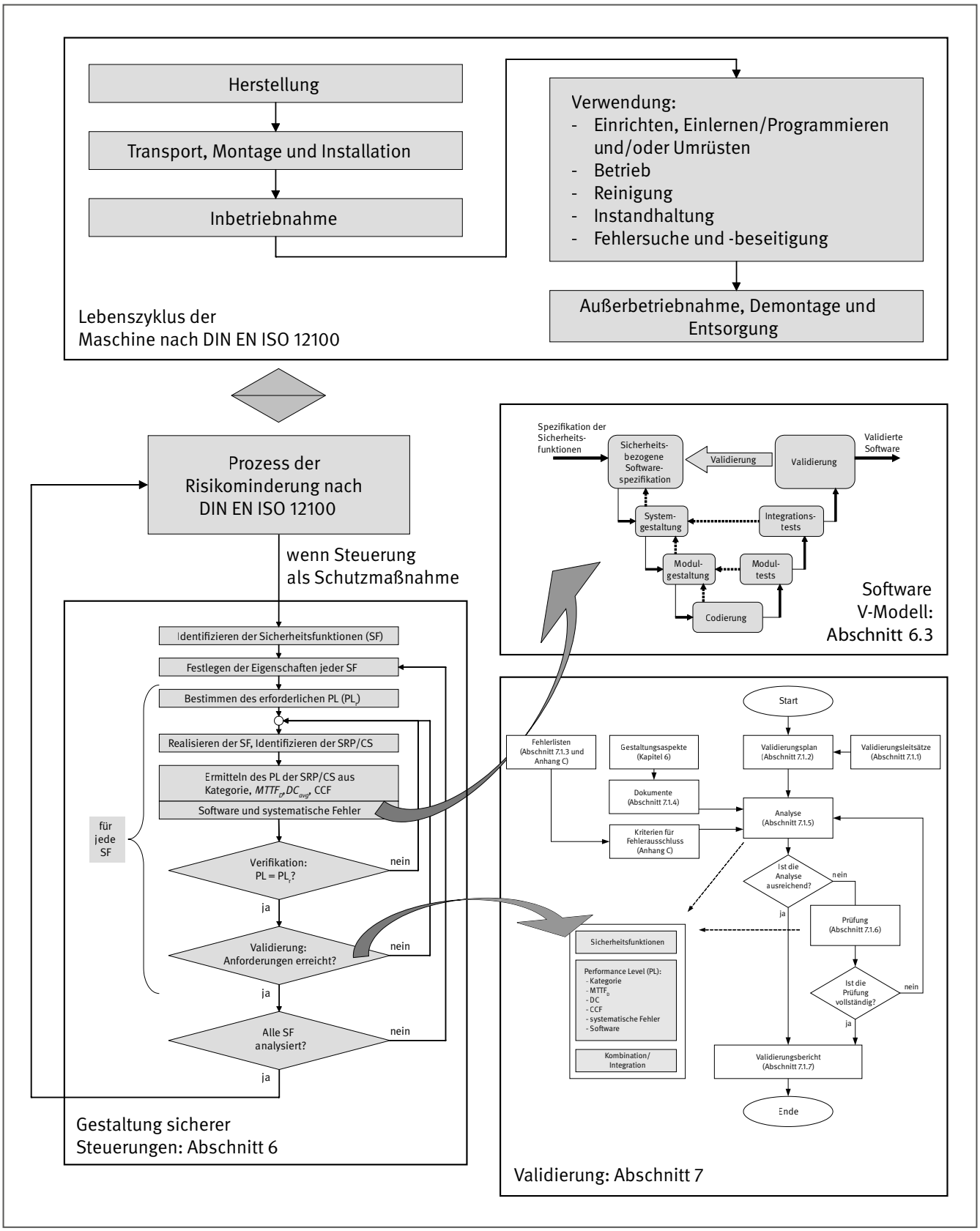
Der Prozess der Risikominderung nach DIN EN ISO 12100 [3] muss, wie in Abbildung 6.3 (siehe Seite 44) dargestellt, auf den gesamten Lebenszyklus einer Maschine ausgerichtet sein. Obwohl in DIN EN ISO 13849-1 nicht explizit ausgeführt, gilt es auch bei der Gestaltung und Integration eines oder mehrerer SRP/CS, den Lebenszyklusgedanken aufzugreifen, um die Aktivitäten entsprechend zu strukturieren. Dass es sich bei dem in der Norm beschriebenen iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen um einen in einzelne Phasen untergliederten Prozess handelt, wird auch aus der Beschreibung der Norm in Kapitel 4 deutlich. Die Phase der Validierung ist, wie aus Abbildung 6.3 ersichtlich, durch eigene strukturierte Abläufe gekennzeichnet, die in Kapitel 7 genauer beschrieben werden. Sehr ausführlich wird die Strukturierung in Lebensphasen durch das bei der Erstellung sicherheitsrelevanter Software verwendete V-Modell gekennzeichnet; Abschnitt 6.3 erläutert dies. Auch wenn der Gestaltungsprozess für SRP/CS z. B. nicht explizit auf die Phase der Instandhaltung eingeht, so wird diese Phase über erforderliche Inhalte in der Benutzerinformation berücksichtigt.

Da SRP/CS Teile einer Maschine sind, können Anforderungen in fast jeder Phase des Lebenszyklus der Maschine auch Einfluss auf ein SRP/CS haben. Alle Phasen im Lebenszyklus der Maschine müssen daher bei der Identifikation und Festlegung der Eigenschaften von Sicherheitsfunktionen berücksichtigt werden. Um dies möglichst umfassend und nachprüfbar zu gestalten, werden Sicherheitsfunktionen zunächst spezifiziert. Das SISTEMA-Kochbuch 6 [23] widmet sich ausführlich diesem Thema: „Definition von Sicherheitsfunktionen – Was ist wichtig?“. SRP/CS, die nicht für eine spezielle Maschinensteuerung entwickelt werden, z. B. ein Lichtgitter oder eine Sicherheits-SPS, bedürfen daher einer besonders genauen Beschreibung ihrer Kenndaten und ihrer Schnittstellen, um eine korrekte Verwendung sicherzustellen.

Mit der Spezifikation der Sicherheitsfunktionen beginnt der Lebenszyklus der SRP/CS. DIN EN ISO 13849-1 listet neben speziellen Aspekten verschiedener Sicherheitsfunktionen auch allgemeine Aspekte auf, die in einer solchen Spezifikation mindestens enthalten sein müssen.

Mit einer solchen Spezifikation werden für alle Beteiligten am Anfang des Entwicklungsprozesses die Rahmenbedingungen festgelegt – es handelt sich um ein sogenanntes Lastenheft und keinesfalls um eine nach der Entwicklung angefertigte Produktbeschreibung. Eine Sicherheitsfunktion wird durch SRP/CS realisiert, die Bestandteil der Maschinensteuerung sind und über Schnittstellen zu weiteren SRP/CS und zur funktionalen Steuerung verfügen. Daher ist es notwendig, eine Spezifikation zu erstellen. Dazu wird im Kasten 6.1 (Seite 45) ein allgemeines Gliederungsschema für eine Spezifikation der Sicherheitsanforderungen aufgezeigt, das die Spezifikation der Sicherheitsfunktionen einschließt. Dieses Gliederungsschema bezieht sich auf SRP/CS, die die gesamte Sicherheitsfunktion ausführen. Für SRP/CS als Subsysteme ist die Spezifikation entsprechend anzupassen.

Abbildung 6.3:
Lebenszyklen von Maschine und SRP/CS



Kasten 6.1: Allgemeines Gliederungsschema für eine Spezifikation der Sicherheitsanforderungen

1 Allgemeine Produkt- und Projektangaben

1.1 Produktidentifikation
1.2 Autor, Version, Datum, Dokumentenname, Dateiname
1.3 Inhaltsverzeichnis
1.4 Begriffe, Definitionen, Glossar
1.5 Versionshistorie und Änderungsvermerke
1.6 Für die Entwicklung relevante Richtlinien, Normen und technische Regeln

2 Funktionale Angaben zur Maschine, soweit sicherheitstechnisch von Bedeutung

2.1 Bestimmungsgemäße Verwendung und vernünftigerweise vorhersehbare Fehlanwendung/-bedienung
2.2 Prozessbeschreibung (Betriebsfunktionen)
2.3 Betriebsarten (z. B. Einrichtbetrieb, Automatikbetrieb, Betrieb mit lokalem Bezug oder von Teilen der Maschine, inklusive der Betriebsartenabfolge)
2.4 Kenndaten, z. B. Zykluszeiten, Reaktionszeiten, Nachlaufwege
2.5 Sonstige Eigenschaften der Maschine
2.6 Sicherer Zustand der Maschine inklusive ihrer zulässigen und unzulässigen Ausfallarten
2.7 Wechselwirkung zwischen Prozessen (siehe auch 2.2) und manuellen Aktionen (Reparatur, Einrichten, Reinigen, Fehlersuche usw.)
2.8 Handlungen im Notfall
2.9 Verhalten der Maschine bei Energieverlust

3 Erforderliche(r) Performance Level (PL_r)

3.1 Referenz auf vorhandene Dokumentation zur Gefährdungsanalyse und Risikobeurteilung der Maschine
3.2 Ergebnisse der Risikobeurteilung für jede ermittelte Gefährdung oder Gefährdungssituation und Festlegung der zur Risikominderung jeweils erforderlichen Sicherheitsfunktion(en)

4 Sicherheitsfunktionen (Angaben gelten für jede Sicherheitsfunktion, siehe auch Tabelle 4 in [23])

- Funktionsbeschreibung („Erfassen – Verarbeiten – Ausgeben“) einschließlich aller funktionalen Eigenschaften (siehe auch Tabellen 5.1 und 5.2)
- Aktivierungs-/Deaktivierungsbedingungen oder -ereignisse (z. B. Betriebsarten der Maschine)
- Verhalten der Maschine beim Auslösen der Sicherheitsfunktion
- zu berücksichtigende Wiederanlaufbedingungen
- Leistungskriterien/Leistungsdaten
- Ablauf (zeitliches Verhalten) der Sicherheitsfunktion mit Reaktionszeit
- Häufigkeit der Betätigung (d. h. Anforderungsrate), Erholungszeiten nach Anforderung
- sonstige Daten
- einstellbare Parameter (soweit vorgesehen)
- Einordnung und Zuordnung von Prioritäten bei gleichzeitiger Anforderung und Bearbeitung mehrerer Sicherheitsfunktionen
- Verhalten bei Energieausfall
- funktionales Konzept zur Trennung bzw. Unabhängigkeit/Rückwirkungsfreiheit zu Nicht-Sicherheitsfunktionen und weiteren Sicherheitsfunktionen

5 Vorgaben für den SRP/CS-Entwurf

5.1 Zuweisung, durch welche SRP/CS und in welcher Technologie die Sicherheitsfunktion realisiert werden soll, vorgesehene Betriebsmittel
5.2 Auswahl der Kategorie, vorgesehene Architektur (Struktur) als sicherheitsbezogenes Blockdiagramm mit Beschreibung
5.3 Schnittstellenbeschreibung (Prozessschnittstellen, interne Schnittstellen, Bedienschnittstellen, Bedien- und Anzeigeelemente usw.)
5.4 Einschaltverhalten, Umsetzung des erforderlichen Anlaufverhaltens und Wiederanlaufverhaltens
5.5 Leistungsdaten: Zykluszeiten, Reaktionszeiten usw.
5.6 Verhalten des SRP/CS bei Bauteilausfällen und -fehlern (Erreichen und Aufrechterhalten des sicheren Zustandes) einschließlich Zeitverhalten
5.7 Zu berücksichtigende Ausfallarten von Bauteilen, Baugruppen oder Blöcken und ggf. Begründung für Fehlerausschlüsse
5.8 Konzept zur Umsetzung der Erkennung und Beherrschung von zufälligen und systematischen Ausfällen (Selbsttests, Testschaltungen, Überwachungen, Vergleiche, Plausibilitätsprüfungen, Fehlererkennung durch den Prozess usw.)
5.9 Quantitative Aspekte
5.9.1 Zielwerte für $MTTF_D$ und DC_{avg}

5.9.2 Schalthäufigkeit verschleißbehafteter Bauteile
5.9.3 Häufigkeit von Maßnahmen zur Fehleraufdeckung
5.9.4 Gebrauchsdauer, falls abweichend von der Berechnungsgrundlage der vorgesehenen Architekturen (20 Jahre)
5.10 Betriebs- und Grenzdaten (Betriebs- und Lagertemperaturbereich, Feuchteklasse, IP-Schutzart, Schock-/Vibrations-/EMV-Störfestigkeitswerte, Versorgungsdaten mit Toleranzen usw.) (IP = International Protection, EMV = elektromagnetische Verträglichkeit)
5.11 Anzuwendende Grundnormen für die Konstruktion (zur Ausrüstung, zum Schutz gegen elektrischen Schlag/gefährliche Körperströme, zur Störfestigkeit gegen Umgebungsbedingungen usw.)
5.12 Technische und organisatorische Maßnahmen für einen gesicherten Zugriff auf sicherheitsrelevante Parameter bzw. SRP/CS-Eigenschaften (Manipulationsschutz, Zugangssicherung, Programm-/Datenschutz) und zum Schutz gegen unbefugtes Bedienen (Schlüsselschalter, Code usw.), z. B. bei Sonderbetriebsarten
5.13 Allgemeine technische Voraussetzungen und organisatorische Rahmenbedingungen für die Inbetriebnahme, Prüfung und Abnahme sowie Wartung und Instandhaltung

Eine solche Spezifikation muss, um Gültigkeit zu erlangen, vor dem nächsten Entwicklungsschritt verifiziert werden. Dabei geht es in erster Linie um Vollständigkeit, Korrektheit, Verständlichkeit und Widerspruchsfreiheit. Dass eine solche Verifikation, z. B. in Form einer Inspektion, durch an einem Projekt Unbeteiligte Vorteile hat, dürfte auf der Hand liegen. Wird sicherheitsrelevante Software eingesetzt, so muss aus einer solchen Spezifikation der Sicherheitsanforderungen eine eigenständige Softwarespezifikation abgeleitet werden (siehe Abschnitt 6.3.2).

Mit der Spezifikation ist das erste Dokument im Ablauf der Gestaltung von SRP/CS entstanden. Grundsätzlich hat die Dokumentation einen hohen Stellenwert im Sinne einer nachvollziehbaren Entwicklung. Man sollte beachten, dass ein Produkt unter Umständen von einer anderen Person als der, die es entwickelt hat, weiter gepflegt wird. Details zur erforderlichen Dokumentation im Rahmen des iterativen Gestaltungsprozesses von SRP/CS finden sich im Abschnitt 6.3.8 zu Software und in den Abschnitten 7.1.4 ff. Erwähnt sei an dieser Stelle, dass Dokumente eindeutig identifizierbar sein müssen, eine Versionsverwaltung ist also ein Muss. Für die korrekte Umsetzung von Sicherheitsfunktionen wird nicht zuletzt der Inhalt der Benutzerinformationen maßgeblich sein. DIN EN ISO 13849-1 enthält in Abschnitt 11 eine Liste der Informationen, die in der Benutzerinformation mindestens enthalten sein müssen. Der Inhalt der herstellerinternen technischen Dokumentation von SRP/CS wird in Kapitel 10 der Norm aufgelistet. Auch der Gesetzgeber erteilt Auflagen zur Dokumentation. Kasten 6.2 zeigt den Inhalt der erforderlichen technischen Unterlagen für Maschinen nach europäischer Maschinenrichtlinie 2006/42/EG [2].

Kasten 6.2: Technische Unterlagen für Maschinen: Auszug aus der Maschinenrichtlinie (2006/42/EG), Anhang VII, A

1. Die technischen Unterlagen umfassen:
   a) eine technische Dokumentation mit folgenden Angaben bzw. Unterlagen:
      – eine allgemeine Beschreibung der Maschine,
      – eine Übersichtszeichnung der Maschine und die Schaltpläne der Steuerkreise sowie Beschreibungen und Erläuterungen, die zum Verständnis der Funktionsweise der Maschine erforderlich sind,
      – vollständige Detailzeichnungen, eventuell mit Berechnungen, Versuchsergebnissen, Bescheinigungen usw., die für die Überprüfung der Übereinstimmung der Maschine mit den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen erforderlich sind,
      – die Unterlagen über die Risikobeurteilung, aus denen hervorgeht, welches Verfahren angewandt wurde; dies schließt ein:
        i) eine Liste der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen, die für die Maschine gelten,
        ii) eine Beschreibung der zur Abwendung ermittelter Gefährdungen oder zur Risikominderung ergriffenen Schutzmaßnahmen und gegebenenfalls eine Angabe der von der Maschine ausgehenden Restrisiken,
      – die angewandten Normen und sonstige technische Spezifikationen unter Angabe der von diesen Normen erfassten grundlegenden Sicherheits- und Gesundheitsschutzanforderungen,
      – alle technischen Berichte mit den Ergebnissen der Prüfungen, die vom Hersteller selbst oder von einer Stelle nach Wahl des Herstellers oder seines Bevollmächtigten durchgeführt wurden,
      – ein Exemplar der Betriebsanleitung der Maschine,
      – gegebenenfalls die Einbauerklärung für unvollständige Maschinen und die Montageanleitung für solche unvollständigen Maschinen,
      – gegebenenfalls eine Kopie der EG-Konformitätserklärung für in die Maschine eingebaute andere Maschinen oder Produkte,
      – eine Kopie der EG-Konformitätserklärung.
   b) bei Serienfertigung eine Aufstellung der intern getroffenen Maßnahmen zur Gewährleistung der Übereinstimmung aller gefertigten Maschinen mit den Bestimmungen dieser Richtlinie.

6.1.2 Systematische Ausfälle

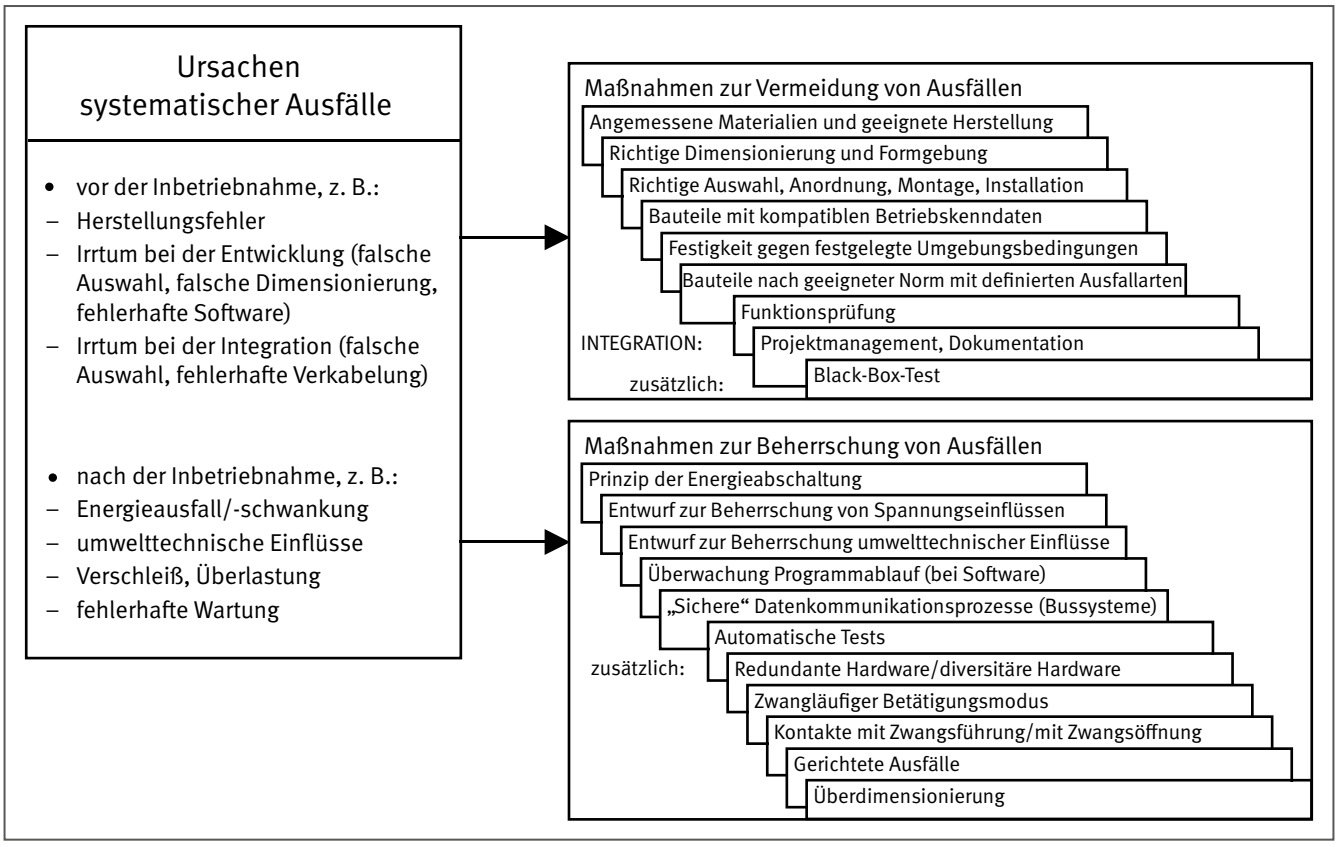
Systematische Ausfälle haben im Gegensatz zu zufälligen Bauteilausfällen Ursachen, die nur durch eine Änderung z. B. der Gestaltung oder des Herstellungsprozesses, der Betriebsverfahren oder der Dokumentation beseitigt werden können. Sie entstehen irgendwann im Laufe des Lebenszyklus eines Produktes, z. B. durch Fehler in der Spezifikation, im Entwurf oder bei einer Änderung von SRP/CS. Die Realisierung mehrkanaliger Strukturen und auch die Betrachtung der Wahrscheinlichkeit von Bauteilausfällen sind wichtige Elemente der sicherheitstechnischen Gestaltung. Was helfen die schönsten Zahlen zur Ausfallwahrscheinlichkeit, wenn prinzipielle Aspekte nicht berücksichtigt wurden? Wird beispielsweise ein Produkt nicht richtig oder in der falschen Umgebung eingesetzt, droht möglicherweise ein systematischer Ausfall. Dieser Tatsache wird DIN EN ISO 13849-1 im Zusammenspiel mit Teil 2 gerecht, wenn sie für das Erreichen eines PL fordert, auch mögliche systematische Ausfälle zu berücksichtigen. Grundsätzlich lässt sich sagen, dass schon viele der grundlegenden und bewährten Sicherheitsprinzipien gegen systematische Ausfälle wirken (siehe Anhang C). Diese sind gemäß DIN EN ISO 13849-2 zu berücksichtigen und vervollständigen Anhang G der Norm.

Im informativen Anhang G der Norm ist eine Liste von Maßnahmen und damit indirekt auch von zu betrachtenden Einflüssen aufgeführt. Die Maßnahmen gliedern sich in solche zur Vermeidung von Ausfällen (G.3 und G.4) und solche zur Beherrschung (G.2). Abbildung 6.4 gibt eine Übersicht. Die Maßnahmen zur Vermeidung von Ausfällen müssen sich dabei durch alle Lebensphasen eines Produktes ziehen und werden demnach in diesem Report teilweise auch im Kapitel 7 unter dem Aspekt der Validierung angesprochen. Obwohl nicht explizit aufgeführt, gilt es, gerade bei Änderungen, Fehlerbehebung und bei der Wartung entsprechende Sorgfalt walten zu lassen. Oft sind gerade in diesen Phasen Details aus der Entwicklung nicht (mehr) gegenwärtig. Maßnahmen zur Beherrschung von Ausfällen müssen dagegen in ein Produkt implementiert werden und entfalten ihre Wirkung im Betrieb. Neben Basisanforderungen listet die Norm auch Maßnahmen zur Auswahl auf, von denen eine oder mehrere unter Berücksichtigung der Komplexität der SRP/CS und des PL angewendet werden sollen (in Abbildung 6.4 als „zusätzlich“ gekennzeichnet).

Die Maßnahmen sind in der Norm größtenteils kurz erläutert. Es sei darauf hingewiesen, dass Diversität im Allgemeinen, also nicht nur wie in Abbildung 6.4 für Hardware aufgeführt, in der täglichen Praxis des IFA ein großer Nutzen unterstellt wird – vergleiche dazu auch die Ausführungen zu Anforderungen an Software im Abschnitt 6.3.10.

Aufmerksamen Leserinnen und Lesern dieses Reports könnte sich im Weiteren die Frage stellen, worin der Unterschied zu den Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF, siehe Abschnitt 6.2.15) liegt. Solche Ausfälle sind natürlich auch als systematische Ausfälle zu betrachten. Allerdings richtet sich diese CCF-Betrachtung nur auf Strukturen, die mehrkanalig sind oder zumindest eine Testeinrichtung besitzen (Kategorien 2, 3 und 4). Ein weiterer Unterschied ist der „Versuch“, CCF-Aspekte zahlenmäßig (quantitativ) zu betrachten, wohingegen die Betrachtung nach Anhang G der Norm rein qualitativ ist. Mit ausreichenden Maßnahmen gegen systematische Ausfälle nach

Abbildung 6.4:
Maßnahmen gegen systematische Ausfälle nach Anhang G der Norm



Anhang G der Norm und Beachtung grundlegender und bewährter Sicherheitsprinzipien erscheint es nicht besonders schwierig, die Anforderungen an Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) zu erfüllen.

Dass konkrete Anforderungen durchaus anwendungs- und technologiespezifisch sein können und demnach manchmal auch eine Auslegung der allgemeinen Anforderungen erforderlich ist, soll anhand von drei Beispielen erläutert werden.

Beispiel 1:
Maßnahmen zur Beherrschung von Auswirkungen eines Energieausfalls

Bei der Gestaltung der sicherheitsbezogenen Teile von Steuerungen sind auch Störungen der Energieversorgung (elektrische Spannung, Luftdruck in der Pneumatik, Hydraulikdruck) zu berücksichtigen (siehe Abschnitt 5.2.8 und Anhang G der Norm). So können z. B. Spannungsausfall, Spannungsschwankungen und Über- bzw. Unterspannung den sicheren Zustand einer Maschine gefährden. Dies trifft insbesondere auf das Hochhalten von Lasten mit elektrischen und hydraulischen Antrieben (Vertikalachsen) zu. Solche Störungen können ihre Ursachen in Bauteilfehlern innerhalb der SRP/CS haben, dann werden ihre Auswirkungen auf den Performance Level in der Verifikation berücksichtigt. Liegen die Ursachen jedoch im Versorgungsnetz begründet oder wurde die Netz-Trenneinrichtung (Hauptschalter) der Maschine betätigt, so entziehen sich diese Vorfälle einer quantitativen Berücksichtigung und können nur als systematische Ausfälle – teilweise sogar als Betriebszustand – betrachtet werden, die vom SRP/CS beherrscht werden müssen, sodass der sichere Zustand erreicht und/oder aufrechterhalten wird. Die Norm schlägt seit ihrer dritten Ausgabe für diesen Fall vor, jeweils unterschiedliche Sicherheitsfunktionen vorzusehen:

a) mit verfügbarer Energie und

b) ohne verfügbare Energie.

Wenn man davon ausgehen kann, dass die Energieversorgung in der Regel vorhanden ist, kann sich durch diesen Ansatz für beide Sicherheitsfunktionen eine unterschiedliche Bewertung der Risikoparameter im Risikographen der DIN EN ISO 13849-1 ergeben. Dies könnte für die Sicherheitsfunktion ohne verfügbare Energie auf einen geringeren PLr führen.

Beispiel 2:
Versagen von Pneumatik- bzw. Hydraulikventilen

DIN EN ISO 13849-2, Tabellen B.1 „Grundlegende Sicherheitsprinzipien der Pneumatik“ und B.2 „Bewährte Sicherheitsprinzipien der Pneumatik“, legt u. a. fest, dass bei der Konstruktion und Herstellung von pneumatischen Bauteilen auf die „Anwendung geeigneter Werkstoffe und Herstellungsverfahren“ und „geeignetes Vermeiden einer Verunreinigung der Druckluft“ geachtet werden muss. Diese Anforderungen beziehen sich vor allem auf die Auswahl der Werkstoffe, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Reibung, Verschleiß, Korrosion und Temperatur bzw. auf die Berücksichtigung von hoch wirksamer Filtration der Druckluft/Abscheidung von Feststoffen und Wasser.

Weiterhin sind in den Tabellen C.1 und C.2 in ähnlicher Weise die Anforderungen an hydraulische Bauteile festgelegt. Auch hier müssen „ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Druckmediums“ getroffen und auf die „richtige Dimensionierung und Formgebung“ geachtet werden.

Dennoch können bei selten geschalteten fluidtechnischen Bauelementen aufgrund der konstruktiven Eigenschaften (Spalt zwischen Schieber und Gehäuse) erhöhte Haftkräfte entstehen:

- Bei Pneumatikventilen mit Weichdichtungen können die Dichtungen durch chemische Einflüsse der Schmiermittel (Öl mit Additiven in der Druckluft, eingebracht durch Kompressor, Öler oder Initialschmierung) quellen oder der Schmierfilm kann durch die Dichtkantenpressung bei längerem Verbleiben in einer Schaltstellung kollabieren und somit die Haftkraft erhöhen.

- Bei Hydraulikventilen kann bei längerem Verbleiben in einer Schaltstellung sogenanntes Silting auftreten. Hierbei lagern sich während der Haltezeit zwischen den Schaltspielen feine Schmutzpartikel im Dichtspalt ab und verursachen dadurch ein Klemmen des Ventilschiebers.

Aus diesen Gründen ist konstruktiv generell ein hoher Kraftüberschuss (z. B. Federkraft) für die Rückstellung des Ventilschiebers in die „sichere Schaltstellung“ erforderlich. Bei nicht mechanischen Federn ist der Erhalt der Rückstellfunktion durch geeignete Maßnahmen sicherzustellen. Weiterhin gilt es, die oben beschriebenen Effekte, wie auch in der Norm neu erwähnt, durch zyklisches Schalten zu verhindern. Entsprechende Schaltzyklen bzw. Testzyklen im Abstand von z. B. < 8 Stunden sollen Ausfälle durch Nichtschalten verhindern.

Beispiel 3:
Trennung sicherheitsbezogener von anderen Funktionen

Normen funktionaler Sicherheit thematisieren generell die Trennung sicherheitsbezogener Funktionen von anderen Funktionen (Nicht-Sicherheitsfunktionen) – so auch DIN EN ISO 13849-2, und zwar z. B. als bewährtes Sicherheitsprinzip für Elektrik unter dem Stichwort „Verringerung von Fehlermöglichkeiten“. Diese Anforderung gilt sowohl für Hardware als auch für Software. Gleichwohl kann es Gründe geben, die eine gänzliche Trennung nicht sinnvoll erscheinen lassen. In diesen Fällen ist zumindest zu erreichen, dass es klar definierte funktionale und technische Schnittstellen gibt, mit deren Hilfe Rückwirkungen auf den sicherheitsrelevanten Teil vermeidbar bzw. auch beherrschbar werden.

Anschaulich lässt sich diese Anforderung am Beispiel der Erstellung von Anwendungssoftware darstellen. Die weitestgehende Art der Trennung von Standard-Anwendungssoftware und sicherheitsrelevanter Anwendungssoftware (SRASW, siehe Abschnitt 6.3) ist natürlich, diese mit getrennten Programmiersystemen (sogenannte Engineering-Suiten) zu erstellen und auf verschiedenen SPS (Speicherprogrammierbaren Steuerungen) ablaufen zu lassen. Insbesondere aus wirtschaftlichen Gründen wird man jedoch versuchen, die gesamte Anwendungssoftware mit nur einem Programmiersystem und ggf. in einem

gemeinsamen Engineering-Ablauf zu erstellen. Dabei ist allerdings eine Vielzahl von Aspekten zu berücksichtigen; z. B. die Anforderung, dass sicherheitsrelevante Variablen, Ergebnisse oder Ausgänge nicht von nicht sicherheitsrelevanten Softwareteilen (Programm, Funktionsbaustein, Funktion/Anweisung u. Ä.) überschrieben werden dürfen. Verknüpfungen beider Welten sind zwar zulässig, jedoch nur unter Einhaltung festgelegter Konventionen. Dabei müssen sicherheitsrelevante Signale und Funktionen immer die Priorität behalten: So ist eine „ODER"-Verknüpfung beispielsweise keinesfalls erlaubt. Inzwischen unterstützen Softwareentwicklungswerkzeuge solche Ansätze und haben vorgegebene Funktionen und automatisch kontrollierende
Regeln implementiert (in den Editoren und Compilern). Verknüpfungsfehler, die sich eventuell nur in unvorhersehbaren Betriebssituationen auswirken bzw. mit angemessenem Aufwand zur Abnahme/Inbetriebnahme nicht aufzudecken sind, können so sehr anwenderfreundlich verhindert werden.

Eine vollständige Analyse der Einflüsse funktionaler Standardteile einer Steuerung auf die sicherheitsrelevanten Teile – übrigens auch für Sicherheitsfunktionen untereinander – wird bei der Konstruktion also nicht erspart bleiben. Doch ist die Analyse, wo (technisch) und wie (funktional) solche Einflüsse möglich sind, durch den Einsatz o. g. Entwicklungswerkzeuge ungleich einfacher und schneller auszuführen. Zu der noch wesentlicheren Frage „Wie sollen festgestellte Einflüsse abgestellt (vermieden oder beherrscht) werden?" muss man ggf. gar nicht erst übergehen.

6.1.3 Ergonomie

Die europäische Maschinenrichtlinie 2006/42/EG (MRL) fordert im Anhang I Abschnitt 1.1.6 vom Maschinenhersteller, dass Belästigung, Ermüdung sowie körperliche und psychische Fehlbeanspruchung des Bedienungspersonals unter Berücksichtigung ergonomischer Prinzipien bereits bei der Konzeption der Maschine auf das mögliche Mindestmaß zu reduzieren sind. Dies gilt daher auch für die Schnittstellen zwischen dem Bedienpersonal einer Maschine/Maschinenanlage und den SRP/CS. Darunter fallen sowohl konkrete Schutzeinrichtungen, wie z. B. eine Schutztür mit Positionsschalter, als auch die Bedienung einer Sicherheitsfunktion, z. B. über Taster oder sogar über eine dafür geeignete Softwareoberfläche eines Displays. Weiterhin sind ein von der Maschine vorgegebener Arbeitsrhythmus und Überwachungstätigkeiten, die dauernde Aufmerksamkeit erfordern, zu vermeiden.

Welche Bedeutung ergonomische Prinzipien für SRP/CS haben und dass nicht immer jede bestimmungsgemäße Verwendung oder vorhersehbare Fehlanwendung von SRP/CS bei der Konstruktion einer Maschine berücksichtigt wird, zeigt der HVBG-Report „Manipulation von Schutzeinrichtungen an Maschinen" [29] auf. Auf der Webseite www.stopp-manipulation.org sind Hilfsmittel und weitere Informationen zum Thema Manipulation verfügbar.

DIN EN ISO 13849-1 fordert daher die Verwendung ergonomischer Prinzipien und listet dazu in Abschnitt 4.8 eine Fülle hilfreicher Normen auf. Damit Maschinenkonstrukteure die Gestaltung der Mensch-Maschine-Schnittstelle der SRP/CS überprüfen können, entwickelte das IFA die Checkliste „Ergonomische Maschinengestaltung" . Im Dezember 2010 wurden diese Checkliste und weitere Dokumente als DGUV Information 209-068/069 (bisher: BGI/GUV-I 5048-1/2) überarbeitet [30]. Konkreter behandelt werden u. a. handbediente Stellteile; Tastaturen, Tasten und Eingabegeräte; Displays und Anzeigen; optische Gefahrensignale und die Softwareergonomie von Bedienoberflächen. Eine Konstruktionshilfe bei der nutzergerechten Gestaltung von Bediensystemen für Maschinen bietet z. B. die VDI/VDE-Richtlinie 3850 [31].

6.2 Quantifizierung der Ausfallwahrscheinlichkeit

Die von der Norm zur Ermittlung des PL geforderte zahlenmäßige Bestimmung der Ausfallwahrscheinlichkeit, oft (auch in anderen Normen) vereinfacht „Quantifizierung" genannt, kann streng genommen niemals exakt, sondern nur mithilfe statistischer Methoden oder anderer Abschätzungen näherungsweise erfolgen. Zwar sind die Haupteinflussgrößen genannt, die bei dieser „Bestimmung" berücksichtigt werden sollen, die Wahl der Methode zur Ermittlung der Ausfallwahrscheinlichkeit aus diesen Einflussgrößen bleibt aber frei. Hier ist grundsätzlich jede abgesicherte und anerkannte Methode erlaubt wie z. B. Zuverlässigkeits-Blockdiagramme, Fehlerbaum-Methode, Markov-Modellierung oder Petri-Netze. Je nachdem, wer die Ausfallwahrscheinlichkeit bestimmt, sei es der Steuerungshersteller, der Maschinenanwender oder eine Prüfstelle, bestehen unter Umständen unterschiedliche Vorlieben für und Erfahrungen mit verschiedenen Methoden und daher wird hier ausdrücklich jede geeignete Methode erlaubt.

Andererseits besteht für diejenigen, die bisher mit der Quantifizierung der Ausfallwahrscheinlichkeit unerfahren sind, sicherlich Bedarf nach mehr oder weniger Hilfestellung seitens DIN EN ISO 13849-1. Dieser Tatsache wurde Rechnung getragen, indem ein vereinfachter Ansatz erarbeitet wurde, der trotz wissenschaftlich fundierter Grundlagen (Markov-Modellierung) Schritt für Schritt eine einfache Möglichkeit der Quantifizierung beschreibt. Zwar werden dort an einigen Stellen Abschätzungen zur sicheren Seite getroffen, die den geschätzten Zahlenwert der Ausfallwahrscheinlichkeit gegenüber exakteren Methoden verschlechtern können, dafür ist die Methode aber auch für Nicht-Mathematiker praktikabel und das Verfahren ist weitgehend eindeutig und damit nachvollziehbar. Im Folgenden wird dieses vereinfachte Verfahren ausführlich im Allgemeinen und anhand eines durchgerechneten praktischen Beispiels (siehe Abschnitt 6.5) vorgestellt. Weitere Details zu einzelnen Spezialthemen können in den Anhängen nachgelesen werden.

6.2.1 Vorgesehene Architekturen ...

Die Struktur oder Architektur einer Sicherheitssteuerung bestimmt die Toleranz gegenüber Fehlern (Fehlertoleranz) und stellt das Gerüst dar, auf dem alle anderen quantifizierbaren Aspekte aufbauen, um schließlich den PL der sicherheitsbezogenen Teile von Steuerungen zu bilden. Die Erfahrungen des IFA mit der Industrie seit 1985 bestätigen, dass es nur wenige Grundtypen von Sicherheitssteuerungen im Maschinenbau gibt, auf die sich der überwiegende Teil aller realisierten Steuerungen zurückführen lässt (bzw. auf Kombinationen dieser Grundtypen, siehe weiter unten): Dies sind das einkanalige ungetestete

System mit unterschiedlich zuverlässigen Bauteilen am einen Ende des Spektrums, das im Mittelfeld durch Tests aufgewertet werden kann, und schließlich das zweikanalige hochwertig getestete System am anderen Ende. Systeme mit mehr als zwei Kanälen oder andere „exotische“ Strukturen sind im Maschinenbau extrem selten vertreten und können mit dem vereinfachten Verfahren nur bedingt bewertet werden. Meist reicht es aber selbst bei mehr als zwei Kanälen aus, die beiden zuverlässigsten zu berücksichtigen, um den PL mit dem vereinfachten Verfahren der vorgesehenen Architekturen hinreichend genau abzuschätzen. Daher werden Systeme mit mehr als zwei Kanälen in DIN EN ISO 13849-1 nicht betrachtet. Das SISTEMA-Kochbuch 4 [32] hilft in einigen dieser Fälle: „Wenn die vorgesehenen Architekturen nicht passen“. Neben der „horizontalen“ Einteilung in verschiedene funktionale oder testende Kanäle ist meist auch eine „vertikale“ Einteilung in eine Sensorebene (Eingabegeräte, Input „I“), eine Verarbeitungsebene (Logik „L“) und eine Aktorebene (Ausgabegeräte, Output „O“) hilfreich.

Mit voller Absicht wird die Kontinuität zu den in der Maschinenbauindustrie und -normung etablierten Kategorien der DIN EN 954-1 gewahrt, die nach demselben Muster fünf Strukturen als Kategorien definiert. DIN EN ISO 13849-1 ergänzt die alte Kategoriedefinition geringfügig um quantitative Anforderungen an die Bauteilzuverlässigkeit ($MTTF_D$), den Diagnosedeckungsgrad von Tests (DC_{avg}) und die Widerstandsfähigkeit gegen Ausfälle infolge gemeinsamer Ursache (CCF). Daneben bildet sie die Kategorien auf fünf strukturelle Grundtypen, sogenannte vorgesehene Architekturen (Designated Architectures), ab. Zwar können sich gleiche Kategorien im Einzelnen strukturell immer noch unterschiedlich darstellen, die Vergröberung durch Abbildung auf die zugehörige vorgesehene Architektur ist aber dennoch innerhalb des vereinfachten Ansatzes als Näherung statthaft. Beispielsweise ist die Anzahl „vertikaler“ Blöcke (Input, Logik, Output) in einem Kanal in der Regel für die PL-Bestimmung mathematisch und sicherheitstechnisch kaum relevant.

Bei komplexeren Sicherheitsfunktionen kann es vorkommen, dass sich die gesamte Sicherheitskette nicht mehr auf eine der fünf Grundtypen alleine abbilden lässt. Dann hilft meist eine Zerlegung der Sicherheitskette in mehrere Abschnitte, sogenannte Subsysteme, von denen sich jedes einzeln auf eine vorgesehene Architektur abbilden lässt. Wie diese Subsysteme wieder zusammengesetzt und aus den einzelnen Performance Level wieder ein Gesamtwert ermittelt werden kann, wird in Abschnitt 6.4 näher erläutert. Die folgenden Ausführungen beziehen sich auf Steuerungen (SRP/CS), die ohne Zerlegung in Subsysteme einer Kategorie zugeordnet werden können. Sie lassen sich aber sinngemäß auf Subsysteme übertragen, die nur einen Teil einer Sicherheitsfunktion ausführen.

6.2.2 … und Kategorien

Die Kategorien klassifizieren sicherheitsbezogene Teile einer Steuerung (SRP/CS) in Bezug auf ihre Widerstandsfähigkeit gegen Fehler und ihr Verhalten im Fehlerfall, basierend auf der Zuverlässigkeit und/oder der strukturellen Anordnung der Teile (siehe Tabelle 6.2). Eine höhere Widerstandsfähigkeit gegenüber Fehlern bedeutet eine höhere mögliche Risikoreduzierung. Für die Bestimmung der Ausfallwahrscheinlichkeit und des PL bilden die Kategorien deshalb das Rückgrat, das durch die Bauteilzuverlässigkeit ($MTTF_D$), die Tests (DC_{avg}) und die Widerstandsfähigkeit gegenüber Ausfällen infolge gemeinsamer Ursache (CCF) komplettiert wird.

Kategorie B ist die Basiskategorie, deren Anforderungen auch in den übrigen Kategorien eingehalten werden müssen. In den Kategorien B und 1 wird die Widerstandsfähigkeit gegen Fehler überwiegend durch die Auswahl und Verwendung geeigneter Bauteile erreicht. Beim Auftreten eines Fehlers kann die Sicherheitsfunktion unwirksam werden. Kategorie 1 hat gegenüber Kategorie B eine höhere Widerstandsfähigkeit gegen Fehler durch die Verwendung besonderer, sicherheitstechnisch bewährter Bauteile und Prinzipien.

In den Kategorien 2, 3 und 4 wird eine verbesserte Leistungsfähigkeit hinsichtlich der vorgegebenen Sicherheitsfunktion überwiegend durch strukturelle Maßnahmen erreicht. In Kategorie 2 wird die Ausführung der Sicherheitsfunktion in regelmäßigen Abständen in der Regel durch technische Einrichtungen (Testeinrichtung TE) selbsttätig überprüft. Zwischen den Testphasen kann die Sicherheitsfunktion beim Auftreten eines Fehlers allerdings ausfallen. Durch geeignete Auswahl der Testintervalle kann bei Anwendung der Kategorie 2 eine geeignete Risikoreduzierung erreicht werden. Bei den Kategorien 3 und 4 führt das Auftreten eines einzelnen Fehlers nicht zum Verlust der Sicherheitsfunktion. In Kategorie 4, und wenn immer in Kategorie 3 in angemessener Weise durchführbar, werden solche Fehler selbsttätig erkannt. In Kategorie 4 ist darüber hinaus die Widerstandsfähigkeit gegenüber einer Anhäufung von unbemerkten Fehlern gegeben.

Bei der Fehlerbetrachtung ist es notwendig abzuwägen, welche Bauteilfehler unterstellt werden müssen und welche begründet ausgeschlossen werden können. Hinweise auf die in Betracht zu ziehenden Fehler werden in Anhang C gegeben.

In den Kategorien 3 und 4 müssen auch Ausfälle infolge gemeinsamer Ursache, die ein gleichzeitiges Versagen mehrerer Kanäle hervorrufen können, in ausreichendem Maße beherrscht werden. Das gilt ebenso für die Kategorie 2, da die Testeinrichtung mit ihrem eigenen Abschaltpfad ebenfalls einen zweiten Kanal darstellt. Grundsätzlich lässt sich sagen, dass viele der grundlegenden und bewährten Sicherheitsprinzipien nicht nur gegen zufällige Hardwareausfälle, sondern auch gegen systematische Ausfälle wirken, die sich irgendwann im Laufe des Produktlebenszyklus in das Produkt einschleichen können, z. B. Fehler im Produktentwurf oder bei der Modifikation.

6.2.3 Kategorie B

Die SRP/CS müssen nach den zutreffenden Normen unter Verwendung der grundlegenden Sicherheitsprinzipien für die bestimmte Anwendung so gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert werden, dass sie

- den zu erwartenden Betriebsbeanspruchungen (z. B. Zuverlässigkeit hinsichtlich ihres Schaltvermögens und ihrer Schalthäufigkeit),
- dem Einfluss des im Arbeitsprozess verwendeten Materials (z. B. aggressive chemische Substanzen, Stäube, Späne),

- anderen relevanten äußeren Einflüssen (z. B. mechanischen Erschütterungen, elektromagnetischen Störungen, Unterbrechungen oder Störungen der Energieversorgung)

standhalten können.

Bezüglich elektromagnetischer Störungen (EMV) verweist die Norm auf besondere Anforderungen in den entsprechenden Produktnormen, z. B. DIN EN 61800-3 für Antriebssysteme. Sie betont die Wichtigkeit der Anforderungen an die Störfestigkeit besonders für die funktionale Sicherheit der SRP/CS. Wenn keine Produktnorm vorhanden ist, sollen zumindest die Anforderungen der DIN EN 61000-6-2 an die Störfestigkeit befolgt werden. In Anhang K ist eine detaillierte Beschreibung zum Thema EMV und funktionale Sicherheit im Maschinenbereich zu finden.

Diese allgemeinen Grundsätze lassen sich in den in Anhang C aufgeführten grundlegenden Sicherheitsprinzipien allgemein, aber auch technologiebezogen, darstellen. Die allgemeinen grundlegenden Sicherheitsprinzipien gelten dabei vollständig für alle Technologien, während die technologiebezogenen Prinzipien zusätzlich für die jeweilige Technologie erforderlich sind. Da Kategorie B die Basiskategorie für jede andere Kategorie ist (siehe Tabelle 6.2), sind die grundlegenden Sicherheitsprinzipien generell bei der Konstruktion sicherheitsrelevanter Teile von Steuerungen und/oder Schutzeinrichtungen anzuwenden.

Tabelle 6.2:
Zusammenfassung der Anforderungen für Kategorien; die drei rechten Spalten zeigen die wesentlichen Änderungen gegenüber der Kategoriedefinition der ersten Ausgabe der Norm (EN 954-1)

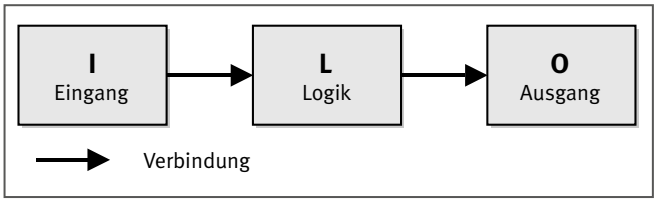
Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Kanals	DC_{avg}	CCF
B	SRP/CS(en) und/oder ihre Schutzeinrichtungen sowie ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengebaut und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können. Grundlegende Sicherheitsprinzipien müssen verwendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	überwiegend durch die Auswahl von Bauteilen charakterisiert	niedrig bis mittel	kein	nicht relevant
1	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	überwiegend durch die Auswahl von Bauteilen charakterisiert	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 getestet werden (siehe Abschnitt 6.2.14).	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Tests führen. Der Verlust der Sicherheitsfunktion wird durch den Test erkannt.	überwiegend durch die Struktur charakterisiert	niedrig bis hoch	mindestens niedrig	Maßnahmen erforderlich, siehe Anhang F
3	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass • ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und • wenn immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Sicherheitsfunktion führen.	überwiegend durch die Struktur charakterisiert	niedrig bis hoch	mindestens niedrig	Maßnahmen erforderlich, siehe Anhang F
4	Die Anforderung von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass • ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und • der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird. Wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hoher DC_{avg}). Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.	überwiegend durch die Struktur charakterisiert	hoch	hoch einschließlich der Fehleranhäufung	Maßnahmen erforderlich, siehe Anhang F

Für die Bauteile, die mit Kategorie B übereinstimmen, sind keine weitergehenden besonderen sicherheitstechnischen Maßnahmen erforderlich. Daher kann die $MTTF_D$ jedes Kanals niedrig oder mittel sein (Definition von „niedrig“ und „mittel“ siehe weiter unten). Tritt ein Bauteilausfall auf, kann er zum Verlust der Sicherheitsfunktion führen. Es sind keine Überwachungsmaßnahmen gefordert, d. h. auch kein DC_{avg}. Auch Ausfälle infolge gemeinsamer Ursache sind bei einkanaligen Steuerungen nicht relevant, daher werden keine Anforderungen hinsichtlich CCF gestellt.

Wegen dieser sehr rudimentären Widerstandsfähigkeit gegen Ausfälle ist der maximal erreichbare PL von Kategorie-B-Systemen grundsätzlich auf PL = b beschränkt.

Die vorgesehene Architektur für Kategorie B in Abbildung 6.5 entspricht einem einkanaligen System mit Eingabe- (Input I), Verarbeitungs- (Logik L) und Ausgabeebene (Output O).

Abbildung 6.5:
Vorgesehene Architektur für Kategorie B und Kategorie 1



6.2.4 Kategorie 1

Zusätzlich zu den Anforderungen für Kategorie B, z. B. Verwendung grundlegender Sicherheitsprinzipien, müssen SRP/CS der Kategorie 1 unter Verwendung sicherheitstechnisch bewährter Bauteile und Prinzipien gestaltet und gebaut werden.

Ein bewährtes Bauteil für eine sicherheitsbezogene Anwendung ist ein Bauteil, das entweder

- in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet oder
- unter Anwendung von Prinzipien, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen zeigen, hergestellt und verifiziert wurde.

In Anhang C wird eine Übersicht über bekannte sicherheitstechnisch bewährte Bauteile verschiedener Technologien gegeben.

Neuentwickelte Bauteile und die Anwendung der Sicherheitsprinzipien können als gleichwertig „bewährt“ betrachtet werden, wenn sie die zweite oben genannte Bedingung erfüllen. Die Entscheidung, ein bestimmtes Bauteil als bewährt zu akzeptieren, hängt von der Anwendung ab. Komplexe elektronische Bauteile, z. B. speicherprogrammierbare Steuerungen (SPS), Mikroprozessoren oder anwendungsspezifische integrierte Schaltungen (ASIC) dürfen generell nicht als gleichwertig zu „bewährt“ betrachtet werden.

Die Bewährtheit eines Bauteils ist abhängig von seiner Anwendung und bedeutet nur, dass ein gefahrbringender Ausfall unwahrscheinlich ist. Entsprechend ist die zu erwartende gefahrbringende Ausfallrate größer Null und geht als $MTTF_D$ in die PL-Bestimmung ein. Demgegenüber wird bei der Annahme eines Fehlerausschlusses (siehe Abschnitt 6.2.10) eine „unendliche hohe“ $MTTF_D$ unterstellt, die nicht in die Berechnung eingeht.

Wegen der erwarteten höheren Bauteilzuverlässigkeit muss die $MTTF_D$ des in Kategorie 1 nur einfach vorhandenen Kanals hoch sein, an DC_{avg} und CCF werden aber wie in Kategorie B keine Anforderungen gestellt. Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. Jedoch ist die $MTTF_D$ des Kanals in Kategorie 1 größer als in Kategorie B. Folglich ist der Verlust der Sicherheitsfunktion weniger wahrscheinlich und der maximale PL, der mit Kategorie 1 erreicht werden kann, ist PL = c.

Die vorgesehene Architektur für Kategorie 1 ist die gleiche wie für Kategorie B (siehe Abbildung 6.5), da die Unterschiede in der Bauteilzuverlässigkeit und nicht in der Struktur liegen.

6.2.5 Kategorie 2

Zusätzlich zu den Anforderungen für Kategorie B (z. B. Verwendung grundlegender Sicherheitsprinzipien) müssen SRP/CS der Kategorie 2 bewährte Sicherheitsprinzipien verwenden und so gestaltet sein, dass ihre Sicherheitsfunktionen in angemessenen Zeitabständen z. B. durch die Maschinensteuerung getestet werden. Die Sicherheitsfunktion(en) muss/müssen getestet werden

- beim Anlauf der Maschine und
- vor dem Einleiten einer Gefährdungssituation, z. B. Start eines neuen Zyklus, Start anderer Bewegungen, sobald die Sicherheitsfunktion benötigt wird und/oder periodisch während des Betriebs, wenn die Risikobeurteilung und die Betriebsart zeigen, dass dies notwendig ist.

Diese Tests können automatisch eingeleitet werden. Jeder Test der Sicherheitsfunktion(en) muss entweder

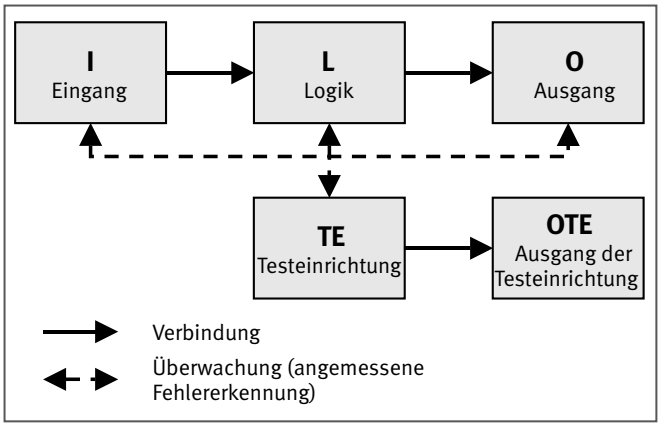
- den Betrieb zulassen, wenn keine Fehler erkannt wurden, oder
- eine Ausgabe für die Einleitung geeigneter Steuerungsmaßnahmen erzeugen (OTE), wenn ein Fehler erkannt wurde.

Grundsätzlich und für PL_r = d zwingend muss die Ausgabe (OTE) einen sicheren Zustand einleiten, der bis zur Behebung des Fehlers beibehalten wird. Bis PL_r = c kann es alternativ – wenn das Einleiten eines sicheren Zustands nicht praktikabel ist (z. B. durch Verschweißen des Kontakts des finalen Schaltglieds) – ausreichen, wenn der Ausgang der Testeinrichtung, OTE, nur eine Warnung bereitstellt.

Für die vorgesehene Architektur der Kategorie 2 (Abbildung 6.6) berücksichtigt die Berechnung der $MTTF_D$ und DC_{avg} nur die Blöcke des Funktionskanals (d. h. I, L und O). Die $MTTF_D$ der Blöcke des Testkanals (d. h. TE und OTE) geht bei Anwendung des vereinfachten Verfahrens der Norm indirekt ein, da dort vorausgesetzt wird, dass die $MTTF_D$ des Testkanals mindestens

halb so groß wie die $MTTF_D$ des Funktionskanals ist. Für die $MTTF_D$ des Funktionskanals sind Werte von niedrig bis hoch erlaubt. DC_{avg} muss mindestens niedrig sein. Ausreichende Maßnahmen gegen CCF müssen ebenfalls angewendet werden (siehe Abschnitt 6.2.15 und Anhang F).

Abbildung 6.6:
Vorgesehene Architektur für Kategorie 2; gestrichelte Linien kennzeichnen vernünftigerweise durchführbare Fehlererkennung



Der Test darf selbst nicht zu einer Gefährdungssituation führen (z. B. aufgrund einer Erhöhung der Ansprechzeit). Die Testeinrichtung darf als Bestandteil des Funktionskanals oder getrennt davon vorgesehen sein (weitere Hinweise unten). In einigen Fällen ist die Kategorie 2 nicht anwendbar, da sich der Test der Sicherheitsfunktionen nicht bei allen Bauteilen durchführen lässt. Da die Sicherheitsfunktion zwischen den Tests unbemerkt ausfallen kann, ist die Testhäufigkeit ein kritischer Parameter. Außerdem könnte die Testeinrichtung selbst früher als der Funktionskanal unbemerkt ausfallen. Bei der vereinfachten Quantifizierung des PL mithilfe der vorgesehenen Architektur und des Säulendiagramms (Abbildung 6.10, Seite 61) wird daher Folgendes vorausgesetzt:

- Der $MTTF_D$-Wert des Testkanals ist nicht kleiner als der halbe $MTTF_D$-Wert des Funktionskanals und

- die Testrate ist mindestens 100-mal höher als die mittlere Anforderungsrate der Sicherheitsfunktion (ausnahmsweise mindestens 25-mal höher, siehe Abschnitt 6.2.14) oder die Testung erfolgt unmittelbar bei Anforderung der Sicherheitsfunktion und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand (in der Regel wird die Maschine angehalten) ist kürzer als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855).

Wegen dieser Einschränkungen und weil mit der vorgesehenen Architektur in der Praxis mit externen Testeinrichtungen nur schwer ein DC_{avg} von mehr als 90 % erreicht wird, können unerkannte Erstfehler zum Verlust der Sicherheitsfunktion führen. Aus diesen Gründen wird der maximale PL, der mit Kategorie 2 erreicht werden kann, auf PL = d begrenzt.

Die Interpretation der Anforderungen an eine Kategorie 2 birgt einige Schwierigkeiten, über die teilweise nur im Einzelfall entschieden werden kann. Folgende Empfehlungen können dazu ausgesprochen werden:

- Die Norm fordert die Testung der Sicherheitsfunktion. Sofern dies nicht bei allen Bauteilen möglich ist, ist Kategorie 2 nicht anwendbar (Anmerkung 1 in DIN EN ISO 13849-1:2016, Abschnitt 6.2.5). Daraus lässt sich folgern, dass alle Komponenten des Funktionskanals getestet werden müssen. Der Funktionskanal umfasst alle Bauelemente, die mit mindestens einer Ausfallart den Ausfall der Sicherheitsfunktion bewirken können. Nach Norm muss DC_{avg} für den Funktionskanal mindestens niedrig sein.

- Die „Testung der Sicherheitsfunktion“ ist nicht immer als Testung des Funktionskanals „in einem Zug“ möglich. Idealerweise erfolgt diese aktiv durch die Testeinrichtung selbst oder die Testeinrichtung verfolgt passiv durch eigene Bauelemente die Abarbeitung der Sicherheitsfunktion. Im passiven Fall muss eine ausreichende Testhäufigkeit durch die Applikation sichergestellt werden. Alternativ können aber auch die Blöcke (I, L, O) oder Bauteile im Funktionskanal einzeln überwacht werden, wobei die Diagnose immer möglichst nah an der „echten Ausführung der Sicherheitsfunktion“ bleiben sollte.

- Der Hinweis „Die Testeinrichtung darf als Bestandteil des Funktionskanals oder getrennt davon vorgesehen sein.“ bedeutet, dass zwar durchaus ausführende Elemente der Testeinrichtung im Funktionskanal angesiedelt sein dürfen, z. B. in einem aus Elektronik bestehenden SRP/CS. Der die Diagnosebefunde bewertende Teil der Testeinrichtung muss jedoch typischerweise extern zum Funktionskanal, z. B. als separater Watchdog realisiert werden. Nur so können die Anforderungen zur Unabhängigkeit von Funktionskanal und Testkanal erfüllt werden. Die Diagnoseinformation für die Testeinrichtung sollte möglichst aussagefähig in Bezug auf die sicherheitsbezogene Funktionsfähigkeit der überwachten Teile des Funktionskanals sein. Sie sollte daher eine gewisse Mindestkomplexität aufweisen, sodass die Testeinrichtung eine fundierte Entscheidung über die Funktionsfähigkeit treffen kann. Die komplette Verschmelzung von TE mit dem Funktionskanal ist nicht akzeptabel, z. B. bei einem On-Chip-Watchdog ohne Trennung nach DIN EN 61508-2, Anhang E (Besondere Architekturanforderungen an integrierte Schaltkreise mit On-Chip-Redundanz) oder bei einer Testeinrichtung, die nur durch Software realisiert ist und über ein per Software generiertes Abschaltsignal direkt auf OTE zugreift.

- Abschnitt 6.2.14 und Anhang E geben weitere Hinweise, speziell auch zur erforderlichen Testhäufigkeit, zur Zuverlässigkeit der Testeinrichtung, zur Einleitung der Tests (automatisch, manuell, bei Anforderung der Sicherheitsfunktion) und zu Diagnosemaßnahmen.

6.2.6 Kategorie 3

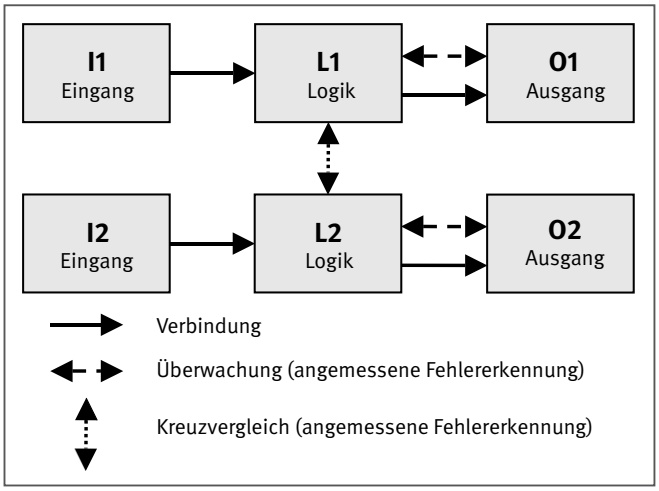
Zusätzlich zu den Anforderungen für Kategorie B (z. B. Verwendung grundlegender Sicherheitsprinzipien) müssen SRP/CS der Kategorie 3 bewährte Sicherheitsprinzipien verwenden und so gestaltet werden, dass ein einzelner Fehler nicht zum Verlust der

Sicherheitsfunktion führt. Wann immer in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

Für die $MTTF_D$ jedes Kanals sind Werte von niedrig bis hoch auswählbar. Da nicht alle Fehler erkannt werden müssen oder die Fehleranhäufung unerkannter gefahrbringender Fehler zu einer Gefährdungssituation führen kann, reicht minimal ein niedriger DC_{avg}. Zur Frage der Testhäufigkeit siehe Abschnitt 6.2.14. Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) müssen angewendet werden.

Die Forderung nach Einfehlersicherheit bedeutet nicht zwangsweise eine Realisierung als zweikanaliges System, da z. B. auch einkanalige Teile ohne gefahrbringendes Ausfallpotenzial (fehlersicheres Design) sicher gegen Einzelfehler sein können. Dasselbe gilt für Systeme mit hochwertiger Überwachung, die durch einen eigenen Abschaltpfad eine Fehlerreaktion so schnell einleiten, dass ein gefährlicher Zustand vermieden wird. Trotzdem werden Kategorie-3-Systeme überwiegend zweikanalig realisiert, weshalb auch die zugehörige vorgesehene Architektur entsprechend gewählt wurde (Abbildung 6.7). Eine rein „logische Zweikanaligkeit“, z. B. durch redundante Software auf einkanaliger Hardware, wird allerdings in der Regel nicht einfehlersicher gegen Hardwareausfälle sein.

Abbildung 6.7:
Vorgesehene Architektur für Kategorie 3: gestrichelte Linien kennzeichnen vernünftigerweise durchführbare Fehlererkennung



6.2.7 Kategorie 4

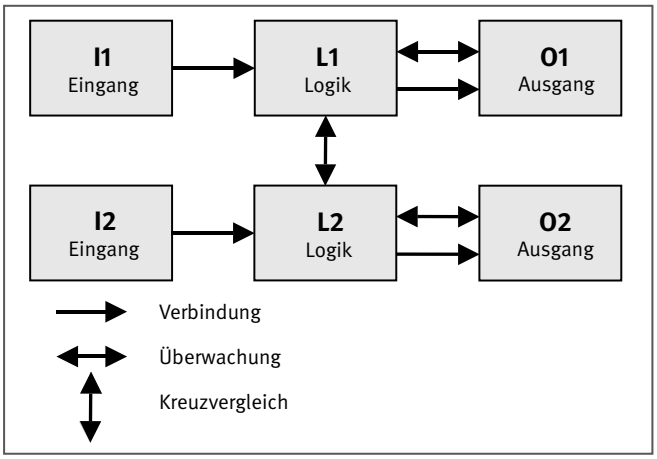
Zusätzlich zu den Anforderungen für Kategorie B (z. B. Verwendung grundlegender Sicherheitsprinzipien) müssen SRP/CS der Kategorie 4 bewährte Sicherheitsprinzipien verwenden und so gestaltet werden, dass

- ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion führt und
- der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird, z. B. unmittelbar beim Einschalten oder am Ende eines Maschinenzyklus. Ist diese Erkennung nicht möglich, dann darf die Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen (in der Praxis kann die Betrachtung einer Fehlerkombination für zwei Fehler ausreichend sein).

Da es sich um die Kategorie mit der höchsten Widerstandsfähigkeit gegen Fehler handelt (höchster Beitrag zur Risikoreduzierung), müssen sowohl die $MTTF_D$ jedes Kanals als auch der DC_{avg} hoch sein (zur Frage der Testhäufigkeit siehe Abschnitt 6.2.14.) und ausreichende Maßnahmen gegen CCF angewendet werden.

Weil die Unterschiede zur Kategorie 3 primär in der $MTTF_D$ und im DC_{avg} liegen, ist die vorgesehene Architektur für Kategorie 4 (Abbildung 6.8) ähnlich derjenigen für Kategorie 3. Allerdings symbolisieren die durchgezogenen Linien für die Überwachung den höheren DC_{avg}.

Abbildung 6.8:
Vorgesehene Architektur für Kategorie 4



6.2.8 Blöcke und Kanäle

Zur vereinfachten Quantifizierung der Ausfallwahrscheinlichkeit ist eine Darstellung der sicherheitsrelevanten Steuerung in Form von abstrahierten Blöcken und Kanälen hilfreich. Die Bezeichnung „Blöcke“ hat in diesem Zusammenhang eine eigene, feststehende Bedeutung. Es handelt sich hier um Funktionsblöcke nur in dem Sinne, dass die Sicherheitsfunktion in kleineren, seriell und parallel angeordneten Einheiten ausgeführt wird. Für die Abbildung der Hardwarestruktur auf ein sicherheitsbezogenes Blockdiagramm können folgende Regeln gelten:

- Die Blöcke sollen in abstrakter Form alle Steuerungsbauteile abbilden, die sich auf die Ausführung der Sicherheitsfunktion beziehen.
- Wird die Sicherheitsfunktion in mehreren redundanten Kanälen ausgeführt, sollen diese in separaten Blöcken dargestellt werden. Dies spiegelt die Tatsache wider, dass bei Ausfall eines Blocks die Ausführung der Sicherheitsfunktion durch die Blöcke des anderen Kanals nicht beeinträchtigt wird.
- Die Aufteilung der Blöcke innerhalb eines Kanals ist eher willkürlich; zwar schlägt DIN EN ISO 13849-1 pro Kanal drei Blöcke vor (Eingangsebene I, Logikebene L und Ausgangsebene O),

dies ist aber mehr als Verständnishilfe gedacht. Weder die genaue Grenze zwischen I, L und O noch die Anzahl der Blöcke in einem Kanal haben signifikante Auswirkungen auf die in Form des PL berechnete Ausfallwahrscheinlichkeit.

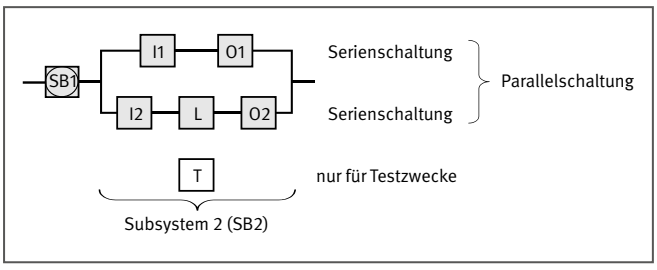
- Für jede sicherheitsrelevante Hardwareeinheit soll die Blockzugehörigkeit eindeutig festgelegt sein, z. B. als Stückliste. Dies erlaubt die Berechnung der mittleren Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$) des Blocks, basierend auf der $MTTF_D$ der Hardwareeinheiten, die zu diesem Block gehören (z. B. durch die Ausfalleffektanalyse FMEA oder das „Parts Count"-Verfahren, siehe Abschnitt 6.2.13).

- Nur rein zu Testzwecken verwendete Hardwareeinheiten, deren Ausfall die Ausführung der Sicherheitsfunktion in den verschiedenen Kanälen nicht direkt beeinträchtigen kann, können als separater Block zusammengefasst werden. Die Norm stellt für die Kategorien 3 und 4 keine direkten Anforderungen an dessen Zuverlässigkeit, aber in Anlehnung an Kategorie 2 kann als Richtschnur gelten, dass dieser mindestens die halbe $MTTF_D$ des einzelnen (symmetrisierten, siehe unten) Kanals haben sollte, und auch systematische Ausfälle und CCF sollten berücksichtigt werden.

6.2.9 Sicherheitsbezogenes Blockdiagramm

Das sicherheitsbezogene Blockdiagramm ist dem bekannteren Zuverlässigkeitsblockdiagramm [33] entlehnt. Gemeinsam ist beiden das Prinzip, dass die (Sicherheits-)Funktion so lange ausgeübt werden kann, wie von links nach rechts entlang der funktionalen Verbindungslinien eine Kette nicht gefährlich ausgefallener Blöcke besteht. Das sicherheitsbezogene Blockdiagramm stellt aber zusätzlich Testmechanismen dar, z. B. den Kreuzvergleich redundanter Kanäle oder Tests durch separate Testeinheiten. Ein allgemeines Beispiel eines sicherheitsbezogenen Blockdiagramms ist in Abbildung 6.9 gezeigt.

Abbildung 6.9:
Allgemeines Beispiel eines sicherheitsbezogenen Blockdiagramms; I1 und O1 bilden den ersten Kanal (Serienschaltung), während I2, L und O2 den zweiten Kanal bilden (Serienschaltung); mit beiden Kanälen wird die Sicherheitsfunktion redundant ausgeführt (Parallelschaltung); T wird nur für die Testung verwendet



Gemäß dieser Definition lassen sich folgende Regeln für die Darstellung einer Sicherheitssteuerung als sicherheitsbezogenes Blockdiagramm aufstellen:

- Die Serienschaltung von Blöcken als sogenannter „Kanal" (z. B. I, L und O) bringt zum Ausdruck, dass der Ausfall eines Blocks zu einem Ausfall der gesamten Kette führen kann. Fällt z. B. eine Hardwareeinheit in einem Kanal gefährlich aus, kann der gesamte Kanal die Sicherheitsfunktion nicht weiter ausführen.

- Die Parallelschaltung von Blöcken bzw. Kanälen symbolisiert die mehrfach redundante Ausführung der Sicherheitsfunktion oder entsprechender Teile davon. Zum Beispiel wird eine durch mehrere Kanäle ausgeführte Sicherheitsfunktion aufrechterhalten, solange mindestens ein Kanal keinen Ausfall hat.

- Nur für Testzwecke verwendete Blöcke, die bei ihrem Ausfall die Ausführung der Sicherheitsfunktion in den verschiedenen Kanälen nicht beeinträchtigen, können als separater Testkanal dargestellt werden. Zwar wird durch den Ausfall von Testmaßnahmen die Zuverlässigkeit des Systems insgesamt herabgesetzt, dies hat aber zunächst nur einen geringen Einfluss, solange die Abarbeitung der reinen Sicherheitsfunktion in den einzelnen Kanälen weiter gewährleistet bleibt.

Die Definition der Blöcke und Kanäle geht einher mit der Bestimmung der Kategorie und ist der erste Schritt bei der quantitativen Bestimmung des PL. Dazu werden weitere Kennwerte benötigt: die Bewertung der Bauteilzuverlässigkeit ($MTTF_D$), der Tests (DC_{avg}) und der Relevanz von Ausfällen infolge gemeinsamer Ursache (CCF). Weitere Hinweise auf dem Weg „vom Schaltbild zum Performance Level", speziell zur Ableitung des sicherheitsbezogenen Blockdiagramms, finden sich im SISTEMA-Kochbuch 1 [34]. Dort wird auch die Bezeichnung des „gekapselten Subsystems" eingeführt. Dieses bezeichnet ein Subsystem, für das der Hersteller bereits PL, PFH_D und Kategorie angibt und dessen genaue interne Struktur und Kennwerte nicht transparent sind. Diese Kennwerte setzen die Einhaltung der vom Hersteller spezifizierten Einsatzbedingungen voraus, dazu kann z. B. extern zu realisierende Diagnose gehören. Im sicherheitsbezogenen Blockdiagramm wird es auf Subsystemebene einkanalig als Kreis in einem Block (siehe Subsystem „SB1" in Abbildung 6.9) dargestellt, in die quantitative Bestimmung des PL geht es nur mit seinen Kennwerten PFH_D und PL ein, die Angabe der Kategorie ist informativ.

6.2.10 Fehlerbetrachtungen und Fehlerausschluss

In einer realen Steuerung ist die Zahl theoretisch möglicher Fehler schier unbegrenzt. Es ist daher notwendig, sich bei der Bewertung auf die relevanten Fehler zu beschränken. Bestimmte Fehler können ausgeschlossen werden, wenn Folgendes berücksichtigt wird:

- die technische Unwahrscheinlichkeit ihres Auftretens (um Größenordnungen geringere Wahrscheinlichkeit im Verhältnis zu anderen möglichen Fehlern und der zu erreichenden Risikoreduzierung)

- die allgemein anerkannte technische Erfahrung, unabhängig von der betrachteten Anwendung, und

- die technischen Anforderungen in Bezug auf die Anwendung und auf die spezielle Gefährdung

Welche Bauteilfehler auftreten können und welche Fehler ausgeschlossen werden können, erläutert DIN EN ISO 13849-2. Dabei sind folgende Punkte zu beachten:

- Die Fehlerlisten stellen nur eine Auswahl dar, daher müssen – wenn notwendig – neue Fehlermodelle erstellt werden (z. B. bei neuen Komponenten) oder je nach Applikation weitere Fehlerarten berücksichtigt werden. Dies ergibt sich z. B. auf der Grundlage einer FMEA.

- Folgefehler werden zusammen mit dem auslösenden Erstfehler als ein einzelner Fehler bewertet, genauso wie Mehrfachfehler, die eine gemeinsame Ursache haben (CCF, Common Cause Failure).

- Das gleichzeitige Auftreten von zwei oder mehreren Fehlern unterschiedlicher Ursache gilt als höchst unwahrscheinlich und braucht deswegen nicht betrachtet zu werden.

Weitere Informationen zum Fehlerausschluss finden sich in Anhang C und im Teil 2 der DIN EN ISO 13849. Wenn Fehler ausgeschlossen werden, bei denen der Ausschluss nicht unmittelbar einleuchtet (z. B. das Ablösen von Leiterbahnen bei richtig dimensioniertem Platinenlayout), muss eine genaue Begründung in der technischen Dokumentation gegeben werden.

Fehlerausschlüsse sind bei entsprechenden Voraussetzungen auch für Komponenten möglich, z. B. für die elektrischen Öffnerkontakte und die mechanische Betätigung von elektromechanischen Positionsschaltern oder Not-Halt-Geräten. Die Gültigkeit von Fehlerausschlüssen kann dabei auf niedrige PL begrenzt sein, siehe z. B. Tabelle D.8 der DIN EN ISO 13849-2 und Anhang D dieses Reports. Für diese Komponenten ist bei Fehlerausschluss keine Berücksichtigung von Ausfallraten ($MTTF_D$) und Überwachungsmaßnahmen (DC) notwendig.

6.2.11 Mittlere Zeit bis zum gefahrbringenden Ausfall – $MTTF_D$

Die Zuverlässigkeit der einzelnen Komponenten, aus denen die Steuerung aufgebaut wird, geht entscheidend in die Gesamtzuverlässigkeit des Systems ein. Als Zuverlässigkeitskennwert fließt daher die sogenannte mittlere Zeit bis zum gefahrbringenden Ausfall $MTTF_D$ (Mean Time to Dangerous Failure) in den PL mit ein. Dass es hier um Ausfälle geht, also Bauteildefekte, die zu einer Nicht-(Mehr-)Ausführung der vorgesehenen Funktion führen, ist klar ersichtlich. Die anderen Namensbestandteile bedürfen allerdings einiger Erläuterung:

- „Mittlere“ weist darauf hin, dass es sich um einen statistischen Mittelwert handelt, der sich nicht auf ein Einzelbauteil bezieht, sondern als Erwartungswert der mittleren Lebensdauer des typischen Bauteils definiert ist. Der Erwartungswert des Einzelbauteils kann dabei dem Mittelwert einer Vielzahl gleichartiger Bauteile gleichgestellt werden. Es handelt sich also nicht um eine garantierte Mindestlebensdauer im Sinne einer ausfallfreien Zeit. Diese gemittelte Sichtweise schlägt sich auch darin nieder, dass üblicherweise keine Anpassung der Lebensdauerwerte an die Einsatzbedingungen (z. B. Last, Temperatur, Klima) erfolgt – solange die Bauteile innerhalb ihrer spezifizierten Einsatzbedingungen eingesetzt werden. Hier geht man üblicherweise davon aus, dass die höhere Belastung in einer Anwendung eines Geräts durch eine niedrigere Belastung in einer anderen Applikation wieder ausgemittelt wird. Sind allerdings in allen Anwendungen erhöhte Belastungen – z. B. durch extreme Temperatur – zu erwarten, so müssen diese Bedingungen bei der Bestimmung der $MTTF_D$ berücksichtigt werden.

- „Zeit“ legt nahe, dass die Zuverlässigkeit als Zeit im Sinne einer Lebensdauer angegeben wird. Üblicherweise wird die $MTTF_D$ in Jahren (abgekürzt „a“) angegeben. Andere Notationsformen, die in eine $MTTF_D$ umgerechnet werden können, sind z. B. Ausfallraten oder Schaltspiele. Ausfallraten werden üblicherweise mit dem kleinen griechischen Buchstaben λ (Lambda) bezeichnet und in der Einheit „FIT“ ($= 10^{-9}/h$, d. h. Ausfälle in einer Milliarde Bauteilstunden) notiert. Die Beziehung zwischen λ_D und $MTTF_D$ ist bei einer über die Lebensdauer konstanten Ausfallrate λ_D mit $MTTF_D = 1/\lambda_D$ gegeben, wobei die Umrechnung von Stunden auf Jahre natürlich zu berücksichtigen ist. Bei Bauteilen, die überwiegend durch ihre mechanische Betätigung verschleißen, ist es üblich, die Zuverlässigkeit in Schaltspielen, z. B. als B_{10D}-Wert anzugeben, d. h. die mittlere Anzahl von Zyklen, nach der 10 % der Bauteile gefährlich ausfallen. Hier kann eine Umrechnung in $MTTF_D$ durch Einbeziehen der in der Anwendung zu erwartenden mittleren Anzahl jährlicher Betätigungen n_{op} (Number of Operations) erfolgen. Mehr Einzelheiten dazu finden sich im Anhang D.

- „Gefahrbringend“ stellt klar, dass nur solche Ausfälle, die das Ausführen der Sicherheitsfunktion beeinträchtigen, letztlich in den PL einfließen (Ausfall zur unsicheren Seite). Im Gegensatz dazu können ungefährliche Ausfälle zwar den sicheren Zustand provozieren (Betriebshemmung) oder die Verfügbarkeit oder Produktivität einer Maschine herabsetzen, weiterhin wird aber die Sicherheitsfunktion erfolgreich ausgeführt oder der sichere Zustand eingeleitet bzw. aufrechterhalten. In redundanten Strukturen bezieht sich das Attribut „gefahrbringend“ allerdings auf jeden einzelnen Kanal. Führt ein Ausfall in einem Kanal zu einem Außerkraftsetzen der Sicherheitsfunktion, so wird dieser Ausfall als gefahrbringend bezeichnet, selbst wenn ein weiterer Kanal die Sicherheitsfunktion noch erfolgreich ausführen kann.

Sowohl ein einzelnes Bauelement – z. B. ein Transistor, Ventil oder Schütz – als auch ein Block, ein Kanal oder die Steuerung insgesamt kann eine $MTTF_D$ besitzen. Diese Gesamt-$MTTF_D$ versteht sich als – unter Umständen über mehrere Kanäle symmetrisierter – Wert für einen Kanal und basiert auf der $MTTF_D$ aller an den SRP/CS beteiligten Bauteile. Nach dem Bottom-up-Prinzip wird dazu sukzessive die betrachtete Einheit vergrößert. Zur Minimierung des Aufwands ist es oft hilfreich, dass nur sicherheitsrelevante Bauteile in die Betrachtung einbezogen werden, d. h. solche, deren Ausfälle die Ausführung der Sicherheitsfunktion mittelbar oder unmittelbar negativ beeinflussen können. Zur Erleichterung sind zusätzlich Fehlerausschlüsse möglich, die der Tatsache Rechnung tragen, dass bestimmte Ausfälle extrem unwahrscheinlich sind und ihr Beitrag zur Gesamtzuverlässigkeit vernachlässigbar klein ist. Allerdings ist die Annahme von Fehlerausschlüssen an Bedingungen geknüpft, die im Detail in DIN EN ISO 13849-2 niedergelegt und im Abschnitt 6.2.10 näher beschrieben sind. Demnach können unter bestimmten Voraus-

setzungen z. B. Leitungskurzschlüsse oder bestimmtes mechanisches Versagen aufgrund der Konstruktion ausgeschlossen werden.

6.2.12 Datenquellen für Einzelbauteile

Eine der in diesem Zusammenhang meistgestellten Fragen betrifft die Beschaffung verlässlicher Ausfalldaten für die sicherheitsrelevanten Komponenten. Hier ist der Hersteller z. B. mit seinem technischen Datenblatt allen anderen Quellen vorzuziehen. Viele Komponentenhersteller, z. B. in der Elektromechanik oder Pneumatik, stellen solche Daten mittlerweile zur Verfügung. Aber auch wenn es keine Herstellerangaben gibt, lassen sich typische Beispielwerte aus etablierten Datensammlungen (siehe Anhang D) ermitteln. Da dort allerdings meist nicht zwischen ungefährlichen und gefahrbringenden Ausfällen unterschieden wird, kann als einfache Näherung davon ausgegangen werden, dass im Mittel nur die Hälfte aller Ausfälle gefahrbringend ist. Im Bewusstsein der Verfügbarkeitsproblematik für Zuverlässigkeitswerte listet DIN EN ISO 13849-1 einige typische Werte auf, die allerdings sehr konservativ abgeschätzt sind und daher nur sinnvoll verwendet werden können, wenn die vorgenannten Datenquellen nicht verfügbar sind. Neben $MTTF_D$-Werten für mechanische, hydraulische und elektronische Komponenten finden sich hier B_{10D}-Werte für pneumatische und elektromechanische Komponenten. Einzelheiten dazu sind in Anhang D beschrieben.

Eine komfortable Quelle für Zuverlässigkeitsdaten von Bauteilen, die für den Einsatz in sicherheitsgerichteten Steuerungen gedacht sind, sind die in großer Zahl verfügbaren SISTEMA-Bibliotheken (siehe Anhang H). Hier sind sowohl $MTTF_D$- oder B_{10D}-Werte für Elemente und Bauteile zu finden als auch PL- und PFH_D-Werte für ganze Subsysteme.

6.2.13 FMEA versus „Parts Count"-Verfahren

Sind die $MTTF_D$-Werte aller sicherheitsrelevanten Bauteile zusammengetragen, helfen einige simple Regeln, daraus den $MTTF_D$-Kennwert der Steuerung zu berechnen. Dabei gibt es verschiedene Methoden – aufwendig durch eine genaue Ausfalleffektanalyse FMEA (Failure Modes and Effects Analysis) oder schnell und einfach nach dem „Parts Count"-Verfahren mit ein paar Abschätzungen zur sicheren Seite. Dies beginnt schon bei dem kleinen Unterschied zwischen *MTTF* und $MTTF_D$: Wie groß ist der gefährliche Anteil der Ausfälle eines bestimmten Bauelements? In einer aufwendigen FMEA können alle denkbaren Ausfallarten aufgelistet, jeweils als „ungefährlich" oder „gefahrbringend" bewertet und in der anteiligen Häufigkeit ihres Auftretens geschätzt werden. Da die Auswirkungen eines Bauteilausfalls auf den Block über die sichere oder unsichere Ausfallrichtung entscheiden, sind unter Umständen detaillierte Analysen des von einem Ausfall hervorgerufenen Effekts nötig. Dafür entpuppen sich vielleicht mehr Ausfallarten als „sicher" als bei einer vereinfachten Bewertung, wie DIN EN ISO 13849-1 sie vorschlägt: Beim „Parts Count"-Verfahren wird mit einem konservativen Ansatz pauschal davon ausgegangen, dass sich ungefährliche und gefahrbringende Anteile die Waage halten. Daher wird die $MTTF_D$ hier immer als doppelt so groß angenommen wie die *MTTF* – sofern keine genaueren Informationen vorliegen.

Grundlage ist wieder das Prinzip des statistischen Mittels, d. h. eine zu günstige Bewertung eines Bauelements wird durch eine zu pessimistische eines anderen Bauelements wettgemacht. Es ist durchaus möglich, das „Parts Count"-Verfahren und eine FMEA zu kombinieren. Dort, wo die Werte allein durch „Parts Count" zu einer ausreichend kleinen PFH führen, muss keine FMEA vorgenommen werden. Gelingt es jedoch nicht, dann ist insbesondere an den Bauteilen, die schlechtere $MTTF_D$-Werte aufweisen, eine Untersuchung der Ausfallrichtungen hilfreich, z. B. durch eine partielle FMEA. Weitere Erläuterungen zu diesem Thema finden sich in Anhang B.

So wie bei anderen Methoden der Quantifizierung wird bei der Bewertung nach DIN EN ISO 13849-1 allen $MTTF_D$-Werten eine konstante Ausfallrate während der Einsatzdauer des Bauteils unterstellt. Selbst wenn dies, z. B. bei stark verschleißbehafteten Bauteilen, nicht direkt dem Ausfallverhalten entspricht, so wird dennoch durch eine Abschätzung zur sicheren Seite eine solche $MTTF_D$ als Näherungswert bestimmt, die während der Gebrauchsdauer des Bauteils Gültigkeit hat. Üblicherweise werden Frühausfälle vernachlässigt, da Komponenten mit ausgeprägten Frühausfällen den Verfügbarkeitsanforderungen an eine Maschinensteuerung nicht gerecht werden und daher im Markt nur eine geringe Rolle spielen. Dieses Vorgehen hat den Vorteil, dass die $MTTF_D$ immer gleich dem Kehrwert der zugehörigen gefährlichen Ausfallrate λ_D ist. Da sich die gefahrbringenden Ausfallraten λ_D der Bauteile in einem Block einfach aufsummieren, ergibt sich aus dem $MTTF_D$-Werten der beteiligten Bauteile (N Bauteile mit Laufindex i) in folgender Weise die $MTTF_D$ des Blocks:

$$\lambda_D = \sum_{i=1}^{N} \lambda_{Di} \text{ bzw.} \frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}} \quad (1)$$

Derselbe Zusammenhang gilt auch für die Ermittlung der $MTTF_D$ jedes Kanals aus den $MTTF_D$-Werten der zugehörigen Blöcke. Steht die $MTTF_D$ für jeden Kanal fest, so tritt eine weitere Vereinfachung in Form einer Klassenbildung in Kraft. Die ermittelten Werte werden in drei typische Klassen eingeteilt (Tabelle 6.3).

Tabelle 6.3:
Klasseneinteilung der $MTTF_D$ jedes Kanals

$MTTF_D$ für jeden Kanal	
Bezeichnung	**Bereich**
Nicht angemessen	0 Jahre ≤ $MTTF_D$ < 3 Jahre
Niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
Mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
Hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre
nur in Kategorie 4 zulässig	100 Jahre < $MTTF_D$ ≤ 2 500 Jahre

Weniger als drei Jahre mittlere (nicht garantierte!) Lebensdauer wird für Komponenten der Sicherheitstechnik als nicht angemessen betrachtet. Mehr als 100 Jahre dürfen nur bei Kategorie 4 in Rechnung gestellt werden, um die Bauteilzuverlässigkeit gegenüber den anderen wichtigen Einflussgrößen wie Struktur oder

Tests nicht überzubewerten. Ergeben sich tatsächlich für einen Kanal weniger als drei Jahre, sollten die Bauteile durch solche mit höherer Zuverlässigkeit ausgetauscht werden, da sonst nicht einmal PL a erreicht werden kann. Mehr als 100 Jahre mittlere Lebensdauer sind nicht unüblich, tragen aber wegen der „Kappung" nicht mehr zum PL bei, da in der Bauteilzuverlässigkeit bereits der Höchstwert von 100 Jahren (in Kategorie 4 liegt der Höchstwert bei 2500 Jahren) in Rechnung gestellt wird.

Sind mehrere Kanäle an einer Steuerung beteiligt, so ist zunächst nicht klar, welcher Wert stellvertretend für das ganze System herangezogen werden soll. Natürlich könnte man hier vorsichtigerweise den kleineren Wert nehmen, zu immer noch sicheren, aber besseren Ergebnissen führt allerdings folgende Mittelungsformel (C1 und C2 bezeichnen hierbei die beiden Kanäle, die symmetrisiert werden):

$$MTTF_D = \frac{2}{3}\left(MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right) \quad (2)$$

Bei ausgeglichenen Kanälen entspricht der so ermittelte $MTTF_D$-Kennwert der $MTTF_D$ eines Kanals. Bei unausgewogenen Kanälen ergibt sich eine mittlere $MTTF_D$, die minimal zwei Drittel des besseren Wertes betragen kann. Hier kann zusätzlich der Effekt auftreten, dass der bessere Kanal vorher auf 100 Jahre (bei Kategorie 4 sind es 2500 Jahre) $MTTF_D$ gekappt wurde und der symmetrisierte Wert dadurch weniger als 100 Jahre bzw. 2500 Jahre beträgt. Es ist daher in der Regel effektiver, möglichst Kanäle ausgeglichener Zuverlässigkeit zu realisieren. Das Resultat dieses Verfahrens ist in jedem Fall, unabhängig von der Zahl und Ausführung der Kanäle, ein auf einen einzigen Steuerungskanal bezogener $MTTF_D$-Kennwert, der – über die Steuerung gemittelt – das Niveau der Bauteilzuverlässigkeit angibt.

6.2.14 Diagnosedeckungsgrad von Test- und Überwachungsmaßnahmen – *DC*

Eine weitere einflussreiche Größe für den PL sind die (Selbst-) Test- und Überwachungsmaßnahmen in SRP/CS. Durch wirksame Tests lässt sich z. B. eine schlechte Zuverlässigkeit der Komponenten teilweise kompensieren. Die Güte der Tests wird in DIN EN ISO 13849-1 mit dem sogenannten Diagnosedeckungsgrad *DC* (Diagnostic Coverage) gemessen. Der *DC* ist definiert als Anteil der erkannten gefahrbringenden Ausfälle an allen denkbaren gefahrbringenden Ausfällen, wobei die Bezugsgröße eine Komponente, ein Block oder das gesamte SRP/CS sein kann. Im letzteren Fall handelt es sich um den durchschnittlichen Diagnosedeckungsgrad DC_{avg} (average), der bei der vereinfachten Bestimmung des PL mit dem Säulendiagramm eine wichtige Rolle spielt.

Wie an vielen Stellen in der Norm gibt es wieder einen genaueren, aber aufwendigeren, und einen einfachen Weg zur Bestimmung des DC_{avg}, der von einer Reihe Abschätzungen zur sicheren Seite lebt. Der genaue, aufwendige Weg führt über eine Ausfalleffektanalyse (FMEA) und orientiert sich an der DC-Definition. Dabei werden für jedes Bauteil die erkennbar gefahrbringenden DD (dangerous detectable) bzw. unerkennbar gefahrbringenden DU (dangerous undetectable) Ausfallarten und ihr Anteil an der Gesamtausfallrate des Bauteils bestimmt. Durch Summation und Verhältnisbildung ergibt sich schließlich der DC-Wert der entsprechenden Betrachtungseinheit:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{\sum \lambda_{DD}}{\sum \lambda_{D}} \quad (3)$$

Der von DIN EN ISO 13849-1 favorisierte Weg beruht auf einer begründeten konservativen Schätzung des *DC* direkt auf Bauteil- oder Blockebene und der anschließenden Berechnung des DC_{avg} aus den einzelnen DC-Werten über eine Mittelungsformel. Viele Tests lassen sich typischen Standardmaßnahmen zuordnen, für die in Anhang E der Norm DC-Schätzwerte gelistet sind. Diese Maßnahmen sind in ein grobes Raster aus vier Eckwerten (0, 60, 90 und 99 %) eingeordnet. Eine ausführliche Liste der in der Norm genannten typischen Testmaßnahmen findet sich in Anhang E, die Anwendung ist u. a. im Beispiel einer Planschneidemaschinensteuerung (siehe Abschnitt 6.5) erläutert.

Bei der Bestimmung des *DC* einer Komponente oder eines Blocks sind verschiedene Randbedingungen zu beachten:

- Die Erkennung eines gefahrbringenden Ausfalls ist nur der Anfang. Zum erfolgreichen Abschluss eines Tests ist die rechtzeitige Einleitung eines sicheren Zustands, aus dem heraus keine Gefährdung mehr besteht, erforderlich. Dazu gehört ein wirksamer Abschaltpfad, was z. B. bei einkanalig getesteten Systemen (Kategorie 2) dazu führt, dass ein zweites Abschaltelement vorhanden sein muss. Dieses ist nötig, um den sicheren Zustand einzuleiten bzw. aufrechtzuerhalten, wenn der Test ein Versagen des regulären Abschaltelements (Block „O" im sicherheitsbezogenen Blockdiagramm) festgestellt hat. Nur bei niedrigem Risiko (bis PL_r = c) und wenn das Einleiten eines sicheren Zustands nicht möglich ist (z. B. durch Verschweißen des Kontakts des finalen Schaltglieds), kann es in Kategorie 2 ausreichen, wenn der Ausgang der Testeinrichtung, OTE, nur eine Warnung bereitstellt.

- Sowohl das Auslösen eines Tests, dessen Ausführung als auch die erforderliche Abschaltung sollten bevorzugt automatisch von SRP/CS durchgeführt werden. Nur in Ausnahmefällen ist es akzeptabel, hier auf eine manuelle Intervention, z. B. der Bedienperson einer Maschine, angewiesen zu sein. Denn die Praxis zeigt leider oft, dass die erforderlichen Maßnahmen aus Bequemlichkeit, wegen Arbeitsdrucks oder fehlerhafter Information bzw. Organisation nicht ausreichend umgesetzt werden. Hier ist eine enge Einbindung in den Arbeitsprozess oder ein hoher organisatorischer Aufwand und Disziplin nötig, um manuelle Tests wirksam umzusetzen. Gleichwohl berücksichtigt die Bestimmung des *DC* die Fehleraufdeckung bei Anforderung der Sicherheitsfunktion, d. h., es werden nicht nur automatisch ausgelöste Tests in programmierbarer Elektronik betrachtet. Gerade bei elektromechanischen Bauteilen, z. B. Relais oder Schützen, kann eine Erkennung des Fehlers „Nichtabfall" üblicherweise nur bei Anforderung der Sicherheitsfunktion erfolgen. Für die Fehleraufdeckung bei Anforderung muss die Häufigkeit der Anforderung der Sicherheitsfunktion berücksichtigt werden, um eine

ausreichende Testhäufigkeit, wie im nächsten Spiegelstrich beschrieben, zu gewährleisten.

- Ein weiterer Aspekt ist die Frage nach der notwendigen Testhäufigkeit. Ein Test, der zu selten ausgeführt wird, wird unter Umständen durch das Eintreten eines Gefährdungsereignisses überholt und bietet damit nur trügerische Sicherheit. Als Faustregel gilt: Die Testhäufigkeit konkurriert immer mit anderen Häufigkeiten, daher kann eine ausreichende Häufigkeit nicht generell genannt werden. Außerdem dienen Tests nicht nur zur Aufdeckung zufälliger, sondern auch systematischer Ausfälle.

  Beim einkanalig getesteten System der Kategorie 2 muss der Test erfolgreich sein, bevor die nächste Anforderung der Sicherheitsfunktion – also eine potenzielle Gefährdung – erfolgt. Hier steht die Testhäufigkeit also in Konkurrenz zur Häufigkeit der Anforderung der Sicherheitsfunktion. In diesem Fall wird ein Faktor von 100 als ausreichend angesehen, also eine mindestens 100-mal höhere Testrate als die mittlere Anforderungsrate der Sicherheitsfunktion. Bis hinunter zu einem Faktor von 25 ergibt sich demgegenüber eine maximale Erhöhung der Ausfallwahrscheinlichkeit von ca. 10 % (siehe auch Abschnitt 4 in [32]). Darunter ist es wesentlich von der Synchronisation von Anforderung und Testung abhängig, ob die Testung überhaupt zur Geltung kommt. Falls in einkanalig getesteten Systemen allerdings der Test gleichzeitig mit der Anforderung der Sicherheitsfunktion so schnell ausgeführt wird, dass der sichere Zustand erreicht wird, bevor es zu einer Gefährdung kommt, dann werden keine Bedingungen an die Testhäufigkeit gestellt (dies gilt – in Anlehnung an die unten genannten Empfehlungen für die Testhäufigkeit in zweikanaligen Systemen – solange von mindestens einer Anforderung im Jahr ausgegangen werden kann). Ein Spezialfall hiervon ist die kontinuierliche Testung (z. B. analoge Über-/Unterspannungsüberwachung), bei der die Anforderungen an die Testhäufigkeit immer erfüllt sind, wenn der sichere Zustand schnell genug erreicht wird.

  In zweikanaligen Systemen der Kategorien 3 und 4 steht die Testhäufigkeit in Konkurrenz zur Häufigkeit des Auftretens eines zweiten gefahrbringenden Ausfalls. Denn erst, wenn der zweite Kanal ausfällt, bevor ein Test den Ausfall des ersten bemerkt hat, besteht die Gefahr der Nichtausführung der Sicherheitsfunktion – Kategorie-4-Systeme tolerieren gemäß Definition sogar die Anhäufung unerkannter Fehler. In der Praxis existieren verschiedene Empfehlungen für die minimal erforderliche Testrate in Kategorie 3 und 4.

  In DIN EN 61800-5-2 [20] zur Sicherheit elektrischer Leistungsantriebssysteme werden für den Fall, dass die Testung nicht durchgeführt werden kann, ohne den Arbeitszyklus der Maschine zu unterbrechen, und wo keine vertretbare technische Lösung implementiert werden kann, folgende minimale Testhäufigkeiten als akzeptabel angesehen: ein Test pro Jahr für PL d mit Kategorie 3, ein Test pro drei Monate für PL e mit Kategorie 3 und ein Test pro Tag für PL e in Kategorie 4.

  In DIN EN ISO 14119 [35] und in einer „Recommendation for Use“ der Notifizierten Prüfstellen im Maschinensektor [36] wird für elektromechanische Ausgänge (Relais oder Schütze) ein automatischer oder manueller Test in folgender Häufigkeit gefordert: mindestens einmal pro Monat für PL e mit Kategorie 3 oder 4 und mindestens einmal in zwölf Monaten für PL d mit Kategorie 3. Der Test soll bevorzugt automatisch erfolgen oder das Testintervall soll automatisch überwacht und nur im Ausnahmefall durch organisatorische Maßnahmen sichergestellt werden.

  Bei den hier genannten Testraten handelt es sich um Minimalanforderungen, die dann gelten, wenn keine häufigeren Tests möglich sind, z. B. weil der Test nur bei Anforderung der Sicherheitsfunktion durchgeführt werden kann (Signalwechsel erforderlich, z. B. bei Elektromechanik oder Fluidtechnik) oder weil dafür eine Unterbrechung des Arbeitszyklus der Maschine nötig ist, z. B. beim Start der Maschine zu Beginn der Schicht. Automatische Tests, die nicht diesen Einschränkungen unterliegen – z. B. Prozessor- oder Speichertests in elektronischen Systemen – können oft ohne großen Aufwand deutlich häufiger realisiert werden. Hier hat sich ein Test mindestens einmal pro Schicht für Kategorie 3 in der Praxis bewährt; in Kategorie 4 wurde schon zuzeiten der Vorgänger-Norm DIN EN 954-1 eine minimale Testhäufigkeit von einmal pro Stunde gewählt.

- Ein weiterer Punkt ist die Zuverlässigkeit der Testeinrichtung selbst: Hier gelten seitens der Norm nur die für alle Kategorien gültigen Basis-Anforderungen der Kategorie B, also die Übereinstimmung mit den zutreffenden Normen, um den zu erwartenden Einflüssen standhalten zu können, und die Verwendung grundlegender Sicherheitsprinzipien. Bewährte Sicherheitsprinzipien sollten – soweit möglich – ebenfalls umgesetzt werden. Wenn gefährliche Ausfälle der Testeinrichtung durch deren zyklische Einbindung in den Prozess erkannt werden, kann von diesen Basisanforderungen abgewichen werden. Grundsätzlich sollte darüber hinaus gelten, dass die Testeinrichtung nicht vor der von ihr überwachten Komponente ausfallen sollte. Andererseits ist es aber auch nicht effektiv, viel mehr in die Zuverlässigkeit der Testeinrichtung zu investieren als in die Sicherheitseinrichtungen, die die eigentliche Sicherheitsfunktion ausführen. DIN EN ISO 13849-1 hält sich daher mit Anforderungen an die Zuverlässigkeit der Testeinrichtungen zurück. Bei den Kategorien 3 und 4 wird auf die Einfehlertoleranz vertraut, da inklusive des Ausfalls der Testeinrichtung insgesamt drei gefahrbringende Ausfälle notwendig sind, bevor die Sicherheitsfunktion nicht mehr ausgeführt wird. Dass dieser Fall unbemerkt auftreten kann, wird als extrem unwahrscheinlich und daher nicht entscheidend angesehen. Bei Kategorie 2 gibt es zumindest bei der vereinfachten PL-Bestimmung anhand des Säulendiagramms eine Nebenbedingung, die bei der Berechnung der „Kategorie-2-Säulen“ zugrunde gelegt wurde: Hier sollte die gefahrbringende Ausfallrate des Testkanals nicht mehr als doppelt so hoch sein wie die gefahrbringende Ausfallrate des davon überwachten Funktionskanals.

- Die Wirksamkeit einer bestimmten Testmaßnahme, z. B. Fehlererkennung durch den Prozess, kann sehr stark von der Anwendung abhängig sein und durchaus zwischen 0 und 99 % schwanken. Hier ist bei der Auswahl eines der DC-Eckwerte besondere Sorgfalt notwendig. Weitere Erläuterungen dazu gibt Anhang E.

- Bei der Bestimmung des DC_{avg}-Wertes für elektromechanische Kontakte ist eine ggf. vorliegende Reihenschaltung von Positionsschaltern zu berücksichtigen. Hier kann es zur Maskierung von Fehlern kommen, sodass der DC_{avg}-Wert und der erreichbare PL reduziert werden müssen. Details hierzu sind im Anhang E zu finden.

- Es kann vorkommen, dass Komponenten oder Blöcke durch mehrere Tests überwacht werden oder dass auf verschiedene Teile unterschiedliche Tests wirken und hieraus ein Gesamt-DC für die Komponente oder den Block ermittelt werden muss. Anhang E gibt einige Hilfestellungen zu diesen Fragen.

- Mit der DC_{avg}-Formel (4) ist es rechnerisch möglich, Blöcke mit unterschiedlichem DC so zusammenzufassen, dass die Mindest-DC_{avg}-Anforderungen für die realisierte Kategorie erfüllt sind, auch wenn einzelne Blöcke einen *DC* unter 60 % oder gar keine Diagnose (*DC* = 0 %) aufweisen. Hier ist im Einzelfall zu prüfen, ob diese Form der Realisierung mit den Anforderungen der Kategorie übereinstimmt. Kategorie 3 fordert z. B., dass, wenn immer in angemessener Weise durchführbar, ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden muss. Kategorie 2 fordert pauschal den „Test der Sicherheitsfunktion“. Kategorie 4 fordert ebenfalls die Erkennung des einzelnen Fehlers und nur „wenn diese Erkennung nicht möglich ist“, die Ausführung der Sicherheitsfunktion auch bei Anhäufung unerkannter Fehler.

- Speziell bei programmierbaren elektronischen Systemen ist eine Vielzahl komplexer Fehler denkbar, sodass auch an die Komplexität der Tests entsprechende Anforderungen gestellt werden. Hier verlangt DIN EN ISO 13849-1, falls mehr als 60 % DC für die (programmierbare oder komplexe) Logik gefordert werden, mindestens eine Maßnahme für variante Speicher, invariante Speicher und die Verarbeitungseinheit – soweit vorhanden – mit mindestens je 60 % *DC*.

Sind die DC-Werte aller Blöcke schließlich bekannt, wird der DC_{avg}-Wert für das System mit der Näherungsformel (4) berechnet. Diese gewichtet die einzelnen *DC* mit der zugehörigen $MTTF_D$, denn sehr zuverlässige Teile (hohe $MTTF_D$) sind weniger auf wirksame Tests angewiesen als unzuverlässigere Teile (die Summen in Zähler und Nenner werden über N Blöcke des gesamten Systems gebildet):

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}} \quad (4)$$

Mit dem DC_{avg}-Wert steht schließlich ein Kennwert bereit, der im Mittel über die gesamten SRP/CS das Qualitätsniveau der Test- und Überwachungsmaßnahmen beschreibt. Bevor dieser Wert neben der Kategorie (fünf Klassen) und der $MTTF_D$ jedes Kanals (drei Klassen) in die vereinfachte Quantifizierung des PL eingeht, erfolgt eine Einordnung in eine der vier Klassen in Tabelle 6.4.

Tabelle 6.4:
Die vier Klassen des Diagnosedeckungsgrades im vereinfachten Ansatz der DIN EN ISO 13849-1

Diagnosedeckungsgrad (*DC*)	
Bezeichnung	**Bereich**
kein	*DC* < 60 %
niedrig	60 % ≤ *DC* < 90 %
mittel	90 % ≤ *DC* < 99 %
hoch	99 % ≤ *DC*

Bei der anschließenden Weiterverwendung des DC_{avg} in der vereinfachten Quantifizierung durch das Säulendiagramm (siehe Abschnitt 6.2.16) wird nur der jeweils untere Eckwert einer DC_{avg}-Klasse (0, 60, 90 oder 99 %) verwendet. Hier greift also eine weitere Vereinfachung, die auf einer Abschätzung zur sicheren Seite beruht.

Im Einzelfall kann es durch dieses grobe vereinfachte Raster allerdings zu Artefakten kommen, wenn z. B. eine unzuverlässige Komponente mit für die SRP/CS überdurchschnittlichem *DC* durch eine zuverlässigere Komponente ersetzt wird (nähere Erläuterungen dazu am Ende von Anhang G).

6.2.15 Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache – CCF

Der letzte Parameter, der bei der vereinfachten Quantifizierung der Ausfallwahrscheinlichkeit eine Rolle spielt, betrifft Ausfälle infolge einer gemeinsamen Ursache CCF (Common Cause Failure). Dabei handelt es sich um korrelierte gefahrbringende Ausfälle, z. B. in beiden Kanälen eines redundanten SRP/CS, die auf eine einzige Ursache zurückzuführen sind. Beispiele hierfür sind ungünstige Umgebungsbedingungen oder Überbelastungen, die beim Entwurf der Steuerung nicht ausreichend berücksichtigt wurden. Bei unzureichender Trennung der Kanäle kann es dann zu gefahrbringenden Folgefehlern kommen, die die beabsichtigte Einfehlertoleranz außer Kraft setzen. Die Relevanz dieser Effekte in einem konkreten System lässt sich nur schwer quantitativ abschätzen (siehe auch Anhang F). Im Anhang D der DIN EN 61508-6 [37] wird dazu das sogenannte Beta-Faktor-Modell bemüht, das die Ausfälle infolge gemeinsamer Ursache als β mal λ_D ins Verhältnis setzt zur gefahrbringenden Ausfallrate eines Kanals lD. Ohne eine genaue FMEA kann β für reale SRP/CS allerdings bestenfalls geschätzt werden. DIN EN ISO 13849-1 bietet dazu eine Checkliste aus acht wichtigen Gegenmaßnahmen an, die mit 5 bis 25 Punkten bewertet werden:

- physikalische Trennung der Signalpfade unterschiedlicher Kanäle (15 Punkte)

- Diversität in der Technologie, der Gestaltung oder den physikalischen Prinzipien der Kanäle (20 Punkte)

- Schutz gegen mögliche Überbelastungen (15 Punkte) und

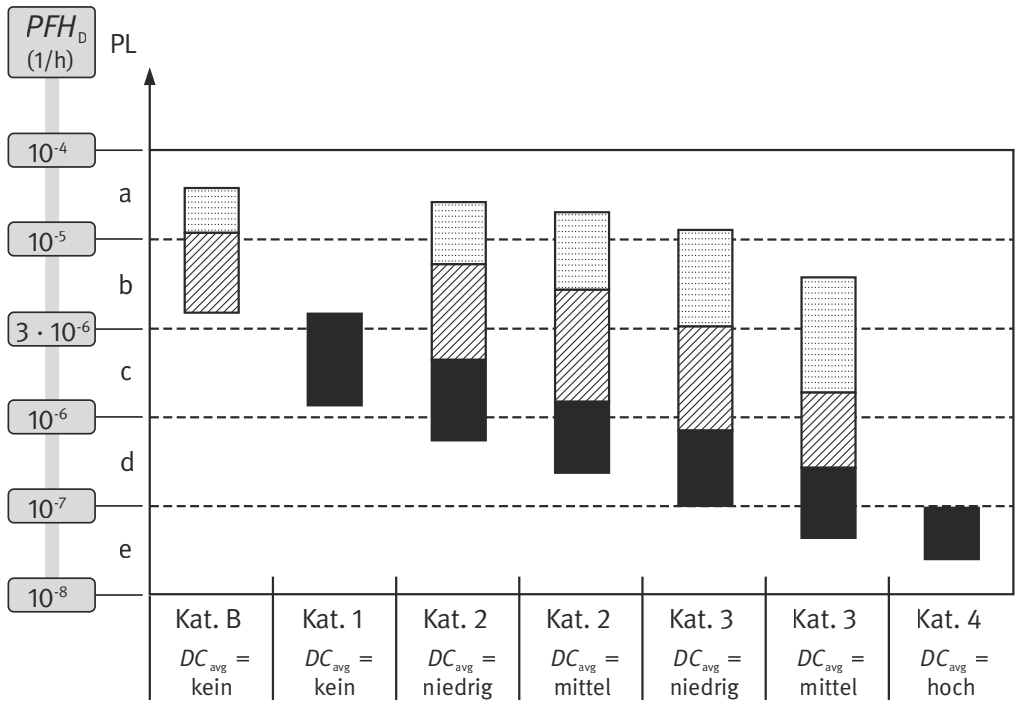
- Verwendung bewährter Bauteile (5 Punkte)

- Ausfalleffektanalyse in der Entwicklung zur Aufdeckung potenzieller Ausfälle infolge gemeinsamer Ursache (5 Punkte)
- Schulung des Konstruktions-/Montagepersonals hinsichtlich CCF und ihrer Vermeidung (5 Punkte)
- Schutz vor durch Verunreinigung (mechanische und fluidische Systeme) bzw. elektromagnetische Beeinflussung (elektrische Systeme) ausgelösten Ausfällen infolge gemeinsamer Ursache (25 Punkte)
- Schutz vor durch ungünstige Umgebungsbedingungen ausgelösten Ausfällen infolge gemeinsamer Ursache (10 Punkte)

Die für eine Gegenmaßnahme genannten Punkte sollen nur vollständig oder gar nicht vergeben werden, eine „halbe Umsetzung" der Gegenmaßnahmen wird nicht durch Punkte belohnt. Allerdings können subsystemweise unterschiedliche Maßnahmenbündel gegen CCF wirken. Werden alle acht Gegenmaßnahmen erfüllt, würde sich eine maximale Summe von 100 Punkten ergeben. Allerdings fordert DIN EN ISO 13849-1 nur eine Mindestsumme von 65 Punkten – und dies auch nur für SRP/CS in den Kategorien 2, 3 und 4. Bei Kategorie-2-Systemen geht es dabei darum, gefährliche Ausfälle in Test- und Funktionskanal durch gemeinsame Ursachen, die ein unerkanntes Auftreten eines gefährlichen Fehlers bewirken können, zu vermeiden. Bei der Erstellung des Säulendiagramms zur vereinfachten Quantifizierung wurden die 65 Punkte mit einem Beta-Faktor von 2 % gleichgesetzt. Hier wurde die Vergröberung gegenüber den fünf Kategorien und drei bzw. vier $MTTF_D$- und DC_{avg}-Klassen noch weiter forciert und auf eine simple Ja/Nein-Entscheidung reduziert. Während die Vorteile einer redundanten Struktur schon bei einem Beta-Faktor ab 10 % fast vollständig zunichte gemacht werden, minimiert ein Beta-Faktor von höchstens 2 % die Relevanz von Ausfällen infolge gemeinsamer Ursache auf ein vertretbares Maß.

6.2.16 Vereinfachte PL-Bestimmung durch das Säulendiagramm

Nachdem die vier wesentlichen quantitativen Parameter zur Ermittlung der Ausfallwahrscheinlichkeit bestimmt wurden, ist es trotzdem keine einfache Aufgabe, hieraus den für die SRP/CS erreichten PL zu ermitteln. Obwohl grundsätzlich alle geeigneten Methoden erlaubt sind, schlägt DIN EN ISO 13849-1 ein einfaches grafisches Verfahren vor, das auf komplexeren Berechnungen und Abschätzungen zur sicheren Seite beruht – das sogenannte Säulendiagramm (siehe Abbildung 6.10).



Legende

PFH_D Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde

PL Performance Level

$MTTF_D$ jedes Kanals = niedrig

$MTTF_D$ jedes Kanals = mittel

$MTTF_D$ jedes Kanals = hoch

Abbildung 6.10: Säulendiagramm zur vereinfachten PL-Bestimmung aus der Kategorie (Kat.; inklusive Maßnahmen gegen CCF), dem DC_{avg} und der $MTTF_D$

Dieses Diagramm wurde auf der Grundlage der vorgesehenen Architekturen für die Kategorien durch Markov-Modellierung ermittelt, weitere Erläuterungen dazu gibt Anhang G. Bei Anwendung des Säulendiagramms wird zunächst durch die erreichte Kategorie – dabei müssen für die Kategorien 2, 3 und 4 ausreichende Maßnahmen gegen CCF getroffen werden – in Kombination mit der erreichten DC_{avg}-Klasse auf der horizontalen Achse die relevante Säule bestimmt. Die Höhe der von den SRP/CS erreichten $MTTF_D$ auf der ausgewählten Säule legt den auf der vertikalen Achse abzulesenden PL fest. Mit dieser Methode ist auch ohne genaue quantitative Daten eine schnelle qualitative Abschätzung des erreichten PL möglich. Falls genaue Werte gefragt sind, z. B. neben dem PL auch ein Wert für die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde PFH_D, so helfen die Tabellen in Anhang K der Norm weiter. Ähnliches leistet auch die Software SISTEMA des IFA (siehe Anhang H), die das Säulendiagramm quantitativ auswertet, und die handliche PLC-Drehscheibe [16] des IFA.

Bei der Ableitung des Säulendiagramms wurden nicht nur vorgesehene Architekturen berücksichtigt, sondern auch einige Bedingungen vorausgesetzt, die bei dessen Anwendung beachtet werden müssen:

- Als Gebrauchsdauer der SRP/CS werden 20 Jahre unterstellt, innerhalb derer die Bauteilzuverlässigkeiten durch konstante Ausfallraten beschrieben oder angenähert werden können. Durch Verwendung stark verschleißbehafteter Bauteile (siehe T_{10D}-Wert in Anhang D) oder aus anderen Gründen kann die tatsächliche Gebrauchsdauer die angenommenen 20 Jahre unterschreiten. Dann ist durch vorsorglichen Austausch der betroffenen Bauteile oder der betroffenen SRP/CS die Anwendung des Säulendiagramms zu rechtfertigen. Den Anwendern und Anwenderinnen sind diese Informationen in geeigneter Form mitzuteilen, zum Beispiel über die Benutzerinformationen und durch Kennzeichnung auf den SRP/CS. Soll die Gebrauchsdauer von vorneherein mehr als 20 Jahre betragen oder nachträglich über 20 Jahre hinaus verlängert werden, ergeben sich Abweichungen vom Säulendiagramm. In Anhang G ist dargestellt, wie damit umgegangen werden kann.

- Bei den Säulen für Kategorie 2 wurde unterstellt, dass die Testhäufigkeit ausreichend groß ist (siehe auch Abschnitt 6.2.14 und Anhang E) und dass außerdem der Testkanal mindestens halb so zuverlässig ist wie der Funktionskanal.

Durch die Begrenzung der anrechenbaren $MTTF_D$ jedes Kanals auf 100 Jahre – bei Kategorie 4 sind es 2500 Jahre – kann ein hoher PL nur mit bestimmten Kategorien erreicht werden. Obwohl dies mit dem vereinfachten Ansatz der vorgesehenen Architekturen und des Säulendiagramms zusammenhängt, gelten die damit verbundenen Einschränkungen auch bei einer unabhängigen Bestimmung der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde nach anderen Methoden. Wie schon erwähnt, gelten für einige Kategorien folgende Einschränkungen durch die Architektur, die verhindern sollen, dass die Bauteilzuverlässigkeit gegenüber den anderen Einflussgrößen überbewertet wird:

- Mit Kategorie B kann maximal PL = b erreicht werden.
- Mit Kategorie 1 kann maximal PL = c erreicht werden.
- Mit Kategorie 2 kann maximal PL = d erreicht werden.
- Mit Kategorie 3 oder 4 ist auch PL = e erreichbar.

Außer dem quantitativen Aspekt der Ausfallwahrscheinlichkeit müssen zum Erreichen eines bestimmten PL aber auch qualitative Aspekte beachtet werden. Zu diesen gehören systematische Ausfälle (siehe Abschnitt 6.1.2) und Softwarefehler, auf die in Abschnitt 6.3 näher eingegangen wird.

6.2.17 PL-Bestimmung für den Ausgangsteil des SRP/CS (Energieübertragungselemente) nach Abschnitt 4.5.5 der Norm

Als Reaktion auf Forderungen aus der praktischen Anwendung wurde in der dritten Ausgabe der Norm ein alternatives einfaches Verfahren zur Bestimmung der PFH_D und quantifizierbarer Aspekte des PL aufgenommen. Dieses in Abschnitt 4.5.5 der Norm beschriebene Verfahren ist nur in bestimmten Fällen anwendbar, und zwar

- für den Ausgangsteil (Energieübertragungselemente) 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 λ_D, B_{10D} o. Ä.) verfügbar sind.

Die Vereinfachung der PFH_D-Bestimmung zielt hier hauptsächlich auf die realisierte Kategorie inklusive DC_{avg} und CCF. 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 (neue Definition 3.1.39 in der Norm). Ein solcher Nachweis ist im Maschinenbau bisher unüblich. Unklar ist auch, warum die Anforderung sich nur auf systematische Fehler bezieht und die zufälligen Bauteilfehler nicht berücksichtigt.

Tabelle 6.5 stellt in Anlehnung an Tabelle 7 im neuen Abschnitt 4.5.5 der Norm – abhängig von der realisierten Kategorie und unter den an das Verfahren geknüpften Zusatzbedingungen – den abschätzbaren PFH_D-Wert und den damit erreichbaren PL dar.

Folgende Zusatzbedingungen sind an das Verfahren geknüpft:

- Da die geschätzten PFH_D-Werte auf dem vereinfachten Verfahren zur Abschätzung eines PL (Säulendiagramm) beruhen, gelten dafür auch dieselben Voraussetzungen wie für die vorgesehenen Architekturen. Es werden also eine Gebrauchs-

Tabelle 6.5:
PL und PFH_D als Abschätzung zur sicheren Seite basierend auf Kategorie, DC_{avg} und der Verwendung bewährter oder betriebsbewährter Bauteile

	PFH_D in 1/h		Kategorie B	Kategorie 1	Kategorie 2	Kategorie 3	Kategorie 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						
Es gelten weitere Zusatzbedingungen, siehe Abschnitt 6.2.17.							

dauer von 20 Jahren und konstante Ausfallraten innerhalb der Gebrauchsdauer unterstellt. In Kategorie 2 müssen die Tests ausreichend häufig durchgeführt werden. Eine reduzierte Testrate, die nur das 25-Fache der Anforderungsrate beträgt, ist hier nicht vorgesehen.

- 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 zehn Jahre.

- In Kategorie 2, 3 und 4: Verwendung bewährter oder betriebsbewährter Bauteile, Verwendung bewährter Sicherheitsprinzipien. In Kategorie 2 hat es keinen Sinn, diese Anforderung auch auf den Testkanal auszudehnen, da mit einem einkanaligen System der Kategorie 1 das gleiche Ergebnis (PFH_D und PL) erreicht werden kann.

- 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“

Die DC-Anforderung aus den beiden letzten Aufzählungspunkten bezieht sich auf jedes Bauteil im Subsystem und geht damit über die jeweilige allgemeine Kategorie-Anforderung, die sich auf DC_{avg} bezieht, hinaus. Da es sich hier aber um den Ausgangsteil des SRP/CS mit mechanischen, hydraulischen oder pneumatischen Bauteilen handelt, wird meist pro Kanal nur ein Bauteil vertreten sein. Daher stellt die Anforderung an den *DC* jedes Bauteils im Vergleich zum DC_{avg} des Subsystems in der Praxis eigentlich keine Verschärfung dar.

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 [Gleichung (4) dieses Reports] zurückgegriffen werden kann, wird hier DC_{avg} einfach als arithmetischer Mittelwert der Einzel-DCs aller Komponenten in den Funktionskanälen des Ausgangsteils gebildet.

6.2.18 Bussysteme als „Verbindungsmittel“

Die einzelnen Blöcke Eingabeeinheit, Logik und Ausgabeeinheit einer vorgesehenen Architektur müssen nicht nur logisch, sondern auch physikalisch miteinander verbunden werden. Dazu definiert die Norm „Verbindungsmittel“, die als Teil der SRP/CS betrachtet werden. Der Name Verbindungsmittel erscheint fachlich zunächst aus der Sicht der Elektro- oder Fluidtechnik merkwürdig, ist aber der Oberbegriff für elektrische sowie fluidtechnische Leitungen und sogar für mechanische Stößel usw. Somit gelten alle Anforderungen der Norm auch für diese „Verbindungsmittel“. Unter dem Aspekt der Fehlerbetrachtung ist also z. B. ein Leitungskurzschluss ein anzunehmender Fehler. Wie aber sieht es mit dem Einsatz von Bussystemen zur Übertragung von sicherheitsrelevanten Informationen aus? Natürlich kann es nicht Gegenstand der Norm sein, ein solch komplexes Thema detailliert zu beleuchten, zumal es bereits Berufsgenossenschaftliche Prüfgrundsätze (GS-ET-26 [38]) und eine Norm (DIN EN 61784-3 [39]) zu diesem Thema gibt. Bussysteme, die den in diesen Publikationen beschriebenen Anforderungen genügen, lassen sich ohne Weiteres auch unter dem Dach der DIN EN ISO 13849-1 einsetzen. Auf dem Markt gibt es eine

größere Anzahl von Bussystemen, die für den sicherheitstechnischen Einsatz geeignet sind.

In den oben erwähnten Publikationen wird ein spezielles Fehlermodell verwendet, um dem Einsatz eines Blackbox-Kanals für die sicherheitsrelevante Datenübertragung Rechnung zu tragen – d. h. an diesen Übertragungskanal selbst werden z. B. keine speziellen Anforderungen zur Fehleraufdeckung gestellt. Das Modell nimmt als Fehlermöglichkeiten die Wiederholung, den Verlust, die Einfügung, falsche Abfolge, Verfälschung und die Verzögerung sicherheitsrelevanter Nachrichten sowie die Kopplung von sicherheitsrelevanten und nicht sicherheitsrelevanten Nachrichten an. Weitere Aspekte können Fehler sein, die Nachrichten systematisch verfälschen, z. B. vollständig invertieren. Durch Maßnahmen in sogenannten Sicherungsschichten, die dann in sicherheitsbezogenen Teilen von Steuerungen realisiert werden, lassen sich Übertragungsfehler mit hinreichender Wahrscheinlichkeit ausschließen. Geeignete Maßnahmen sind z. B. laufende Nummer, Zeitmarke, Zeiterwartung, Empfangsbestätigung, Kennung für Sender und Empfänger und Datensicherung. Gerade die Betrachtung der Datensicherung ist oft mit komplexen Berechnungen verbunden. Ziel dieser Betrachtungen ist es, die Restfehlerwahrscheinlichkeit R und die daraus abgeleitete Restfehlerrate Λ – (in Anlehnung an das kleine λ – als Fehlerrate von Bauteilen) zu bestimmen. Genau dieser Wert lässt sich dann unter dem Aspekt der für einen PL geforderten durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde als Anteil für die Übertragung sicherheitsrelevanter Nachrichten einrechnen. Beide oben genannten Publikationen begrenzen den Wert der Restfehlerrate auf 1% des zulässigen Maximalwertes der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde. Tatsächlich sind von Herstellern bisher angegebene Werte oft auf einen SIL (siehe Kapitel 3) bezogen, in der Praxis sind diese Werte aber kompatibel für einen Einsatz unter einem geforderten PL (siehe auch Abbildung 3.2). Durch die 1%-Regel ist der Beitrag zur Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde quasi vernachlässigbar bzw. kann den für die SRP/CS ermittelten Werten hinzugerechnet werden. Umfassende Informationen zu Bussystemen für die Übertragung sicherheitsrelevanter Informationen gibt z. B. [40].

Sollen ein in der Regel von unabhängiger Stelle geprüftes Bussystem bzw. dessen Komponenten für die Realisierung von Sicherheitsfunktionen eingesetzt werden, so sind vor allem die Planung des Einsatzes und die korrekte Implementierung unter dem Aspekt der Fehlervermeidung von großer Bedeutung. Eine Vielzahl von Parametern will korrekt mit mehr oder weniger Unterstützung durch zugehörige Tools eingestellt werden.

Kommt keines der bekannten, bereits beurteilten Profile für funktionale Sicherheit zum Einsatz, gilt es, die oben genannten Fehlerannahmen zu Übertragungsfehlern zu berücksichtigen, entsprechende (Gegen-)Maßnahmen zu implementieren und die Restfehlerrate Λ unter Berücksichtigung der typischen Bitfehlerrate von 0,01 bei der Berechnung der Gesamt-Ausfallwahrscheinlichkeit PFH_D zu berücksichtigen. Der Prüfgrundsatz GS-ET-26 [38] gibt Hinweise zur Berechnung der Restfehlerate Λ.

6.3 Entwicklung sicherheitsbezogener Software

„Wer eine Software programmiert und darin jahrelange Erfahrung hat, macht selbstverständlich keine Fehler mehr“, diese oder ähnliche Aussagen sind oft zu hören. Dabei ist gerade diese Selbstüberschätzung der größte Fehler, den man machen kann. Software ist in der Regel kompliziert und deshalb gibt es auch im Gegensatz zur Hardware zunehmend mehr Versagen durch Softwarefehler. Wie oft wundert man sich am PC, dass ein Peripheriegerät nicht mehr funktioniert, wie oft war es dann ein Teil der Software, der sich mit einem anderen, z. B. Treiber, nicht vertrug? Dagegen sind Hardwarefehler eher selten. Normale, das heißt einfache Software für einfache Funktionen hat nach [41] etwa 25 Fehler pro 1000 Programmzeilen. Gute Software hat nach [41] etwa zwei bis drei Fehler pro 1000 Programmzeilen und die Software im Space-Shuttle hat (laut NASA) weniger als einen Fehler pro 10 000 Zeilen. Was bedeutet das in der Praxis: Ein Mobiltelefon hat bis zu 200 000 Programmzeilen und damit bis zu 600 Softwarefehler. Ein PC-Betriebssystem hat 27 Millionen Programmzeilen und damit bis zu 50 000 Fehler, das Space-Shuttle bis zu 300 Fehler und die Software für das Verteidigungssystem SDI bis zu 10 000 Fehler. Diese Programmfehler „schlummern“ in den Produkten und werden sich unter bestimmten Bedingungen und in bestimmten Situationen auf die Funktion auswirken. Wie keine zweite Technologie übernimmt Software eine höhere Verantwortung als je zuvor und damit also auch die Programmierenden.

Als eine der wesentlichen Neuerungen der DIN EN ISO 13849-1 gegenüber ihrer Vorgängernorm DIN EN 954-1 werden erstmals Anforderungen an die Software und deren Entwicklung gestellt. Um es vorweg deutlich herauszustellen: Die Anforderungen in Abschnitt 4.6 der Norm ermöglichen es, sicherheitsbezogene Software für alle SRP/CS im Maschinensektor und für alle erforderlichen Performance Level von a bis e zu entwickeln. Dieser Abschnitt richtet sich in erster Linie an Anwendungsprogrammierende, die Sicherheitsfunktionen für eine Maschine, z. B. in einer applikationsorientierten Sprache auf einer speicherprogrammierbaren Steuerung (SPS), entwickeln. Für die Entwicklung von SRESW (Safety-Related Embedded Software – sicherheitsbezogene eingebettete Software), also Firmware oder Softwarewerkzeuge für elektronische Sicherheitskomponenten, ist dagegen der Neuigkeitswert dieser Anforderungen in DIN EN ISO 13849-1 nicht so hoch. Solche „Embedded Software“-Entwicklungen für die meist zertifizierten Komponenten unterliegen oft auch den sehr komplexen Anforderungen der für IEC-Normen zur Funktionalen Sicherheit verbindlichen Sicherheitsgrundnorm DIN EN bzw. IEC 61508-3 [42] (und aller weiteren sieben Teile).

Für die Programmierung von SRASW (Safety-Related Application Software – sicherheitsbezogene Anwendungssoftware) ist der IFA Report 2/2016 „Sicherheitsbezogene Anwendungssoftware von Maschinen“ [43] erschienen. Dieser Report beschreibt die Matrixmethode des IFA zur Spezifikation, Verifikation, Validierung und Dokumentation von SRASW. Diese Matrixmethode kann auch mit dem Tool SOFTEMA des IFA [44] angewendet werden. Der Report gibt darüber hinaus detaillierte, weiterführende Informationen zur Programmierung von SRASW. Die folgenden Darstellungen beschränken sich daher darauf, die normativen Anforderungen der

DIN EN ISO 13849-1 zu sicherheitsbezogener Software kurz vorzustellen.

Die Grundgedanken dieses Abschnitts können auf beide Softwaretypen bezogen werden. Einzelne Anforderungen werden aber eher für die Anwendungsprogrammierung von SRASW konkretisiert. Dahingegen zeigt das Beispiel der Steuerung einer Planschneidemaschine in Abschnitt 6.5 die Entwicklung einer SRESW.

Die Anforderungen an die Softwareentwicklung richten sich nach dem verwendeten Softwaretyp (SRASW oder SRESW) und dem Sprachtyp. Wie auch in anderen aktuellen Normen mit Softwareanforderungen wird zwischen den Sprachtypen FVL (Full Variability Language, Programmiersprache mit nicht eingeschränktem Sprachumfang) und LVL (Limited Variability Language, Programmiersprache mit eingeschränktem Sprachumfang) unterschieden. Üblicherweise wird SRASW in LVL programmiert, z. B. in einer grafischen Sprache, die in IEC 61131-3 definiert ist. Es gelten dann die Anforderungen aus Abschnitt 4.6.3 der DIN EN ISO 13849-1.

Sobald aber SRASW in FVL (z. B. eine SPS in der Hochsprache „C“) programmiert wird, müssen die Anforderungen für SRESW, Abschnitt 4.6.2 der Norm, erfüllt werden. Muss in diesem Fall die SRASW einen Performance Level von e erfüllen, so verweist DIN EN ISO 13849-1 am Ende des Abschnitts 4.6.2 ein einziges Mal – aber mit Ausnahmen – auf die Anforderungen der Norm IEC 61508-3:1998.

6.3.1 Software ohne Fehler …

… gibt es in der Praxis leider nicht. Fehler in der Software entstehen nicht wie bei der Hardware durch zufällige Bauteilausfälle, sondern haben systematische Ursachen. Umso mehr muss bei der Entwicklung von sicherheitsbezogener Software, die ja zur Risikominimierung beitragen soll, alles Angemessene getan werden, um Fehler zu vermeiden. Was angemessen ist, orientiert sich einerseits am erforderlichen Performance Level PL_r. Andererseits ist bekannt, in welchen Phasen der Softwareentwicklung sich sicherheitskritische Fehler bevorzugt und mit besonders gravierender Wirkung einschleichen und solange unentdeckt bleiben, bis sie beim Betrieb zum Ausfall führen. Gemeint sind die Phasen Spezifikation, Gestaltung und Modifikation. Daher zielen die Anforderungen der DIN EN ISO 13849-1 – und die Erläuterungen in diesem Abschnitt – besonders auf die Fehlervermeidung in diesen Phasen. Leider werden diese Phasen der Anwendungsprogrammierung in der Praxis oft mit eher weniger Aufmerksamkeit bedacht.

Um eine gute Qualität sicherheitsbezogener Software zu erreichen, ist es nahe liegend, entsprechende aktuelle und bewährte Entwicklungsmodelle des „Software Engineering“ aufzugreifen. Für sicherheitsbezogene Systeme wird dabei meist auf das „V-Modell“ referenziert [45]. Da das aus der Literatur bekannte V-Modell eher für sehr komplexe Software zum Einsatz kommt, wird dieses Entwicklungsmodell in DIN EN ISO 13849-1, Abschnitt 4.6.1, nur in einer vereinfachten Form (Abbildung 6.11) gefordert. Diese wird für die Bedingungen der sicherheitsbezogenen SRP/CS im Maschinensektor und dort speziell für die Entwicklung von SRASW als praxisgerecht und zielführend bewertet. Das eigentliche Ziel dabei ist es, lesbare, verständliche, testbare und wartbare Software zu erhalten. Diese Anforderungen empfinden Programmierende, die üblicherweise keine sicherheitsrelevante Software erstellen, als mühsam. Die Erfüllung dieser Anforderungen gibt ihnen aber die Bestätigung, die Software hinreichend gut entwickelt zu haben.

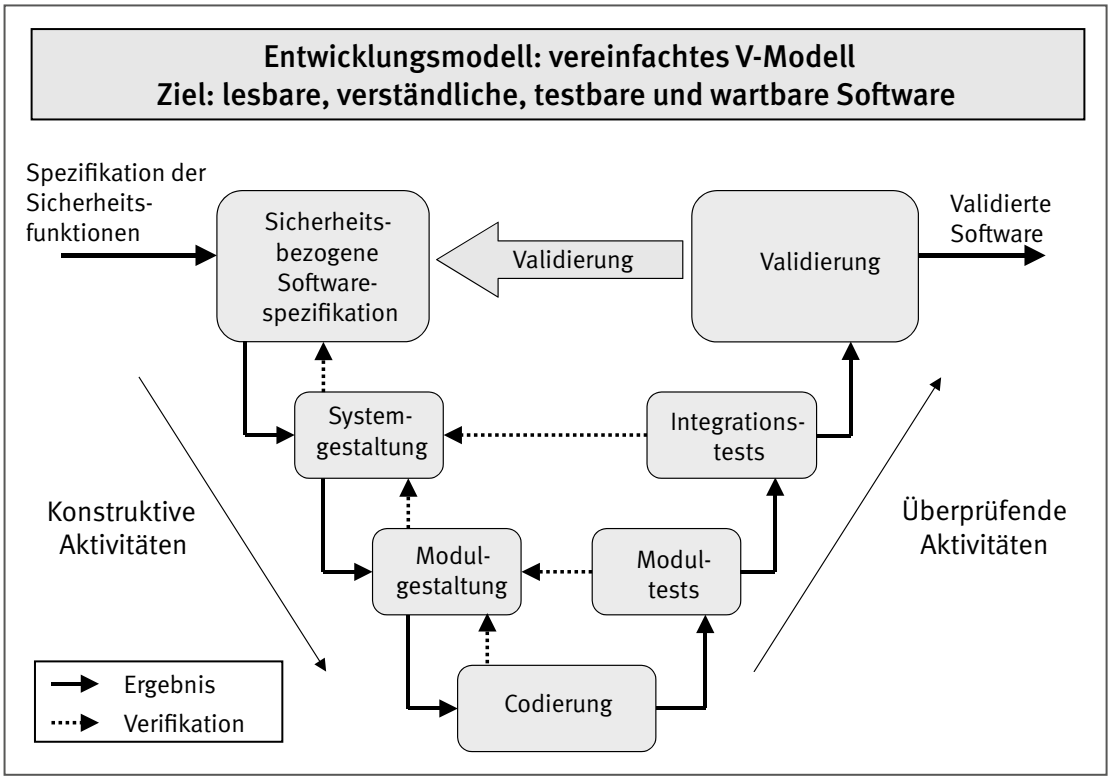


Abbildung 6.11: Vereinfachtes V-Modell für die Entwicklung sicherheitsbezogener Software

Neben den Phasen sind in Abbildung 6.11 wichtige Begriffe dargestellt, deren Bedeutung (auf Software bezogen) vorab definiert werden soll.

Ergebnis

Bezeichnet das, was in einer Phase erstellt wurde, z. B. die Spezifikation, den Softwareentwurf, den Code und als abschließendes Ergebnis die getestete validierte Software. Es kann aber z. B. auch ein Testplan sein, als Ergebnis der Spezifikationsphase, der erst in einer viel späteren Phase benötigt wird, um dann die Software systematisch validieren zu können. Das Ergebnis bzw. die Ergebnisse der vorherigen Phasen dienen als Eingabe für die nächsten Phasen. Dies wird durch den Pfeil dargestellt.

Verifikation

Bezeichnet die qualitätssichernde Aktivität, mit der geprüft wird, ob das Ergebnis einer Phase den Vorgaben der Vorgängerphase entspricht. Beispielsweise wird während oder zum Abschluss der Codierungsphase verifiziert, ob der Code tatsächlich die vorgegebene Modulgestaltung realisiert und dabei die Programmierrichtlinien eingehalten wurden.

Validierung

Die Softwarevalidierung ist hier eine abschließende spezielle Form der Verifikation der gesamten Software. Es wird geprüft, ob die Anforderungen der Softwarespezifikation zur Funktionalität der Software umgesetzt wurden.

Im Folgenden werden einige Phasen des vereinfachten V-Modells und damit gleichzeitig der „Fahrplan“ für die Softwareentwicklung beschrieben. Der abwärtsgerichtete Teil des „V“ beschreibt die konstruktiven und der aufwärtsgerichtete die überprüfenden Aktivitäten der Entwicklung.

6.3.2 Schnittstelle zur Gesamtsicherheit: Softwarespezifikation

Ausgehend von der übergeordneten Spezifikation der Sicherheitsfunktionen der SRP/CS wird hier in einem Dokument beschrieben, welche Teilfunktionen davon die Software realisieren muss. Weiterhin werden

- Funktionen, die Hardwarefehler aufdecken und beherrschen,
- Leistungsmerkmale wie maximale Reaktionszeit,
- Reaktionen im Fehlerfall,
- vorgesehene Schnittstellen zu anderen Systemen usw.

dargestellt.

Neben diesen funktionalen Anforderungen ist auch der von den Sicherheitsfunktionen zu erreichende PL, der PL_r, anzugeben, damit die notwendigen fehlervermeidenden Maßnahmen (siehe weiter unten) ausgewählt werden können.

Diese Spezifikation (auch „sicherheitsbezogenes Software-Lastenheft“ genannt) ist zu verifizieren, indem z. B. eine an der Erstellung dieses Dokuments unbeteiligte Person gegenliest. Diese muss erstens bestätigen, dass dieses Lastenheft mit der übergeordneten Spezifikation übereinstimmt, und zweitens, dass auch die Anforderungen an die Form, wie eine Softwarespezifikation zu schreiben ist, erfüllt sind. Die Spezifikation sollte so strukturiert und ausführlich erstellt werden, dass sie gleichzeitig als Checkliste zur späteren Validierung dienen kann.

Die gesamte Sicherheit einer Maschine bzw. Maschinenanlage wird durch alle sicherheitsbezogenen Teile der Steuerung und deren Funktionen (Komponenten aller Technologien, Elektronik, Software) gewährleistet. Hier ist also eine Beschreibung der Sicherheit für die Maschine bzw. Maschinenanlage in Form einer Spezifikation notwendig. Das Dokument muss nicht Hunderte von Seiten umfassen, sondern kann sich durchaus in verständlicher Form auf das Wesentliche beschränken. Nach den Festlegungen zur Gesamtheit der Maschine oder Maschinenanlage wird es eine Teilmenge von Arbeiten für Programmierende geben. Die Softwarespezifikation ist damit Teil des Gesamtkonzepts und folglich als „Vertrag“ mit einem „Unterauftrag“ zur Programmierung zu bewerten.

Zunächst macht die Softwarespezifikation Vorgaben für die Gestaltung und die Codierung der Software. Die anderen an der Sicherheit beteiligten Elemente müssen sich auf die Umsetzung der Funktionen in der Software verlassen können. Daher ist die Spezifikation auch Grundlage für die Abnahme der Software: Die Validierung der Softwarefunktionen muss zeigen, ob der „Vertrag“ erfüllt wurde. Im Bereich der SRASW ist dies sogar wörtlich zu nehmen, da Projektierung und Programmierung einer Steuerung oft vom Verantwortlichen der Gesamtsicherheit an andere Unternehmen oder Unternehmensbereiche vergeben werden. Dann sollte die Spezifikation auch eine vertragsverbindliche Schnittstelle zu externen oder internen Dienstleistern sein.

6.3.3 System- und Modulgestaltung für das „sicherheitsbezogene Pflichtenheft“

Die Softwarearchitektur ist durch das Betriebssystem oder Entwicklungswerkzeug meist bereits festgelegt. In der Gestaltung wird darüber hinaus festgelegt, mit welcher Struktur und mit welchen Modulen die spezifizierten Sicherheitsteilfunktionen realisiert werden sollen. Zu entscheiden ist, welche bereits vorhandenen Bibliotheksfunktionen eingesetzt werden und ob eventuell projektspezifische neue Funktionen entwickelt werden müssen. In diesem Abschnitt ist mit dem Begriff Softwarefunktion/-modul auch immer ein Funktionsbaustein gemeint.

Das Software-Gestaltungsdokument sollte Aufbau und Ablauf der Software durch Grafiken auch für außen stehende Personen verständlich beschreiben. Dies kann umso kompakter sein, je mehr das Programm auf wieder verwendeten, bereits validierten Softwarefunktionen basiert, die schon an anderer Stelle dokumentiert sind. In der Modulgestaltung werden zusätzlich die projektspezifisch neu zu erstellenden Softwarefunktionen, ihre Schnittstellen und Testfälle für deren Modultest spezifiziert. System- und Modulgestaltung können bei weniger komplexen SRP/CS zusammengefasst werden und ergeben das „sicherheitsbezogene Softwarepflichtenheft“.

6.3.4 Endlich programmieren

Danach geht es zur eigentlichen Codierung. Im Sinne der Fehlervermeidung sind hierbei drei Dinge zu beachten:

- Lesbaren und verständlichen Code schreiben, damit dieser später leichter getestet und fehlerfreier modifiziert werden kann. Verbindliche Programmierrichtlinien helfen z. B., das Programm besser zu kommentieren und die Variablen bzw. Bausteine selbsterklärend zu benennen.

- Defensiv programmieren, das heißt, immer mit internen oder externen Fehlern rechnen und diese aufdecken. Kennt man z. B. das zeitliche Verhalten von Eingangssignalen, so kann man mit dieser Erwartungshaltung Fehler der peripheren Beschaltung aufdecken. Wird eine Zustandsmaschine programmiert, dann wird die Zustandsvariable auf gültigen Wertebereich überwacht usw.

- Der Code muss statisch, d. h. ohne Ausführung, analysiert werden: Für niedrige PL reicht ein Code-Review, für PL d und e sollte der Daten- und Steuerfluss zusätzlich – möglichst werkzeugbasiert – überprüft werden. Typische Fragen sind: Entspricht der Code der vorherigen Gestaltung der Software? Gibt es keine Stellen, in denen Signale mit geringerem PL (z. B. aus einer Standard-SPS) ein Signal mit höherem PL überstimmen? Wo und durch welche Module werden Variablen initialisiert, beschrieben und dann dem Sicherheitsausgang zugewiesen? Welche Softwarefunktionen werden bedingt ausgeführt?

6.3.5 Prüfe, was sich ewig bindet: Modultest, Integrationstest und Validierung

Im Modultest werden die projektspezifisch neu entwickelten Softwarefunktionen getestet und simuliert, um zu prüfen, ob sie so codiert sind, wie in der Modulgestaltung spezifiziert. Spätestens beim Integrationstest wird, z. B. während der typischen Inbetriebnahme der SPS einer Maschine, die Gesamtsoftware auf korrekten Ablauf auf der Hardware (Integration) und der Übereinstimmung mit der Systemgestaltung (Verifikation) getestet. Beides sind noch Verifikationsmaßnahmen, d. h., man schaut dabei in die Software „hinein“. Ob die Sicherheitsteilfunktionen der Software wie spezifiziert funktionieren, ergibt die bereits oben beschriebene Softwarevalidierung. Für die höheren PL d und e wird auch ein erweiterter Funktionstest notwendig.

Einzelne Softwarefunktionen, die zertifiziert oder bereits qualitätsgesichert validiert wurden, müssen nicht nochmals verifiziert werden. Sobald aber mehrere dieser Funktionen projektspezifisch zusammengeschaltet werden, ist diese resultierende neuartige Teilsicherheitsfunktion zu validieren. Auch bei zertifizierten Bausteinen kann es aufgrund falscher Parametrierung und Verknüpfung zu gefährlichen systematischen Ausfällen kommen.

6.3.6 Struktur der normativen Anforderungen

Nachdem der Entwicklungsprozess skizziert ist, werden normative Anforderungen an die Software selbst, an die benutzten Entwicklungswerkzeuge sowie an die Entwicklungsaktivitäten beschrieben. Diese Anforderungen tragen ebenfalls zur Fehlervermeidung bei. Der dazu erforderliche Aufwand soll – ähnlich wie bei der Hardware der programmierbaren SRP/CS – der jeweils notwendigen Risikominderung entsprechend angemessen sein. Daher werden die Anforderungen bzw. deren Wirksamkeit mit zunehmendem PL_r sinnvoll gesteigert.

Abbildung 6.12 zeigt, dass es sowohl bei SRASW als auch bei SRESW für alle PL zunächst ein geeignetes Bündel von Basismaßnahmen gibt. Diese Basismaßnahmen können als softwarespezifische grundlegende Sicherheitsprinzipien verstanden werden. Sie genügen für die Entwicklung von Software für PL a oder b. Für Software, die in SRP/CS für PL c bis e eingesetzt wird, gelten neben den Basismaßnahmen zusätzliche fehler-

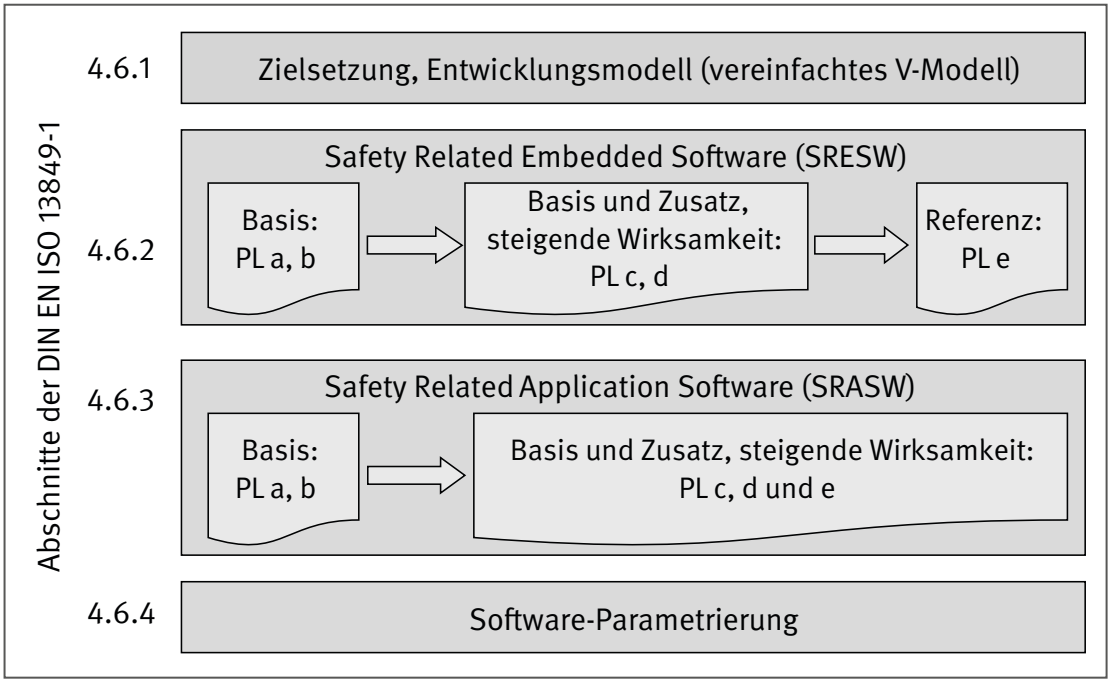


Abbildung 6.12: Abstufung der Anforderungen an sicherheitsbezogene Software (DIN EN ISO 13849-1)

vermeidende Maßnahmen. Letztere sind für PL c mit geringerer Wirksamkeit, für PL d mit mittlerer Wirksamkeit und für PL e mit höherer Wirksamkeit gefordert. Unabhängig davon, ob die Software nur in einem oder in beiden Kanälen einer beliebigen Kategorie mitwirkt: Als Maßstab für die Anforderungen gilt immer der PL_r der realisierten Sicherheitsfunktion(en).

Der Aspekt „höhere Wirksamkeit" bezieht sich auf den zunehmenden Grad der Fehlervermeidung. Dies soll an der wichtigen Aktivität der Spezifikation illustriert werden. So kann es z. B. für PL c ausreichend sein, wenn Programmierende die Spezifikation selbst verfassen und andere sie gegenlesen („internes Review"). Soll aber die gleiche Software für PL e eingesetzt werden, so muss ein höherer Grad der Fehlervermeidung erreicht werden. Dann kann es notwendig sein, dass nicht die Programmierenden selbst die Spezifikation schreiben, sondern z. B. der „Projektleiter Software". Darüber hinaus könnte das Review dieser Spezifikation gemeinsam mit einer unabhängigeren Person, die z. B. für die Hardware-Projektierung zuständig ist, durchgeführt werden. Mehr Personen sehen (meist) mehr Fehler. Im Rahmen dieses Reports können die Anforderungen im Einzelnen sowie ihre mehr oder weniger wirksamen Ausprägungen leider nicht vollständig diskutiert werden. Daher sollen nur einige besondere Fälle angesprochen werden:

- Häufig realisiert eine zusammengehörende Software der SRP/CS mehrere Sicherheitsfunktionen SFx mit jeweils unterschiedlichen PL_r, z. B. SF1 und SF2 mit PL_r c, SF3 mit PL_r e. Beim Entwicklungszyklus, den Werkzeugen oder der Wirksamkeit der Aktivitäten (z. B. bei Modifikationen) wird man in der Praxis aber kaum zwischen den Sicherheitsfunktionen unterschiedlicher PL_r differenzieren können. In diesem Fall richten sich die Anforderungen zur Fehlervermeidung daher nach dem höchsten PL_r, hier e.

- Redundante SRP/CS, von denen nur ein Kanal programmierbar ist: Obwohl die programmierbare Elektronik nur einen Kanal darstellt, entspricht die Gesamtstruktur der Kategorie 3 oder 4. Mit diesen Strukturen werden häufig Sicherheitsfunktionen höherer PL_r, z. B. d oder e, realisiert. Wird eine programmierbare Elektronik in einem Kanal des Steuerungsteils in diversitärer Redundanz mit einer anderen Technologie als der programmierbar-elektronischen (z. B. fluidtechnisch) in dem anderen Kanal eingesetzt, dann können als Empfehlung des IFA aufgrund der geringeren Wahrscheinlichkeit eines gefährlichen Ausfalls durch systematische Fehler in dieser SRASW die normativen Anforderungen um eine PL-Stufe abgesenkt werden, z. B. anstelle von Anforderungen für PL_r d dann für PL_r c. Unabhängig davon sind auch die normativen Anforderungen an die SRESW einzuhalten (Abschnitt 6.3.10).

- Verwendung von Standard-SPS: Die Schaltungsbeispiele in diesem Report (siehe Kapitel 8, Seite 95 ff.) demonstrieren, dass sicherheitsbezogene Steuerungen prinzipiell auch mit Standard-SPS aufgebaut werden können. Es dürfte nur bei PL e sehr schwer sein, für die Hardware der SPS den erforderlichen hohen Diagnosedeckungsgrad *DC* von mindestens 99 % zu erreichen – sofern diese Diagnose durch die SRASW realisiert werden muss. Für PL a bis d werden die Softwareanforderungen an die Standard-SPS im Abschnitt 6.3.10 beschrieben. Zusätzlich müssen bei der Anwendungsprogrammierung die Anforderungen zur Fehlervermeidung bei SRASW (Abschnitte 4.6.1 und 4.6.3 der Norm) entsprechend dem PL_r erfüllt werden. Besonderer Berücksichtigung bedarf auch das Thema der systematischen Eignung.

- Bonus bei der Erstellung diversitärer SRESW: Bei zweikanaligen SRP/CS für Sicherheitsfunktion(en) mit PL_r e kann die SRESW beider Kanäle verschieden realisiert werden. Geht der Grad dieser Diversität so weit, dass der Code, die Gestaltung und sogar die Spezifikation unterschiedlich erstellt wurden, kann diese Software auch entsprechend den Anforderungen für PL d der DIN EN ISO 13849-1 entwickelt werden. Dabei ist es unerheblich, ob die SRP/CS nun verschiedene oder zwei identische Hardwarekanäle haben.

6.3.7 Passende Softwarewerkzeuge

Keine Software ohne Werkzeuge: Dies gilt besonders für sicherheitsbezogene Software. Daher sind Auswahl und Güte dieser Werkzeuge für die Fehlervermeidung und somit die Qualität der Sicherheitsfunktion entscheidende Faktoren. In DIN EN ISO 13849-1 werden vier Elemente betont:

- Entwicklungswerkzeuge:
  Zur Entwicklung sind geeignete und für den Einsatz bewährte Werkzeuge gefordert. In der Regel werden für SRASW zertifizierte Werkzeuge für Sicherheitskomponenten eingesetzt. Merkmale wie die Vermeidung und Aufdeckung von semantischen Fehlern, Einhaltung von Sprachteilmengen oder Überwachung von Programmierrichtlinien entlasten die Programmierenden und erhöhen die Softwarequalität.

- Bibliotheken:
  Die Systemgestaltung sollte vorhandene oder mitgelieferte Bibliotheken berücksichtigen und validierte Funktionen – soweit praktikabel – einsetzen. Es gilt: Je mehr das Programm auf bereits validierten oder sogar zertifizierten Funktionen basiert, umso weniger projektspezifische Softwareteile sind vor Inbetriebnahme noch selbst oder von einer externen Organisation zu validieren. Zur Systemintegration ist man gut beraten, für typische wiederkehrende Funktionen entsprechende Bausteine/Module mit dem notwendigen Aufwand nach DIN EN ISO 13849-1 selbst zu entwickeln, sodass sie auch von unabhängigen Personen regelmäßig und ohne Fehler wieder verwendbar bzw. prüfbar sind. Auch einzelne Bibliotheksfunktionen erfordern Spezifikation, Gestaltung, Testplan, Validierung usw.

- Geeignete Programmiersprachen:
  Für SRASW werden applikationsorientierte Sprachen, z. B. gemäß DIN EN 61131-3 [46], empfohlen. Selbst diese Sprachen sind bereits über das notwendige Maß hinaus sehr umfangreich und enthalten teilweise fehlerträchtige Konstrukte. Daher sollten Programmierende die Syntax nur eingeschränkt einsetzen. Entsprechende Sprachteilmengen werden meist durch das Werkzeug vorgegeben.

- Programmierrichtlinien:
  Zur Codierung der Softwarefunktionen sind geeignete Programmierrichtlinien zu beachten [47]. Dies sollten bestehende und akzeptierte Regeln einer anerkannten Organisa-

tion sein. Alternativ kann ein Unternehmen selbst passende Programmierregeln aufstellen, sofern diese praktisch oder theoretisch fundiert sind. Programmierrichtlinien regeln die Benutzung kritischer Sprachkonstrukte, den Umfang und die Schnittstelle von Softwarefunktionen, die Formatierung und Kommentierung des Codes, symbolische Namen von Funktionen und Variablen usw.

Diese Werkzeuge und Richtlinien sollten im Gestaltungsdokument vorgegeben werden.

6.3.8 Ungeliebt, aber wichtig: Dokumentation und Konfigurationsmanagement

Bevor der Hersteller die EG-Konformitätserklärung für eine Maschine ausstellt, muss er eine technische Dokumentation ausarbeiten. In Bezug auf die sicherheitsbezogene Software sind damit zunächst die Spezifikation der realisierten Sicherheitsfunktionen (Lastenheft), das Gestaltungsdokument (Pflichtenheft) sowie das gut kommentierte Programm gemeint. Zusätzlich sind die benutzten zertifizierten oder selber validierten Bibliotheksfunktionen mit ihrer Identifikation (Versionsnummer, Autor, Datum usw.) aufzulisten. Die Anwendung von eigenen Programmierrichtlinien und Sprachteilmengen ist ebenfalls zu dokumentieren. Falls das Werkzeug diese bereits enthält, genügt ein entsprechender Hinweis auf diese Merkmale. Bleibt noch die Dokumentation der Testaktivitäten: Oft werden Integrationstest und Validierung der Sicherheitsfunktionen zusammen durchgeführt. Diese Tests sind selbstverständlich zu planen und mit Testergebnissen zu dokumentieren.

Was ist mit Konfigurationsmanagement gemeint? Besonders bei sicherheitsbezogener Software ist verständlich und daher zu fordern, dass deren Entwicklung für alle Beteiligten und spätere Prüfungen nachvollzogen werden kann:

- Wer hat wann spezifiziert, programmiert, in Betrieb genommen, verifiziert, validiert?
- Womit wurde entwickelt, z. B. Werkzeuge und ihre Einstellungen, wieder verwendete Funktionen und ihre Identifikation, Programmierrichtlinie?
- Welche Programmversionen sind in welchen SRP/CS geladen?

Diese und weitere notwendige Informationen sowie alle relevanten Entwicklungsdokumente sind für eine spätere Nutzung – z. B. bei einer Modifikation nach einigen Jahren Betrieb – zu dokumentieren und geeignet zu archivieren.

6.3.9 Software ist ständig im Fluss: Modifikation

Erfahrungsgemäß wird auch eine zunächst getestete SRASW noch während der Inbetriebnahme einer Anlage/Maschine eifrig erweitert und angepasst. Diesen Vorgang nennt man „Modifikation“. Oft gehen diese Änderungen so weit, dass nicht nur die Codierung, sondern auch die ursprüngliche Spezifikation nicht mehr passt: Sie müsste eigentlich überarbeitet werden. Durch geänderte Sicherheitsfunktionen an der einen Seite der Anlage/Maschine können auch die anderen, zunächst nicht modifizierten Sicherheitsfunktionen betroffen sein. Oder es ergeben sich durch die Modifikationen Lücken im Sicherheitskonzept. Dies gilt es zu überprüfen und gegebenenfalls die notwendigen Phasen des V-Modells zu wiederholen.

Die Praxis zeigt aber, dass auch an einer installierten Maschine oder Maschinenanlage immer mal ein Not-Halt oder eine Schutztür ergänzt werden muss. Oft wird auch der Bearbeitungsprozess optimiert: Das Sicherheitskonzept ist ebenfalls anzupassen. Die existierende Software muss „modifiziert“ werden. Wohl gemerkt: bei SRP/CS, die schon länger und meist ohne durch Softwarefehler bedingte Ausfälle betrieben wurden – was auch bedeuten könnte, dass ein vorhandener „versteckter“ Fehler nur noch nicht wirksam wurde. Dies kann sich aber nach einer Modifikation ändern, wenn die Software z. B. nicht ausreichend strukturiert wurde und einzelne Module/Funktionen somit untereinander nicht vollständig rückwirkungsfrei sind.

In den beschriebenen Situationen zeigt sich oft Murphys Gesetz: Das Programm wurde schon vor etlichen Jahren geschrieben, mit der ursprünglichen Programmierung Befasste haben dringendere Aufgaben oder sind mittlerweile in anderen Unternehmen tätig. Hier zahlt es sich für die Sicherheit, aber auch Wirtschaftlichkeit der Maschinen oder Maschinenanlage aus, wenn die Software die oben genannten Merkmale aufweist: Lesbarkeit, Struktur, Verständlichkeit und auch das Merkmal, einfach und fehlervermeidend modifiziert werden zu können – unabhängig vom jeweils verfügbaren Personal.

Im Prinzip muss man nach einer Modifikation wieder dort im Entwicklungsprozess, also im V-Modell, einsteigen, wo etwas geändert wurde (Abbildung 6.11), z. B.:

- Bei geänderter Codierung sind Modul- und Integrationstest sowie die Validierung erneut durchzuführen.
- Musste gar die Spezifikation geändert werden, ist diese ebenfalls erneut zu verifizieren, z. B. durch Review (Gegenlesen) eines Kollegen oder einer Kollegin, damit sich keine Fehler an anderer Stelle der Spezifikation einschleichen. Dementsprechend müssen alle Entwicklungs- und Verifikationsmaßnahmen sowie die Validierung der betroffenen Sicherheitsfunktionen wiederholt werden.

Bei dem beschriebenen Aufwand ist es verständlich, dass der Einfluss einer Modifikation auf die Sicherheitsfunktionen systematisch zu untersuchen und zu dokumentieren ist. Da Modifikationen einen erheblichen Effekt auf die korrekte Ausführung der Sicherheitsfunktion haben können, muss schon zu Beginn ein geeignetes Verfahren festgelegt werden, gegebenenfalls einschließlich der Benennung verantwortlicher Personen.

6.3.10 Anforderungen an die Software von Standardkomponenten in SRP/CS

Sicherheitsbezogene Steuerungen werden oft auch mit Standardkomponenten für den industriellen Anwendungsbereich realisiert. Da die Norm Anforderungen an die Realisierung von SRESW und SRASW formuliert, sind diese auch in Bezug auf elektronische programmierbare Standardkomponenten zu erfüllen. Im Vergleich zu geprüften Sicherheitskomponenten ergeben sich jedoch Einschränkungen.

Anforderungen an SRESW

Die Verwendung von zugekauften industriellen Standardkomponenten, die nicht speziell für den Einsatz in Sicherheitsfunktionen entwickelt wurden, die aber Embedded-Software enthalten, wurde bisher in DIN EN ISO 13849-1 nicht thematisiert. Es gibt aber in der Praxis viele SRP/CS-Beispiele, die solche Standardkomponenten wie 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 für solche Standardkomponenten die Einhaltung der SRESW-Anforderungen in der Regel durch den Hersteller nicht bestätigt wird und durch den Integrator nicht nachträglich geleistet werden kann, wurde die Erfüllung der SRESW-Anforderungen bisher nicht nachgewiesen.

In DIN EN ISO 13849-1, Abschnitt 4.6.2, wird nun für solche Standardkomponenten der Verzicht auf den Nachweis der SRESW-Anforderungen unter folgenden Bedingungen erlaubt:

- 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 beim Einsatz von Standardkomponenten für SRP/CS nach Norm weitere, mehr hardwarebezogene Anforderungen zu beachten, z. B. hinsichtlich Vermeidung und Beherrschung systematischer Fehler oder Eignung für die zu erwartenden Umweltbedingungen, z. B. Klima, Vibration, elektromagnetische Verträglichkeit (EMV). Diese Anforderungen gelten unabhängig von 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 Frequenzumrichter.

Die qualitätsgesicherte Entwicklung nach ISO 900x wird in der Norm nicht explizit gefordert, kann aber in Hinsicht auf den Einsatz von Standardkomponenten als grundlegendes Sicherheitsprinzip angesehen werden.

Tabelle 6.6 zeigt die möglichen Kombinationen von PL und Kategorie mit Standardkomponenten und ob bzw. wie die Anforderungen an SRESW zu erfüllen sind.

Tabelle 6.6:
Anforderungen an die SRESW von Standardkomponenten (nach DIN EN ISO 13849-1)

Kombination Nr.	PL	Kategorie	Bedingungen	Anforderungen an SRESW der Standardkomponente
1	a, b	B, 2, 3	• Übereinstimmung mit zutreffenden Produktnormen • qualitätsgesicherte Entwicklung als grundlegendes Sicherheitsprinzip	Keine SRESW-Anforderungen an industrielle Standardkomponenten gestellt.
2	a, b, c	1	Generell keine Realisierung mit elektronischen Komponenten möglich, weil diese nicht als bewährte Bauteile nach DIN EN ISO 13849-1, Abschnitt 6.2.4, gelten	
3	c, d	2, 3	• wie Nr. 1 • zwei Kanäle mit technologischer Diversität, SRASW realisiert erforderliche Fehlererkennung (DC)	Keine SRESW-Anforderungen an industrielle Standardkomponenten gestellt.
4	c, d	2, 3	zwei Kanäle ohne technologische Diversität, SRASW realisiert erforderliche Fehlererkennung (DC)	Volle SRESW-Anforderungen nach DIN EN ISO 13849-1, Abschnitt 4.6.2, auch an industrielle Standardkomponenten gestellt. Sicherheitsbewertung durch den Komponentenhersteller erforderlich.
5	e	3, 4	PL e ist nach Abschnitt 4.6.2 der Norm für Standardkomponenten nicht möglich.	

Bleibt noch zu klären, was „Technologische Diversität“ bedeutet. Es meint, dass aufgrund der Diversität (der technischen Unterschiedlichkeit) zweier Kanäle die Wahrscheinlichkeit eines gefährlichen Ausfalls des SRP/CS durch einen Fehler in der SRESW stark verringert wird. Hier sind systematische Ausfälle und Ausfälle infolge gemeinsamer Ursache relevant.

In den folgenden Beispielen kann „technologische Diversität“ üblicherweise als erfüllt angesehen werden:

- Ein Kanal (Funktionskanal oder Testkanal) enthält Bauteile mit Embedded-Software. Der zweite Kanal enthält ausschließlich Bauteile ohne Embedded-Software, also mechanische, elektronische, elektromechanische, pneumatische oder hydraulische Bauteile.

- Beide Kanäle benutzen diversitäre Embedded-Software, z. B. verschiedene Betriebssysteme, auf gleicher oder unterschiedlicher Hardware.
  Anmerkung: Bei Verwendung gleicher Hardware muss besonders auf die systematische Eignung der Bauteile für den geforderten Performance Level geachtet werden.

- Beide Kanäle verwenden unterschiedliche Hardware (z. B. Mikroprozessoren mit unterschiedlichen Prozessorkernen), da angenommen wird, dass die Programmierung der zugehörigen eingebetteten Software in einer anderen Entwicklungsumgebung stattgefunden hat.

In den folgenden Beispielen kann „technologische Diversität“ üblicherweise nicht als erfüllt angesehen werden:

- Beide Kanäle benutzen gleichartige Bauteile von unterschiedlichen Herstellern ohne nähere Informationen zur Diversität der Embedded-Software. Hier kann üblicherweise nicht ausgeschlossen werden, dass beide Hersteller gleiche Embedded-Softwareteile benutzen, unter Umständen sogar auf identischer Hardware (Brandlabeling).

- Beide Kanäle verwenden Bauteile eines Herstellers unterschiedlichen Typs, ohne nähere Informationen zur Embedded Software.

Anforderungen an SRASW

Die Anforderungen an SRASW orientieren sich an dem PL, den das Subsystem mit der programmierbaren Standardkomponente erreichen soll. Wird z. B. eine Standardkomponente in einem Kanal in diversitärer Redundanz mit einer anderen Technologie (z. B. fluidtechnisch) in dem anderen Kanal in Kategorie 3 oder 4 eingesetzt, dann können als Empfehlung des IFA aufgrund der geringeren Wahrscheinlichkeit eines gefährlichen Ausfalls durch systematische Fehler in der SRASW die Anforderungen für SRASW im PL um eine Stufe abgesenkt werden (z. B. von PL d auf PL c). Dies lässt sich aus Abschnitt 7.4.3 „Synthese von Elementen zum Erreichen der erforderlichen systematischen Eignung“ der DIN EN 61508-2 [48] ableiten. Bei Kategorie 2 können nur die Anforderungen für die SRASW des Testkanals abgesenkt werden. Weitere Fälle werden im IFA Report 2/2016 [43], Kapitel 9, beschrieben.

6.4 Kombination von SRP/CS als Subsysteme

Bisher war in diesem Kapitel nur die Rede von einer kompletten Steuerung als SRP/CS, die sich als Ganzes auf eine Kategorie oder vorgesehene Architektur mit einem entsprechenden Performance Level abbilden lässt. Die Sicherheitsfunktion wird von einer solchen Steuerung, beginnend bei einem auslösenden Ereignis bis zum Erreichen des sicheren Zustands, vollständig alleine ausgeführt. In der Realität ist es aber oft notwendig, verschiedene SRP/CS als Subsysteme hintereinander zu schalten, die jeweils in Teilen die Sicherheitsfunktion ausführen. Solche Subsysteme können in unterschiedlichen Technologien aufgebaut sein und/oder verschiedene Kategorien oder Performance Level realisieren. Häufig werden etwa unterschiedliche Technologien in der Sensor- bzw. Logikebene (z. B. Elektronik in Kategorie 3) gegenüber der Antriebsebene (z. B. Hydraulik in Kategorie 1) verwendet, oder zugekaufte Geräte werden verkettet, z. B. Lichtgitter, elektronische Steuerung und pneumatische Ventilebene wie in Abbildung 6.13 (siehe Seite 72) dargestellt.

Einer der großen Vorteile des PL-Konzepts gegenüber den Kategorien ist es, dass damit ein Verfahren existiert, um Subsysteme verschiedener Kategorien, aber ähnlicher Performance Levels zu einem Gesamtsystem gemischter Kategorien, aber mit definiertem Gesamt-PL kombinieren zu können. In der Praxis können verschiedene Konstellationen auftreten, deren Behandlung im Folgenden näher erläutert wird:

- Gesamte Steuerung in einer Kategorie, keine Subsysteme: Für diesen Fall gelten die oben angeführten Erläuterungen, z. B. zu den vorgesehenen Architekturen.

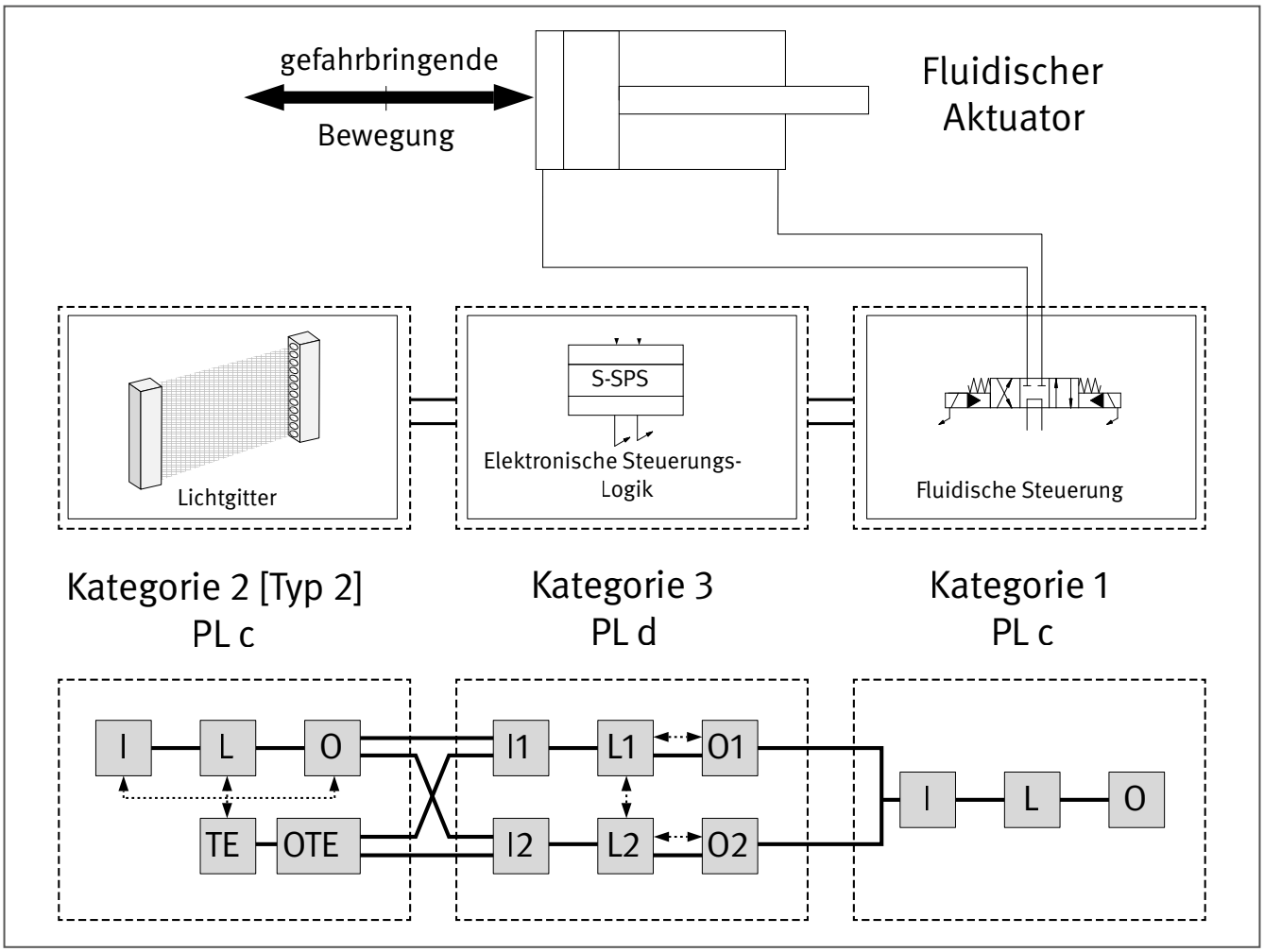
- Teilsteuerung/Subsystem in einer Kategorie: Für diesen Fall gelten ebenfalls die oben angeführten Erläuterungen, z. B. zu den vorgesehenen Architekturen, allerdings ist die genaue Definition des Anteils an der Sicherheitsfunktion und der Schnittstellen notwendig, an die weitere Subsysteme angeschlossen werden können, um die Sicherheitsfunktion zu komplettieren (siehe unten).

- Reihenschaltung von Subsystemen (z. B. unterschiedlicher Kategorie): Hier wird im Folgenden ein Verfahren vorgestellt, um aus den Kenndaten der Subsysteme (PL, durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde PFH_D) den PL und die PFH_D des Gesamtsystems zu ermitteln. Dabei ist ebenfalls die genaue Definition des Anteils an der Sicherheitsfunktion und der Schnittstellen zu beachten.

- Integration „gekapselter Subsysteme“, z. B. als zugekaufte Subsysteme, von denen an Kenndaten zur quantitativen Bestimmung des PL nur PFH_D und PL (oder SIL) bekannt sind und ggf. informativ die Kategorie (hierzu siehe Abschnitt 6.2.9 und Abbildung 6.14).

- Behandlung von Spezialfällen, z. B. Parallelschaltung von Subsystemen oder Verwendung von Subsystemen nur in einem Kanal einer Gesamtsteuerung.

Abbildung 6.13:
Reihenschaltung von Subsystemen zur Realisierung einer Sicherheitsfunktion



Die Reihenschaltung mehrerer Subsysteme auch unterschiedlicher Technologie sieht typischerweise aus wie in Abbildung 6.13 beispielhaft skizziert: Lichtgitter, elektronische Steuerung und Hydraulikventil werden hintereinander geschaltet, um insgesamt die Sicherheitsfunktion (Stillsetzung der gefahrbringenden Bewegung bei Unterbrechung eines Lichtstrahls) auszuführen. Der Hydraulikzylinder selbst ist kein Steuerungsteil und daher nicht Gegenstand einer PL-Bewertung.

Eine Kette ist immer nur so stark wie ihr schwächstes Glied: Diese Regel gilt für die Verknüpfung von Steuerungsteilen sowohl unterschiedlicher Kategorien als auch unterschiedlicher Performance Level. Wie die Praxis schon oft gezeigt hat, ist eine hydraulische Steuerung der Kategorie 1 wegen der hohen $MTTF_D$ der Komponenten unter Umständen vergleichbar sicher wie eine elektronische der Kategorie 3 mit mittlerem DC_{avg} und niedriger $MTTF_D$. Da Zu- und Abschläge zur Kategorie durch $MTTF_D$ und DC_{avg} im PL bereits berücksichtigt sind, orientiert sich der PL für die Zusammenschaltung am niedrigsten PL in der Serienschaltung und nicht an der niedrigsten Einzelkategorie. Mit der Anzahl der Steuerungselemente und ihrem jeweiligen PFH_D-Beitrag steigt auch die Gesamt-Ausfallwahrscheinlichkeit PFH_D des Gesamt-Systems. Daher kann der PL der Reihenschaltung gegenüber dem niedrigsten Subsystem-PL noch um eine Stufe verringert sein, wenn z. B. durch die PFH_D-Addition die PFH_D-Grenze zum nächstkleineren PL überschritten wird.

In der Regel liegen die Werte der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde PFH_D für alle Subsysteme vor (geeignet sind auch Werte für SIL und PFH_D nach DIN EN 61508 [10] oder DIN EN 62061 [11]). Dann kann daraus durch Aufaddieren der für den Gesamt-PL relevante PFH_D-Wert gebildet werden:

$$PFH_D = \sum_{i=1}^{N} PFH_{Di} = PFH_{D1} + PFH_{D2} + \ldots + PFH_{DN} \quad (5)$$

mit

N = Zahl der an der Sicherheitsfunktion beteiligten Subsysteme

PFH_D = durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde des Gesamtsystems

PFH_{Di} = durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde des i-ten Systems

Der Gesamt-PL wird dann begrenzt durch

- den niedrigsten PL aller an der Sicherheitsfunktion beteiligten Subsysteme (Begrenzung durch nicht quantifizierbare Aspekte wie Software und systematische Eignung) und

- den PL, der sich nach Tabelle 6.1 auf Seite 42 aus der nach Gleichung (5) berechneten PFH_D (Begrenzung durch quantifizierbare Aspekte) bestimmt.

Sind – in seltenen Fällen – PFH_D-Werte von an der Sicherheitsfunktion beteiligten Subsystemen nicht bekannt, so kann als grobe Abschätzung des erreichten Gesamt-PL auf der Basis der Subsystem-PL folgendes alternative Verfahren der DIN EN ISO 13849-1 verwendet werden:

- Zunächst wird der niedrigste PL aller in Reihe geschalteter Subsysteme ermittelt, dies ist $PL_{niedrig}$.

- Anschließend wird die Häufigkeit des Auftretens von $PL_{niedrig}$ in der Reihenschaltung der Subsysteme abgezählt, dies ist $N_{niedrig}$.

- Aus $PL_{niedrig}$ und $N_{niedrig}$ lässt sich dann nach Tabelle 6.7 der Gesamt-PL bestimmen.

Tabelle 6.7:
Vereinfachte PL-Bestimmung für in Reihe geschaltete Subsysteme

$PL_{niedrig}$	$N_{niedrig}$	Gesamt-PL
a	≥ 4	kein PL, nicht erlaubt
	≤ 3	a
b	≥ 3	
	≤ 2	b
c	≥ 3	
	≤ 2	c
d	≥ 4	
	≤ 3	d
e	≥ 4	
	≤ 3	e

Beim Verfahren nach Tabelle 6.7 wird als Näherung für die Subsysteme eine Ausfallwahrscheinlichkeit genau in der Mitte (auf einem logarithmischen Maßstab) des für den jeweiligen $PL_{niedrig}$ gültigen Bereichs angenommen.

Da bei beiden Methoden alle Subsystem-PL immer mindestens so groß sind wie der Gesamt-PL, ist auch gewährleistet, dass bei der Kombination alle Maßnahmen zu nicht quantifizierbaren, qualitativen Aspekten (z. B. systematische Ausfälle oder Software) in ausreichendem Maße berücksichtigt sind. Allerdings ist hier besonderes Augenmerk auf die Schnittstellen zwischen den Subsystemen zu richten:

- Alle Verbindungen (z. B. Leitungen oder Datenkommunikation durch Bussysteme) müssen im PL eines der beteiligten Subsysteme bereits berücksichtigt sein oder Fehler in den Verbindungen müssen ausgeschlossen oder vernachlässigt werden können.

- Die hintereinander geschalteten Subsysteme müssen an den Schnittstellen zueinander passen. Das heißt, jeder Ausgangsstatus eines ansteuernden Subsystems, der die Anforderung der Sicherheitsfunktion signalisiert, muss als auslösendes Ereignis für die Einleitung des sicheren Zustandes des nachgeordneten Subsystems geeignet sein.

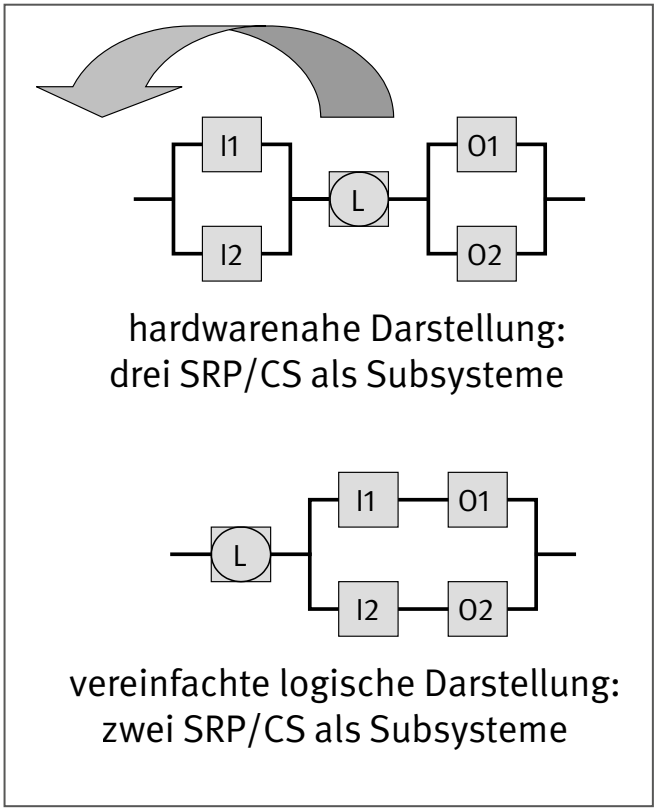
Bei hintereinander geschalteten zweikanaligen Systemen können bei der Addition der Subsystem-PFH_D-Werte geringe Rechenfehler zur unsicheren Seite auftreten. Streng genommen müssten die beiden Ausgänge des ersten Subsystems zusätzlich über Kreuz in die Eingänge des zweiten Subsystems eingelesen und verglichen werden. Oft erfolgt die kreuzweise Verdoppelung der Eingangsinformationen allerdings bereits intern auf der Eingangsebene des zweiten Subsystems. Um den Verkabelungsaufwand nicht unnötig in die Höhe zu treiben, ist die geringfügige PFH_D-Unterschätzung bei der Addition tolerabel.

Mit den bisher beschriebenen Regeln lassen sich Subsysteme bereits viel flexibler kombinieren, als dies in der ersten Ausgabe der Norm als DIN EN 954-1 auf der Basis der Kategorien möglich war. Diese Subsysteme können sehr unterschiedlicher Natur sein, z. B. hinsichtlich Technologie oder Kategorie, aber auch nach anderen Normen für sicherheitsbezogene Teile von Maschinensteuerungen entwickelt, die sich statt auf einen PL auf einen SIL beziehen (vgl. Abbildung 3.2).

In verknüpften Subsystemen kann es vorkommen, dass sich zweikanalige und (getestete) einkanalige Teile abwechseln. Abbildung 6.14 (siehe Seite 74) zeigt beispielhaft ein gekapseltes Logik-Subsystem (z. B. eine Sicherheits-SPS), an das zweikanalige Eingangs- und Ausgangselemente angeschlossen sind. Da im sicherheitsbezogenen Blockdiagramm bereits eine Abstraktion von der Hardwareebene stattfindet, ist die Reihenfolge der Subsysteme prinzipiell austauschbar. Es empfiehlt sich daher, wie in Abbildung 6.14 gezeigt, Subsysteme gleicher Struktur zusammenzufassen. Dadurch wird die PL-Bestimmung einfacher und unnötige Abschneideeffekte, z. B. die mehrfache Begrenzung der $MTTF_D$ eines Kanals auf 100 Jahre, werden vermieden.

Trotzdem bleiben Spezialfälle übrig, für die sich bisher keine oder nur sehr grobe Regeln angeben lassen. Ein Spezialfall betrifft die Parallelschaltung von Subsystemen: Hier lassen sich weder hinsichtlich der quantifizierbaren Aspekte (z. B. zweimal Kategorie 1 parallel ergibt noch keine Kategorie 3, da die Fehlererkennung fehlt) noch hinsichtlich der qualitativen Aspekte (z. B. systematische Ausfälle, Software, Ausfall infolge gemeinsamer Ursache) einfache und allgemein gültige Regeln aufstellen. Daher bleibt meist nur eine Neubewertung des Gesamtsystems, wobei unter Umständen auf einzelne Zwischenergebnisse (z. B. $MTTF_D$ oder *DC* von Blöcken) zurückgegriffen werden kann.

Abbildung 6.14:
Gemischte Subsysteme lassen sich im sicherheitsbezogenen Blockschaltbild umsortieren, z. B. indem gekapselte Subsysteme (hier „L“) vorgezogen werden



Einen weiteren Spezialfall stellt die Integration von bereits mit einem PL (oder SIL) oder einer durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde PFH_D versehenen Subsystemen als Block in einem SRP/CS dar. Hier kann als grobe Regel ohne Ansehen der inneren Struktur des Subsystems der Kehrwert der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde PFH_D als Block-$MTTF_D$ angesetzt werden. Da alle unter Umständen intern realisierten Diagnosemaßnahmen des Subsystems bereits in der Ausfallwahrscheinlichkeit berücksichtigt sind, können für den DC des Blocks nur zusätzliche, von außen auf das Subsystem wirkende Diagnosemaßnahmen herangezogen werden. Ausführlichere Hinweise finden sich in Abschnitt 2 von [32]. Dort wird in Abschnitt 3 auch der Fall angesprochen, dass mehr als zwei Funktionskanäle parallel geschaltet werden.

Eine weitere Frage, die sich in diesem Zusammenhang stellen könnte, betrifft die Zuordnung einer Kategorie für ein Gesamtsystem, das aus Subsystemen realisiert ist, die nur eine Angabe zur durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde PFH_D mitbringen. Hier fehlen neben Angaben zur inneren Struktur auch Angaben zur $MTTF_D$ jedes Kanals und zu DC_{avg}, für die je nach Kategorie Mindestanforderungen gelten. Daher gilt dasselbe wie für die Parallelschaltung: Als Alternative zu einer sehr groben Abschätzung bleibt nur die Neubewertung, unter Umständen unter Verwendung von Zwischenergebnissen.

6.5 PL-Bestimmung am Beispiel einer Planschneidemaschine mit diversitärer Redundanz in der Logiksteuerung (Kategorie 4 – PL e)

In diesem Abschnitt wird – begleitend zur allgemeinen Beschreibung – illustriert, wie man den PL in der Praxis ermittelt. Damit ist dieses ausführlich beschriebene Beispiel gleichzeitig eine Brücke zu Kapitel 8, in dem eine große Anzahl von Schaltungsbeispielen verschiedener PL, verschiedener Kategorien und unterschiedlicher Technologie präsentiert wird.

Die im Folgenden grau unterlegten Textkästen entsprechen der Kurzbeschreibung im Stil von Kapitel 8. Darüber hinaus werden zusätzliche Erläuterungen gegeben, deren Erwähnung bei jedem Schaltungsbeispiel in Kapitel 8 den Rahmen sprengen würde.

6.5.1 Sicherheitsfunktionen

Das Steuerungsbeispiel einer Planschneidemaschine in Abschnitt 5.7 wird hier wieder aufgegriffen. Von den sieben dort genannten Sicherheitsfunktionen wird exemplarisch die Realisierung von SF2 beschrieben, für die ein erforderlicher Performance Level PL_r = e ermittelt wurde. Da die verschiedenen Sicherheitsfunktionen unter Umständen auf dieselben Komponenten zurückgreifen, sind alle Sicherheitsfunktionen bei der Realisierung zu berücksichtigen. So fordert z. B. die Produktnorm für Planschneidemaschinen DIN EN 1010-3 für die Absicherung an der Bedienseite zusätzlich zu einer Zweihandschaltung (ZHS), z. B. im Hinblick auf die Sicherheitsfunktion SF3, eine – hier nicht gezeigte – berührungslos wirkende Schutzeinrichtung (BWS).

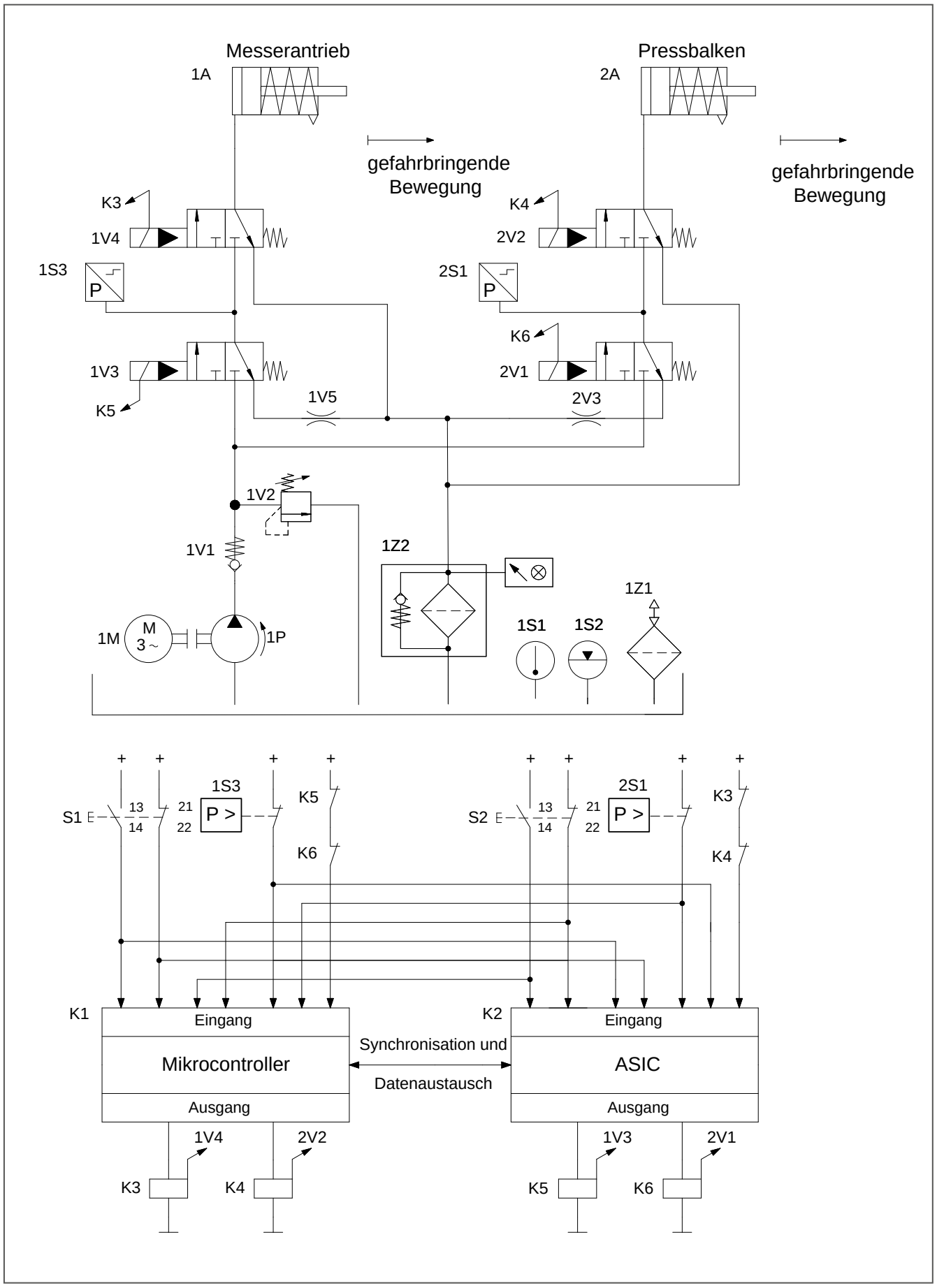
Sicherheitsfunktion (SF2)

- Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung.

6.5.2 Realisierung

Realisiert als Zweihandschaltung lässt sich diese Sicherheitsfunktion folgendermaßen beschreiben: Beim Loslassen mindestens eines der beiden Stellteile S1 und S2 wird die gefahrbringende Bewegung von Pressbalken und Messer unterbrochen und sowohl Messer als auch Pressbalken kehren durch Federkraft in ihre Ausgangslage zurück. Ein Neustart wird solange verhindert, bis beide Stellteile losgelassen wurden und ein neuer Zyklus durch die Zweihandschaltung eingeleitet wird. Zur Ortsbindung der Hände werden zwei Stellteile verwendet, die zum Start der Maschine synchron betätigt werden müssen (für Details, z. B. zur Manipulationssicherheit, siehe DIN EN 574). Die elektrischen Signale müssen zeitlich und logisch ausgewertet werden, wozu sich z. B. eine programmierbare Elektronik anbietet, die in der Regel auch die Bewegung des Pressbalkens und Messers steuert. Diese werden hier wegen der erforderlichen hohen Kräfte hydraulisch angetrieben. Im Sinne des Kapitels 5 (siehe Abschnitt 5.3.2) enthält die Sicherheitsfunktion beide Aktoren – Pressbalken und Messer –, da sie sich an derselben Gefahrenstelle befinden. Abbildung 6.15) zeigt in einem

Abbildung 6.15:
Prinzipschaltbild der elektrischen Ansteuerung eines hydraulischen Messerantriebs und eines hydraulischen Pressbalkens (wesentliche Bauelemente)



elektrohydraulischen Prinzipschaltplan, wie die sicherheitsrelevanten Steuerungsteile konkret realisiert werden. Die hier wie auch im Kapitel 8 gewählte Darstellung als Prinzipschaltplan muss aus Gründen der Übersichtlichkeit natürlich viele Details unterschlagen. Neben dem Großteil der funktionalen Steuerungsteile, die für ein prozessgerechtes Funktionieren der Maschine notwendig sind, werden auch sicherheitsrelevante Details wie Schutzbeschaltungen (Sicherungen, EMV) oder „Peripherie“ (Energieversorgung, Takt usw. für den Logikteil) ausgelassen. Wegen der notwendigen Einfehlersicherheit bzw. Toleranz gegenüber Anhäufung unerkannter Fehler sind in der Praxis z. B. auch Entkopplungselemente zwischen den verbundenen Eingängen beider Logikkanäle erforderlich, damit ein fehlerhafter Eingang eines Kanals nicht auch den anderen Kanal stört. Es ist daher wichtig zu verstehen, dass ein solcher Prinzipschaltplan keine direkte Vorlage zum Nachbau ist, sondern die sicherheitstechnische Struktur illustrieren soll.

6.5.3 Funktionsbeschreibung

Um den Schaltplan zu verstehen, ist eine Funktionsbeschreibung, die die Schaltungsstruktur und Signalpfade erläutert, unumgänglich. Dadurch soll es möglich sein, den funktionalen Ablauf bei der Ausführung der Sicherheitsfunktion (unter Umständen in verschiedenen Kanälen) und die realisierten Testmaßnahmen zu erkennen.

6.5.4 Sicherheitsbezogenes Blockdiagramm

Die Schaltungsbeschreibung in Verbindung mit dem Schaltplan und ggf. weiteren beschreibenden Dokumenten (ausführliche Spezifikation) ermöglicht die Bestimmung einer Steuerungskategorie und die Abbildung der realen Schaltung auf ein abstrahiertes sicherheitsbezogenes Blockdiagramm (Abbildung 6.16). In diesem Beispiel wird sehr schnell deutlich, dass die Sicherheitsfunktion zweikanalig ausgeführt wird. Daher kommt Kategorie 3 oder 4 in Betracht. Wegen der hochwertigen Diagnosemaßnahmen, die auch Fehlerkombinationen beherrschbar machen, liegt Kategorie 4 nahe. Der konkrete Nachweis hierzu erfolgt als Verifikationsschritt in Kapitel 7, ebenso wie die Überprüfung der quantitativen Anforderungen an $MTTF_D$, DC_{avg} und CCF (siehe unten). Bei der Umsetzung in das sicherheitsbezogene Blockdiagramm sind die Erläuterungen in den Abschnitten 6.2.8 und 6.2.9 hilfreich. Es hat sich bewährt, dazu den Signalpfad, beginnend an der Aktorseite, zu verfolgen, indem man sich fragt „Wie wird die gefahrbringende Bewegung angesteuert bzw. unterbunden?“, um dann über die Logik bis zu den Sensoren zu gelangen. Das SISTEMA-Kochbuch 1 [34] erläutert diesen Schritt „Vom Schaltbild zum Performance Level“ genauer. In diesem Beispiel ist zu beachten, dass die Stellteile S1 und S2 zueinander nicht redundant sind, auch wenn dies auf den ersten Blick so erscheinen mag, denn jeder Taster schützt unabhängig eine Hand der Bedienperson. Die Redundanz beginnt vielmehr in jedem Taster durch Verwendung von elektrischen Öffner-Schließer-Kombinationen. Jeder Steuerungskanal überwacht beide Hände bzw. Stellteile durch Auswertung mindestens je eines elektrischen Schaltkontakts. Im sicherheitsbezogenen Blockschaltbild ist daher in jedem Kanal ein Schließerkontakt, z. B. S1/13-14, und ein Öffnerkontakt, z. B. S2/21-22, enthalten. Das sicherheitsgerichtete Blockdiagramm unterscheidet sich hier deutlich vom funktionalen Schaltplan.

Funktionsbeschreibung

- Die Betätigung der Stellteile S1 und S2 der Zweihandschaltung startet die gefahrbringenden Bewegungen (Bearbeitungszyklus) des Pressbalkens und des Messers. Wird während dieses Zyklus auch nur ein Stellteil der Zweihandschaltung losgelassen oder erfolgt ein Signalwechsel in der Peripherie der Maschine nicht wie durch die Steuerung erwartet, stoppt der Zyklus und die Maschine geht in den sicheren Zustand.
- Mit Drücken der Stellteile S1 und S2 werden die ansteigenden Flanken der Signale beiden Verarbeitungskanälen K1 (Mikrocontroller) und K2 (ASIC) zugeführt. Erfüllen diese Signale die Anforderungen an die Gleichzeitigkeit (500 ms) nach der relevanten Norm DIN EN 574, setzen beide Verarbeitungskanäle die Ausgänge (Hilfsschütze K3 bis K6) für eine gültige Schnittanforderung.
- Die beiden Verarbeitungskanäle arbeiten synchron und werten auch interne Zwischenzustände der zyklischen Signalverarbeitung gegenseitig aus. Abweichungen von definierten Zwischenzuständen führen zum Stopp der Maschine. Ein Verarbeitungskanal wird durch einen Mikrocontroller K1 und der andere durch einen ASIC K2 gebildet. K1 und K2 führen während des Betriebs im Hintergrund Selbsttests durch.
- Fehler in den Stellteilen S1/S2 und in den Hilfsschützen K3 bis K6 (mit zwangsgeführten Rücklesekontakten) werden durch Kreuzvergleich in den Verarbeitungskanälen erkannt.
- Über die Druckschalter 1S3 und 2S1 werden Ausfälle der Ventile 1V3/1V4 und 2V1/2V2 bemerkt.
- Ein Ausfall der Ventile oder ein Hängenbleiben im offenen Zustand von 1V4 bzw. 2V2 wird durch eine stark verzögerte Rückzuggeschwindigkeit der Hydraulikzylinder bemerkt. Durch geeignete Auswertung der Drucksignale (Druckabfallzeit) erfolgt dies auch steuerungstechnisch.
- Ein Ausfall der Ventile oder ein Hängenbleiben im offenen Zustand von 1V3 bzw. 2V1 wird unmittelbar durch die Überwachung des Signalwechsels der Druckschalter 1S3 bzw. 2S1 bemerkt. Denn dann würde ein Druck signalisiert, obwohl kein Druck anstehen dürfte.
- Alle Maschinenzustände werden durch beide Verarbeitungskanäle überwacht. Durch den zyklischen Ablauf eines Schnittes werden alle Systemzustände ebenfalls zyklisch durchlaufen und Fehler können somit aufgedeckt werden.

Aus der konkreten Realisierung der Sicherheitsfunktion ergeben sich unter Umständen Einschränkungen oder Empfehlungen für die Anwendung. Zum Beispiel ist die Wirksamkeit einer Fehlererkennung durch den Arbeitsprozess naturgemäß sehr eng mit der Anwendung verbunden.

Bemerkungen

- Anwendung z. B. an Planschneidemaschinen (DIN EN 1010-3)

6.5.5 Eingangsgrößen zur quantitativen Bewertung des erreichten PL

An dieser Stelle sind alle Basisinformationen für die Bewertung des erreichten PL vorhanden. Mit Kenntnis der Kategorie und des sicherheitsbezogenen Blockdiagramms können für die einzelnen Blöcke zunächst $MTTF_D$ und *DC* bestimmt und außerdem die Maßnahmen gegen CCF für vorhandene Redundanzen bewertet werden. Daran schließen sich die „rechnerischen" Schritte zur Bestimmung der $MTTF_D$ jedes Kanals, des DC_{avg} und schließlich des PL an.

Um die $MTTF_D$-Ermittlung zu erläutern, sei zunächst der Block „K1" vorgestellt: Obwohl das Prinzipschaltbild (Abbildung 6.15) nur den Mikrocontroller zeigt, umfasst dieser Block weitere Elemente, die für die praktische Funktion notwendig sind (z. B. Schwingquarz). Alle Elemente, deren gefahrbringender Ausfall die Ausführung der Sicherheitsfunktion im betroffenen Kanal verhindern könnte, sind zu berücksichtigen. Dies sind in der Regel alle Elemente im sicherheitskritischen Signalpfad, z. B. zur Entkopplung, Rücklesung, zum EMV-Schutz oder Schutz vor Überspannungen. Diese Elemente sind meist im Sinne der grundlegenden und bewährten Sicherheitsprinzipien oder zum Erreichen des DC notwendig. Abbildung B.2 (siehe Seite 237) zeigt diese Herangehensweise anhand eines weiteren einfachen Beispiels. Als einfaches tabellarisches Verfahren zur Ermittlung der Block-$MTTF_D$ auf der Basis der Element-$MTTF_D$ bietet sich das „Parts Count"-Verfahren an, das in Tabelle 6.8 gezeigt wird (Abbildung B.3 auf Seite 239 zeigt im Vergleich das Vorgehen bei einer Ausfalleffektanalyse).

Die in der zweiten Spalte genannten Ausfallraten der Elemente wurden mithilfe der Datensammlung SN 29500 [49] ermittelt, was unter „Berechnung der Ausfallwahrscheinlichkeit" durch das Kürzel „[D]" gekennzeichnet wird (siehe Abschnitt 7.6).

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Bei 240 Arbeitstagen/Jahr, 8 Arbeitsstunden/Tag und 80 Sekunden Zykluszeit beträgt n_{op} 86 400 Zyklen/Jahr. Für S1 und S2 sowie K3 bis K6 ergibt sich bei einem B_{10D}-Wert von 2 000 000 Zyklen [H] eine $MTTF_D$ von 232 Jahren. Für den Mikrocontroller alleine wird eine $MTTF_D$ von 1142 Jahren ermittelt [D]. Der gleiche Wert wird auch für den ASIC eingesetzt [D]. Zusammen mit der zugehörigen Beschaltung ergibt sich für die Blöcke K1 und K2 jeweils eine $MTTF_D$ von 806 Jahren. Für die Hydraulikventile 1V3, 1V4, 2V1 und 2V2 gibt der Hersteller eine $MTTF_D$ von jeweils 150 Jahren [H] an. Diese Werte ergeben eine $MTTF_D$ jedes Kanals von 31,4 Jahren („hoch").
- DC_{avg}: Nach DIN EN ISO 13849-1, Anhang E, ergeben sich als DC-Werte für S1/S2: 99 % (Kreuzvergleich von Eingangssignalen ohne dynamischen Test mit häufigem Signalwechsel), für K1/K2: 90 % (Selbsttest durch Software und Kreuzvergleich), für K3 bis K6: 99 % (direkte Überwachung über zwangsgeführte Kontakte), für 1V3/2V1: 99 % (indirekte Überwachung durch den Druckschalter) und für 1V4/2V2: 99 % (indirekte Überwachung durch die Funktion und Messung einer geänderten Druckabfallzeit). Diese Werte ergeben einen DC_{avg} von 98,6 % („hoch").
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_D$ pro Kanal (31,4 Jahre) und DC_{avg} = 98,6 %, im Toleranzbereich von „hoch". Damit ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls von $9{,}7 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Die Validierung wird in der Fortsetzung dieses Beispiels in Abschnitt 7.6 näher beschrieben. Da gleiche Elemente mehrfach auftreten können (dritte Spalte), wird in der vierten Spalte die Gesamtausfallrate für jeden Elementtyp errechnet. Durch die globale Näherung, dass nur die Hälfte der Ausfälle gefahrbringend ist, ergibt sich der halbierte Wert in Spalte 5. Durch einfache Summation ergibt sich schließlich die Gesamtrate gefahrbringender Ausfälle für den Block K1. Spalte 6 zeigt die zugehörigen $MTTF_D$-Werte in Jahren, die sich als Kehrwerte der

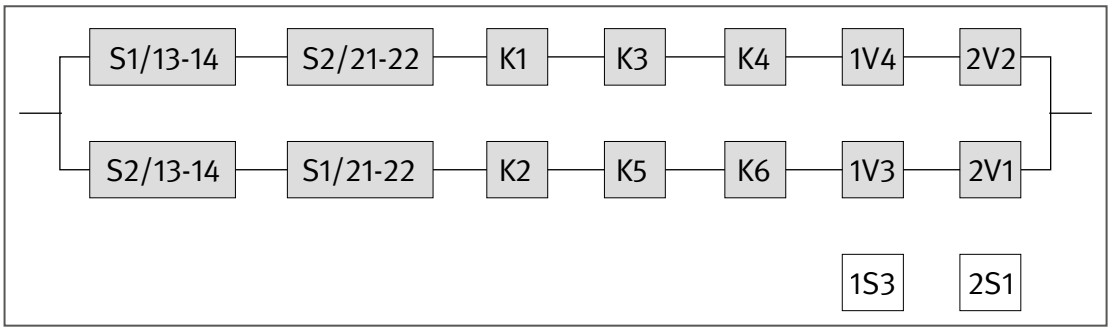


Abbildung 6.16: Sicherheitsbezogenes Blockdiagramm zum SRP/CS für die ausgewählte Sicherheitsfunktion SF2 an der Planschneidemaschine

gefahrbringenden Ausfallraten (aus Spalte 5, nach Umrechnung von Stunden in Jahre) ergeben. Für den Block K1 beträgt dieser Wert gerundet 806 Jahre. Da die verwendete Datenbank für den Mikrocontroller und den ASIC gleiche Ausfallraten nennt und die Beschaltung ähnlich ist, gilt für den Block K2 der gleiche $MTTF_D$-Wert von 806 Jahren.

Tabelle 6.8:
„Parts Count"-Verfahren für den „Mikrocontroller"-Block K1, basierend auf Ausfallraten λ, die der Datensammlung SN 29500 [48] entnommen wurden (angegeben in FIT, d. h. 10^{-9}/h)

Bauteil	Ausfallrate λ in FIT nach SN 29500	Anzahl	Gesamtausfallrate λ in FIT	Gesamtrate gefahrbringender Ausfälle λ_D in FIT	$MTTF_D$ in Jahren als Kehrwert von λ_D
Widerstand, Metallschicht	0,2	7	1,4	0,7	163 079
Kondensator, keine Leistung	1	4	4	2	57 078
Diode universal	1	3	3	1,5	76 104
Optokoppler mit Bipolar-Ausgang	15	2	30	15	7 610
Mikrocontroller	200	1	200	100	1 142
Schwingquarz	15	1	15	7,5	15 221
Transistor Bipolar-Kleinleistung	20	1	20	10	11 416
Hilfsrelais Kunststoffdicht	10	1	10	5	22 831
Summe für den „Mikrocontroller"-Block K1				141,7	806 Jahre

Für die Blöcke S1/S2 und K3 bis K6 werden Herstellerdaten (Kürzel „[H]") verwendet. Da Zuverlässigkeitsdaten nur für S1/S2 insgesamt (Betätigungsmechanik plus Öffnerkontakt und Schließerkontakt) verfügbar sind, können diese Werte als Abschätzung zur sicheren Seite für jeden der Kanäle verwendet werden, obwohl in jeden Kanal neben der Betätigungsmechanik nur die Schließerkontakte (z. B. S1/13-14) oder die Öffnerkontakte (z. B. S2/21-22) eingehen. Die angenommenen B_{10D}-Werte werden mit den aus Anhang D bekannten Formeln in $MTTF_D$-Werte umgerechnet:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{Zyklus}} \cdot 3\,600\,\frac{s}{h} = \frac{240\ \text{Tage/Jahr} \cdot 8\ \text{h/Tag}}{80\ \text{s/Zyklus}} \cdot 3\,600\,\frac{s}{h} = 86\,400\,\frac{\text{Zyklen}}{\text{Jahr}} \tag{6}$$

$$MTTF_D = \frac{B_{10D}}{0{,}1 \cdot n_{op}} = \frac{2\,000\,000\ \text{Zyklen}}{0{,}1 \cdot 86\,400\ \text{Zyklen/Jahr}} = 231{,}5\ \text{Jahre} \tag{7}$$

Die Betriebszeit elektromechanischer Komponenten wird auf den sogenannten T_{10D}-Wert (Zeit, nach der bis zu 10 % der betrachteten Bauteile gefährlich ausgefallen sind) begrenzt. Da dieser T_{10D}-Wert hier allerdings größer ist als die angenommene Gebrauchsdauer von 20 Jahren, ist er für die weitere Berechnung nicht relevant.

$$T_{10D} = \frac{B_{10D}}{n_{op}} = \frac{2\,000\,000\ \text{Zyklen}}{86\,400\ \text{Zyklen/Jahr}} = 23{,}2\ \text{Jahre} \tag{8}$$

Für die Hydraulikventile 1V3, 1V4, 2V1 und 2V2 gibt ebenfalls der Hersteller eine $MTTF_D$ von jeweils 150 Jahren [H] an.

In der Summe für einen Kanal (S1, S2, K1, K3, K4, 1V4, 2V2) ergibt sich nach Abschnitt 6.2.13 eine $MTTF_D$ von 31,4 Jahren, also „hoch":

$$\frac{1}{MTTF_D} = \frac{1}{232\ \text{Jahre}} + \frac{1}{232\ \text{Jahre}} + \frac{1}{806\ \text{Jahre}} + \frac{1}{232\ \text{Jahre}} + \frac{1}{232\ \text{Jahre}} + \frac{1}{150\ \text{Jahre}} + \frac{1}{150\ \text{Jahre}} = \frac{1}{31{,}4\ \text{Jahre}} \tag{9}$$

Da der zweite Kanal die gleiche $MTTF_D$ aufweist, entfällt die sonst erforderliche Symmetrisierung.

Die Validierung der angenommenen DC-Werte wird ebenfalls in Kapitel 7 näher beschrieben. Für K1 und K2 werden z. B. hochwertige Selbsttests durch Software und Kreuzvergleich inklusive der für Rechnersysteme erforderlichen speziellen Maßnahmen für variante und invariante Speicher und die Verarbeitungseinheit durchgeführt. In der Summe ergibt sich für das SRP/CS nach Abschnitt 6.2.14 ein DC_{avg} von 98,6 %, der unter Ausnutzung der 5-%-Toleranz im Bereich von „hoch“ liegt.

$$DC_{avg} = \frac{2 \cdot \left(\frac{99\,\%}{232\ \text{Jahre}} + \frac{99\,\%}{232\ \text{Jahre}} + \frac{90\,\%}{806\ \text{Jahre}} + \frac{99\,\%}{232\ \text{Jahre}} + \frac{99\,\%}{232\ \text{Jahre}} + \frac{99\,\%}{150\ \text{Jahre}} + \frac{99\,\%}{150\ \text{Jahre}} \right)}{2 \cdot \left(\frac{1}{232\ \text{Jahre}} + \frac{1}{232\ \text{Jahre}} + \frac{1}{806\ \text{Jahre}} + \frac{1}{232\ \text{Jahre}} + \frac{1}{232\ \text{Jahre}} + \frac{1}{150\ \text{Jahre}} + \frac{1}{150\ \text{Jahre}} \right)} = 98{,}6\,\% \quad (10)$$

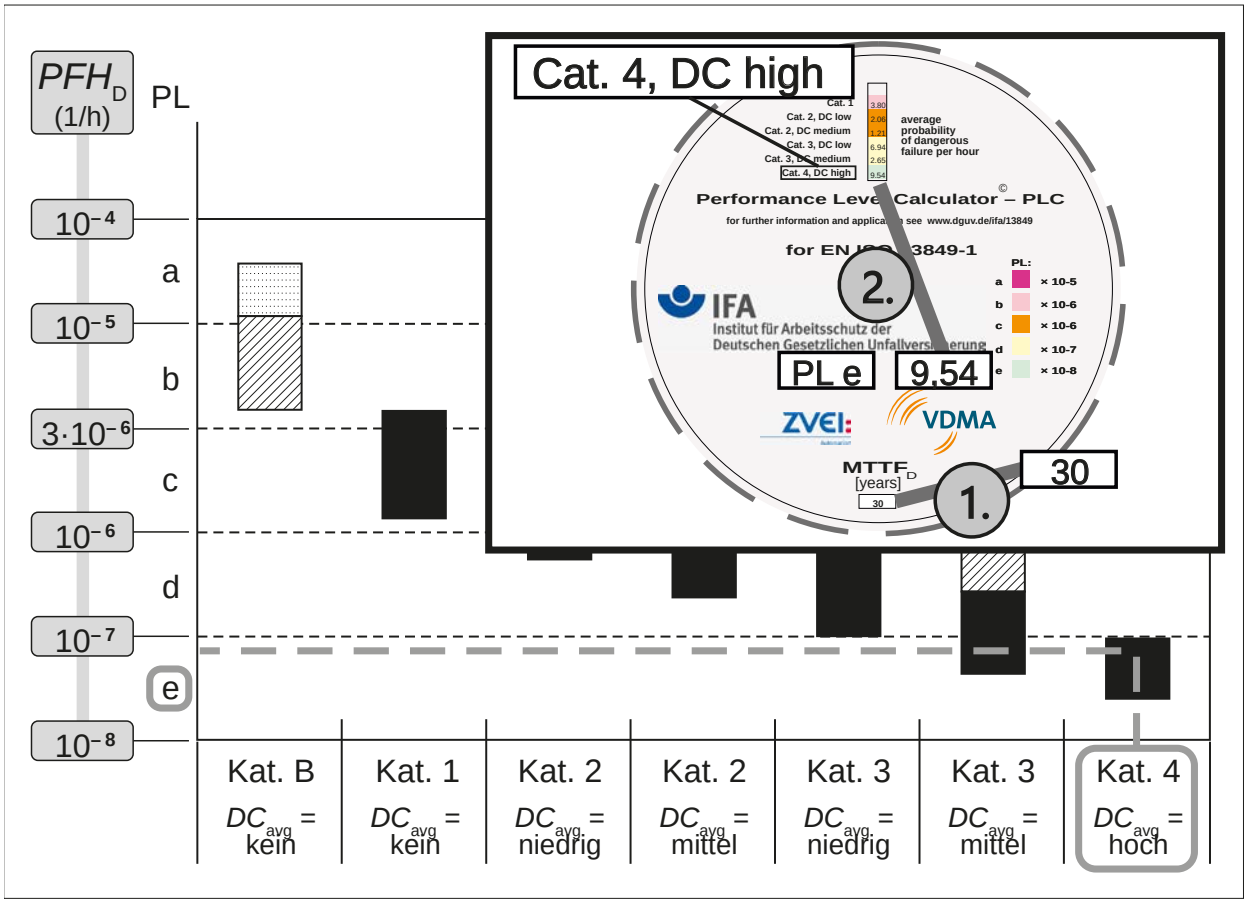
Die im grauen Kasten auf Seite 77 rechts genannten Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) sind weitgehend selbsterklärend, dennoch wird die Validierung in Kapitel 7 näher erläutert. Zusätzlich wirkt im elektrischen Subsystem die Maßnahme „Diversität“ und im hydraulischen Subsystem die Maßnahme „Verwendung bewährter Bauteile“ (siehe Anhang F). Mit der Erfüllung der Anforderungen an CCF, DC_{avg} „hoch“ und $MTTF_D$ „hoch“ werden auch die quantitativen Anforderungen für Kategorie 4 erfüllt.

6.5.6 Mehrere Wege zur quantitativen PL-Bestimmung

Bis zur PL-Bestimmung auf der Grundlage quantifizierbarer Aspekte ist es nun nicht mehr weit. Mit den Ergebnissen für Kategorie, DC_{avg} und $MTTF_D$ lässt sich grafisch durch das Säulendiagramm bestätigen, dass PL e erreicht wird (siehe Abbildung 6.17). Die tabellarischen Werte in Anhang K der Norm oder die darauf basierende PLC-Drehscheibe des IFA [16] liefern folgendes Ergebnis:

Kategorie	CCF	DC_{avg}	$MTTF_D$	PFH_D
4	OK	„hoch“	„hoch“ (abgerundet 30 Jahre)	$9{,}5 \cdot 10^{-8}$/Stunde (PL e)

Abbildung 6.17:
PL-Bestimmung mithilfe des Säulendiagramms bzw. der Drehscheibe



Sehr viel mehr Komfort bei der Verwaltung, Dokumentation und Berechnung aller Zwischenergebnisse bietet die vom IFA kostenlos zur Verfügung gestellte Software SISTEMA (siehe Anhang H). Alle bisher dargestellten quantitativen Anforderungen zur PL-Bestimmung lassen sich damit einfach erfassen und alle Rechenschritte inklusive der rechnerischen PL-Bestimmung sind automatisiert. Als besondere Option ist eine Berechnung mit den genauen DC_{avg}- und $MTTF_D$-Werten möglich. Für DC_{avg} wird mit dem genauen (hier schlechteren) Wert 98,6 % gerechnet, statt die 5-%-Toleranz zu DC_{avg} „hoch“ auszunutzen und gerundete 99 % anzusetzen (zu den Toleranzen bei *DC* und $MTTF_D$ vgl. Anmerkungen 2 in den Tabellen 4 und 5 der Norm). Die noch innerhalb des Toleranzbereichs liegende Unterschreitung der 99-%-Marke für Kategorie 4 wird von SISTEMA allerdings mit einem Warnhinweis quittiert. Die Rechnung mit dem genauen $MTTF_D$-Wert von 31,4 Jahren bringt ein vergleichbares Ergebnis gegenüber der Rechnung mit dem abgerundeten Wert von 30 Jahren für $MTTF_D$ „hoch“. Es ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde von $9{,}7 \cdot 10^{-8}$/Stunde (siehe Abbildung 6.18).

Es schließt sich nun die Bewertung der nicht quantifizierbaren qualitativen Aspekte bei der PL-Bestimmung an, zunächst für systematische Ausfälle.

6.5.7 Systematische Ausfälle

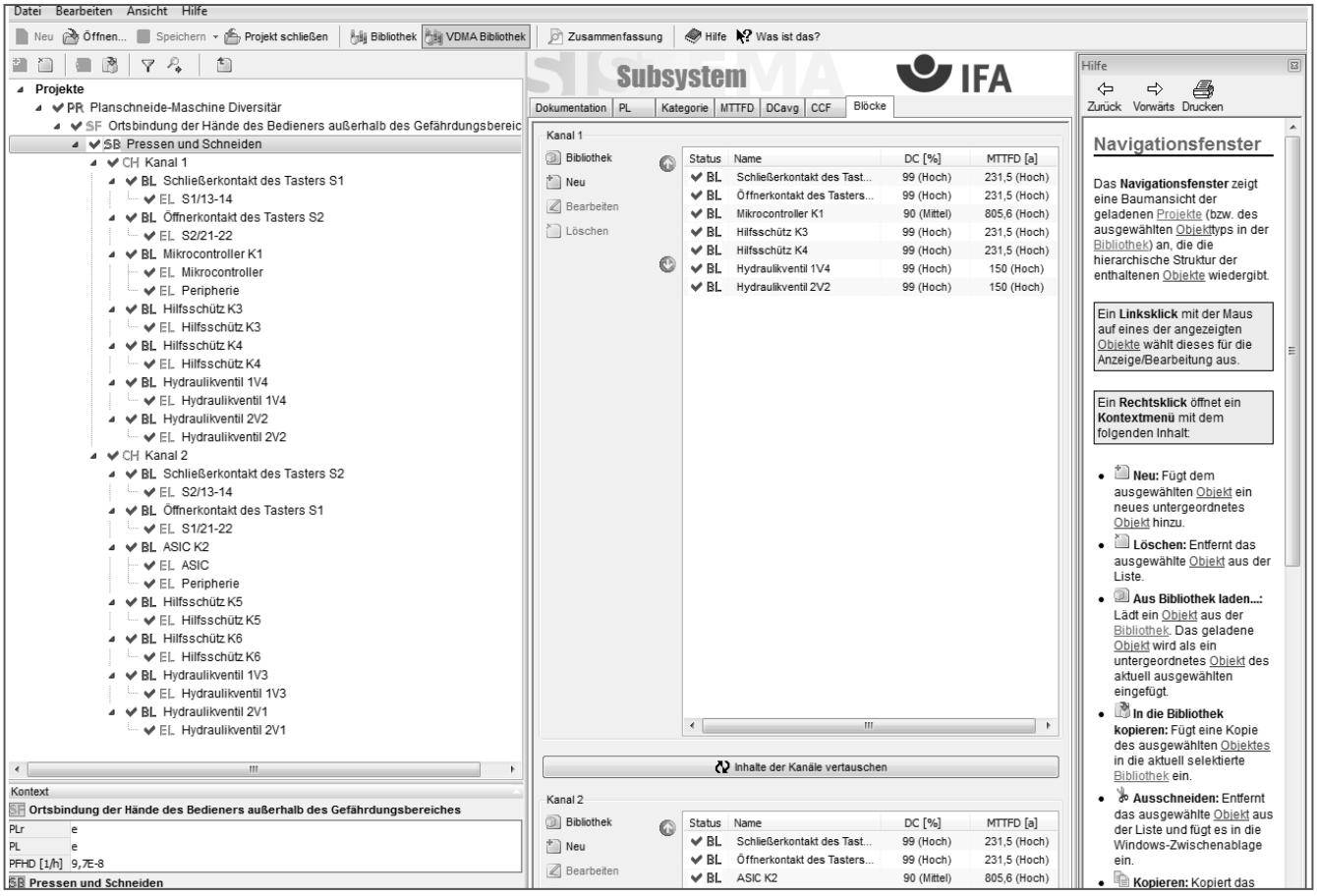
Der gewählte Entwurf der Steuerung verwendet mit einem diversitären Ansatz für die Logiksteuerung eine höchst wirksame Maßnahme gegen den Einfluss systematischer Ausfälle. Selbstverständlich müssen im Zuge der Realisierung weitere Maßnahmen implementiert werden, um z. B. die Auswirkungen von Spannungsausfall, Spannungsschwankungen, Überspannung und Unterspannung zu beherrschen. Einige der erforderlichen Maßnahmen sind schon in dem gewählten Entwurf zu erkennen, u. a.:

- Verwendung des Ruhestromprinzips; hierdurch ist sichergestellt, dass der energielose Zustand nicht zu einem Ansteuersignal führen kann (z. B. bei einem Drahtbruch).

- Ausfallerkennung durch automatische Tests; hier werden in den beiden Steuerungskanälen jeweils verschiedene Tests ausgeführt, die frühzeitig Fehler erkennen können und jeweils unabhängig vom Nachbarkanal den sicheren Zustand selbst einleiten können.

- Testung durch redundante Hardware; hierdurch können mithilfe der konstruktionsbedingten Diversität zusätzlich Fehler durch Umwelteinflüsse beherrscht werden, die sich in den einzelnen Kanälen nicht gleichartig auswirken.

Abbildung 6.18:
PL-Bestimmung mithilfe von SISTEMA



- Verwendung von Hilfsschützen mit zwangsgeführten Kontakten; durch das Rücklesen entsprechender Kontakte können gefährliche Ausfälle der Hilfsschütze und unter Umständen anderer Schaltungsteile erkannt werden.

- Überwachung des Programmablaufs; der ASIC wird z. B. genutzt, um den Programmablauf des Mikrocontrollerkanals zu überwachen.

Auf zwei Details zu systematischen Ausfällen, die im ersten Fall mit der Applikation und im zweiten Fall mit dem Entwurfsprozess zusammenhängen, sei besonders hingewiesen:

- Bei der Gestaltung des Hydrauliksystems für Planschneidemaschinen ist der Papierstaubanfall zu berücksichtigen. So kann z. B. mit Papierstaub verunreinigtes Hydrauliköl die sichere Funktion einer Planschneidemaschine gefährden. Aus diesem Grund muss im Besonderen auf eine gute Filtrierung des Druckmediums geachtet werden. Weiterhin muss das externe Einbringen von Papierstaub in das Hydrauliksystem durch z. B. Abstreifringe an Kolbenstangen und Tankbelüftungsfilter verhindert werden.

- Fehlervermeidende Maßnahmen bei der ASIC-Entwicklung gemäß ASIC-Entwicklungs-Lebenszyklus nach DIN EN 61508-2. In dieser Norm ist für die Entwicklung eines ASICs ein V-Modell in Anlehnung an das aus der Softwareentwicklung bekannte V-Modell vorgesehen.

6.5.8 Ergonomische Aspekte

In diesem Beispiel gibt es eine sicherheitsrelevante Schnittstelle zwischen dem Benutzer und der Steuerung: die Zweihandschaltung (ZHS) mit den Stellteilen S1 und S2. Hier sind einige ergonomische Aspekte zu berücksichtigen, damit keine Person während der geplanten Verwendung und vernünftigerweise vorhersehbaren Fehlanwendung unmittelbar oder auf Dauer durch Fehlbelastungen gefährdet wird. Diese Benutzerschnittstellen können für die meisten Maschinen mit der Checkliste Ergonomische Maschinengestaltung, DGUV Informationen 209-068 und 209-069 [30], überprüft werden. Folgende Aspekte sind dabei u. a. zu betrachten:

- Höhe und Orientierung der Stellteile in Bezug auf die Bedienperson

- Greif- und Beinraum bei der üblicherweise stehenden Bedienung

- mit der Bedienaufgabe abgestimmte Anordnung und gute Erreichbarkeit außerhalb des Gefahrenraums

- Beobachtbarkeit des Schneidevorgangs vom Ort der ZHS aus

- Mindestabmessungen und Form der Stellteile (ergonomische Gestaltung unter Beachtung der Vorgaben nach DIN EN 574)

- leichte Betätigung mit geringen Kräften, aber unbeabsichtigtes Betätigen durch konstruktive Maßnahmen verhindern

- widerstandsfähige Gestaltung sowie geeignete Kennzeichnung und Farbgebung der Taster

- Gestaltung der ZHS, die eine Manipulation und damit Umgehung der Ortsbindung verhindert

6.5.9 Anforderungen an die Software, speziell SRESW

Im Folgenden wird die Realisierung der sicherheitsbezogenen Firmware für den Mikrocontroller K1 beispielhaft dargestellt. Es handelt sich um eine Embedded-Software (SRESW), für die PL_r = e gilt. Aufgrund des diversitären Ansatzes für die Logiksteuerung – der zweite Kanal wird als ASIC ausgeführt – können die Anforderungen entsprechend der Anmerkung in Abschnitt 4.6.2 der Norm heruntergestuft werden: *„Wenn Diversität in Spezifikation, Entwurf und Codierung für die beiden Kanäle des SRP/CS in Kategorie 3 oder 4 verwendet wird, kann ein PL_r = e mit den oben erwähnten Maßnahmen für PL_r von c oder d erreicht werden.“*

Der Entwicklungsprozess für die Firmware orientiert sich am V-Modell in Abbildung 6.11 und ist in das zertifizierte Qualitätsmanagement des Herstellers eingebettet. Auf der Basis der Spezifikation der gesamten sicherheitsbezogenen Steuerung wird zunächst die Spezifikation der Softwaresicherheitsanforderungen für die Firmware, das Lastenheft, geschrieben. Dieses Dokument beschreibt den Anteil, den die Firmware zu den Sicherheitsfunktionen der Maschine beiträgt, geforderte Reaktionszeiten bezogen auf K1, Reaktionen bei erkannten Fehlern, Schnittstellen zu anderen Subsystemen, Abhängigkeiten von Betriebsarten usw. Zusätzlich werden alle nach Abschnitt 6.3.2 der Norm für PL c oder d geforderten fehlervermeidenden Maßnahmen festgelegt. Die Spezifikation wird dann z. B. vom „Projektleiter Sicherheit“ gegengelesen (Review) und gegebenenfalls werden Änderungen eingepflegt. Nach Freigabe der Spezifikation kann die Systemgestaltung beginnen.

Zur Softwarearchitektur: Der Mikrocontroller erhält kein Betriebssystem, sondern es werden mehrere Tasks definiert, die per Timerinterrupt, durch eine einfache Taskverwaltung gesteuert, in definierten Zeitabständen zur Ausführung kommen. Einige niederprioritäre Tasks sind für die Standardfunktionen der Planschneidemaschine reserviert, während die hochprioritären Tasks die oben spezifizierten sicherheitsbezogenen Funktionen ausführen. Die Determiniertheit dieser Taskaufrufe ist für die geforderte hohe Synchronität der beiden Kanäle und die kurzen Reaktionszeiten notwendig. In Leerlaufzeiten der Tasks werden die zyklischen Selbsttests für die Beherrschung zufälliger Hardwareausfälle ausgeführt.

Die Gestaltung der Softwarearchitektur und der erforderlichen Softwaremodule und Funktionen zur Realisierung der oben beschriebenen Software werden in einem weiteren Dokument, dem Pflichtenheft zur System- und Modulgestaltung, zusammengefasst. Für die Fehlervermeidung während des gesamten Lebenszyklus sind die geeignete Modularisierung und in diesem Fall auch eine deutliche Abgrenzung der SRESW zur nicht sicherheitsbezogenen Software besonders wichtig. Wo für das Verständnis notwendig, sind Aufbau und Ablauf der Software

grafisch dargestellt. Ergänzt werden Vorgaben über die einzusetzende Programmiersprache, hier ANSI C mit compilerspezifischen Spracherweiterungen, und die Entwicklungswerkzeuge, z. B. Compiler, Versionsverwaltung, Konfigurationsmanagement; alle bereits mit langjähriger positiver Erfahrung im Einsatz. Ebenso werden die Programmierrichtlinien und Methoden zur toolgestützten statischen Analyse für die Verifikation der Codierung festgelegt. Die Planung von Modul- und Integrationstest wird ebenfalls schon in diesem Dokument festgeschrieben. Nach einem erneuten Review z. B. durch den „Entwicklungsleiter Software“ wird das Pflichtenheft als Vorgabe für die Codierung freigegeben. In diesem Review wird auch verifiziert, ob die Anforderungen der Softwarespezifikation erfüllt sind.

Nun beginnt die eigentliche Codierung unter Berücksichtigung der Programmierrichtlinie. Die Programmierrichtlinie schreibt neben Regeln für die bessere Lesbarkeit des Codes u. a. auch die eingeschränkte Verwendung von kritischen Sprachkonstrukten vor. Die Einhaltung der Programmierrichtlinie wird mitlaufend zur Codierung durch entsprechende Tools gewährleistet. Für die semantische (inhaltliche) Verifikation des fertigen Codes gegen das Pflichtenheft führt die Programmiererin/der Programmierer im Kollegenkreis ein Walk-Through durch, bei dem gleichzeitig der Programmablauf und der Datenfluss von kritischen Signalen analysiert werden.

Mit den üblichen Modultests werden die Funktionen und Schnittstellen einerseits auf Korrektheit und andererseits auf Übereinstimmung mit der Modulgestaltung geprüft. Es folgt die Integration der Software und der Tests gemeinsam mit der Hardware des Mikrocontrollers K1. Danach wird K1 zusammen mit dem ASIC-Kanal K2 verschaltet, um die Synchronisierung, den Datenaustausch und die Fehlererkennung beider Kanäle gemeinsam zu testen. Alle Tests werden dokumentiert.

Bei diesem Integrationstest könnte sich ergeben, dass der Mikrocontroller nicht so leistungsfähig ist wie vorher angenommen. In diesem Fall müsste die Softwarearchitektur, konkret die zeitliche Einplanung der Tasks und auch die Zuordnung von Funktionen zu den Tasks, geändert werden. Die Spezifikation der Softwaresicherheitsanforderungen würde sich dadurch nicht ändern, aber die System- und Modulgestaltung müsste angepasst und erneut einem Review unterzogen werden, um die Übereinstimmung mit der Spezifikation zu gewährleisten. Dies wäre ein Beispiel dafür, wie notwendige technische Änderungen während der Entwicklung zu einem erneuten Durchlauf des V-Modells führen können, damit die Änderungen qualitätsgesichert umgesetzt werden. Die Änderungen würden codiert und die Modul- sowie Integrationstests müssten erneut durchgeführt werden.

Für den Fall, dass die Firmware nach Auslieferung der ersten Serienprodukte noch geändert werden müsste, sollten entsprechende Maßnahmen wie Einflussanalyse der Änderungen und angemessene Entwicklungsaktivitäten nach V-Modell bereits in der Entwicklungsorganisation festgelegt werden.

6.5.10 Kombination von SRP/CS

Da die gesamten SRP/CS durchgängig in einer Kategorie strukturiert sind und keine Subsysteme kombiniert werden, ist eine diesbezügliche Betrachtung nach Abschnitt 6.4 nicht notwendig. Gleichwohl müssen die verschiedenen Komponenten und Technologien an den Schnittstellen natürlich zueinander passen. Validierungsaspekte zur Integration werden in Kapitel 7 angesprochen.

6.5.11 Weitere Erläuterungen

Da auch in diesem ausführlichen Schaltungsbeispiel viele sicherheitsrelevante Designaspekte nur angerissen werden können, ist hier wie bei den meisten folgenden Schaltungsbeispielen eine Liste mit hilfreicher Literatur angefügt, die weitere Erläuterungen bereitstellt und auf zusätzliche zu beachtende Anforderungen hinweist.

Weiterführende Literatur

- DIN EN 1010-3: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 3: Schneidmaschinen (06.10). Beuth, Berlin 2010
- DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (02/11). Beuth, Berlin 2011
- DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze (12.08). Beuth, Berlin 2008

Weitere Ausführungen, speziell hinsichtlich der Verifikation und Validierung, folgen in der Fortsetzung dieses Beispiels einer Planschneidemaschine in Kapitel 7.

7 Verifikation und Validierung

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Der gesamte Abschnitt wurde umfassend redaktionell überarbeitet.
- In Abschnitt 7.1.2 zum Verifikations- und Validierungsplan sind weitere Details zu dessen typischen Inhalten hinzugekommen. Abschnitt 7.1.3 enthält nun weitere Informationen (Referenzen) zu Fehlerlisten. Ebenso ergänzt sind in Abschnitt 7.1.4 die üblichen Dokumentationsformen der für V&V-Aktivitäten benötigten Dokumentation.
- Als nun eigenständiger Abschnitt sind in Abschnitt 7.2 die Informationen zur Verifikation der Spezifikation und der Technischen Dokumentation zusammengefasst.
- In Abschnitt 7.5 zur Benutzerinformation wurde nunmehr auf eine Aufzählung erforderlicher Inhalte verzichtet. Stattdessen sind Referenzen auf Standards für Inhalte und Gestaltung von Benutzerinformationen gegeben.
- Auf die Inbetriebnahmeprüfung wird in Abschnitt 7.6 Bezug genommen.
- Der neue Abschnitt 7.7 widmet sich, der Thematisierung in DIN EN ISO 13849-2, 4.1. c) folgend, dem Aspekt der Verifikation der Benutzerschnittstelle.
- Das Beispiel zur Verifikation und Validierung der Planschneidemaschine in Abschnitt 7.8 wurde aktualisiert.

Auf das mit dem neuen Anhang E der DIN EN ISO 13849-2 [6] informativ behandelte „Beispiel für die Validierung von Fehlverhalten und Mitteln zur Diagnose“ geht der Report nicht ein.

Bezüglich der datierten Verweisung von DIN EN ISO 13849-2 [6] auf ISO 13849-1:2006 sei der Hinweis gegeben, dass sich der Report auch in diesem Abschnitt auf die bereits aktuellere Ausgabe DIN EN ISO 13849-1:2016 stützt.

Verifikation und Validierung bezeichnen qualitätssichernde Maßnahmen zur Vermeidung von Fehlern während des Entwurfes und der Realisierung sicherheitsbezogener Teile von Steuerungen (SRP/CS), die Sicherheitsfunktionen ausführen. Besonders Teil 2 der DIN EN ISO 13849 [6] beschäftigt sich ausgiebig mit diesem Thema.

Die **Verifikation** umfasst die Analysen und Prüfungen für SRP/CS bzw. deren Teilaspekte, die feststellen, ob die erzielten Resultate einer Entwicklungsphase bzw. eines Konstruktionsabschnittes den Vorgaben für diese Phase entsprechen, also z. B. ob das Schaltungslayout dem Schaltungsentwurf entspricht oder ob in der Spezifikation die für die vorgesehenen Anwendungen relevanten Anforderungen umfassend (vollständig) zusammengestellt sind.

Als **Validierung** wird der Nachweis darüber bezeichnet, ob eine Eignung bezogen auf die gestellten Anforderungen gegeben ist. Es wird also während oder am Ende des Entwicklungs-/Konstruktionsprozesses überprüft, ob im Allgemeinen die spezifizierten funktionalen und konstruktiven Anforderungen an den sicherheitsrelevanten Teil der Maschinensteuerung erreicht wurden bzw. im Kontext der DIN EN ISO 13849, ob das SRP/CS für jede Sicherheitsfunktion die entsprechenden Anforderungen dieser Norm erfüllt.

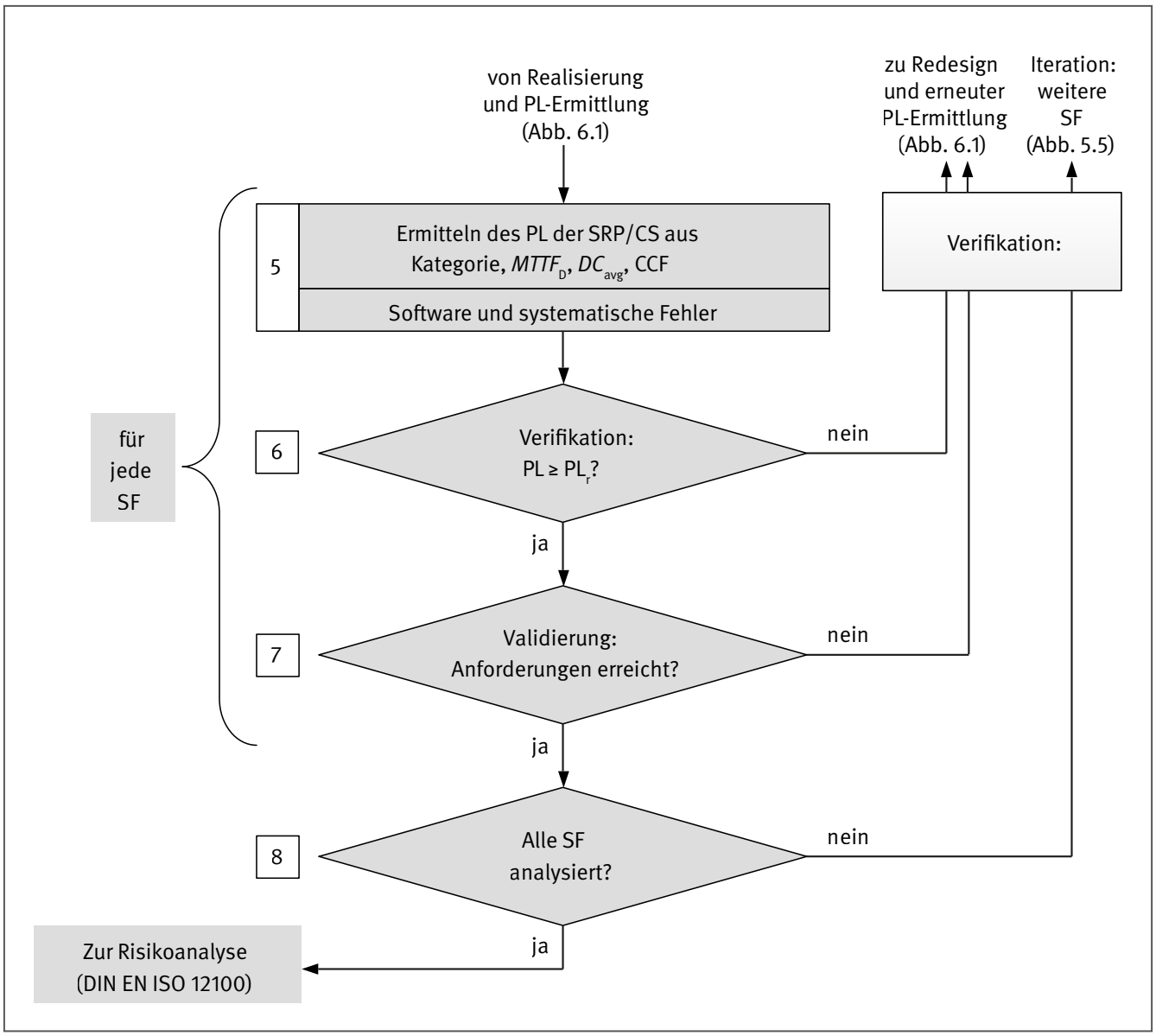
Der Prozess der Beurteilung einer Sicherheitsfunktion in ihrer Realisierung durch SRP/CS ist also ein Zusammenspiel aus Verifikations- und Validierungsschritten, die sowohl Teilaspekte als auch die Gesamtheit der SRP/CS behandeln. Die Begriffe Verifikation und Validierung werden folgend auch als V&V-Aktivitäten bezeichnet.

Hinweis: Dieses Kapitel 7 behandelt das Verifikations- und Validierungsverfahren für SRP/CS im Sinne eines Nachweisprozesses zur Übereinstimmung mit der Norm DIN EN ISO 13849. Weder können hier Einzelheiten der Methoden genannter V&V-Aktivitäten „gelehrt“ noch können alle für eine Konformität des Produkts zur Maschinenrichtlinie notwendigen Teilprüfungen wie beispielsweise zum Schutz gegen elektrischen Schlag, zur technischen (elektrischen, hydraulischen, pneumatischen) Ausrüstung oder zur Ergonomie behandelt werden.

7.1 Das Verfahren der Verifikation und Validierung

Abbildung 7.1 (siehe Seite 84) zeigt den relevanten Ausschnitt des iterativen Prozesses zur Gestaltung von SRP/CS der DIN EN ISO 13849-1 [5], Abbildung 3, der sich mit den Aktivitäten der Verifikation und Validierung befasst.

Abbildung 7.1:
V&V-Aktivitäten der DIN EN ISO 13849-1



Zur Planung der Durchführung von V&V-Aktivitäten mit den dort relevanten Tätigkeiten und einem sinnvollen Vorgehen kann Abbildung 7.2 herangezogen werden. Sie entstammt Teil 2 der DIN EN ISO 13849, wurde jedoch grafisch verändert, um die V&V-Aktivitäten deutlicher darzustellen.

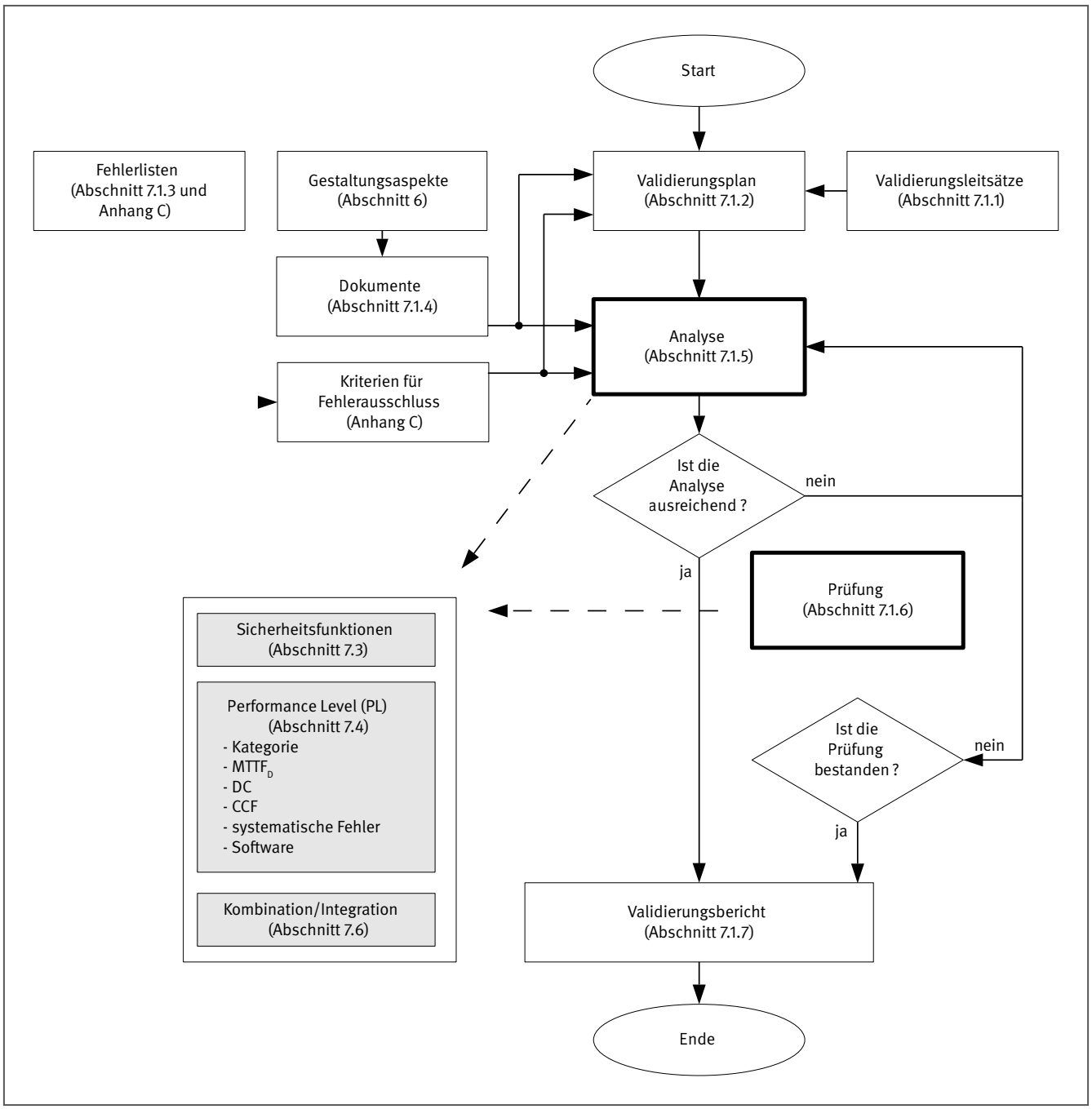
Die wichtigsten Aspekte des Verfahrens der Verifikation und Validierung werden nachfolgend erläutert.

7.1.1 Leitsätze für die Verifikation und Validierung

Verifikation und Validierung sollen die Konformität der Gestaltung des SRP/CS mit den Bewertungsgrundlagen sicherstellen. Da DIN EN ISO 13849-1 als B-Norm für Maschinensteuerungen unter der Maschinenrichtlinie harmonisiert ist, müssen die V&V-Aktivitäten zeigen, dass jedes sicherheitsbezogene Teil und jede seiner ausgeführten Sicherheitsfunktionen die Anforderungen der DIN EN ISO 13849-1 erfüllt. Der Fokus hierbei liegt bei den festgelegten Eigenschaften der Sicherheitsfunktionen und den Anforderungen für den festgelegten Performance Level (siehe auch Abschnitte 7.3 und 7.4). In DIN EN ISO 13849-2 ist zudem vorgegeben, die ergonomische Gestaltung der Benutzerschnittstelle(n) im V&V-Verfahren aufzugreifen.

Diese Aktivitäten sollten so früh wie möglich während der Entwicklung bzw. Konstruktion begonnen werden, sodass Fehler oder Abweichungen von den Spezifikationen rechtzeitig erkannt und behoben werden können. Das mit den Maßnahmen der

Abbildung 7.2:
Übersicht zum Verifikations- und Validierungsverfahren nach DIN EN ISO 13849-2



Verifikation und Validierung betraute Personal soll nach Möglichkeit nicht in den Gestaltungsprozess der sicherheitsbezogenen Teile einbezogen sein, d. h. unabhängig von Entwurf und Realisierung agieren können. Dies können dann andere Personen, andere Abteilungen oder andere Stellen sein, die der Konstruktionsabteilung hierarchisch nicht unterstehen. Der Grad der Unabhängigkeit sollte dabei dem Risiko, also dem erforderlichen Performance Level (PL_r), angemessen sein.

Verifikation und Validierung werden methodisch durch Analyse und Prüfung geleistet.

7.1.2 Verifikations- und Validierungsplan

Ein Verifikations- und Validierungsplan ist dazu vorgesehen, die Durchführung des V&V-Verfahrens für die festgelegten Sicherheitsfunktionen, der Sicherheitsintegrität und allen nachzuvollziehenden Betriebs- und Umgebungseinflüssen zu beschreiben. Das „Validierungsverfahren“ nach DIN EN ISO 13849-2, mit dem natürlich ebenfalls die Verifikationsaktivitäten gemeint sind, setzt die Erstellung eines Verifikations- und Validierungsplans voraus, legt jedoch weder Form noch Inhalt im Detail fest. In einem Verifikations- und Validierungsplan (V&V-Plan) werden alle den Entwicklungs- bzw. Konstruktionsverlauf begleitenden V&V-Aktivitäten verbindlich festgelegt. Er sollte folgende Angaben enthalten:

- Identifikationen des bzw. der betrachteten SRP/CS, ggf. derer Komponenten sowie möglicher Varianten/Variationen

- Identifikation der Sicherheitsfunktionen mit Zuordnung der beteiligten SRP/CS

- Referenzenliste aller Bezugsdokumente (einschließlich der anzuwendenden Normen und technischen Regeln) mit Anforderungsbeschreibungen, Spezifikationen und Lasten aus dem Anwendungsbereich zum betrachteten SRP/CS sowie firmeninterne Gestaltungsregeln, z. B. eigene Hardwaredesignregeln und Programmierregeln/-leitfäden

- Referenzenliste der anzuwendenden Prüfnormen (dies sind Normen zu Prüfverfahren und zur Prüfungsdurchführung, nicht zu Produktanforderungen – beispielsweise die DIN EN 60068 – Reihe zu Umgebungseinflüssen)

- die durchzuführenden Analysen und Prüfungen; ggf. mit zusätzlichen Hinweisen auf eine erforderliche Abfolge der festgelegten Analyse- und Prüfverfahren

- Kennzeichnung, ob und welche Qualifizierungen für einzelne Komponenten bereits vorliegen; mit Nennung der Verweise auf die früheren Nachweisdokumente

- anzuwendende Fehlerlisten (siehe auch Abschnitt 7.1.3 und Anhang C)

- weitere Referenzen zu Dokumenten mit Bezug zur Erstellung von Nachweisen; z. B. QM-Handbuch, Verfahrensanweisungen, Vorlagen/Muster für V&V-Aktivitäten

- für die jeweiligen Analysen und Prüfungen verantwortliches Personal (Person, Abteilung oder Stelle/ggf. Prüfstelle)

- vorgesehene (Prüfungs-)Umgebungsbedingungen und einzusetzende Ausrüstung/Prüfmittel/Werkzeuge/Hilfsmittel zur Durchführung der Analysen und Prüfungen sowie weitere einzuhaltende Betriebsbedingungen; diese Angaben können auch in den Ergebnisdokumenten der einzelnen V&V-Aktivitäten aufgelistet sein

- die vorgesehene, d. h. zu erstellende Ergebnisdokumentation (Berichte bzw. Protokolle) sowie detaillierende, weiterführende Dokumentation zur Durchführung der V&V-Aktivitäten (z. B. Prüfspezifikationen, Test(fall)spezifikationen, Checklisten)

- Bewertungskriterien für Analyse- und Prüfergebnisse einschließlich der Maßnahmen, die durchzuführen sind, wenn eine Analyse/Prüfung nicht bestanden wurde

- formale Aspekte wie Dokument-Identifikation, Version/Stand und Änderungshistorie, Autoren/Verantwortliche, Freigabevermerk(e), Unterschrift(en) etc.

Den Verifikations- und Validierungsplan erstellt man sinnvollerweise in einer frühen Entwicklungsphase (Empfehlung: parallel zur Spezifikation), dann mit allen Vorteilen für das weitere Projektmanagement. Zudem ist es bewährte Praxis, den V&V-Plan durch eine in Fragen des Qualitätsmanagements (QM) und der Qualitätssicherung (QS) kompetente Person per Review oder Inspektion überprüfen zu lassen.

Im Fall der Konstruktion größerer bzw. komplexerer Gesamt-SRP/CS besteht die Möglichkeit, im V&V-Plan festzuhalten, welche Validierungen erst nach einem Einbau in eine Maschine leistbar sind bzw. ob hierfür alternativ Testautomaten oder ersetzende Simulatoren (z. B. per „Hardware-in-the-loop Simulation“) vorgesehen werden können.

7.1.3 Fehlerlisten

Im V&V-Verfahren sind Überlegungen und Nachweise zum Verhalten des SRP/CS bei Ausfällen vorzunehmen. Die Grundlage einer Fehlerbetrachtung ist in Form der Benennung zu betrachtender Fehler (entspricht der Terminologie „anzunehmende Ausfallarten“) und Fehlerausschlüsse in den Anhängen A bis D der DIN EN ISO 13849-2 zu finden. Im Anhang C dieses Reports sind die Themen Fehlerlisten, anzunehmende Fehler/Ausfallarten und Fehlerausschlüsse ausführlich behandelt. Diese allgemeinen Fehlerlisten stützen sich auf Erfahrungen. In wenigen weiteren Normen, z. B. DIN EN 61800-5-2 [20] zur funktionalen Sicherheit von elektrischen Leistungsantriebssystemen und DIN EN 61784-3 [39] zur funktional sicheren Übertragung bei Feldbussen, finden sich spezialisierende Fehlerlisten. Die Norm DIN EN 61508-2:2011 zur funktionalen Sicherheit programmierbarer elektronischer Systeme enthält im Anhang A.2, Tabelle A.1, noch einige Präzisierungen zu Fehlern bei CPU, RAM, ROM und Takt. Generell ist das Fehlermodell für hochintegrierte Bauteile der Mikroelektronik (Mikroprozessoren, DSPs, ASICs, FPGAs, SoCs etc.) jedoch von einer gewissen Abstraktheit geprägt. Von großem Vorteil sowohl bei der Realisierung als auch bei Nachweisen ist es, wenn bei den Fehlerdiagnosemaßnahmen (Selbsttests, Überwachungsroutinen, Überwachungsbauteile) Standardelemente – in Software und Hardware – verwendet werden. Solche Standardelemente sind z. B. die Standard-CPU-Selbsttests im BGIA-Report 7/2006 „Selbsttests für Mikroprozessoren mit Sicherheitsaufgaben“ [50], Speicher-Selbsttests namens „Galpat“, „March“, „Checkerboard“ u. v. a. m. sowie kommerzielle „Watchdog-/Überwachungsbausteine für IEC 61508-/IEC 26262-Anwendungen“. Für Bauteile/Bauelemente, die in den Fehlerlisten der DIN EN ISO 13849-2 nicht enthalten sind, z. B. im Fall neuartiger Technologie, sollen eigene spezielle Fehlerlisten mit Fehlern und Fehlerausschlüssen in vergleichbarer Weise ergänzt werden. Kommt es zur Annahme von Fehlerausschlüssen, müssen diese ausreichend begründet sein. Der Teil individuell ergänzter Fehlerlisten zählt dann zu den zu bewertenden technischen Unterlagen.

Zur Software gibt es weder bei der SRESW noch der SRASW (siehe Abschnitt 6.3) normative Fehlerlisten. Auch in der allgemeinen Literatur ist das Thema Softwarefehler eher beispielhaft und nicht mit umfassenden Fehlerlisten behandelt. Eine sehr gute Unterstützung mit umfassendem „Fehlerwissen“ findet man bei PC-basierten Werkzeugen der statischen Softwareanalyse (zur Syntax-, Semantik- und Codierregel-Prüfung).

Zu „Ausfällen infolge gemeinsamer Ursache“ (CCF) sind prinzipiell die gleichen Fehler zu betrachten, dies mit den in Anhang F genannten möglichen Ursachen für CCF und den entsprechenden Gegenmaßnahmen.

7.1.4 Dokumente für V&V-Aktivitäten

Wie Abbildung 7.1 andeutet, sind für die Durchführung jeder V&V-Aktivität eingehende Dokumentationen erforderlich. Dies sind technische Unterlagen, die im gesamten V&V-Verfahren von Bedeutung sind (insbesondere die Spezifikationen) oder im Ablauf des SRP/CS-Entwurfs und dessen Realisierung entstanden sind und nur bei einigen oder einzelnen Analysen/Prüfungen notwendig sein können. Zusammengefasst sollten in ausreichendem Maße folgende Inhalte berücksichtigt sein:

- Vollständige Spezifikation der Anforderungen an die Sicherheitsfunktionen sowie der Anforderungen an den Entwurf des SRP/CS: Die Beschreibung der Anforderungen muss alle Leistungsmerkmale, Eigenschaften, Betriebsarten, Zustands- und Ablauferwartungen enthalten, aus denen Bewertungskriterien ableitbar sind.

- Betriebs- und Umgebungsbedingungen mit Bemessungsdaten, die sich aus den vorgesehenen Anwendungen bzw. aus anzuwendenden Normen ergeben, Bemessungsdaten für Bauteile

- Funktionsbeschreibung zur Ausführung sämtlicher Sicherheitsfunktionen mit Zustands- und Ablaufbeschreibungen: Die Behandlung von Ausfällen/Fehlern im SRP/CS, d. h., die Reaktionen und Zustände des SRP/CS bei den möglichen Ausfall-/Fehlerarten, muss darin einbezogen sein – ebenso das Bedienkonzept mit allen Interaktionen von Verwendern.

- Konstruktionsbeschreibung der SRP/CS (mit Spezifika für eingesetzte mechanische, elektrische, elektronische, hydraulische und pneumatische Bauteile) mittels angemessener Zeichnungen/Skizzen, Diagramme, Pläne, Daten und erläuternden Texten: Dies sind z. B. Übersichtszeichnungen, Struktur-/Blockdiagramme, Ablauf-/Zustandsübergangsdiagramme, Verdrahtungspläne und Anschluss- bzw. Schnittstellenbeschreibungen, Prinzipschaltpläne, Schaltpläne, Elektropläne, Fluid(schalt)pläne, Montagepläne, Tabellen technischer Daten bzw. Bemessungsdaten für Komponenten, ggf. Datenblätter.

- Fehleranalyse/Fehlerauswirkungsanalyse, z. B. als FMEA/FMEDA (deutsch: Fehlermöglichkeits- und Einfluss- und Diagnoseanalyse, auch: Ausfalleffektanalyse), unter Berücksichtigung der angewandten Fehlerlisten; für Kategorie 4 Fehleranhäufung eingeschlossen

- Beschreibung der getroffenen technischen Maßnahmen zur Fehlerbeherrschung (Fehlerdiagnosemaßnahmen)

- bei der Gestaltung berücksichtigte grundlegende und bewährte Sicherheitsprinzipien und dokumentierte Ermittlung der quantifizierbaren Aspekte PFH_D, $MTTF_D$, DC_{avg} und CCF für den Performance Level PL jedes SRP/CS („Quantifizierungsdokumentation“ genannt) einschließlich der Liste zu Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache

- vollständige Softwaredokumentation (siehe Abschnitt 6.3)

- für den Entwurf und die Realisierung zugrunde gelegte Gestaltungsregeln wie Designregeln für Analog- und Digitalschaltungen, Programmierrichtlinien, u. Ä.

- Nachweise (Zertifikate, Prüfberichte, Technische Protokolle) zu bereits validierten Bauteilen, Baugruppen oder SRP/CS; auch: Nachweise zu erreichten Zuverlässigkeits-Kennwerten, wenn diese auf eine andere Weise als der nach DIN EN ISO 13849 erreicht wurden. Angaben und ggf. Nachweise zu bewährten Bauteilen

Die Dokumente müssen vollständig, die Inhalte widerspruchsfrei, logisch aufgebaut, leicht verständlich und nachvollziehbar sein.

7.1.5 Analyse

Die Beurteilung eines SRP/CS oder von dessen Teilaspekten davon erfolgt in weiten Bereichen durch Analyse. Dabei kommen sowohl manuell leistbare Analysemethoden zum Einsatz wie Inspektionen, Reviews oder Walkthroughs für die Spezifikation, von technischen Unterlagen und der Begleitinformationen als auch (oftmals PC-basierte) Analysewerkzeuge, wie z. B. Schaltungssimulatoren, Werkzeuge zur statischen und dynamischen Hardware-/Softwareanalyse oder auch FMEA-/FMEDA-Tools und Fehlersimulatoren zur Analyse von Komponenten und Schaltungen bei Fehlern. An Grenzen der Analysemöglichkeiten stößt man, wenn es um Nachweise zu Betriebs- und Umgebungsbedingungen geht. Mit neuen Methoden und Verfahren in der Produktentwicklung (Stichwort: modellbasierte oder virtuelle Entwicklungsmethoden) werden sicherlich auch neue Analyseverfahren und Analysewerkzeuge hinzukommen. Die notwendige Entscheidung, wo zusätzlich zur Anwendung analytischer Verfahren auch Prüfungen erfolgen müssen, wird auf einfachem Weg im V&V-Plan dokumentiert.

7.1.6 Prüfung

Prüfungen müssen immer dann durchgeführt werden, wenn für den betreffenden Teilaspekt keine Analysen möglich sind oder die alleinige Begutachtung durch Analyse nicht ausreichend ist, um zu zeigen, dass die Anforderungen erfüllt werden. Das Prüfen muss systematisch geplant und in logischer Weise ausgeführt werden, zumeist anhand real ausführbarer Entwicklungsstufen wie z. B. Prototypen, Funktionsmuster oder Software/Code. Die Prüfungen müssen so nah wie möglich an der vorgesehenen Betriebskonfiguration durchgeführt werden – unter welchen Umgebungsbedingungen ist vorher festzulegen. Eine manuelle oder automatische Durchführung ist möglich.

Die Messunsicherheiten bei Nachweisen durch Prüfung müssen angemessen sein. DIN EN ISO 13849-2 gibt Hinweise auf einzuhaltende Grenzen.

In den Abschnitten 7.3 bis 7.7 werden die typischen V&V-Aktivitäten der Einzelaspekte – Sicherheitsfunktionen, PL, Kategorie, $MTTF_D$, *DC* und CCF, Software, Benutzerinformation und Benutzerschnittstelle – beschrieben; im Abschnitt 7.8 dann als Beispiel anhand einer Planschneidemaschine.

7.1.7 Ergebnisdokumentation

Alle Analyse- und Prüfaktivitäten müssen inklusive ihrer Ergebnisse dokumentiert werden. Hierbei ist es wichtig, dass die herangezogenen Anforderungsspezifikationen und Beurteilungsgrundlagen datiert bzw. versioniert referenziert werden, das unter Analyse/Prüfung stehende Objekt (Dokument, Software, Prüfling …) eindeutig identifiziert, eingestellte Konfigurationen festgehalten, die Analyse-/Prüfbedingungen samt Aufbau und Ablauf wiedergegeben und alle Verifikations-/Validierungspunkte/-fälle samt Ergebnissen aufgezeichnet werden. Formale Angaben wie Dokumentidentifikation, Durchführende, Datum, Unterschrift etc. dürfen natürlich nicht fehlen. Je nach Automationsgrad und zum Einsatz kommenden Werkzeugen und Hilfsmitteln der V&V-Maßnahme wird auch die Ergebnisdokumentation variieren, jedoch sollten die genannten Inhalte als minimaler Dokumentationsumfang gelten. Ein Dokumentationsmanagement ist also auch aus den Bedarfen des V&V-Verfahrens abgeleitet angemessen. Jedwede Unterstützung und Hilfsmittel hierfür, z. B. Protokollvorlagen bis zum Dokumentenmanagementsystem, dürfen als wertvoll angesehen werden.

7.1.8 Abschluss oder Iteration

Die Kombination der an einer Sicherheitsfunktion beteiligten SRP/CSen erreicht einen Performance Level PL. Dieser ist abschließend mit dem erforderlichen Performance Level PL_r für diese Sicherheitsfunktion zu vergleichen. Eine ausreichende Sicherheitsqualität wurde erreicht, wenn in der Bewertung von „$PL \geq PL_r$?“ in Abbildung 7.2 ein positives Ergebnis feststeht.

Wurden nicht alle in der Spezifikation des SRP/CS festgelegten Anforderungen erfüllt, muss man auch an dieser Stelle in den Gestaltungs- und Realisierungsprozess zurückkehren. Wurden die V&V-Aktivitäten für alle Sicherheitsfunktionen mit positivem Ergebnis abgeschlossen, so ist nach Norm die Bewertung des SRP/CS abgeschlossen. Ansonsten muss das V&V-Verfahren mit den noch offenen Sicherheitsfunktionen fortgesetzt werden.

In den Gestaltungs- und Realisierungsprozess zurückzukehren bedeutet auch, die Bestandteile des V&V-Verfahrens, die nicht bestanden wurden, zu identifizieren und zuzuordnen, mit welchen V&V-Aktivitäten diese neu zu durchlaufen sind. Hierzu kann der V&V-Plan (siehe Abschnitt 7.1.2) geeignete Elemente enthalten und Einträge bekommen.

In den Prozessen der Entwicklung/Konstruktion des SRP/CS muss also der Fall negativer Ergebnisse aufgegriffen sein. Entsprechend sind Verfahren und Maßnahmen des Managements fehlerhafter Ergebnisse erforderlich (für Dokumente, Aufzeichnungen, Daten, Konfigurationen, Software, Muster/Prototypen etc.).

7.2 Verifikation der Spezifikation und der Technischen Dokumentation

Das zur SRP/CS-Realisierung mit Abstand meistgenannte Dokument (nicht nur in diesem Report) ist „die Spezifikation“.

Gemeint ist die Spezifikation aller Anforderungen (englisch: Requirements Specification), die Spezifikation der Sicherheitsfunktionen, die Spezifikation der – natürlich sicherheitsbezogenen – Gestaltung mit dem Schwerpunkt Sicherheitsintegrität sowie die Spezifikation der vorgesehenen Betriebs-, Umgebungs- und Anwendungsbedingungen. Im Kapitel 6 dieses Reports – speziell in Kasten 6.1 – werden umfassend Hinweise zum notwendigen Inhalt gegeben. Der Einsatz rechnerunterstützter Spezifikationswerkzeuge und formaler Methoden zur Spezifikationserstellung ist möglich, wenngleich unüblich.

Die Verifikation adressiert somit das Dokument „Spezifikation“ und erfolgt als Inspektion und Review. Bewährt hat sich hierbei eine Zweiteilung in der Vorgehensweise: zum einen (und zuerst) die Verifikation durch erfahrenes Personal beim Hersteller selbst und zusätzlich durch eine kompetente „externe“ Stelle – ggf. eine Prüfinstitution.

Zur Verifikation der gesamten Entwicklungs-/Konstruktionsdokumente enthält DIN EN ISO 13849-2 den Abschnitt 12, der auf die erforderlichen Inhalte der Technischen Dokumentation (Abschnitt 10 der Norm) verweist. Als Verifikationsaktivitäten für die Entwicklungs-/Konstruktionsdokumente („Technische Dokumentation“) sind Analysen angemessen. Inspektion, Review und Walkthrough gelten als typische Methoden hierzu; bei Bedarf nachzuschlagen u. a. in DIN EN 61508-7 [10].

7.3 Validieren der Sicherheitsfunktion

Zur Validierung der realisierten Sicherheitsfunktion(en) zählen die Aktivitäten, welche die vollständige Übereinstimmung mit den in der Spezifikation festgelegten funktionalen Eigenschaften und Leistungskriterien nachweisen. Hilfreich zur Frage, ob die Sicherheitsfunktion(en) korrekt definiert und umgesetzt wurde(n), ist auch die Überprüfung der Umsetzung der in Abschnitt 5.3.1 gelisteten Punkte zur Festlegung von Sicherheitsfunktionen.

Um eine Aussage darüber treffen zu können, ob die funktionalen Anforderungen erfüllt wurden, sind folgende typische Teilprüfungen durchzuführen:

- Funktionstest
- Test zum Verhalten des SRP/CS bei unüblichen, nicht erwarteten, im Ablauf inkorrekten oder außerhalb der Spezifikation liegenden (ungültigen) Eingangssignalen, Bedienungsabläufen oder Eingaben mittels sogenanntem „erweiterten Funktionstest“
- Simulation (sofern leistbar)
- Leistungstests (funktionale Kennwerte, Reaktionszeit …)

Zur abschließenden Beurteilung der korrekten Integration aller Sicherheitsfunktionen an der kompletten Maschine gehört allerdings eine Reihe weiterer Aspekte, z. B. die Bemessung von Nachläufen und Sicherheitsabständen.

7.4 Verifikation des PL des SRP/CS

Dieser Abschnitt beschreibt die üblichen Aktivitäten zum Nachweis des erreichten Performance Levels PL einzelner SRP/CS. Die Vorgehensweise bei Kombination mehrerer SRP/CS wird in Abschnitt 7.6 erläutert.

Der PL eines SRP/CS bestimmt sich zum einen durch quantifizierbare Aspekte bzw. Kennwerte wie $MTTF_D$, *DC*, CCF und die Kategorie und zum anderen durch qualitative Aspekte wie das Verhalten der Sicherheitsfunktion unter Fehlerbedingungen, die Gestaltungsmaßnahmen zur sicherheitsbezogenen Software und zu systematischen Ausfällen sowie durch das funktionale Verhalten unter den zu erwartenden (maximalen) Betriebs- und Umgebungsbedingungen. Im Anschluss an die Beurteilung der Einzelaspekte wird beschrieben, wie die Abschätzung des PL kontrolliert werden kann. So wie DIN EN ISO 13849-1 und -2 geht auch der Report und dieser Abschnitt für die „Abschätzung" des PL von der Wahl des „vereinfachten Verfahrens" aus, das weiter oben im Report erläutert wurde.

7.4.1 Verifikation der Kategorie

Ziel der Verifikationen zur Kategorie ist es zu bestätigen, dass im jeweiligen Entwicklungsschritt alle an die Kategorie gestellten Anforderungen erfüllt werden; siehe Abschnitte 6.2.2 bis 6.2.7 in diesem Report und Abschnitte 9.2.1 bis 9.2.5 in [6].

Folgende Analysen müssen durchgeführt werden:

- Struktur- und Signalpfadanalyse der technischen Schaltungsunterlagen
- Bewertung der Umsetzung und Wirksamkeit der Fehlerdiagnosemaßnahmen
- Inspektion zur Einhaltung grundlegender Sicherheitsprinzipien
- Inspektion zur Umsetzung bewährter Sicherheitsprinzipien (ab Kategorie 1)
- Inspektion zum Einsatz bewährter Bauteile (nur Kategorie 1)
- Bewertung der in Fehlerlisten individuell ergänzten zu betrachtenden Fehler und zulässiger Fehlerausschlüsse, einschließlich ihrer Begründungen

Die Anhänge im Teil 2 der Norm – und auch Anhang C dieses Reports – geben detaillierte Hilfe bei den letzten vier genannten Analysen.

Folgende Teilprüfungen sind zu ergänzen, sofern die Analysen zuvor nicht ausreichend sind bzw. Fehleranalysen am Prüfmuster bestätigt werden sollen:

- Tests zum Verhalten des SRP/CS im Fehlerfall mit Fehlereinbau, d. h. Prüfung der Sicherheitsfunktionen unter Fehlerbedingungen (auch „Ausfalleffektprüfung" genannt) bzw. ersatzweise Fehlersimulation dort, wo Testfälle mit Fehlereinbau nicht leistbar sind,
- Tests zum Verhalten des SRP/CS bei seltenen, unerwarteten, außerhalb der Spezifikation liegenden und fehlerhaften Zuständen von Eingangssignalen und fehlerhaften Abläufen/Eingaben bei der Bedienung mit sog. „erweiterten Funktionstests"

7.4.2 Verifikation der $MTTF_D$-Werte

Die zur Bestimmung des PL herangezogenen $MTTF_D$-Werte sollen mindestens auf ihre Plausibilität überprüft werden. Dazu zählt typischerweise die Beurteilung, ob geeignete Quellenangaben zur Herkunft der Werte vorliegen. Bei den dominanten Bauteilen und stichprobenartig bei allen anderen Bauteilen ist es ratsam, auch die genaue Begründung der Werte nachzuvollziehen. Dazu können u. a. die in Abschnitt 6.2.12 und Anhang D genannten Datenquellen herangezogen werden. Für die Werte B_{10D}, T_{10D} und n_{op} wird deren angemessene Bestimmung analytisch nachvollzogen und abschließend die korrekte Berechnung mindestens auf Plausibilität kontrolliert.

7.4.3 Verifikation der DC-Werte

Der den Blöcken oder ggf. Bauteilen zugewiesene Diagnosedeckungsgrad (*DC*) muss nachvollziehbar bemessen sein. Analysiert werden auch hier typischerweise die dargelegten Angaben zur Herkunft der Werte und deren Begründung. In Anhang E sind Hinweise zur Abschätzung der DC-Werte zu finden. Diese können auch bei der Verifikation zugrunde gelegt werden.

Für die realisierte Konstruktion gilt es zu analysieren, ob die beschriebenen Fehlerdiagnosemaßnahmen umgesetzt wurden. Dazu ist es zumeist erforderlich, in der Entwicklungsdokumentation die Fehlerdiagnosefunktionen und -module zu identifizieren und deren Wirksamkeit einzuschätzen. Zusätzlich sollen Tests zum Verhalten des SRP/CS im Fehlerfall (Ausfalleffektprüfung bzw. Test durch Fehlereinbau) zeigen, dass durch die Fehlerdiagnosefunktionen eine korrekte Fehleraufdeckung gegeben ist. Die Berechnung von DC_{avg} ist abschließend mindestens auf Plausibilität zu kontrollieren.

7.4.4 Verifikation der Maßnahmen gegen CCF

Zur Bewertung der ausgewählten Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache CCF (Common Cause Failure) enthält DIN EN ISO 13849-1, Anhang F, ein Verfahren basierend auf einem Punkteschema. Neben der Kontrolle für das Erreichen der Gesamtpunktzahl und der Klärung, dass die ausgewählten Maßnahmen in den entsprechenden Dokumenten umfassend beschrieben sind, wird durch Analyse oder Prüfung gezeigt, dass die Maßnahmen tatsächlich umgesetzt wurden. Zu den hierzu typischen V&V-Aktivitäten zählen die statische Hardwareanalyse und die Funktionsprüfung unter Umgebungsbedingungen (Grenzbedingungen).

7.4.5 Verifikation der technischen Maßnahmen gegen systematische Ausfälle

V&V-Aktivitäten zu technischen Maßnahmen zur Vermeidung und Beherrschung systematischer Ausfälle beurteilen, ob die in DIN EN ISO 13849-1, Anhang G, beschriebenen und in Abschnitt 6.1.2 des Reports weiter erläuterten erforderlichen

Konstruktionsmaßnahmen umgesetzt wurden. Ein entsprechender Nachweis erfolgt typischerweise durch:

- Funktionsprüfung bei Grenzwerten und Veränderungen von Nennwerten sowie Ausfalleffektprüfung/Test durch Fehlereinbau zu den Versorgungseinheiten (z. B. Spannungsausfall, Spannungsschwankungen, Überspannung, Unterspannung, Wechselstromänderung/Frequenzänderung, Taktveränderung und andere Phänomene und Betriebsbeanspruchungen, die zu einem Ausfall führen können)

- Prüfung der Störfestigkeit gegen Umgebungseinflüsse bzw. Funktionstest bei spezifizierten Umgebungsbedingungen (klimatische Bedingungen, mechanische Beanspruchung, elektromagnetische Verträglichkeit etc.); vgl. Abschnitt 10 in [6]

- Analyse zur Implementierung der Programmlaufüberwachung

- Inspektion und Prüfung der sicherheitsbezogenen Eigenschaften zu Datenkommunikationssystemen bzw. beim Einsatz von zertifizierten Komponenten deren Identifikation

- Inspektion von Entwicklungsdokumenten, die die Anwendung grundlegender und bewährter Sicherheitsprinzipien und zusätzlich weiterer getroffener Maßnahmen wie diversitäre Hardware bestätigen

Auf die in DIN EN ISO 13849-2 [6] zur Vermeidung systematischer Ausfälle geforderten Bewertungen organisatorischer Maßnahmen wie Qualitätsmanagementsysteme für den Herstellungsprozess (Abschnitt 9.4 e in [6]) geht dieser Report nicht ein.

7.4.6 Verifikation und Validierung der Software

Die im Rahmen der Spezifikation, des Entwurfs und der Codierung der Software stattfindenden Verifikationsaktivitäten (Inspektion/Review für Softwarespezifikation, Softwareentwurf und Code, statische Softwareanalyse, Modultest, Softwaresimulation, Integrationstest) wurden bereits ausführlich in Abschnitt 6.3 beschrieben. Auch für die Softwareverifikation ist hierbei relevant, dass abhängig vom zu erreichenden PL gestufte Softwaregestaltungsmaßnahmen festgelegt sind.

Die letzte Entwicklungsaktivität im vereinfachten „V-Modell“ ist die Softwarevalidierung. Zu überprüfen ist, ob die Anforderungen der sicherheitsbezogenen Softwarespezifikation an das funktionale Verhalten sowie die Leistungskriterien (z. B. zeitbezogene Vorgaben) korrekt umgesetzt und implementiert wurden. Die Validierung betrachtet hier keine „Interna“ der Software mehr, sondern das „externe“ Verhalten am Ausgang der kompletten, auf die Hardware integrierten Software bei Änderungen an deren Eingängen. Die Software wird dabei als „Blackbox“ betrachtet, die Validierung hierzu ist der Blackbox-Test. Zusätzliche „I/O-Tests“ stellen sicher, dass die sicherheitsbezogenen Eingangs- und Ausgangssignale korrekt verwendet werden. Auf Systemebene (am SRP/CS) erfolgt anschließend der Funktionstest. Eine erweiterte Testfallausführung mit (ggf. simulierten) Fehlerfällen gilt als Nachweis der Wirksamkeit und korrekten Implementierung der durch Software realisierten Fehlererkennung und Fehlerbehandlung (Reaktion im Fehlerfall).

Einzelne Softwarefunktionen, die als „Sicherheits-Funktionsbausteine“ bereits zertifiziert oder qualitätsgesichert validiert wurden, müssen nicht nochmals geprüft werden. Allerdings ist die bereits erfolgte Validierung zu belegen. Sobald aber mehrere dieser Sicherheits-Funktionsbausteine projektspezifisch zusammengeschaltet werden, ist die resultierende gesamte Sicherheitsfunktion zu validieren.

Im besonderen Fall von SRESW, die in SRP/CS mit PL e eingesetzt und nicht diversitär für beide Kanäle entwickelt wurde, müssen bei der Softwareentwicklung die SIL-3-Anforderungen nach Abschnitt 7 der DIN EN 61508-3 [42] vollständig erfüllt werden. Dies schließt die darin geforderten V&V-Aktivitäten ein.

Bei einer späteren Modifikation der sicherheitsbezogenen Software ist in jedem Fall deren Verifikation und Validierung in geeignetem Umfang zu wiederholen. Der im Abschnitt 7.1.2 behandelte Verifikations- und Validierungsplan kann und soll hierbei als planerisches Hilfsmittel einen Dienst erweisen.

Ein weiterer Bereich von Softwareverifikation trifft konfigurierbare, parametrierbare und programmierbare SPR/CS. Im Fall von softwarebasierter Parametrierbarkeit bzw. Programmierbarkeit gehört ein Nachweis zur Implementierung und Wirkung der realisierten Maßnahmen passend zu den Anforderungen in DIN EN ISO 13849-1, Abschnitt 4.6.4, und damit zu den eingesetzten Konfigurationswerkzeugen (ggf. Parametrier-/Programmierprogramme) als Pflichtteil zu den V&V-Aktivitäten hinzu. Sowohl Analysen der Dokumentation dieser „Werkzeuge“ als auch Prüfungen „am Objekt“ kommen hier zum Einsatz.

7.4.7 Kontrolle der Abschätzung des PL

Die Kontrolle der korrekten Abschätzung des PL für jedes SRP/CS besteht insbesondere aus dem Nachvollziehen der richtigen Anwendung des eingesetzten Abschätzungsverfahrens, einschließlich der korrekten Berechnungen.

Wurde das vereinfachte Verfahren zur Abschätzung des PL angewandt, lässt sich anhand Abbildung 6.10 kontrollieren, ob aus den zuvor bestätigten Kategorie-, $MTTF_D$-, und DC_{avg}-Werten der richtige PL für das SRP/CS ermittelt wurde.

7.5 Verifikation der Benutzerinformation

Wichtige Informationen zur sicheren Verwendung des SRP/CS sind in Form von Betriebsanleitung, Montageanleitung, Typenschild und Instandhaltungsanleitung zur Verfügung zu stellen. Diese gesamtheitlich Benutzerinformationen genannten Dokumentationsteile – und der Maschinenrichtlinie folgend auch die Verkaufsprospekte (!) – müssen daraufhin bewertet werden, ob sie alle in Abschnitt 9 und Abschnitt 11 der DIN EN ISO 13849-1 genannten Inhalte enthalten. Zur Form der Ausführung (Sprache, elektronisch vs. Print) stellt DIN EN ISO 13849 keine eigenen Regeln auf. Es gelten die Anforderungen (und Gremienbeschlüsse) auf Ebene der Maschinenrichtlinie. Zur Gestaltung (Layout, Typografie etc.) von Benutzerinformationen können allgemeine Leitlinien wie beispielsweise DIN EN 82079-1: „Erstellen von Gebrauchsanleitungen“ [51] eingesetzt werden.

Deren Anwendung bei der Beurteilung ist jedoch nicht verpflichtend. In aller Regel werden Begleitinformationen per Inspektion und/oder Review analysiert.

7.6 Validieren der Kombination und Integration von SRP/CS

Die einzelnen SRP/CS sind vor der Kombination separat zu validieren. Um systematische Fehler während der Kombination bzw. Integration von SRP/CS zu vermeiden, sind folgende V&V-Aktivitäten durchzuführen:

- Inspektion der Konstruktionsdokumente, die insgesamt die Realisierung der jeweiligen Sicherheitsfunktion beschreiben
- Abgleich der Kenndaten der Schnittstellen zwischen den SRP/CS (z. B. Spannungen, Ströme, Drücke, Informationsdaten)
- FMEA/Fehleranalyse bezogen auf die Kombination bzw. Integration
- Funktionstest
- erweiterter Funktionstest
- Kontrolle der vereinfachten Bestimmung des Gesamt-PL aus den PLs der einzelnen SRP/CS wie in Abschnitt 6.4 beschrieben

Integration von (mehreren) SRP/CS bedeutet noch nicht deren Inbetriebnahme mit zugehörigen Inbetriebnahmeprüfungen an einer Maschine. Die hier genannten Validierungsaktivitäten, ergänzt durch den höchst sinnvollen Schnittstellentest/ „I/O-Test“ sind hierfür jedoch uneingeschränkt geeignet.

Besonders herausfordernd können sicherheitstechnische Retrofits oder die Integration neuer SRP/CS in bestehende Maschinensteuerungen werden. Die rechtzeitige Planung der o. g. V&V-Aktivitäten, ihre konsequente Anwendung trotz aller Nöte bei Aktivitäten, die evtl. erst vor Ort auftreten, und ihre durchgängige Aufzeichnung tragen wesentlich dazu bei, die Integration von SRP/CS zuverlässig umzusetzen.

7.7 Verifikation der Benutzerschnittstelle (ergonomische Gestaltung)

Vorgaben an die Ergonomie der Benutzerschnittstelle beziehen sich in DIN EN ISO 13849 auf universelle Gestaltungsziele wie die Vorbeugung vor gefährlichem Handeln, das Umgehen der SRP/CS und deren Manipulation, auf allgemeine ergonomische Prinzipien wie Einfachheit und diejenigen ergonomischen Prinzipien, die sie mit DIN EN ISO 12100 [3] und ISO 9355 [52] referenziert. Wiederum explizit fordert sie die Berücksichtigung der vorhersehbaren fehlerhaften Bedienung.

Benötigt man bei der Verifikation der Benutzerschnittstellen weitere Grundlagen, so kann die Anwendung von Gestaltungsleitlinien, z. B. der VDI/VDE 3850 „Gebrauchstaugliche Gestaltung von Benutzungsschnittstellen für technische Anlagen“ [31], des VDMA Leitfadens „Software-Ergonomie, Gestaltung von Bedienoberflächen“ [53] oder der Normen DIN EN ISO 9241-11 „Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit“ [54] hilfreich sein.

Abschließend sei in diesem Abschnitt die Meinung bestätigt, dass die Verwendung bereits zertifizierter bzw. baumustergeprüfter SRP/CS und auch Softwarebausteine und -werkzeuge die Verifikation und Validierung der Schaltung für Sicherheitsfunktionen erheblich erleichtert und verkürzt.

7.8 Verifikation und Validierung am Beispiel einer Planschneidemaschine mit diversitärer Redundanz in der Logiksteuerung (Kategorie 4 – PL e)

Begleitend zur allgemeinen Beschreibung der Verifikation und Validierung von Sicherheitsfunktionen und PL werden in diesem Abschnitt die V&V-Aktivitäten am praktischen Beispiel der Planschneidemaschine aus den Abschnitten 5.7 und 6.5 erläutert. An dieser Stelle wird unterstellt, dass alle notwendigen Dokumente und ein Prototyp der Maschine vorhanden sind. Auf der Basis der Dokumente sollen hier stellvertretend für eine der Sicherheitsfunktionen „SF2 – Ortsbindung der Hände des Bedieners außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung“ (Abschnitt 5.7.3) die Schritte der Verifikation und Validierung gezeigt werden. Zu den vorhandenen Dokumenten gehört auch der Verifikations- und Validierungsplan, der die jeweils notwendigen Aktivitäten in den verschiedenen Phasen beschreibt (Abschnitt 7.1.2). Aufgrund der Höhe des Gefährdungspotenzials ist es ratsam, die Arbeiten durch unabhängige Personen, z. B. aus einer anderen Abteilung, durchführen zu lassen (Abschnitt 7.1.1).

In diesem Abschnitt soll die Definition für Verifikation und Validierung aus der Einleitung im Abschnitt 7 verwendet werden. Oft sind die Grenzen jedoch unscharf und eine exakte Zuordnung ist schwierig. So sei auf das Testen von z. B. Software hingewiesen. Diese Tests werden in der Literatur auch Validierung genannt, um festzustellen, ob das Programm oder Programmteile seinen/ihren Zweck (nach Spezifikation) erfüllt oder erfüllen. Hier wäre es auch möglich, diese Schritte als Verifikation zu bezeichnen.

7.8.1 Verifizieren des erreichten PL (siehe auch Block 6 in Abbildung 7.1)

Anhand einer Risikoeinschätzung wurde ermittelt, dass für die auszuführende Sicherheitsfunktion SF2 ein erforderlicher Performance Level PL_r e erreicht werden muss. Diese Analyse steht im Einklang mit der Forderung aus DIN EN 1010-1 [28], die im Verweis auf die Anforderungen der entsprechenden Norm zu Zweihandschaltungen DIN EN 574 [55] die technischen Anforderungen weiter präzisiert. In der Systemspezifikation sind die zu erfüllenden Randbedingungen genannt und durch eine Validierung bestätigt worden. Die jetzt stattfindende Verifikation bestätigt die korrekte Umsetzung der Vorgaben, hier durch die Berechnung des PL unter Zuhilfenahme des Softwaretools SISTEMA. In der Berechnung der Ausfallwahrscheinlichkeit unter Berücksichtigung aller quantifizierbaren Aspekte wird dieser PL erreicht. Auch werden alle Anforderungen an die qualitativen Aspekte wie das Verhalten der Sicherheitsfunktion unter Fehlerbedingungen, einschließlich der umgesetzten fehlererkennen-

den Maßnahmen in der sicherheitsbezogenen Software, die Maßnahmen gegen systematische Ausfälle und das Verhalten unter Umgebungsbedingungen für einen PL e hinreichend erfüllt.

An den oben genannten Aussagen wird deutlich, dass diese zu unterschiedlichen Zeiten der Entwicklung getroffen wurden oder nur in bestimmten Phasen überhaupt gemacht werden können. Der Nachweis z. B. der EMV-Anforderungen kann erst nach Fertigstellung eines Prototypen erfolgen.

Die nachfolgenden Validierungen/Verifikationen stellen keine Reihenfolge im Sinne einer stringenten Abarbeitung dar, sondern hier sollen die Arbeiten für die entsprechenden Phasen des V&V-Modells am Beispiel der SF2 gezeigt werden.

7.8.2 Validieren der sicherheitsbezogenen Anforderungen (siehe auch Block 7 in Abbildung 7.1)

Fehlerlisten

Bei der Bestimmung des PL werden die Fehlerlisten nach DIN EN 13849-2 [6] zugrunde gelegt.

Dokumente

Wie bereits in Abschnitt 7.1.4 erwähnt, bilden Schaltpläne, Stücklisten, die vollständige Spezifikation, Funktionsbeschreibung, weiter die Konstruktionsbeschreibung, Fehler-/Fehlerauswirkungsanalyse, die Softwarespezifikation und Softwaredokumentation u. a. die Grundlage für die Analyse bzw. Prüfung.

Dokumentation

Alle Analyse- und Prüfergebnisse bedürfen der Dokumentation in schriftlicher Form. Hierbei sind die Bewertungskriterien dafür, wann eine Prüfung „bestanden“ oder „nicht bestanden“ ist, wichtig und im Verifikations- und Validierungsplan enthalten.

Validieren der Sicherheitsfunktion

Zur Überprüfung der funktionalen Anforderungen an die Sicherheitsfunktion wird ein Funktionstest durchgeführt, ergänzt um einen erweiterten Funktionstest, um das Verhalten der Sicherheitsfunktion bei seltenen oder nicht festgelegten Eingaben zu überprüfen. Ein Beispiel für einen solchen Test könnte die Überprüfung der Reaktion des SRP/CS sein, wenn zu einer gültigen Schnittanforderung der Zweihandschaltung ein Fehlersignal z. B. an der Peripherie oder durch einen Stoppbefehl ausgelöst durch ein Lichtgitter erfolgt. Weiter werden Leistungstests zu funktionalen Aspekten durchgeführt. Hierzu zählt z. B. die Überprüfung der nach der Norm DIN EN 574 [55] einzuhaltenden Zeit für eine synchrone Betätigung. Nur wenn beide Stellteile S1 und S2 in einem Zeitabschnitt ≤ 0,5 Sekunden betätigt werden, dürfen Ausgangssignale zur Ansteuerung des Pressbalkens und des Messers erzeugt werden.

Die vorgenannten Prüfungen und die Analysen der spezifizierten sicherheitstechnischen Eigenschaften wurden mit positivem Ergebnis („bestanden“) abgeschlossen.

Verifikation des PL des SRP/CS

- Verifikation der Kategorie

  Auf der Basis der vollständigen oder auch verbindlichen Spezifikation sind in einem frühen Stadium der Entwicklung wesentliche Weichenstellungen zur Kategorie des SRP/CS erfolgt. Zum ermittelten PL_r e wurde ebenfalls die Kategorie 4 gewählt. Die Verifikation der Spezifikation ergab, dass die darauf basierende Schaltungsstruktur (diversitäre Redundanz, siehe auch Abschnitt 6.5.2) den Anforderungen für eine Kategorie 4 genügt.

  Für die Zweihandschaltung, wie hier vorgesehen, werden unter Einbeziehung der Entwicklungsunterlagen an einem Prototypen Tests zum Verhalten im Fehlerfall durchgeführt. Hierdurch wird verifiziert, ob auch hier insgesamt die Vorgaben für eine Kategorie 4 eingehalten werden. Dies geschieht durch gezielten Einbau von Fehlern. Die Reaktion der SRP/CS auf die eingebauten Fehler muss den spezifizierten Reaktionen entsprechen. Zunächst wird durch Analyse und dann durch Prüfung getestet, was geschieht, wenn z. B. einzelne Hilfsschütze nicht mehr in der Lage sind, Schaltbefehle auszuführen, oder wie die SRP/CS reagieren, wenn einer der beiden Stellteile S1 oder S2 zeitverzögert oder gar nicht betätigt wird. Die Sicherheitsfunktion bei Einbringung eines einzelnen Fehlers in die SRP/CS muss stets gewährleistet sein. Ein einzelner Fehler muss bei oder vor der nächsten Ausführung der Sicherheitsfunktion erkannt werden. Kann der Fehler nicht erkannt werden, darf eine Anhäufung weiterer Fehler nicht zum Verlust der Sicherheitsfunktion führen. Im zugehörigen Prüfprotokoll wird für jeden Fehlereinbau die erwartete sicherheitsgerichtete Reaktion beschrieben und das Verhalten des SRP/CS mit dem Bewertungskriterium „bestanden“ oder „nicht bestanden“ kommentiert.

  Das Einhalten des Ruhestromprinzips als ein Beispiel für grundlegende Sicherheitsprinzipien wird durch Einbringen von Unterbrechungen und Bewertung der Reaktion darauf nachweisbar. Fällt z. B. die Versorgungsspannung aus, werden der Pressbalken und das Messer über Federkraft zurück in die Ausgangsposition gefahren.

  Plausibilitätskontrollen seien hier als Beispiel für die Umsetzung bewährter Sicherheitsprinzipien genannt: Zwangsgeführte Kontakte der Hilfsschütze K3 bis K6 werden durch beide Kanäle zurückgelesen. Prüfungen werden durchgeführt, um die korrekte Funktion der Rücklesung zu zeigen.

- Verifikation der $MTTF_D$-Werte

  Beispielhaft für die Verifikation der $MTTF_D$-Werte wird hier der für die Ventile 1V3, 1V4, 2V2 und 2V1 angesetzte Wert von 150 Jahren betrachtet (siehe Abbildung 6.15). Die Angabe des Herstellers entstammt einer zuverlässigen Quelle und wurde durch Vergleich mit dem entsprechenden Wert aus Tabelle C.1 der DIN EN ISO 13849-1 [5] erfolgreich auf Plausibilität überprüft (siehe Tabelle D.2 dieses Reports). Die für die Annahme des $MTTF_D$-Wertes vom Hersteller genannten Bedingungen (z. B. Ölwechsel)

Konstruktive Merkmale

- Die Anforderungen von Kategorie B, grundlegende und bewährte Sicherheitsprinzipien, werden eingehalten. Durch diversitär redundante Verarbeitungskanäle (Mikrocontroller und ASIC) führt ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion und systematische Fehler werden weitgehend vermieden.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung aller elektrischen Signale, auch die der Druckschalter, erfolgt in einer mehrkanaligen Steuerung.
- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1.
- K3 bis K6 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L [56]. Die zugehörigen Öffner-Kontakte zur Überwachung der Schließer-Kontakte werden im jeweiligen Nachbarkanal überwacht.
- Alle Signal führenden Anschlussleitungen sind entweder getrennt oder gegen mechanische Beschädigung geschützt verlegt.
- Die Programmierung der Software (SRESW) erfolgt entsprechend den Anforderungen für PL d (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.
- Fehlervermeidende Maßnahmen bei der ASIC-Entwicklung sind gemäß ASIC-Entwicklungs-Lebenszyklus (V-Modell) der Norm DIN EN 61508-2 [48] durchgeführt.

werden in der Betriebsanleitung beschrieben und es wird unterstellt, dass die Bedingungen im Betrieb eingehalten werden.

- Verifikation der DC-Werte

  Für K1 und K2 wird ein *DC* von 90 % aufgrund von Selbstdiagnose nachvollzogen. Hierzu gehören ein Kreuzvergleich von Eingangssignalen und Zwischenergebnissen (von Mikrocontroller und ASIC), eine zeitliche und logische Programmlaufüberwachung und die Erkennung von statischen internen und peripheren Ausfällen. Des Weiteren gehören im Kanal mit dem Mikrocontroller ein CPU-Test, in dem alle verwendeten Befehle getestet werden, sowie qualitativ ausreichende Tests von Arbeitsspeicher (RAM) und Festwertspeicher (ROM) dazu. Im zweiten Kanal (ASIC) finden qualitativ vergleichbare Tests wie im Parallelkanal statt. Durch Verifikation muss gezeigt werden, dass die in der Spezifikation beschriebenen Maßnahmen korrekt umgesetzt wurden.

  Den Hilfsschützen K3, K4, K5 und K6 wird ein *DC* von 99 % zugemessen. Dies ist aufgrund von Plausibilitätsprüfungen über zurückgelesene zwangsgeführte Kontakte der Hilfsschütze angemessen. Die im Rahmen der Verifikation der Kategorie bereits kontrollierten Plausibilitätsprüfungen dienen auch an dieser Stelle als Nachweis der korrekten Funktion.

  Den Tasten S1 und S2 wird ein DC von 99 % zugemessen. Dies wird mit dem Kreuzvergleich und häufigem Signalwechsel begründet. Diese Annahme wird durch die Verifikation bestätigt. Ein Fehlerfallversuch wird an anderer Stelle diese Annahme belegen.

  Die Ventile 2V1, 2V2, 1V3 und 1V4 werden indirekt durch die Druckschalter 2S1 und 1S3 zyklisch überwacht. Da parallel zum Maschinenzyklus die Stellungen der Ventile auf Plausibilität abgefragt werden können, wird für den *DC* ein Wert von 99 % als begründbar angesehen. Auch hier wird am Prototyp durch Fehlerversuche an den Ventilen die Annahme bestätigt.

- Verifikation der Maßnahmen gegen CCF

  Mit 65 Punkten für Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache werden die Mindestanforderungen erfüllt. Zusätzlich wirken in Teilen der Steuerung weitere Maßnahmen. Für die Umsetzung der Maßnahme „physikalische Trennung zwischen den Signalpfaden“ werden 15 Punkte berücksichtigt. Die richtige Umsetzung der Maßnahme ist anhand der Analyse von Entwicklungsunterlagen, wie z. B. Schaltplänen und durch Prüfungen an der Hardware, zu zeigen. Einen wesentlichen Beitrag zur CCF leistet die verwendete Diversität für K1 und K2: Die unterschiedlichen Technologien von K1 und K2 begründen die zugebilligten 20 Punkte für Diversität.

- Verifikation der Maßnahmen gegen systematische Ausfälle

  Die Einhaltung grundlegender und bewährter Sicherheitsprinzipien wirkt stark gegen systematische Ausfälle. Die Aktivitäten zur Verifikation der Kategorie umfassen ebenfalls die Überprüfung der Einhaltung beider Arten von Sicherheitsprinzipien. Somit können die Ergebnisse der dort durchgeführten Analysen und Prüfungen auch in diesem Abschnitt zur Beurteilung herangezogen werden.

  Neben den Prüfungen erfolgt entwicklungsbegleitend eine Inspektion der Dokumentationen, in der die angewandten grundlegenden und bewährten Sicherheitsprinzipien und die Maßnahmen zur Beherrschung und Vermeidung systematischer Ausfälle nach Abschnitt 6.1.2 dieses Reports und Anhang G der Norm beschrieben sind. Dies dient der Beurteilung, ob die Prinzipien und Maßnahmen im Entwicklungsprozess hinreichend berücksichtigt werden.

  Als Beispiel der Beherrschung systematischer Systemausfälle enthält die sicherheitsrelevante Software eine Überwachung des Programmablaufs, um eine fehlerhafte Abarbeitung des Programms erkennen zu können. Die Wirksamkeit der Ablaufüberwachung wird durch eingebrachte Fehler überprüft.

Um die Beständigkeit der SRP/CS gegen die festgelegten Umgebungsbedingungen zu zeigen, finden Prüfungen unter allen erwarteten und vorhersehbar widrigen Bedingungen für u. a. Temperatur, Feuchte und elektromagnetische Beeinflussung statt. Dies ist ein Beispiel für eine Maßnahme zur Vermeidung systematischer Ausfälle. Die Grenzen für Temperatur und Feuchte, in denen die Planschneidemaschine betrieben werden darf, sind in der Spezifikation festgeschrieben und dort durch Verifikation des Dokuments bestätigt worden.

- Verifikation der Software

  Die Entstehung und Validierung der Software wird ausführlich in Abschnitt 6.3 beschrieben. An dieser Stelle wird ergänzend die Verifikation der Software durchgeführt, d. h. die Prüfung der Funktion und auch der Reaktionszeiten der auf der Hardware integrierten Software. Geprüft wird mit funktionalen Tests (Blackbox-Tests) und erweiterten Funktionstests, bei denen einerseits die sicherheitsrelevanten Eingangssignale korrekt zu sicherheitsrelevanten Ausgangssignalen verarbeitet werden müssen und andererseits Testfälle mit eingebauten Fehlern ausgeführt werden, um die spezifizierten Fehlerreaktionen der Firmware des Mikrocontrollers K1 zu verifizieren. Das heißt, es wird geklärt, ob die Vorgaben der Spezifikation in der Software korrekt umgesetzt worden sind.

- Kontrolle der Abschätzung des PL

  Zur Abschätzung des PL wurde das vereinfachte Verfahren nach DIN EN ISO 13849-1 angewendet. Dessen korrekte Anwendung wird nachvollzogen. Die Berechnung der $MTTF_D$ nach Abschnitt 6.2.11 und Anhang D sowie des durchschnittlichen Diagnosedeckungsgrades DC_{avg} nach Anhang E wird ebenso kontrolliert wie die korrekte Ermittlung des PL aus der zuvor bestätigten Kategorie bzw. den bestätigten $MTTF_D$- und DC_{avg}-Werten anhand des Säulendiagramms in Abbildung 6.10.

- Verifikation der Benutzerinformation

  Die Benutzerinformation muss zu Belangen der Zweihandschaltung überprüft werden. Hierzu gehört auch die Erläuterung der Funktion im Zusammenhang mit den zu erreichenden Schutzzielen. Bei der Prüfung ist es freigestellt, wann die Benutzerinformation zum SRP/CS auch auf folgende Punkte überprüft wird: die Beschreibung der bestimmungsgemäßen Verwendung; Angabe von Informationen zum PL und der Kategorie (einschließlich datierter Verweisung auf die Norm); Erläuterung aller Betriebsarten; Beschreibung der Schutzeinrichtungen und Sicherheitsfunktionen mit Ansprechzeiten, Umgebungsbedingungen für den Betrieb und Schnittstellen nach außen; Informationen und technische Daten zum Transport, zur sicheren Montage, Inbetriebnahme und Instandhaltung. Auch hierbei ist das Ergebnis der Überprüfung schriftlich festzuhalten.

- Validieren der Kombination und Integration von SRP/CS

  Die beschriebene Sicherheitsfunktion wird durch ein SRP/CS realisiert. Da jedoch die unterschiedlichen Technologien Elektronik und Hydraulik innerhalb dieses SRP/CS kombiniert werden, sollten einige bei der Kombination von SRP/CS notwendige Prüfungen auch hier durchgeführt werden, sofern sie noch nicht in die Validierung der Kategorie eingeflossen sind. Dazu zählen der Abgleich der Schnittstellenkenndaten zwischen den eingesetzten Technologien sowie Funktionstests und erweiterte Funktionstests.

7.8.3 Prüfung, ob alle Sicherheitsfunktionen analysiert wurden (siehe auch Block 8 in Abbildung 7.1)

Die hier für SF2 gezeigten V&V-Aktivitäten werden für alle vom SRP/CS ausgeführten Sicherheitsfunktionen (SF1 bis SF6) durchgeführt. Der Mehraufwand ist allerdings gering, da viele Sicherheitsfunktionen auf dieselbe Hardware zurückgreifen. Die Analysen und Prüfungen müssen zeigen, dass die umgesetzten Sicherheitsfunktionen korrekt realisiert wurden. Nach Betrachtung aller Sicherheitsfunktionen ist die Bewertung nach DIN EN ISO 13849-1 und -2 abgeschlossen.

8 Schaltungsbeispiele für SRP/CS

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Beispiele Nr. 8, Nr. 26 und Nr. 36 entfallen
- Neues Beispiel Nr. 38 zur hydraulischen Ventilsteuerung eingefügt
- Wesentlich veränderte Beispiele: Nr. 17, Nr. 19 und Nr. 24

In diesem Report wurde zunächst allgemein auf die Gestaltung sicherer Steuerungen eingegangen. Die Abschnitte 5.7, 6.5 und 7.6 illustrierten anschließend am Beispiel einer Planschneidemaschine, wie die Methoden zur Gestaltung sicherer Steuerungen umgesetzt werden können. Die Methoden zur Bestimmung des PL sind hier bzw. in DIN EN ISO 13849-1 zwar Schritt für Schritt beschrieben, einige dieser Schritte, z. B. die Ableitung des sicherheitsbezogenen Blockdiagramms aus dem Schaltplan, erfordern jedoch einige Übung. Im SISTEMA-Kochbuch 1 [33] werden Hinweise zur Ableitung des sicherheitsbezogenen Blockdiagramms und der SISTEMA-Datei aus dem Schaltplan gegeben. Die einzelnen Schritte lassen sich aufgrund der Vielfalt möglicher Sicherheitsfunktionen und ihrer Realisierung aber nur schwer allgemein beschreiben. Daher wird nun in diesem Kapitel die Bewertung einer Vielzahl von Schaltungsbeispielen vorgestellt, die Sicherheitsfunktionen in verschiedenen Kategorien bzw. Performance Level und in verschiedenen Technologien realisieren. Mit dem Begriff Steuerung sind in den Schaltungsbeispielen im Allgemeinen nur die sicherheitsbezogenen Teile von Steuerungen erfasst. Die Beispiele beschränken sich auf wesentliche Gesichtspunkte und dienen deshalb primär dazu, die Methodik zu verdeutlichen. Bei deren Auswahl wurde auf ein breites Spektrum von Technologien und möglichen Anwendungen Wert gelegt. Beim Lesen des Reports zu den Kategorien für sicherheitsbezogene Steuerungen nach DIN EN 954-1 aus dem Jahre 1997 [9] wird man das eine oder andere Beispiel angereichert u. a. um die Berechnung der Ausfallwahrscheinlichkeit wiedererkennen. Im Vergleich zum BGIA-Report 2/2008 [57] wurden einige nicht mehr aktuelle Beispiele entfernt, ein neues wurde aber auch hinzugenommen. Die Beispiele sind eine Interpretation der Kategorien und wurden von den Autoren aufgrund langjähriger Erfahrungen mit sicherheitsbezogenen Maschinensteuerungen und Mitwirkung in nationalen und europäischen Normungsgremien zusammengestellt, um für die Konstruktion eine wirksame Hilfestellung für eigene Entwicklungen zu geben. Da sie von verschiedenen Autoren erstellt wurden, ist naturgemäß eine Varianz, z. B. in der Darstellung von Details oder in der Begründung einzelner Zahlenwerte, vorhanden. Alle Berechnungen für die Schaltungsbeispiele wurden mithilfe der Software SISTEMA (siehe Anhang H) in der zum Zeitpunkt der Erstellung dieses Reportes verfügbaren Version 2.0 ausgeführt. Weitere Schaltungsbeispiele inklusive SISTEMA-Dateien sind auch im IFA Report 7/2013 „Sichere Antriebssteuerungen mit Frequenzumrichtern“ [22] beschrieben.

Die Beschreibung in den Beispielen gliedert sich jeweils nach folgendem Schema:

- Sicherheitsfunktion
- Funktionsbeschreibung
- Konstruktive Merkmale
- Bemerkungen
- Berechnung der Ausfallwahrscheinlichkeit
- Weiterführende Literatur

Unter „Sicherheitsfunktion“ werden neben der Bezeichnung der Sicherheitsfunktion auch die auslösenden Ereignisse und notwendigen Sicherheitsreaktionen genannt.

Unter „Funktionsbeschreibung“ werden aufbauend auf einem Prinzipschaltplan die wesentlichen sicherheitstechnischen Funktionen beschrieben. Das Verhalten im Fehlerfall wird erläutert und Maßnahmen zur Fehlererkennung werden erwähnt.

Unter „Konstruktive Merkmale“ sind die Besonderheiten im Entwurf des jeweiligen Beispiels, so auch die Anwendung bewährter Sicherheitsprinzipien oder die Verwendung bewährter Bauteile, aufgelistet.

Die Schaltbilder sind Prinzipschaltbilder, die sich ausschließlich darauf beschränken, die Sicherheitsfunktion(en) mit den hierzu notwendigen relevanten Komponenten zu zeigen. Nicht dargestellt werden zwecks besserer Übersicht solche schaltungstechnischen Maßnahmen, die in der Regel immer zusätzlich realisiert sein müssen, um z. B. den Berührungsschutz sicherzustellen, Über- und Unterspannungen bzw. Überdruck/Unterdruck zu beherrschen, Isolationsfehler, Erd- und Kurzschlüsse z. B. auf extern verlegten Leitungen aufzudecken oder die erforderliche Störfestigkeit gegen elektromagnetische Einwirkungen zu garantieren. Für die Bestimmung des sicherheitsbezogenen Blockdiagramms unwesentliche Schaltungsdetails wurden somit bewusst weggelassen. Dazu gehören in der Elektrik Schutzbeschaltungen wie Sicherungen und Dioden, z. B. als Freilaufdioden. Ebenfalls nicht aufgeführt sind Entkopplungsdioden in Schaltungen, in denen z. B. Sensorsignale redundant in mehrere Logikeinheiten eingelesen werden. Diese sollen verhindern, dass bei Redundanz im Fehlerfall ein Eingang zu einem Ausgang wird und damit den zweiten Kanal beeinflusst. Um eine Steuerung nach einer Kategorie und einem Performance Level zu realisieren, sind alle diese genannten Bauelemente unerlässlich. Selbstverständlich muss gemäß den Fehlerlisten aus DIN EN ISO 13849-2 z. B. auch der Einfluss von Leitungskurzschlüssen im Zusammenhang mit der jeweiligen Sicherheits-

funktion und abhängig von den Einsatzbedingungen berücksichtigt werden. So müssen grundsätzlich alle verwendeten Bauteile entsprechend ihrer Spezifikation geeignet ausgewählt sein, Überdimensionierung gehört zu den bewährten Sicherheitsprinzipien. In den technologiebezogenen Bemerkungen zur Fluidtechnik sind weitere Beispiele aufgeführt.

Es werden nur diejenigen konstruktiven Merkmale genannt, die für die beschriebenen Sicherheitsfunktionen wichtig sind. Meist ist dies eine „sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung". Andere Sicherheitsfunktionen, wie z. B. die „Verhinderung des unerwarteten Anlaufs" oder eine „manuelle Rückstellungsfunktion" sowie eine „Start-/Wiederaufnahmefunktion", sind nicht durchgängig in allen Beispielen betrachtet. Werden manuell betätigte Einrichtungen (Taster) für die Realisierung solcher Sicherheitsfunktionen verwendet, so ist darauf zu achten, dass die Sicherheitsfunktionen gerade im Zusammenspiel mit Elektronik durch das Loslassen (Öffnen) eines vorher betätigten Tasters realisiert werden.

Unter „Bemerkungen", soweit für das jeweilige Beispiel vorhanden, wird insbesondere auf Besonderheiten im Hinblick auf eine mögliche Anwendung verwiesen.

Unter „Berechnung der Ausfallwahrscheinlichkeit" wird, basierend auf dem aus dem Prinzipschaltplan abgeleiteten sicherheitsbezogenen Blockdiagramm, die rechnerische Bestimmung des PL durch die Parameter Kategorie, $MTTF_D$, DC_{avg} und CCF gezeigt. Die Festlegung der Kategorie leitet sich aus der Funktionsbeschreibung und den konstruktiven Merkmalen ab.

Die in den Berechnungen verwendeten $MTTF_D$-Werte sind als Herstellerwerte (Kennzeichnung „[H]" für Hersteller), typische Werte aus Datenbanken (Kennzeichnung „[D]" für Datenbank) oder als Werte aus der Norm DIN EN ISO 13849-1 (Kennzeichnung „[N]" für Norm) markiert. Die Norm sieht eine Priorisierung von Herstellerdaten vor. Für einige Komponenten waren zum Zeitpunkt der Erstellung des Reports weder verlässliche Herstellerangaben noch Datenbankwerte zu erhalten. Hier wurde das „Parts Count"-Verfahren zu Hilfe genommen, um typische Beispielwerte abzuschätzen (Kennzeichnung „[G]" für geschätzt). Die $MTTF_D$-Werte in diesem Kapitel sind daher teilweise eher als Schätzwerte zu betrachten.

Die Darstellung der angenommenen Maßnahmen zur Diagnose (*DC*) und gegen Ausfälle infolge gemeinsamer Ursache (CCF) beschränkt sich auf allgemein gehaltene Angaben. Konkrete Werte hängen für beide Kriterien von Realisierung, Anwendung oder auch vom Hersteller ab. Es kann daher vorkommen, dass für ähnliche Komponenten in verschiedenen Beispielen unterschiedliche DC-Werte angenommen werden. Auch hier gilt, dass bei einer realen Umsetzung alle Annahmen zu *DC* und CCF überprüft werden müssen und die angenommenen Werte nur unverbindlichen Beispielcharakter haben.

Der Schwerpunkt in der Darstellung liegt eher auf den Kategorien in Form der „Widerstandsfähigkeit gegen Fehler", dem Blockdiagramm und den „rechnerischen" Methoden zur Bestimmung des PL. Einige Teilschritte, z. B. Fehlerausschlüsse, grundlegende und bewährte Sicherheitsprinzipien oder Maßnahmen gegen systematische Fehler (inklusive Software), sind dagegen nur in kurzer Form erwähnt. Hierauf muss bei einer Realisierung entsprechendes Augenmerk gerichtet werden, da Fehleinschätzungen oder unzureichende Umsetzungen bei diesen Maßnahmen die Fehlertoleranz oder Ausfallwahrscheinlichkeit verschlechtern können. Als Hilfe zum Verständnis der Schaltungsbeispiele und für die praktische Umsetzung sei daher auf Kapitel 7 und Anhang C verwiesen, in denen z. B. die grundlegenden und bewährten Sicherheitsprinzipien ausführlich beschrieben sind.

Abschließend wird, soweit vorhanden, auf „Weiterführende Literatur" verwiesen.

Für jede Technologie werden in den folgenden technologiebezogenen Abschnitten einige grundlegende Bemerkungen zum Verständnis der Beispiele und zur Umsetzung der Kategorien gegeben. Einige der Schaltungsbeispiele stellen „Steuerungen verschiedener Technologie" dar. Diese „gemischten" Schaltungsbeispiele sind von der Idee getragen, dass eine Sicherheitsfunktion unabhängig von der Technologie nach dem Verständnis der Norm immer über „Erfassen", „Verarbeiten" und „Schalten" erfolgt.

8.1 Grundlegende technologiebezogene Bemerkungen zu den Steuerungsbeispielen

8.1.1 Elektromechanische Steuerungen

In elektromechanischen Steuerungen werden in erster Linie elektromechanische Bauteile in Form von Schaltern bzw. Befehlsgeräten (z. B. Positionsschalter, Wahlschalter, Taster) und Schaltgeräten (Steuerschütze, Relais, Leistungsschütze) eingesetzt. Diese Geräte besitzen eindeutige Schaltstellungen. Ohne Betätigung von außen oder elektrische Ansteuerung ändern sie in der Regel ihren Schaltzustand nicht. Bei bestimmungsgemäßer Verwendung und entsprechender Auswahl sind sie weitgehend unempfindlich z. B. gegenüber elektrischen und elektromagnetischen Störeinflüssen. Das unterscheidet sie zum Teil erheblich von elektronischen Betriebsmitteln. Durch geeignete Auswahl, Dimensionierung und Anordnung kann auf die Haltbarkeit und das Ausfallverhalten Einfluss genommen werden. Das gilt auch für die verwendeten Leitungen bei entsprechender Verlegung innerhalb und außerhalb der elektrischen Einbauräume.

Aus vorstehenden Gründen entsprechen die elektromechanischen Bauteile in den meisten Fällen den „grundlegenden Sicherheitsprinzipien" und sind auch in vielen Fällen als „sicherheitstechnisch bewährte Bauteile" zu betrachten. Diese Aussage gilt jedoch nur, wenn die Anforderungen der DIN EN 60204-1 [25] für die elektrische Ausrüstung der Maschine/Anlage berücksichtigt werden. In einigen Fällen sind auch Fehlerausschlüsse möglich, z. B. bei einem Steuerschütz in Bezug auf das Anziehen bei fehlender Steuerspannung oder das Nichtöffnen eines zwangläufig betätigten Öffners bei einem Schalter nach DIN EN 60947-5-1 [56], Anhang K.

Detaillierte Informationen zur Modellierung elektromechanischer Bauteile sind im Anhang D enthalten.

8.1.2 Fluidtechnische Steuerungen

Bei fluidtechnischen Anlagen ist als „sicherheitsbezogener Teil der Steuerung“ insbesondere der Ventilbereich zu betrachten, und zwar die Ventile, die gefahrbringende Bewegungen oder Zustände steuern. Die im Folgenden aufgeführten fluidischen Schaltungen sind nur beispielhafte Darstellungen. Die geforderten Sicherheitsfunktionen können in der Regel auch durch andere Steuerungsverknüpfungen mit entsprechenden Ventilausführungen oder evtl. auch durch zusätzliche mechanische Lösungen, wie z. B. Halteeinrichtungen oder Bremsen, erreicht werden.

Bei hydraulischen Anlagen (siehe Abbildung 8.1) sind zusätzlich die Maßnahmen zur Druckbegrenzung im System (1V2) und zur Filtration der Druckflüssigkeit (1Z2) in diesem Zusammenhang zu sehen. Die Bauteile 1Z1, 1S1 und 1S2 in Abbildung 8.1 sind in den meisten hydraulischen Anlagen vorhanden und insbesondere für den Zustand der Druckflüssigkeit und damit für die Ventilfunktionen von großer Bedeutung. Das auf dem Flüssigkeitsbehälter angeordnete Belüftungsfilter 1Z1 verhindert, dass Schmutz von außen eindringt. Die Niveauanzeige 1S2 bewirkt die Einhaltung des Flüssigkeitsspiegels in vorgegebenen Grenzen. Die Temperaturanzeige 1S1 symbolisiert geeignete Maßnahmen zur Begrenzung des Betriebstemperaturbereiches und damit des Betriebsviskositätsbereiches der Druckflüssigkeit. Bei Bedarf müssen Einrichtungen zur Kühlung und/oder Heizung in Verbindung mit einer Temperaturregelung eingesetzt werden (siehe hierzu auch Anhang C).

Die Antriebselemente sowie die Bauteile der Energieumformung und der Energieübertragung sind bei fluidtechnischen Anlagen in der Regel außerhalb des Anwendungsbereiches der Norm.

Bei pneumatischen Anlagen (siehe Abbildung 8.2, Seite 98) sind die Bauteile gegen Gefährdungen bei Energieänderungen und die sogenannte Wartungseinheit zur Aufbereitung der Druckluft in sicherheitstechnischem Zusammenhang mit dem Ventilbereich zu sehen. Um mögliche Energieänderungen sicherheitstechnisch zu beherrschen, wird häufig ein Entlüftungsventil zusammen mit einem Druckschalter eingesetzt. In den Schaltungsbeispielen dieses Kapitels sind diese Bauteile mit 0V1 (Entlüftungsventil) und mit 0S1 (Druckschalter) bezeichnet. Die Wartungseinheit 0Z (siehe Abbildung 8.2) besteht in der Regel aus einem Handabsperrventil 0V10, einem Filter mit Wasserabscheider 0Z10, wobei der Verschmutzungsgrad des Filters überwacht wird, und einem Druckregelventil 0V11 (mit ausreichend dimensionierter Sekundärentlüftung). Mit der Druckanzeige 0Z11 wird die Anforderung an die Überwachung der Anlagenparameter erfüllt.

Die in diesem Kapitel beispielhaft gezeigten fluidtechnischen Schaltungen enthalten außer dem sicherheitsbezogenen Steuerungsteil nur noch die zusätzlichen Bauteile, die zum Verständnis der fluidtechnischen Anlage notwendig sind oder einen direkten steuerungstechnischen Bezug haben. Die Gesamtheit der Anforderungen, die von fluidtechnischen Anlagen erfüllt werden müssen, ist aus [58; 59] zu entnehmen. Als weitere zutreffende Normen sind [60 bis 63] zu nennen.

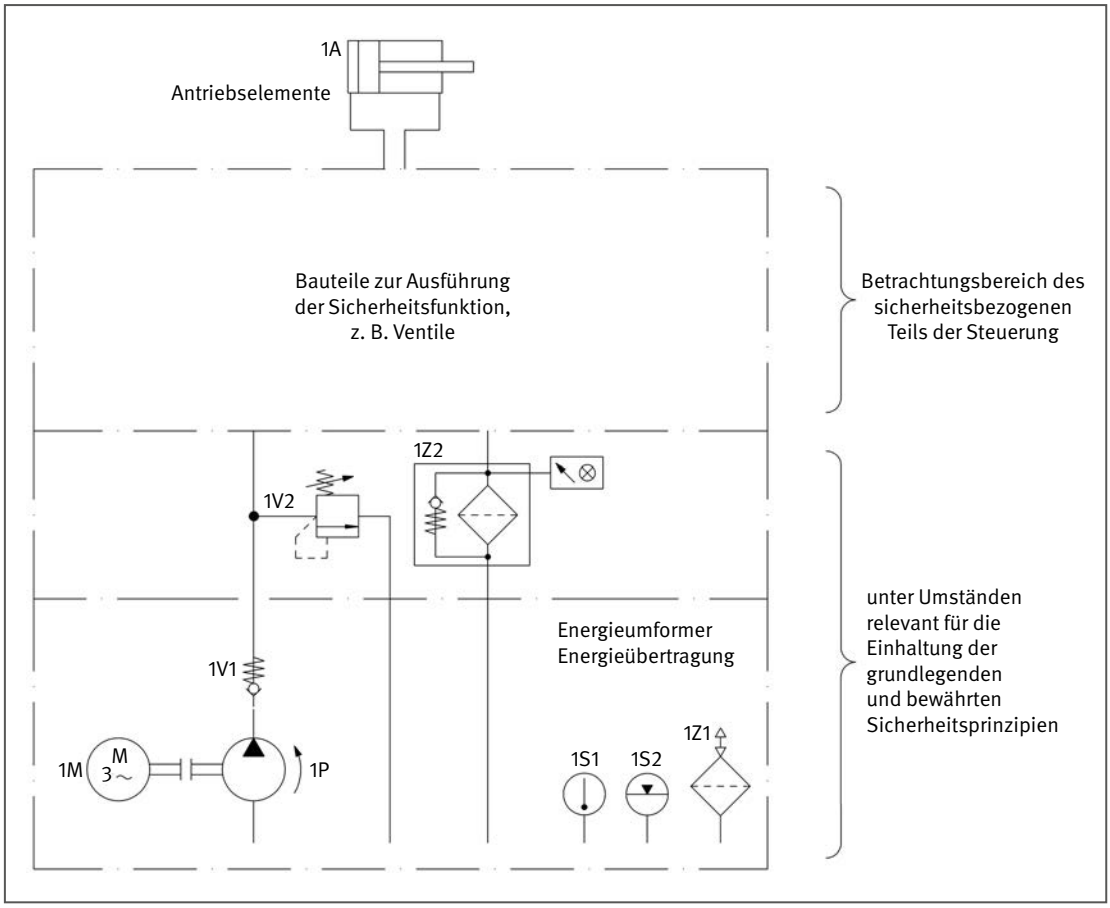


Abbildung 8.1: Anwendungsbereich der DIN EN ISO 13849 bei hydraulischen Anlagen

Die meisten Steuerungsbeispiele sind elektrohydraulische oder elektropneumatische Steuerungen. Verschiedene Sicherheitsanforderungen werden bei diesen Steuerungen durch den elektrischen Steuerungsteil ausgeführt, so z. B. die Anforderungen zur Beherrschung von Energieänderungen in elektrohydraulischen Steuerungen.

Die geforderte Sicherheitsfunktion ist bei den hier aufgeführten Steuerungsbeispielen das Anhalten einer gefahrbringenden Bewegung oder die Umkehrung der Bewegungsrichtung. Die Verhinderung eines unerwarteten Anlaufs ist implizit enthalten. Die geforderte Sicherheitsfunktion kann aber auch z. B. ein definiertes Druckniveau oder ein Druckabbau sein.

Die Strukturen von fluidtechnischen Steuerungen werden in den meisten Fällen in den Kategorien 1, 3 oder 4 ausgeführt. Da die Kategorie B bereits die Einhaltung der zutreffenden Normen und der grundlegenden Sicherheitsprinzipien erfordert, unterscheiden sich fluidtechnische Steuerungen der Kategorien B und 1 im Wesentlichen nicht durch den Steuerungsaufbau, sondern nur durch die höhere sicherheitsbezogene Zuverlässigkeit der relevanten Ventile. Aus diesem Grund werden in diesem Report keine fluidtechnischen Steuerungen der Kategorie B vorgestellt. Weitere Informationen zur Hydraulik und Pneumatik bieten die Internetseiten des IFA unter der Rubrik Praxishilfen (www.dguv.de/ifa, Webcode: d1029520).

8.1.3 Elektronische und programmierbar elektronische Steuerungen

In der Regel sind elektronische Bauteile gegenüber äußeren Umgebungseinflüssen empfindlicher als elektromechanische Komponenten. Werden keine besonderen Maßnahmen ergriffen, können elektronische Bauelemente bei Temperaturen < 0 °C deutlich eingeschränkter eingesetzt werden als elektromechanische Bauelemente. Zusätzlich gibt es Umgebungseinflüsse, die beim Einsatz elektromechanischer Schaltelemente fast bedeutungslos, aber in Elektroniksystemen ein zentrales Problem sind: alle elektromagnetischen Störeinflüsse, die über Leitungen oder über elektromagnetische Felder in Elektroniksysteme

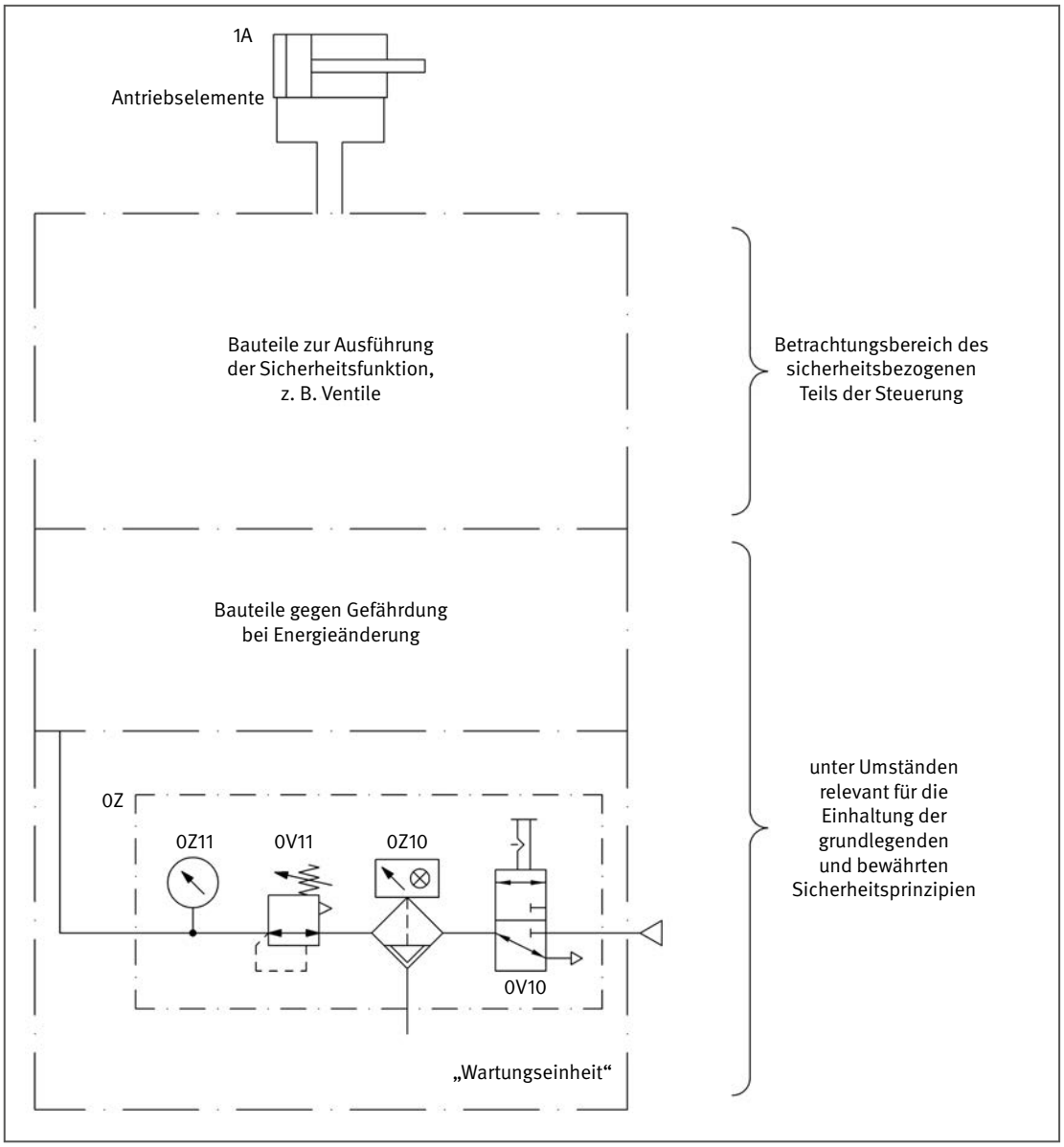


Abbildung 8.2: Anwendungsbereich der DIN EN ISO 13849 bei pneumatischen Anlagen

eingekoppelt werden. Teilweise ist ein erhöhter Aufwand erforderlich, um eine für die Praxis ausreichende Störfestigkeit zu erzielen. Fehlerausschlüsse sind bei elektronischen Bauelementen kaum möglich. Dies hat zur Folge, dass grundsätzlich nicht die Konstruktion eines bestimmten Bauelementes die Sicherheit gewährleisten kann, sondern nur bestimmte Schaltungskonzepte sowie die Anwendung entsprechender Maßnahmen zur Fehlerbeherrschung.

Nach den Fehlerlisten zu elektrischen/elektronischen Komponenten und Bauteilen nach DIN EN ISO 13849-2 werden im Wesentlichen die Fehlerannahmen Kurzschluss, Unterbrechung, Veränderung eines Parameter- oder Kennwertes und sogenannte Stuck-at-Fehler unterstellt. Dies sind durchweg Fehlereffekte, die als bleibend angenommen werden. Transiente (sporadisch auftretende) Fehler wie z. B. sogenannte Soft Errors, bei denen durch hochenergetische Teilchen wie z. B. α-Teilchen eine Kondensatorumladung innerhalb eines Chips erfolgt, sind in der Regel nur schwer zu entdecken und hauptsächlich durch strukturelle Maßnahmen zu beherrschen.

Das Ausfallverhalten elektronischer Bauelemente ist häufig schwierig zu bewerten, in der Regel kann auch keine vorwiegende Ausfallart festgelegt werden. Dies soll an einem Beispiel erläutert werden: Wird ein Relais oder Schütz elektrisch nicht angesteuert, d. h. wird seine Spule nicht vom Strom durchflossen, gibt es keinen Grund dafür, dass sich die Kontakte schließen, wenn das Bauteil im Rahmen seiner Spezifikation verwendet wird. Das bedeutet, dass ein ausgeschaltetes Relais oder Schütz sich durch einen internen Fehler nicht selbsttätig einschaltet. Anders ist das bei den meisten elektronischen Bauteilen, z. B. einem Transistor. Ist ein Transistor gesperrt – d. h., es fließt kein ausreichend hoher Basisstrom –, so ist es trotzdem nicht ausgeschlossen, dass der Transistor durch einen internen Fehler plötzlich ohne äußere Einwirkung leitfähig wird und somit unter Umständen eine gefahrbringende Bewegung einleitet. Auch dieser sicherheitstechnische Nachteil elektronischer Bauelemente muss durch ein entsprechendes Schaltungskonzept beherrscht werden. Insbesondere beim Einsatz hoch integrierter Bausteine ist es teilweise nicht mehr möglich, selbst zu Beginn der Gebrauchsdauer, d. h. zum Zeitpunkt der Inbetriebnahme, nachzuweisen, dass ein Gerät oder eine Anlage völlig fehlerfrei ist. Schon auf Bauelementebene ist ein Nachweis der Fehlerfreiheit durch die Hersteller mit 100%iger Testabdeckung für komplexe integrierte Schaltkreise nicht mehr durchführbar. Ähnliches gilt für die Software programmierbarer Elektronik.

Im Gegensatz zu elektromechanischen Schaltungen haben rein elektronische Schaltungen oft den Vorteil, dass sich Zustände dynamisieren lassen. Hierdurch kann der erforderliche *DC* auch in entsprechend kurzen Zeitabständen und ohne Zustandsänderung externer Signale erreicht werden (Dynamisierung).

Zur Verhinderung von Ausfällen infolge gemeinsamer Ursache sind zwischen verschiedenen Kanälen Entkopplungsmaßnahmen erforderlich. Diese bestehen in der Regel aus galvanisch getrennten Kontakten, Widerstands- oder Diodennetzwerken, Filterschaltungen, Optokopplern und Übertragern.

Systematische Ausfälle können zum gleichzeitigen Versagen redundanter Verarbeitungskanäle führen, wenn dies nicht durch frühzeitige Berücksichtigung, insbesondere während der Entwurfs- und Integrationsphase, verhindert ist. Die Anwendung von Prinzipien wie z. B. Ruhestrom, Diversität oder Überdimensionierung helfen, auch elektronische Schaltungen robust zu gestalten. Nicht zu vernachlässigen sind Maßnahmen, die die Verarbeitungskanäle unempfindlich gegen physikalische Einflüsse machen, wie sie z. B. in einer Industrieumgebung anzutreffen sind (Temperatur, Feuchte, Staub, Vibration, Schock, korrosive Atmosphäre, elektromagnetische Beeinflussung, Spannungsausfall, Über- und Unterspannung usw.).

SRP/CS der Kategorie 1 müssen unter Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien gestaltet und gebaut werden. Da komplexe elektronische Bauteile, z. B. SPS, Mikroprozessor oder ASICs, nicht als bewährt im Sinne der Norm betrachtet werden, gibt es in diesem Report auch keine entsprechenden Beispiele von Elektronik in Kategorie 1.

Für programmierbare Elektronik wird in den Schaltungsbeispielen jeweils eine Aussage darüber getroffen, mit welcher Wirksamkeit, d. h. mit welchem Performance Level, Maßnahmen zur Fehlervermeidung bzw. Fehlerbeherrschung erforderlich sind. Weitere Ausführungen dazu enthält Abschnitt 6.3. Werden im Rahmen einer Entwicklung ASICs eingesetzt, so sind im Entwicklungsprozess fehlervermeidende Maßnahmen erforderlich. Solche enthält zum Beispiel die Norm DIN EN 61508-2 [48], die für die Entwicklung eines ASICs ein V-Modell in Anlehnung an das aus der Softwareentwicklung bekannte V-Modell vorsieht.

Erwähnenswert, weil entsprechende Fragen in der Praxis auftreten, sind folgende Punkte:

- Zwei Kanäle eines SRP/CS dürfen im Allgemeinen nicht über denselben integrierten Schaltkreis geführt werden. In Bezug auf Optokoppler bedeutet diese Anforderung z. B. die Verwendung von Optokopplern in verschiedenen Gehäusen, wenn Signale unterschiedlicher Kanäle verarbeitet werden sollen.

- Für den Einsatz programmierbarer Elektronik ist auch der Einfluss von Betriebssystemen u. Ä. zu berücksichtigen. Ein Standard-PC mit einem marktüblichen Betriebssystem eignet sich nicht für den Einsatz in einer sicherheitsrelevanten Steuerung. Die erforderliche Fehlerfreiheit (realistisch besser: Fehlerarmut) eines Betriebssystems, das nicht für sicherheitstechnische Anwendungen entwickelt wurde, wird sich in der Regel nicht mit vertretbarem Aufwand nachweisen lassen bzw. wird nicht erreichbar sein.

8.2 Schaltungsbeispiele

Tabelle 8.1 zeigt eine Übersicht der Schaltungsbeispiele 1 bis 38. Weitere Beispiele finden sich in [22]. Tabelle 8.2 (siehe Seite 101) nennt alphabetisch sortiert die wichtigsten in den Schaltungsbeispielen verwendeten Abkürzungen.

Hinweis: Bei Beispielen mit mehreren Sicherheitsfunktionen (17, 19, 23, 24) wird jeweils nur die erste Sicherheitsfunktion im sicherheitsbezogenen Blockdiagramm dargestellt.

Tabelle 8.1:
Übersicht der Schaltungsbeispiele

Erreichter PL	Realisierte Kategorie	Technologie/Beispiel Nr.		
		Pneumatik	Hydraulik	Elektrotechnik
b	B			1, 4
c	1	2	3, 38	5, 6, 7
c	2			9
c	3			10, 24
d	2	11	12	13
d	3	14	15, 16	15, 16, 17, 18, 19, 20, 21, 22, 23, 24
e	3	25	27	28, 29, 30
e	4	31	32, 33	33, 34, 35, 37

Tabelle 8.2:
Übersicht der in den Schaltungsbeispielen verwendeten Abkürzungen

Abkürzung	Bedeutung
[D]	B_{10D}- oder $MTTF_D$-Werte aus Datenbanken (siehe z. B. Abschnitt D.2.6)
[G]	Geschätzte B_{10D}- oder $MTTF_D$-Werte (siehe oben)
[H]	B_{10D}- oder $MTTF_D$-Werte auf der Basis von Herstellerangaben
[N]	B_{10D}- oder $MTTF_D$-Werte auf der Basis in DIN EN ISO 13849-1 gelisteter Angaben (siehe z. B. Tabelle D.2 dieses Reports)
µC	Mikrocontroller
B_{10}	Nominale Lebensdauer: mittlere Zahl von Schaltspielen bzw. Schaltzyklen, bei denen bis 10 % der betrachteten Einheiten ausgefallen sind
B_{10D}	Nominale Lebensdauer: mittlere Zahl von Schaltspielen bzw. Schaltzyklen, bei denen bis 10 % der betrachteten Einheiten gefährlich ausgefallen sind
BKK	Brems-/Kupplungskombination
BWS	Berührungslos wirkende Schutzeinrichtung
CCF	Ausfall infolge gemeinsamer Ursache (Common Cause Failure)
CPU	Mikroprozessor (Central Processing Unit)
DC	Diagnosedeckungsgrad (Diagnostic Coverage)
DC_{avg}	Durchschnittlicher Diagnosedeckungsgrad (average Diagnostic Coverage)
FIT	Ausfälle in 10^9 Betriebsstunden (Failures In Time)
FMEA	Ausfalleffektanalyse (Failure Mode and Effects Analysis)
FU	Frequenzumrichter
M	Motor
MFST	Multifunktionsstellteil
$MTTF_D$	Mittlere Zeit bis zum gefahrbringenden Ausfall (Mean Time To Dangerous Failure)
n_{op}	Mittlere Anzahl jährlicher Betätigungen (Number of Operations)
PFH_D	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (Probability of a Dangerous Failure per Hour)
PL	Performance Level
PL_r	Erforderlicher Performance Level (Required PL)
RAM	Arbeitsspeicher, variabler Speicher (Random Access Memory)
ROM	Festwertspeicher, invariabler Speicher (Read-Only Memory)
SBC	Safe Brake Control, stellt ein Ausgangssignal zur Ansteuerung einer Bremse bereit
SDE	Safe De-energization, Druckfreischalter, Entlüften eines Anlagenteils
SLS	Sicher begrenzte Geschwindigkeit (Safely-Limited Speed, siehe Tabelle 5.2)
SPS	Speicherprogrammierbare Steuerung
SRASW	Sicherheitsbezogene Anwender-Software (Safety-Related Application Software)
SRESW	Sicherheitsbezogene eingebettete Software (Safety-Related Embedded Software)
SRP/CS	Sicherheitsbezogener Teil einer Steuerung
SS1-r, SS1-t	Sicherer Stopp 1 (Safe Stop 1, siehe Tabelle 5.2)
SS2-r, SS2-t	Sicherer Stopp 2 (Safe Stop 1, siehe Tabelle 5.2)
SSC	Safe Stopping and closing, Einsperren von Druckluft in den Kolbenräumen ohne Lageregelung
STO	Sicher abgeschaltetes Moment (Safe Torque Off, siehe Tabelle 5.2)
T_{10D}	Zeit, in der bis 10 % der betrachteten Bauteile gefährlich ausgefallen sind
ZHS	Zweihandschaltung

8.2.1 Stellungsüberwachung verriegelter trennender Schutzeinrichtungen mittels Näherungsschalter – Kategorie B – PL b (Beispiel 1)

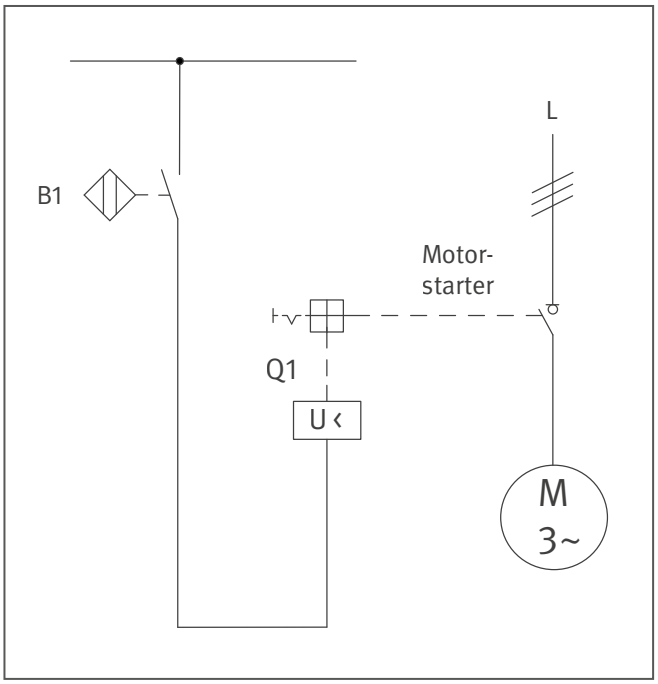


Abbildung 8.3:
Stellungsüberwachung verriegelter trennender Schutzeinrichtungen mittels Näherungsschalter

Sicherheitsfunktion

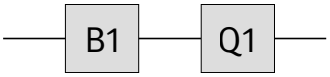
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Die Betätigung des Näherungsschalters beim Öffnen der verriegelten trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der verriegelten trennenden Schutzeinrichtung (z. B. Schutzgitter) wird durch einen Näherungsschalter B1 erfasst, der auf die Unterspannungsauslösung eines Motorstarters Q1 wirkt. Durch das Abfallen von Q1 werden gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Ein Entfernen der Schutzeinrichtung wird bemerkt.
- B1 enthält keine internen Überwachungsmaßnahmen. Es sind keine weiteren Maßnahmen zur Fehlererkennung vorgesehen.

Konstruktive Merkmale

- Grundlegende Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip des Unterspannungsauslösers verwendet.
- Ein stabiler Aufbau der Schutzeinrichtung (Schutzgitter) zur Betätigung des Näherungsschalters ist sichergestellt.
- Die sichere Funktion kann je nach Ausführung des Näherungsschalters durch Umgehen auf eine vernünftigerweise vorhersehbare Art aufgehoben werden. Dies kann erschwert werden, z. B. durch besondere Einbaubedingungen wie verdeckten Einbau (siehe auch DIN EN ISO 14119).
- Die Spannungsversorgung der gesamten Maschine wird abgeschaltet (Stopp-Kategorie 0 nach DIN EN 60204-1).



Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Bei B1 handelt es sich um einen herkömmlichen Näherungsschalter an einem Schutzgitter mit $MTTF_D$ = 1 100 Jahren [H]. Für die Unterspannungsauslösung des Motorstarters Q1 entspricht der B_{10}-Wert näherungsweise der elektrischen Lebensdauer von 10 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Bei täglicher Betätigung des Näherungsschalters ergibt sich mit n_{op} = 365 Zyklen/Jahr für Q1 eine $MTTF_D$ von 548 Jahren. Die Kombination von B1 und Q1 ergibt $MTTF_D$ = 365 Jahre für den Kanal. Dieser Wert wird auf den rechnerischen Maximalwert für Kategorie B, also auf 27 Jahre („mittel“) gekürzt.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie B nicht relevant.
- Die elektromechanische Steuerung entspricht Kategorie B mit mittlerer $MTTF_D$ (27 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}2 \cdot 10^{-6}$/Stunde. Dies entspricht PL b.

Weiterführende Literatur

- DIN EN ISO 14119: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (03.14). Beuth, Berlin 2014
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

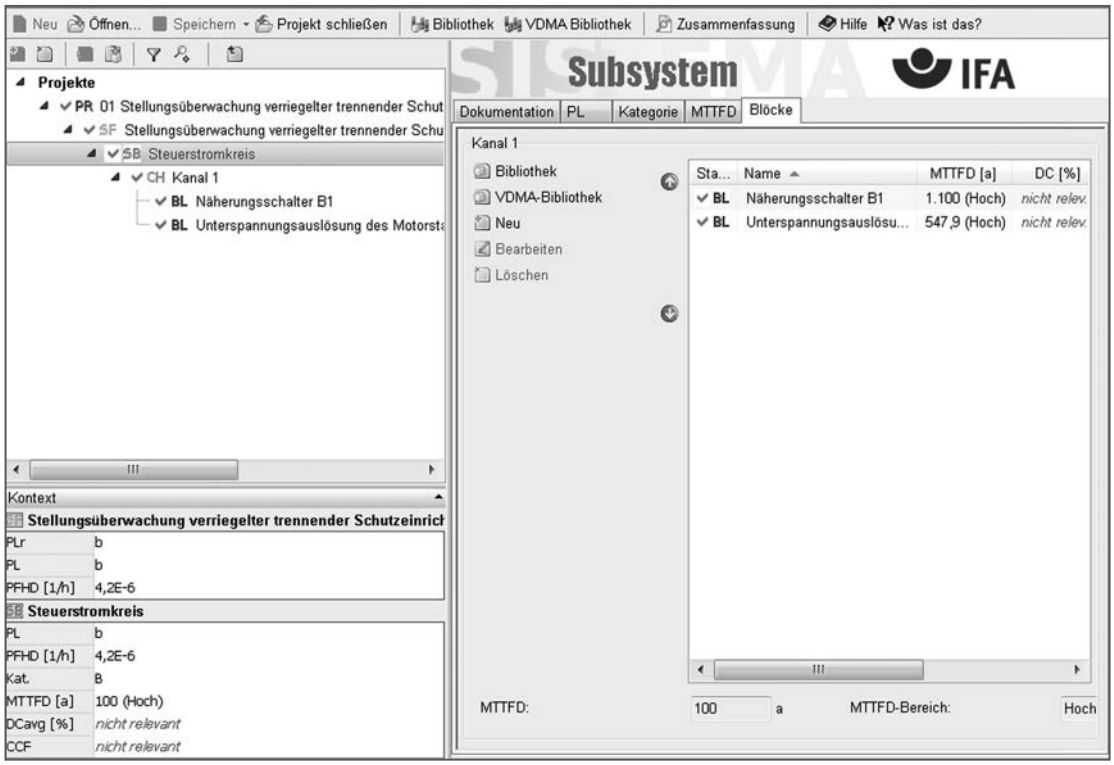


Abbildung 8.4:
PL-Bestimmung mithilfe von SISTEMA

8.2.2 Pneumatisches Ventil (Subsystem) – Kategorie 1 – PL c (Beispiel 2)

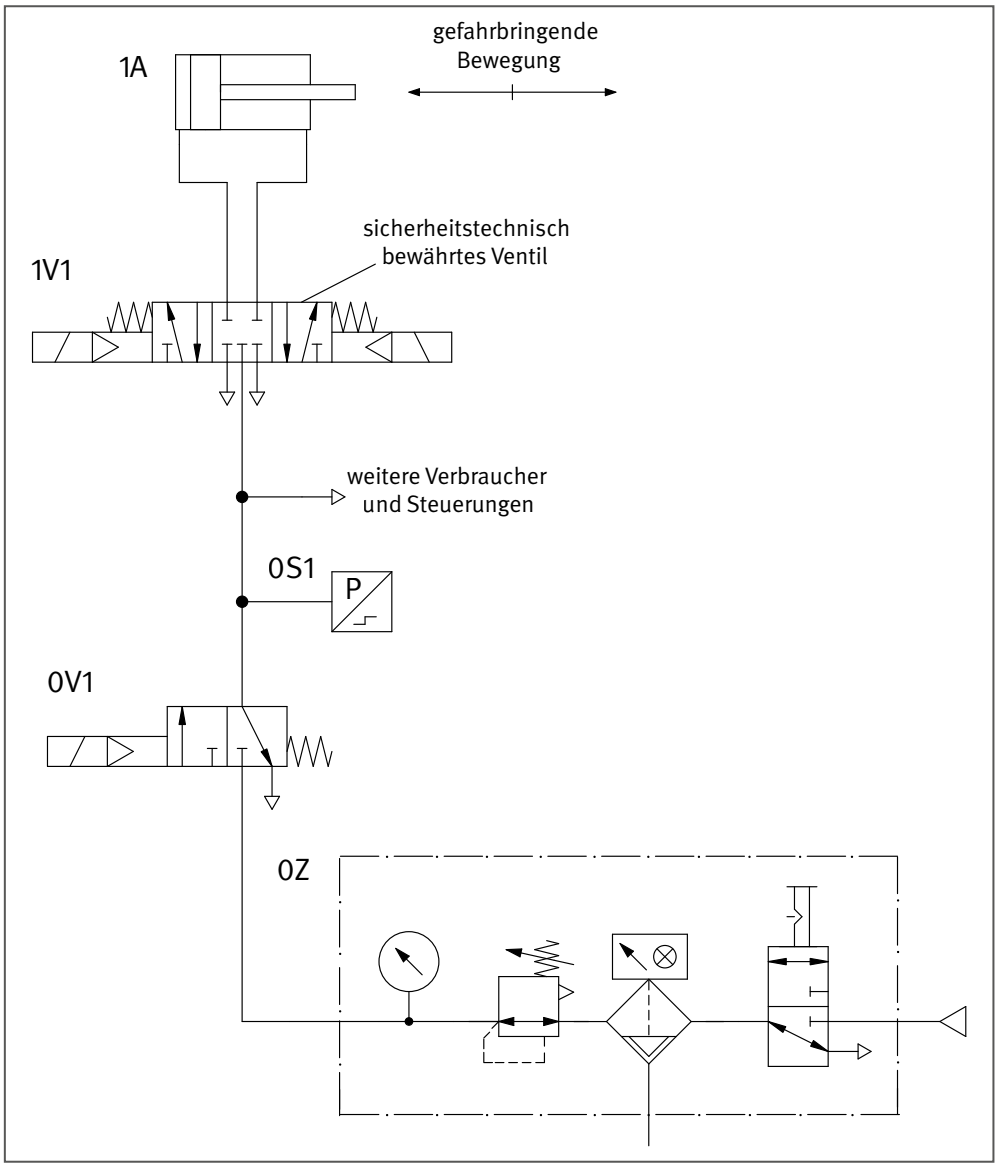


Abbildung 8.5:
Pneumatisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage, realisiert durch SSC
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch ein sicherheitstechnisch bewährtes Wegeventil 1V1 gesteuert.
- Der Ausfall des Wegeventils kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.
- Wenn durch eingesperrte Druckluft eine weitere Gefährdung auftreten kann, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V1 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Bestätigung für das Wegeventil als sicherheitstechnisch bewährtes Bauteil (ausreichend hohe Zuverlässigkeit) erfolgt durch den Hersteller/Anwender.
- Die Sicherheitsfunktion kann auch durch eine Verknüpfung von entsprechenden Ventilen erreicht werden.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für das Wegeventil 1V1 wird ein B_{10D}-Wert von 20 000 000 Schaltspielen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr und $MTTF_D$ = 145 Jahre. Dies ist gleichzeitig der $MTTF_D$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die pneumatische Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer. Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Wegeventil 1V1 ein Wert von 14 Jahren Betriebszeit (T_{10D}) bis zum vorgesehenen Austausch.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (08.16). Beuth, Berlin 2016

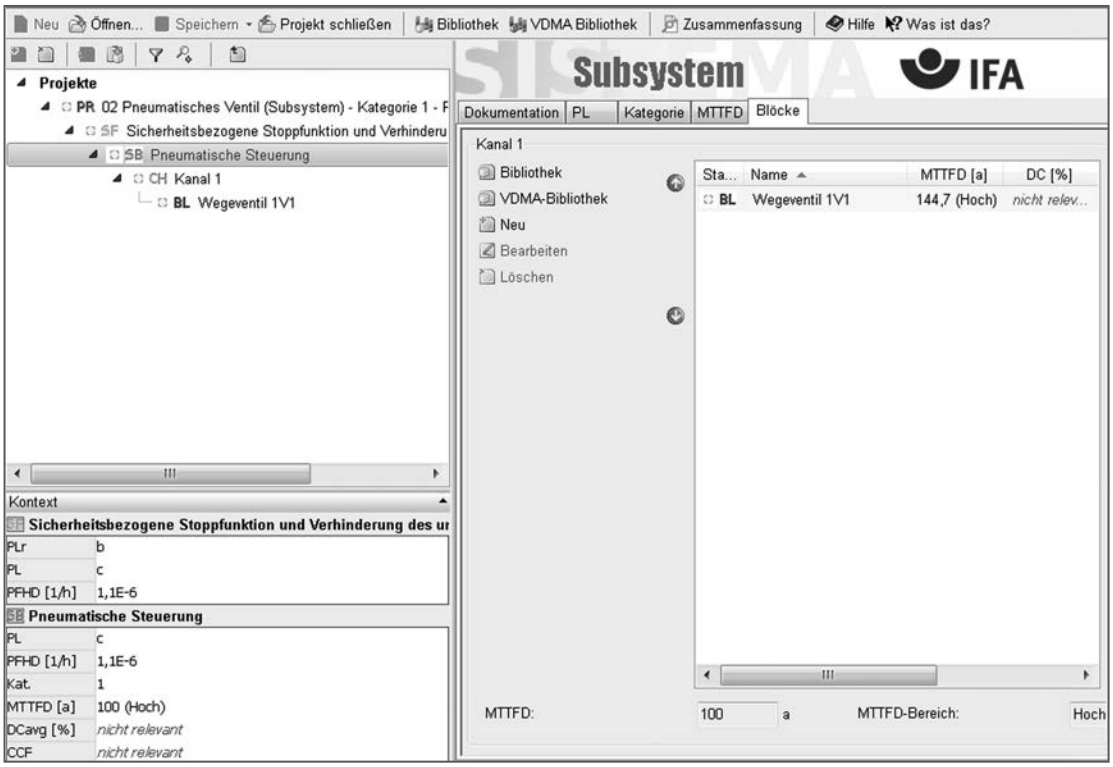


Abbildung 8.6: PL-Bestimmung mithilfe von SISTEMA

8.2.3 Hydraulisches Ventil (Subsystem) – Kategorie 1 – PL c (Beispiel 3)

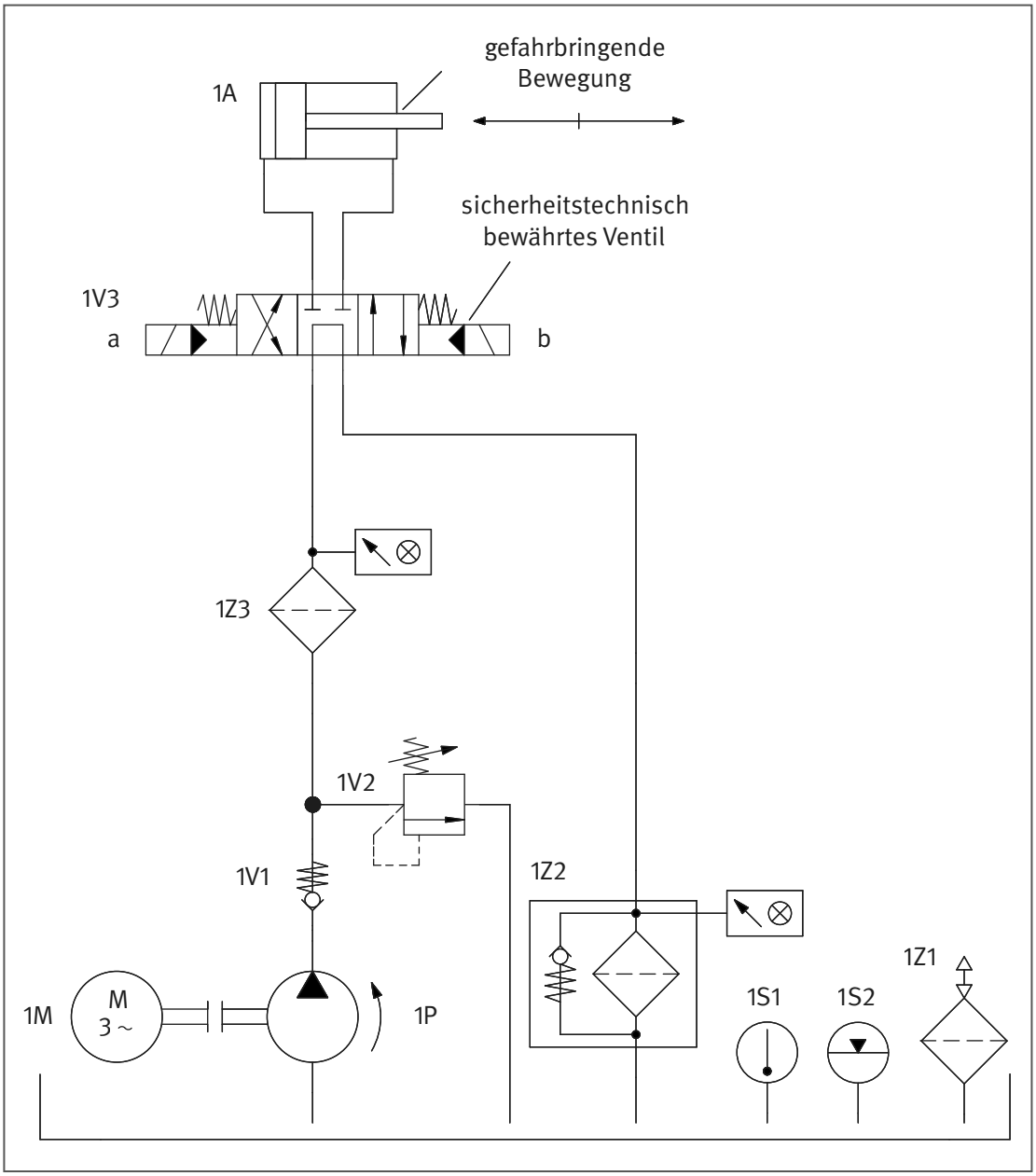


Abbildung 8.7: Hydraulisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch ein sicherheitstechnisch bewährtes Wegeventil 1V3 gesteuert.
- Der Ausfall des Wegeventils kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V3 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Bestätigung für das Wegeventil als sicherheitstechnisch bewährtes Bauteil erfolgt bei Bedarf durch den Hersteller/Anwender.
- Als gezielte Maßnahmen zur Erhöhung der Zuverlässigkeit des Wegeventils sind ein Druckfilter 1Z3 vor dem Wegeventil und geeignete Maßnahmen gegen Schmutzeinzug durch die Kolbenstange am Zylinder (z. B. wirksamer Abstreifer an der Kolbenstange, siehe * in Abbildung 8.7) vorgesehen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für das Wegeventil 1V3 wird eine $MTTF_D$ von 150 Jahren angenommen [H]. Dies ist gleichzeitig der $MTTF_D$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die hydraulische Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

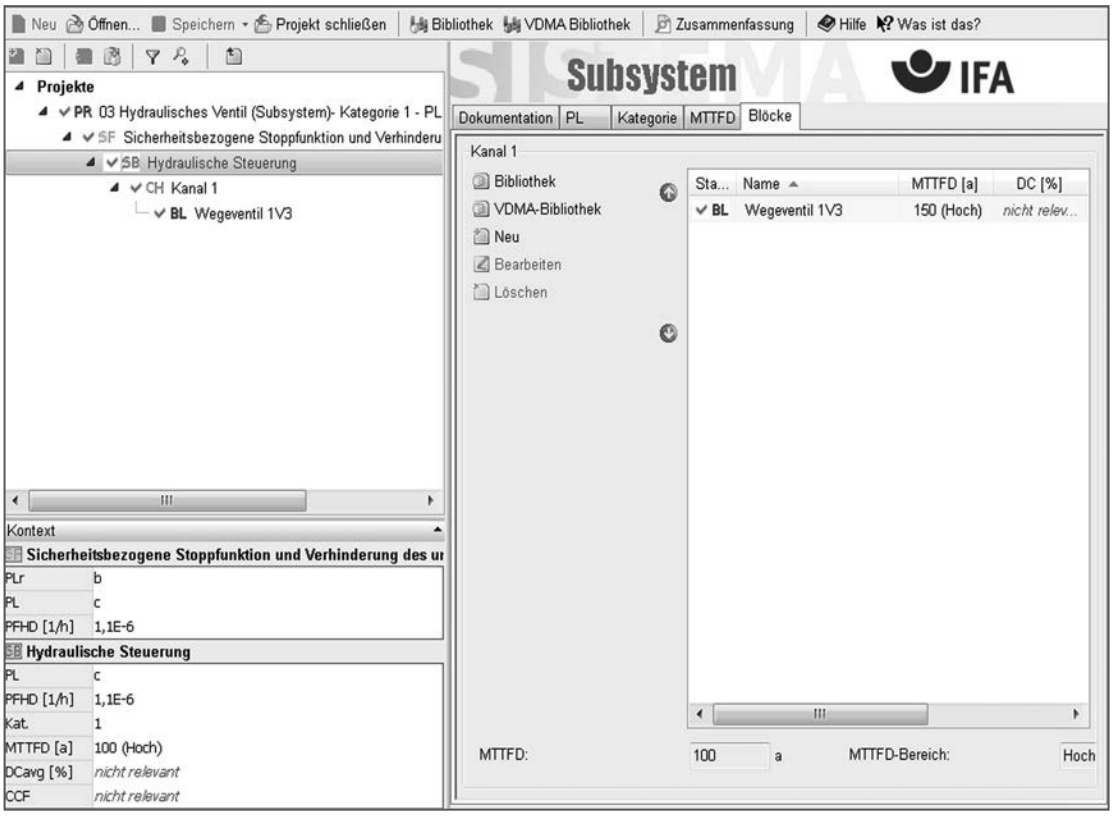


Abbildung 8.8: PL-Bestimmung mithilfe von SISTEMA

8.2.4 Stillsetzen von Holzbearbeitungsmaschinen – Kategorie B – PL b (Beispiel 4)

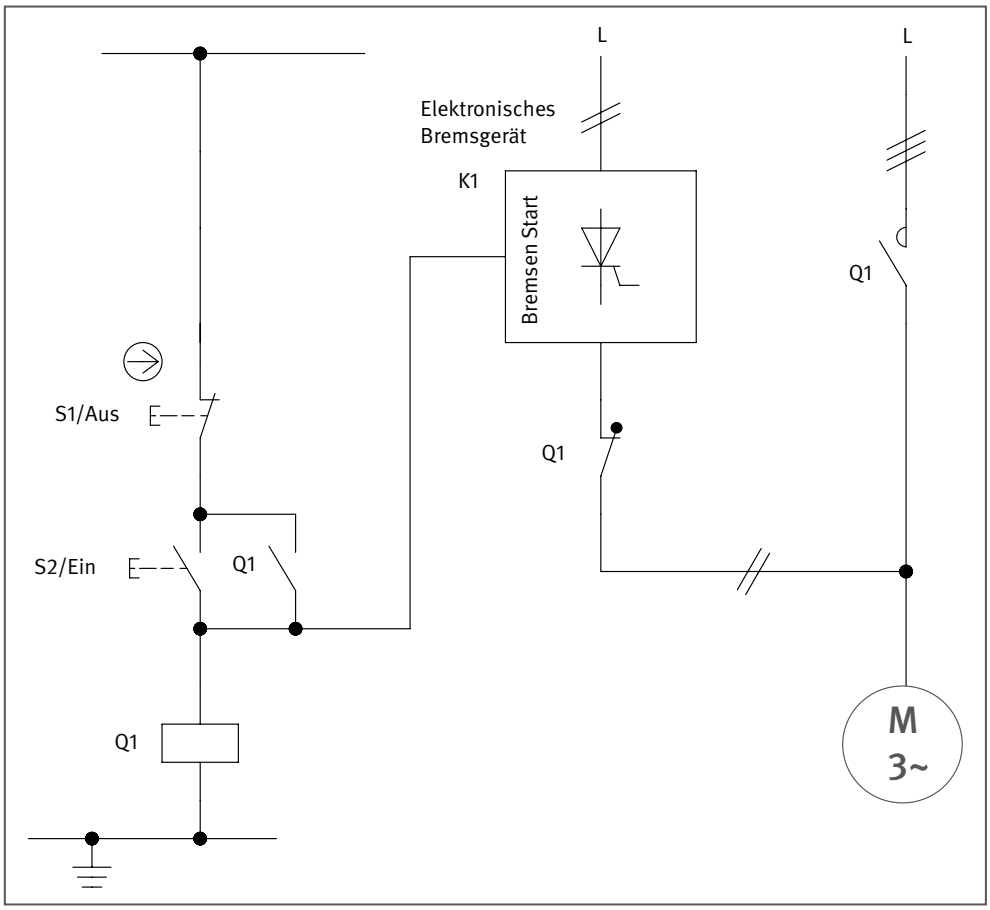


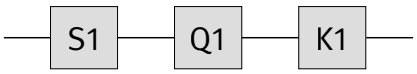
Abbildung 8.9:
Kombination von elektromechanischer Befehlseinrichtung und einfachem elektronischen Bremsgerät zum Stillsetzen von Holzbearbeitungsmaschinen

Sicherheitsfunktion

- Die Betätigung des Aus-Tasters führt zu SS1-t – Sicherer Stopp 1 zeitgesteuert, einem gesteuerten Stillsetzen des Motors innerhalb einer maximal zulässigen Zeit.

Funktionsbeschreibung

- Mit Betätigen des Aus-Tasters S1 wird das Stillsetzen des Motors eingeleitet. Das Motorschütz Q1 fällt ab und die Bremsfunktion wird gestartet. Die Bremsung des Motors erfolgt durch einen Gleichstrom, der im Bremsgerät K1 durch eine Phasenanschnittsteuerung mit Thyristor erzeugt wird und in der Motorwicklung ein Bremsmoment erzeugt.
- Die Stillsetzzeit darf einen maximalen Wert (z. B. 10 Sekunden) nicht überschreiten. Die hierfür erforderliche Höhe des Bremsstroms kann über ein Potenziometer am Bremsgerät eingestellt werden.
- Nach Ablauf der maximalen Bremszeit wird der Thyristor nicht mehr angesteuert und der Strompfad für den Bremsstrom ist unterbrochen. Der Stillsetzvorgang entspricht einem Stopp der Kategorie 1 gemäß DIN EN 60204-1.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen. Als grundlegendes Sicherheitsprinzip wird das Prinzip der Energietrennung (Ruhestromprinzip) angewandt. Zum Schutz gegen unerwarteten Wiederanlauf nach Wiederherstellung der Energieversorgung ist die Steuerung mit einer Selbsthaltung versehen.
- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung). S1 wird daher als bewährtes Bauteil angesehen.
- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.3 der DIN EN ISO 13849-2.
- Das Bremsgerät K1 ist unter Verwendung einfacher elektronischer Bauelemente wie z. B. Transistoren, Kondensatoren, Dioden, Widerstände, Thyristoren aufgebaut. Das sicherheitsrelevante Verhalten wird durch die Auswahl der Bauteile bestimmt. Interne Maßnahmen zur Fehlererkennung sind nicht vorgesehen.

Anwendung

- Bei Holzbearbeitungsmaschinen oder vergleichbaren Maschinen, bei denen das ungebremste Stillsetzen zu einem unzulässig langen Auslaufen der gefahrbringenden Werkzeugbewegungen führen würde. Die Steuerung der Bremsfunktion in Holzbearbeitungsmaschinen muss so ausgeführt sein, dass mindestens PL b erreicht wird (DIN EN ISO 19085-1).

Berechnung der Ausfallwahrscheinlichkeit

- Der Tastschalter S1 und das Schütz Q1 werden für die Berechnung in SISTEMA zu einem Subsystem zusammengefasst, das die Anforderungen der Kategorie 1 erfüllt. Das Bremsgerät K1 bildet ein separates Subsystem in Kategorie B.
- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung).
- $MTTF_D$: Für den Taster S1 wird ein B_{10D}-Wert von $20 \cdot 10^6$ Schaltspielen angegeben [H]. Für das Schütz Q1 wird bei nominaler Last ein B_{10D}-Wert von 1300 000 Schaltspielen [N] angenommen. Bei 300 Arbeitstagen, 8 Arbeitsstunden und 2 Minuten Zykluszeit ist n_{op} = 72 000 Zyklen/Jahr. Die $MTTF_D$ für den Taster S1 beträgt 2777 Jahre und für Q1 180 Jahre. Zusammen ergibt das eine $MTTF_D$ von 169 Jahren, die gemäß Norm für das Subsystem auf 100 Jahre („hoch“) gekürzt wird. Das Schütz Q1 weist eine begrenzte Betriebszeit (T_{10D}) von 18 Jahren auf. Ein rechtzeitiger Austausch wird empfohlen. Die $MTTF_D$ für das Bremsgerät K1 wurde über die „Parts Count“-Methode ermittelt. Mit den Bauteilinformationen aus der Stückliste und den Werten aus der Datenbank SN 29500 [48] ergibt sich eine $MTTF_D$ = 518 Jahre [D], die ebenfalls auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie B und Kategorie 1 nicht relevant.
- Das Subsystem S1/Q1 entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.
- Das Subsystem K1 entspricht Kategorie B mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}2 \cdot 10^{-6}$/Stunde. Dies entspricht PL b.
- Für die sicherheitsbezogene Stoppfunktion ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}4 \cdot 10^{-6}$/Stunde. Dies entspricht PL b.

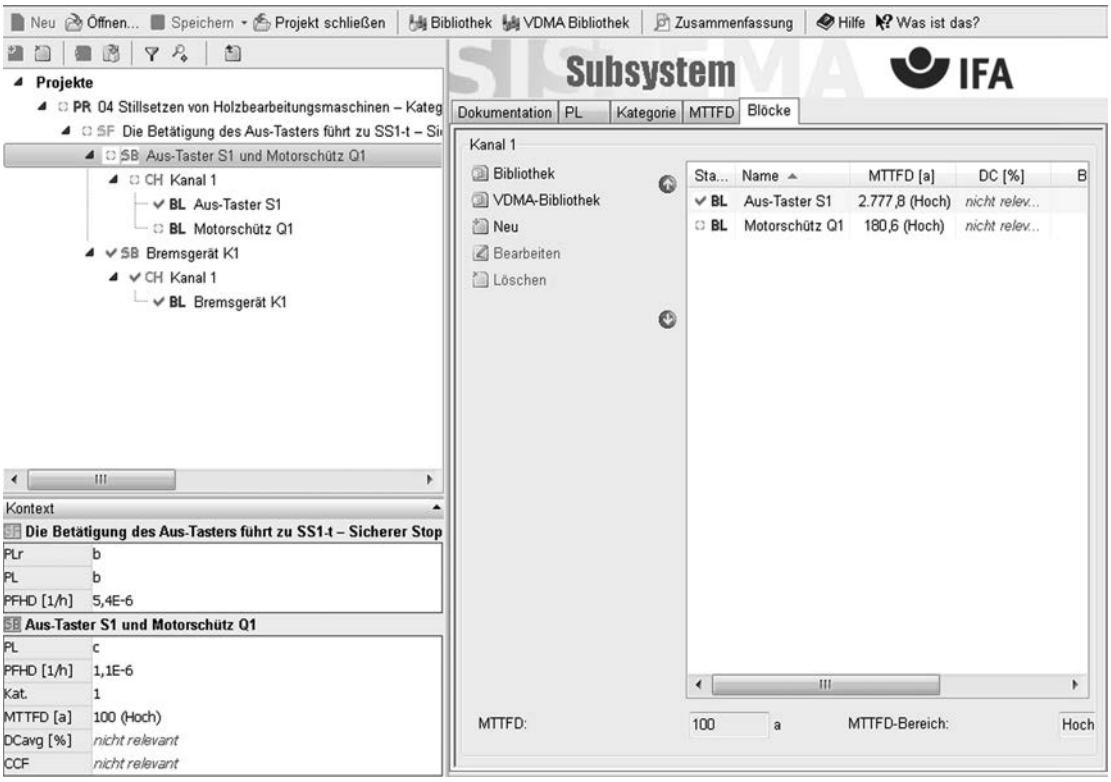


Abbildung 8.10: PL-Bestimmung mithilfe von SISTEMA

8.2.5 Stellungsüberwachung verriegelter trennender Schutzeinrichtungen – Kategorie 1 – PL c (Beispiel 5)

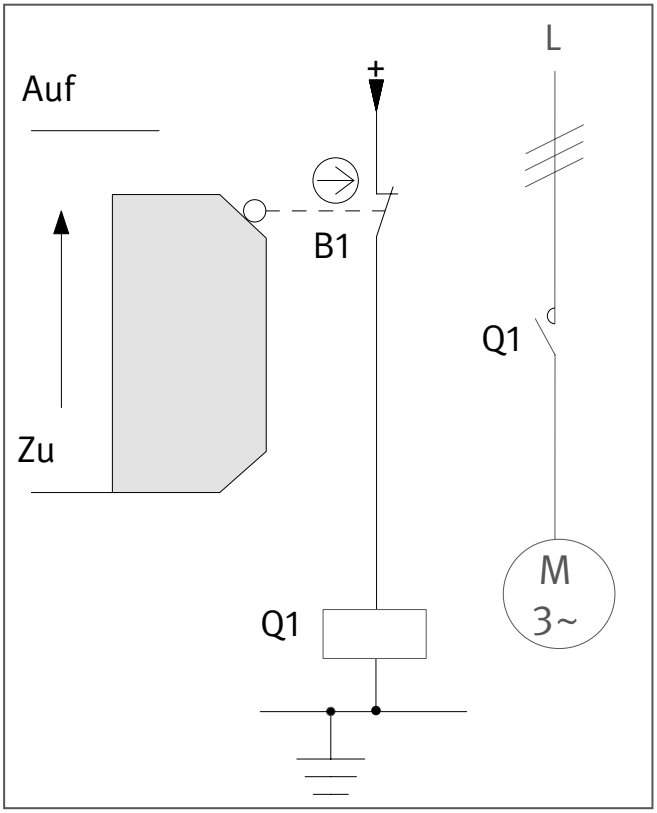


Abbildung 8.11:
Stellungsüberwachung verriegelter trennender Schutzeinrichtungen zur Verhinderung von gefahrbringenden Bewegungen (STO – Sicher abgeschaltetes Moment)

Sicherheitsfunktion

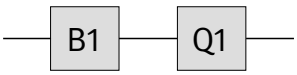
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der verriegelten trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der verriegelten trennenden Schutzeinrichtung (z. B. Schutzgitter) wird durch einen Positionsschalter B1 mit zwangsöffnendem Kontakt erfasst, der ein Schütz Q1 ansteuert. Durch das Abfallen von Q1 werden gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.
- Ein Entfernen der Schutzeinrichtung wird nicht bemerkt.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip verwendet. Die Erdung des Steuerkreises ist als bewährtes Sicherheitsprinzip zu betrachten.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K, und wird daher als bewährtes Bauteil angesehen. Der Öffnerkontakt unterbricht den Stromkreis mechanisch zwangläufig, wenn die Schutzeinrichtung sich nicht in Schutzstellung befindet.
- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.3 der DIN EN 13849-2.
- Die Stellungsüberwachung erfolgt durch einen Positionsschalter. Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt. Die Betätigungselemente des Positionsschalters sind gegen Lageveränderung gesichert. Es werden nur starre mechanische Teile (keine Federelemente in Wirkrichtung der Betätigungskraft) verwendet.
- Der Betätigungshub für den Positionsschalter erfolgt nach Herstellerangabe.



Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für B1 ist eine $MTTF_D$ von $20 \cdot 10^6$ Schaltspielen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 35 040 Zyklen/Jahr und $MTTF_D$ = 5 707 Jahre. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1300 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} ergibt sich für Q1 eine $MTTF_D$ von 742 Jahren. Die Kombination von B1 und Q1 ergibt für den Kanal eine $MTTF_D$ = 656 Jahre, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Damit ist der PL_r b übertroffen.

Weiterführende Literatur

- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (04.10). Beuth, Berlin 2010

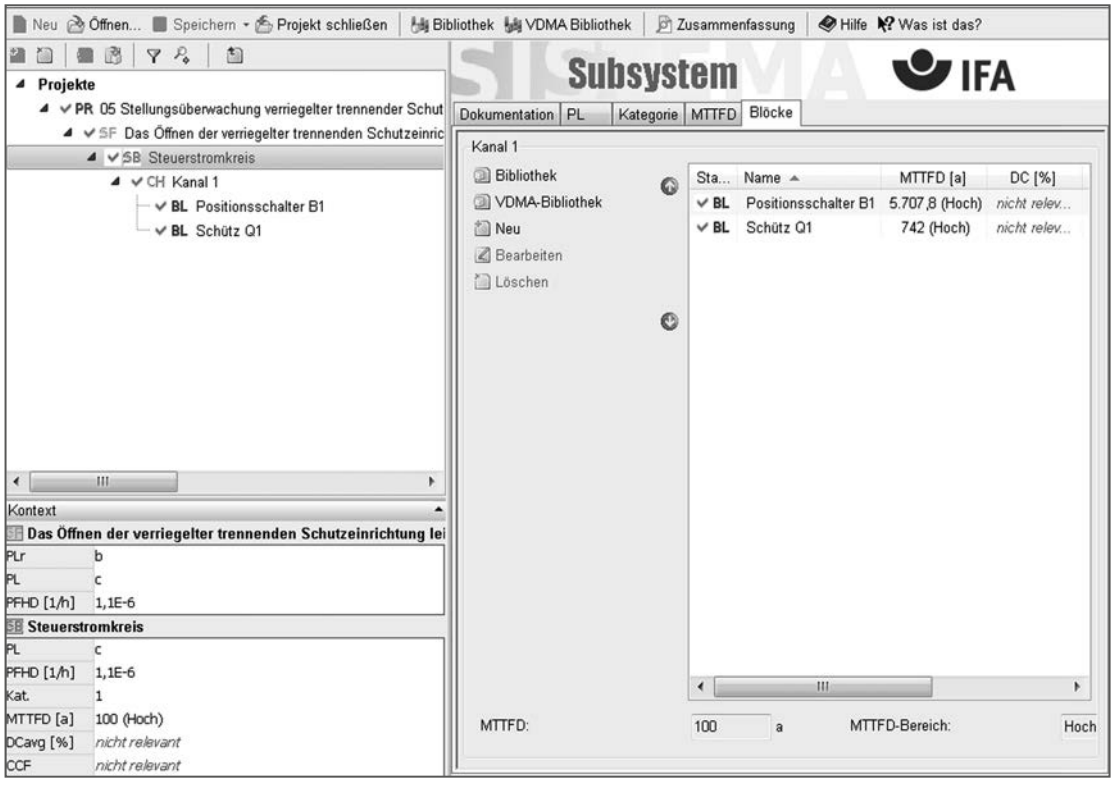


Abbildung 8.12: PL-Bestimmung mithilfe von SISTEMA

8.2.6 Start-Stopp-Einrichtung mit Not-Halt-Gerät – Kategorie 1 – PL c (Beispiel 6)

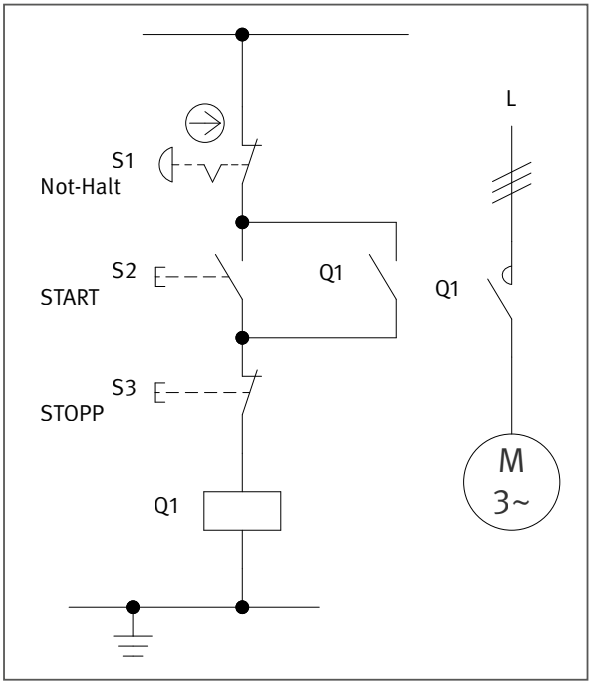


Abbildung 8.13:
Kombinierte Start-Stopp-Einrichtung mit Not-Halt-Gerät

Sicherheitsfunktion

- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Gerätes S1 durch Unterbrechung der Steuerspannung von Schütz Q1 abgeschaltet.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip verwendet. Zusätzlich ist die Erdung des Steuerkreises als bewährtes Sicherheitsprinzip vorhanden.
- Das Not-Halt-Gerät S1 ist ein Schalter mit zwangläufigem Betätigungsmodus entsprechend EN 60947-5-5 und daher ein bewährtes Bauteil nach Tabelle D.3 der DIN EN ISO 13849-2.
- Die Signalverarbeitung erfolgt durch ein Schütz (Stopp-Kategorie 0 nach DIN EN 60204-1).
- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.3 der DIN EN ISO 13849-2.

S1 — Q1

Bemerkung

- Die Funktion zum Stillsetzen im Notfall ergänzt als Schutzmaßnahme die Sicherheitsfunktionen zur Sicherung von Gefahrstellen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Bei S1 handelt es sich um ein handelsübliches Not-Halt-Gerät nach DIN EN ISO 13850, es ist nach DIN EN 60947-5-5 hergestellt. Gemäß DIN EN ISO 13849-1 Tabelle C.1 kann in diesem Fall für Not-Halt-Einrichtungen, unabhängig von der Last ein B_{10D}-Wert von 100 000 Schaltspielen angesetzt werden [N]. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1300 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Werden an 365 Arbeitstagen täglich zwei Betätigungen der Start-Stopp-Einrichtung und jährlich zwölf Betätigungen des Not-Halt-Gerätes angenommen, so ergibt sich mit n_{op} = 742 Zyklen/Jahr für Q1 eine $MTTF_D$ von 35 040 Jahren. Dies ist gleichzeitig die $MTTF_D$ für den Kanal, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (05.16). Beuth, Berlin 2016
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

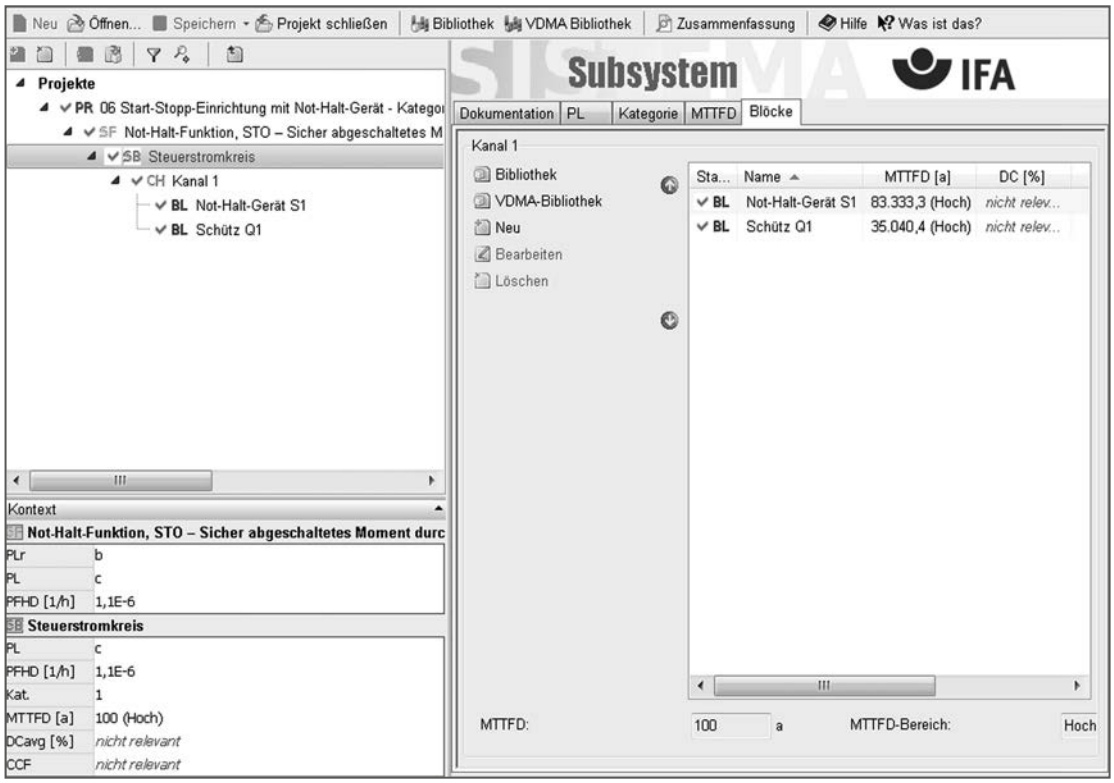


Abbildung 8.14: PL-Bestimmung mithilfe von SISTEMA

8.2.7 Unterspannungsauslösung über Not-Halt-Gerät – Kategorie 1 – PL c (Beispiel 7)

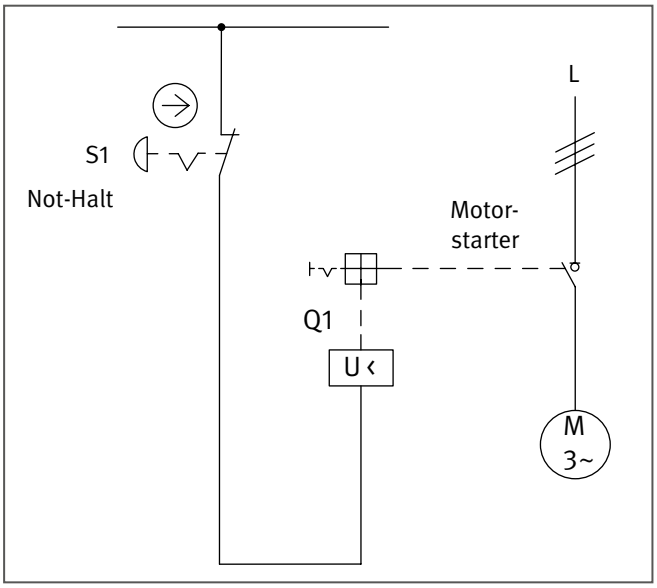


Abbildung 8.15:
Not-Halt-Gerät auf Unterspannungsauslösung der Netztrenneinrichtung (Motorstarter) wirkend

Sicherheitsfunktion

- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes, das auf die Unterspannungsauslösung eines Motorstarters, ggf. der Netztrenneinrichtung, wirkt.

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Gerätes S1 durch Unterspannungsauslösung der Netztrenneinrichtung – hier in Form eines Motorstarters Q1 – unterbrochen.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip des Unterspannungsauslösers verwendet.
- Das Not-Halt-Gerät S1 ist ein Schalter mit zwangläufigem Betätigungsmodus entsprechend EN 60947-5-5 und daher ein bewährtes Bauteil nach Tabelle D.3 der DIN EN ISO 13849-2.
- Der Motorstarter Q1 ist einem Leistungsschalter nach Tabelle D.3 der DIN EN ISO 13849-2 gleichzusetzen. Q1 kann daher als bewährtes Bauteil angesehen werden.
- Es wird die Spannungsversorgung der ganzen Maschine abgeschaltet (Stopp-Kategorie 0 nach DIN EN 60204-1).

S1 — Q1

Bemerkung

- Die Not-Halt-Funktion ergänzt als Schutzmaßnahme die Sicherheitsfunktionen zur Sicherung von Gefahrstellen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Bei S1 handelt es sich um ein handelsübliches Not-Halt-Gerät nach DIN EN ISO 13850, es ist nach DIN EN 60947-5-5 hergestellt. Gemäß DIN EN ISO 13849-1, Tabelle C.1, kann in diesem Fall für Not-Halt-Einrichtungen, unabhängig von der Last ein B_{10D}-Wert von 100 000 Schaltspielen angesetzt werden [N]. Für die Unterspannungsauslösung des Motorstarters Q1 entspricht der B_{10}-Wert näherungsweise der elektrischen Lebensdauer von 10 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Bei jährlich zwölf Betätigungen des Not-Halt-Gerätes ergibt sich mit n_{op} = 12 Zyklen/Jahr für Q1 eine $MTTF_D$ von 16 666 Jahren. Dies ist gleichzeitig die $MTTF_D$ für den Kanal, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (05.16). Beuth, Berlin 20016
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

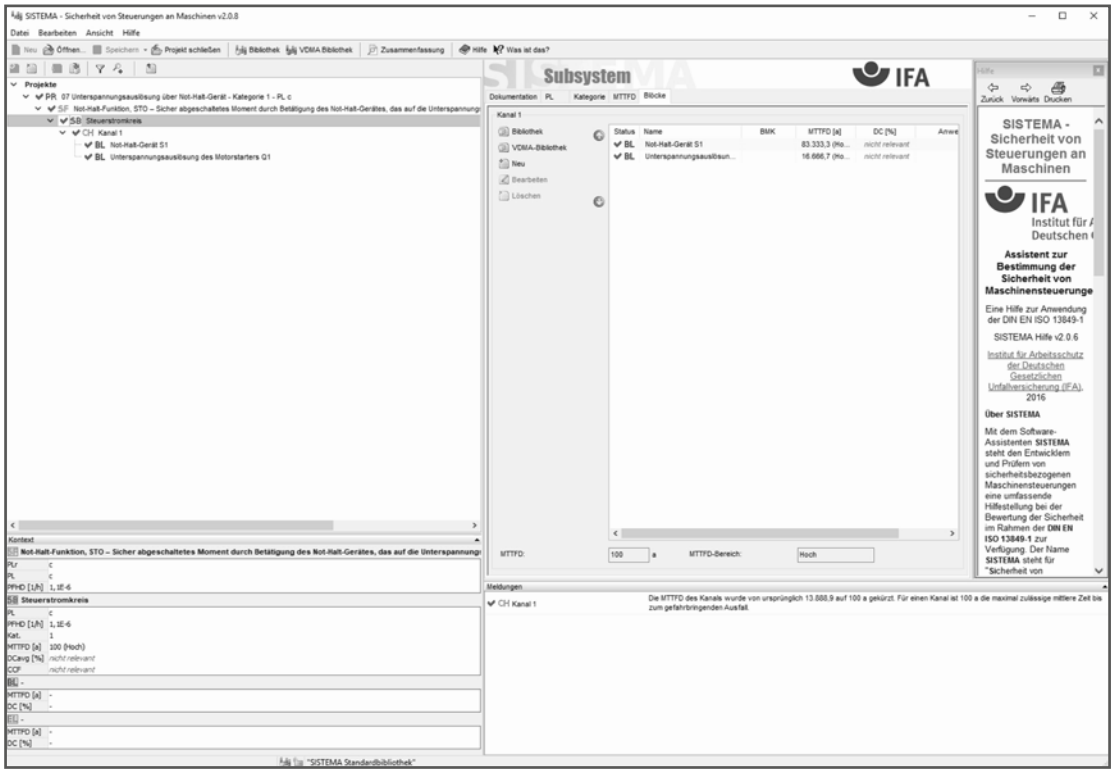


Abbildung 8.16: PL-Bestimmung mithilfe von SISTEMA

8.2.8 Stillsetzen von Holzbearbeitungsmaschinen – Kategorie 1 – PL c (Beispiel 8)

Beispiel entfällt, da es technologisch nicht mehr relevant ist.

8.2.9 Getestete Lichtschranken – Kategorie 2 – PL c mit nachgeschaltetem Kategorie-1-Ausgangsschaltelement (Beispiel 9)

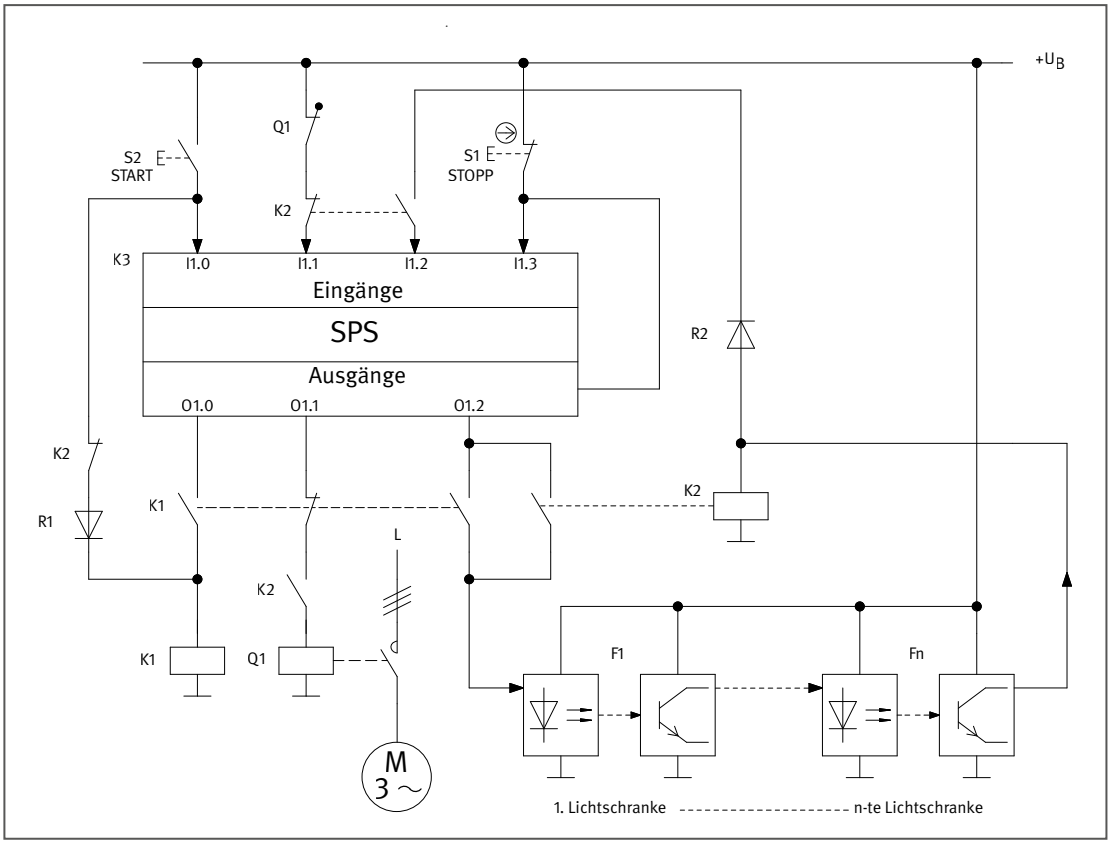


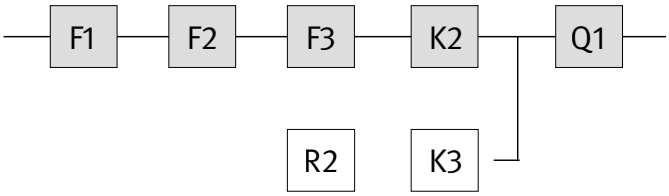
Abbildung 8.17: Testung von Lichtschranken mit einer Standard-SPS

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Bei Lichtstrahlunterbrechung wird eine gefahrbringende Bewegung stillgesetzt (STO – Sicher abgeschaltetes Moment).

Funktionsbeschreibung

- Bei einer Lichtstrahlunterbrechung der *n* kaskadierten Lichtschranken F1 bis Fn wird sowohl kontaktbehaftet durch das Entregen des Hilfsschützes K2 als auch durch den SPS-Ausgang (O1.1) des Testkanals ein Abschaltbefehl erzeugt. Das Stillsetzen der gefahrbringenden Bewegung erfolgt dann über das Hauptschütz Q1.
- Die Testung der Lichtschranken erfolgt vor jedem Start der gefahrbringenden Bewegung nach dem Drücken der Start-Taste S2 durch softwaregesteuertes Ausschalten der Lichtschrankensender mittels SPS-Ausgang O1.2. Die Überwachung der Empfängerreaktion (K2 fällt wieder ab) erfolgt über die SPS-Eingänge I1.1 und I1.2. Bei fehlerfreiem Verhalten gelangt K2 über O1.2 in Selbsthaltung und S2 kann zum Einleiten der gefahrbringenden Bewegung losgelassen werden. K1 wird über O1.0 entregt und über O1.1 wird das Hauptschütz Q1 angesteuert.
- Im Falle eines durch die Testung aufgedeckten Fehlers in einer Lichtschranke oder in K2 werden die Ausgänge O1.1 und O1.2 deaktiviert und es erfolgt keine weitere Ansteuerung des Hauptschützes Q1.
- Beim unterstellten globalen Versagen der SPS (Ausgang O1.0 führt Low-Potenzial, O1.1 und O1.2 führen High-Potenzial) bewirkt eine Lichtstrahlunterbrechung unabhängig von der SPS die Entregung von K2. Um diese Unabhängigkeit sicherzustellen, werden die Lichtschrankenausgänge mithilfe der Entkopplungsdiode R2 von der SPS getrennt. Im ungünstigen Fall können über das Betätigen der Start-Taste die Lichtschranken wieder mit K2 aktiviert werden und somit das Hauptschütz Q1 ansteuern. Somit wäre (nur) die Testeinrichtung ausgefallen. Ein Ausfall der Testeinrichtung wird wegen eines wahrscheinlich in diesem Zusammenhang gestörten funktionalen Prozessablaufs aufgedeckt.
- Während des Tests ist die Ansteuerung von Q1 durch K1 und O1.1 gesperrt.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Es werden spezielle Lichtschranken mit geeigneten optischen Eigenschaften (optischer Öffnungswinkel, Fremdlichtsicherheit usw.) nach DIN EN 61496-2 verwendet.
- Mit nur zwei SPS-Eingängen und einem Relais bzw. Hilfsschütz können mehrere Lichtschranken kaskadiert und überwacht werden.
- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Das Hauptschütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F.
- Der Einsatz der Standardkomponenten F1 bis Fn und K3 erfolgt entsprechend den Hinweisen in Abschnitt 6.3.10.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (Absenkung der Anforderungen im Testkanal wegen Diversität) und den Hinweisen in Abschnitt 6.3.10.
- Die Start-Taste S2 muss außerhalb des Gefahrenbereiches und mit Einblick in den Gefahrenbereich bzw. in die Gefahrstelle angeordnet sein.
- Die Anzahl, Anordnung und Höhe von Lichtstrahlen muss DIN EN ISO 13855 und DIN EN 62046 entsprechen.
- Ist bei der Absicherung von Gefahrbereichen ein „Hintertreten“ möglich, sind weitere Maßnahmen, wie z. B. eine Wiederanlaufsperre, erforderlich. Dazu lässt sich die Start-Taste S2 nutzen. Die SPS K3 kontrolliert dazu die Dauer des Gedrücktseins der Taste auf eine Minimal- und eine Maximalzeit. Nur wenn die Bedingungen eingehalten sind, wird von einem gültigen Start-Befehl ausgegangen.

Bemerkungen

- Das Beispiel ist für den Einsatz in Anwendungen mit seltener Anforderung der Sicherheitsfunktion vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2, nämlich „Testung sehr viel häufiger als Anforderung der Sicherheitsfunktion“ (vgl. Anhang G), erfüllt werden.
- Nach dem Auslösen eines Stopps sind die Lichtschranken bis zum nächsten Start deaktiviert. Dadurch könnte z. B. ein Gefahrenbereich betreten werden, ohne dass dies schaltungstechnisch „registriert“ wird. Durch eine entsprechende Anpassung der Schaltung lässt sich das Verhalten ändern.

Berechnung der Ausfallwahrscheinlichkeit

- Bei der Berechnung der Ausfallwahrscheinlichkeit werden beispielhaft drei Lichtschranken F1 bis F3 berücksichtigt. Wird eine zweite Gefahrstelle abgesichert, so handelt es sich um eine weitere Sicherheitsfunktion, die separat berechnet wird.
- Zur Berechnung der Ausfallwahrscheinlichkeit wird das Gesamtsystem in die zwei Subsysteme „Lichtschranken“ und „Hauptschütz“ (Q1) aufgeteilt.

Für das Subsystem „Lichtschranken“ gilt:

- F1, F2, F3 und K2 stellen den funktionalen Pfad der Kategorie-2-Schaltungsstruktur dar, die SPS K3 (inklusive Entkopplungsdiode R2) stellt die Testeinrichtung dar. S2 und K1 dienen zur Aktivierung der Lichtschrankentestung und sind an der Berechnung der Ausfallwahrscheinlichkeit nicht beteiligt.
- $MTTF_D$: Für F1 bis F3 wird jeweils eine $MTTF_D$ von 100 Jahren [G] angenommen. Für K2 gilt ein B_{10D}-Wert von 20 000 000 Zyklen [N]. Mit 240 Arbeitstagen, 16 Arbeitsstunden und 180 Sekunden Zykluszeit ist n_{op} = 76 800 Zyklen/Jahr. Durch die oben beschriebene Testung verdoppelt sich dieser Wert auf n_{op} = 153 600 Zyklen/Jahr mit einer $MTTF_D$ = 1302 Jahre für K2. Diese Werte ergeben eine $MTTF_D$ des Funktionskanals von 32 Jahren („hoch“). Für K3 wird eine $MTTF_D$ von 50 Jahren [G] angenommen. Der $MTTF_D$-Wert von 228 311 Jahren [N] für die Entkopplungsdiode R2 ist im Vergleich dazu unbedeutend.
- DC_{avg}: DC = 60 % für F1 bis F3 begründet sich durch den beschriebenen Funktionstest, DC = 99 % für K2 folgt aus der direkten Überwachung in K3 mithilfe zwangsgeführter Kontakte. Die Mittelungsformel für DC_{avg} ergibt 61 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Die Kombination der Steuerungselemente im Subsystem „Lichtschranken“ entspricht Kategorie 2 mit hoher $MTTF_D$ des Funktionskanals (32 Jahre) und niedrigem DC_{avg} (61 %). Damit ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls PFH_D von $1{,}9 \cdot 10^{-6}$/Stunde.

Für das Subsystem „Hauptschütz“ wird angenommen:

- B_{10D} = 1300 000 Zyklen [N] mit n_{op} = 76 800 Zyklen/Jahr. Dies führt zu einer $MTTF_D$ von 169 Jahren, die nach Norm auf 100 Jahre begrenzt wird. Die Struktur entspricht Kategorie 1, daher sind DC_{avg} und Ausfälle infolge gemeinsamer Ursache nicht relevant. Es ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls von $1{,}1 \cdot 10^{-6}$/Stunde.
- Die Addition der durchschnittlichen Wahrscheinlichkeiten eines gefährlichen Ausfalls beider Subsysteme ergibt eine PFH_D von $3{,}0 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.
- Ist abzusehen, dass die Sicherheitsfunktion häufiger als für die vorgesehene Architektur der Kategorie 2 zugrunde gelegt angefordert wird (das Verhältnis 100 : 1 wird unterschritten, d. h. häufiger als einmal in fünf Stunden), so kann dies gemäß Anmerkung 1 der Norm in Anhang K bis zu einem Verhältnis von 25 : 1 mit einem Zuschlag von 10 % berücksichtigt werden. Im vorliegenden Fall mit drei Lichtschranken erreicht das Subsystem „Lichtschranken“ noch eine PFH_D von $2{,}1 \cdot 10^{-6}$/Stunde. Die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls PFH_D von $3{,}2 \cdot 10^{-6}$/Stunde erreicht allerdings nur noch PL b. Um PL c zu erreichen, müssten z. B. die Anzahl der Lichtschranken reduziert oder Komponenten mit höherer $MTTF_D$ eingesetzt werden.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Bauteil Q1 ein Wert von 17 Jahren (T_{10D}) Betriebszeit bis zum vorgesehenen Austausch.

Weiterführende Literatur

- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (05.14) und Berichtigung 1 (08.15). Beuth, Berlin 2014 und 2015
- DIN EN 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (06.14). Beuth, Berlin 2014
- DIN EN 62046: Sicherheit von Maschinen – Anwendung von Schutzausrüstungen zur Anwesenheitserkennung von Personen (Normentwurf) (04.13). Beuth, Berlin 2013
- DIN EN ISO 13855: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (10.10). Beuth, Berlin 2010

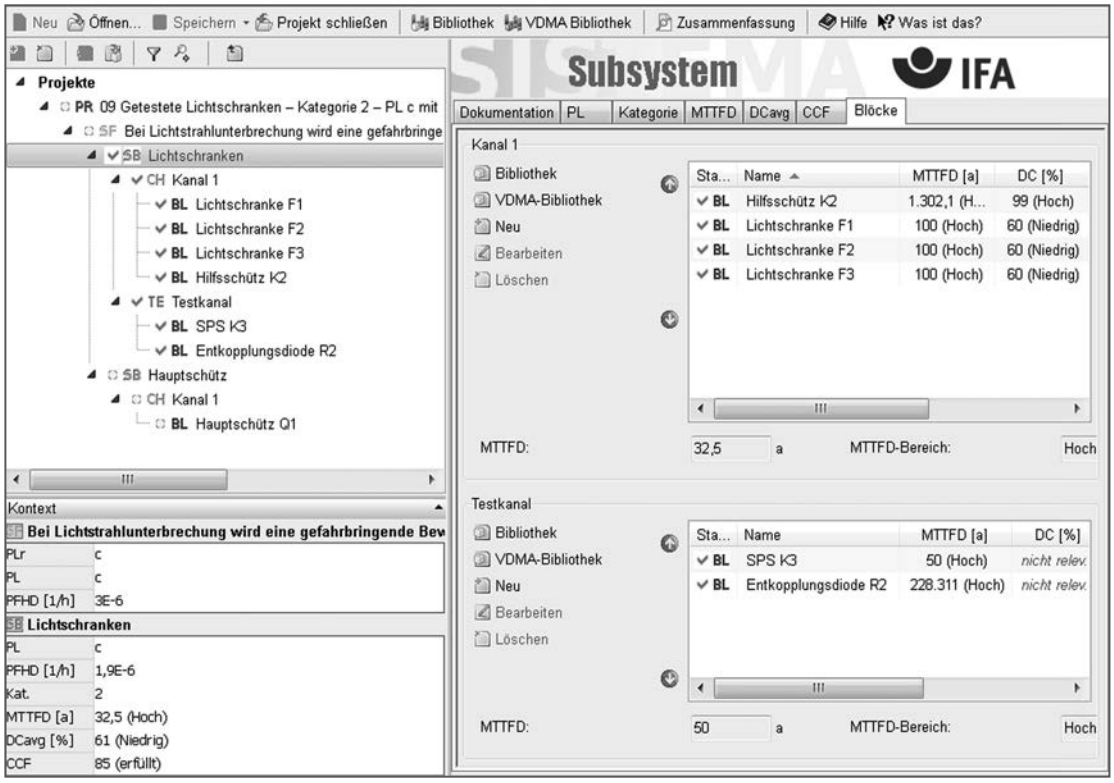


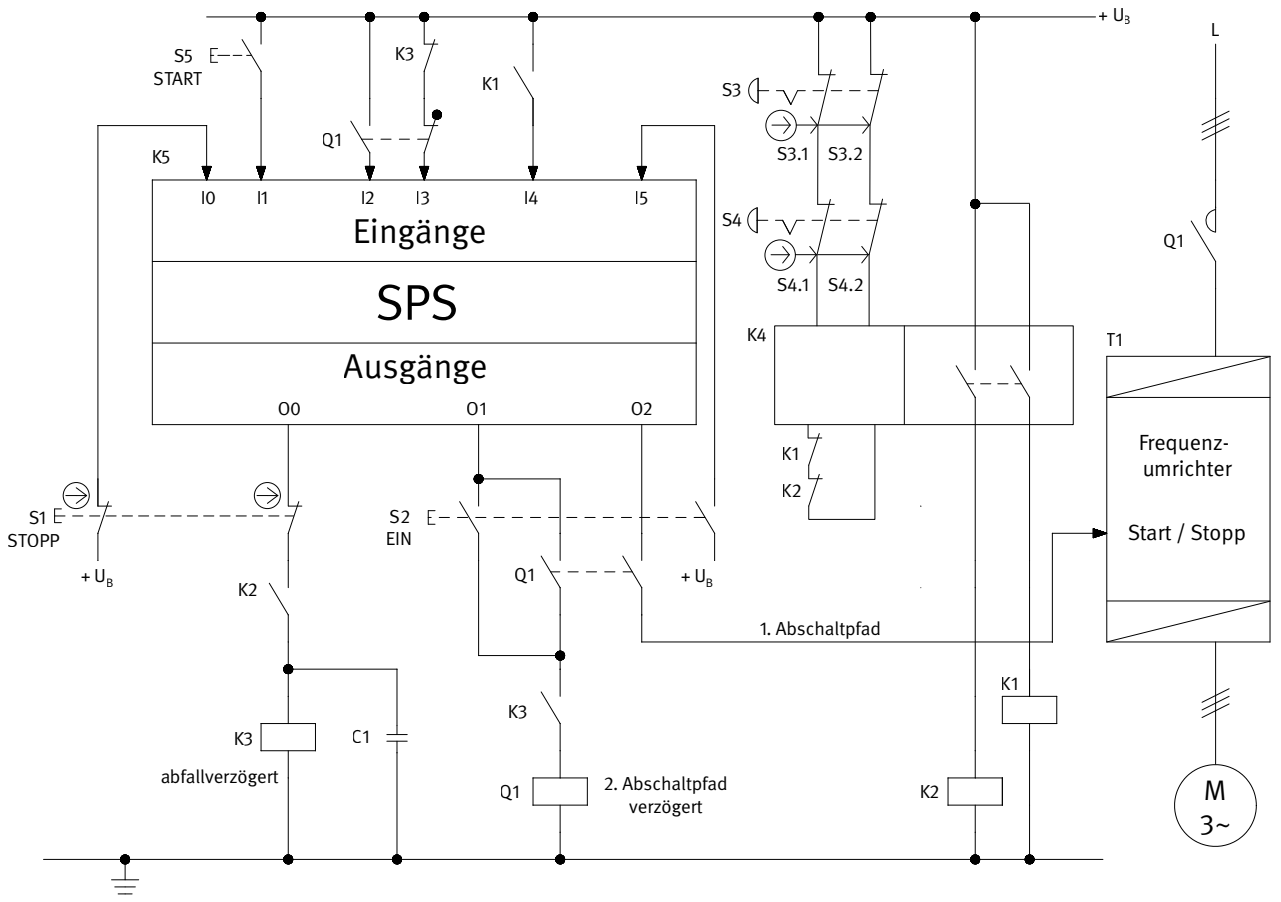
Abbildung 8.18: PL-Bestimmung mithilfe von SISTEMA

8.2.10 Sicheres Stillsetzen eines SPS-gesteuerten Antriebs mit Not-Halt – Kategorie 3 – PL d (Beispiel 10)

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

Die Sicherheitsfunktion wurde umdefiniert und das zugehörige sicherheitsbezogene Blockdiagramm angepasst. Der bisherige Block S3/S4 wurde auf S3 abgeändert. PL und PFH_D-Werte für SPS und Schütze wurden durch Herstellerwerte ersetzt.

Abbildung 8.19: Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Not-Halt-Befehl

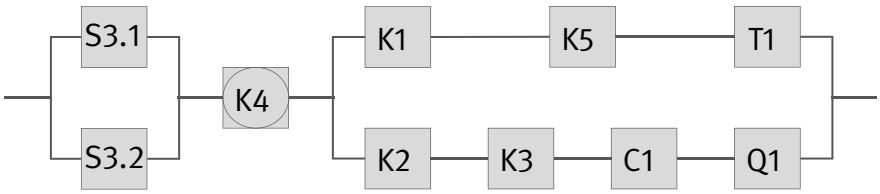


Sicherheitsfunktion

- Bei Betätigung des Not-Halt-Gerätes S3 wird der Antrieb gesteuert stillgesetzt (SS1-t – Sicherer Stopp 1 mit STO nach Verzögerungszeit).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird stillgesetzt, falls entweder die Stopp-Taste S1 oder eines der Not-Halt-Geräte S3 bzw. S4 betätigt wird. In diesem Beispiel wird nur die Betätigung mittels Not-Halt-Gerät S3 betrachtet. Das Stillsetzen des Antriebs im Notfall erfolgt nach Betätigung von S3 zuerst durch Deaktivierung des Not-Halt-Sicherheitsschaltgerätes K4 einhergehend mit dem Entregen der Hilfsschütze K1 und K2. Das Öffnen des Schließerkontaktes K1 am Eingang I4 der SPS K5 bewirkt über den SPS-Ausgang O2 die Rücknahme des Startsignals am Frequenzumrichter (FU) T1. Redundant zur Kette K1-K5-T1 startet mit dem Öffnen des Schließerkontaktes K2 vor dem abfallverzögerten Hilfsschütz K3 eine Bremszeitvorgabe, nach deren Ablauf die Ansteuerung für das Netzschütz Q1 unterbrochen wird. Die Zeitvorgabe ist so gewählt, dass unter ungünstigen Betriebsbedingungen der Stillstand der Maschinenbewegung erreicht wird, noch bevor das Netzschütz Q1 abfällt.



- Das funktionsgemäße Stillsetzen des Antriebs nach einem Stopp-Befehl wird mit dem Öffnen der beiden Öffnerkontakte der Stopp-Taste S1 eingeleitet. Analog zum Stillsetzen im Notfall erfolgt zunächst die Abfrage durch die SPS K5 über Eingang I0 und die Absteuerung des FU mit dem Rücksetzen des SPS-Ausgangs O2. Redundant dazu wird das Hilfsschütz K3 – abfallverzögert mithilfe des Kondensators C1 – entregt und nach Ablauf der Bremszeitvorgabe wird die Ansteuerung für das Netzschütz Q1 unterbrochen.
- Bei einem einzelnen Versagen der SPS K5, des Umrichters T1, des Netzschützes Q1, der Hilfsschütze K1/K2 oder des abfallverzögerten Hilfsschützes K3 wird trotzdem das Stillsetzen des Antriebs sichergestellt, weil immer zwei voneinander unabhängige Abschaltpfade vorhanden sind. Ein Nichtabfallen der Hilfsschütze K1 und K2 wird durch Überwachung der zwangsgeführten Öffnerkontakte innerhalb des Not-Halt-Sicherheitsschaltgerätes K4 spätestens nach dem Entriegeln des betätigten Not-Halt-Gerätes aufgedeckt. Das Nichtabfallen des Hilfsschützes K3 wird wegen der vorhandenen Rückführung des zwangsgeführten Öffnerkontaktes in den SPS-Eingang I3 spätestens vor einem erneuten Ingangsetzen der Maschinenbewegung aufgedeckt. Der Nichtabfall des Netzschützes Q1 wird über den in SPS-Eingang I3 eingelesenen Spiegelkontakt aufgedeckt. Ein Verschweißen dieses Spiegelkontaktes wird durch den hiermit zwangsgeführten Schließer-Hilfskontakt am SPS-Eingang I2 erkannt. Bei einem Fehler im Kondensator C1 weicht die gemessene Abfallzeit des Hilfsschützes K3 von der Zeitvorgabe in der SPS ab. Der Fehler wird erkannt und führt zur Abschaltung und Betriebshemmung der Maschine. Durch organisatorische Maßnahmen wird sichergestellt, dass jedes Not-Halt-Gerät mindestens einmal pro Jahr betätigt wird.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Die Hilfsschütze K1, K2 und K3 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Kontakte der Taster S1, S3 und S4 sind zwangsöffnend ausgeführt entsprechend DIN EN 60947-5-1, Anhang K.
- Das Schütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F.
- Die Standardkomponenten K5 und T1 werden entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL c (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.10.
- Die im Fehlerfall verzögerte Erreichung des Stillstands nur über den zweiten Abschaltpfad darf nicht mit einem verbleibenden inakzeptabel hohen Restrisiko verbunden sein.
- Der sicherheitsrelevante Steuerungsteil des Not-Halt-Sicherheitsschaltgerätes K4 erfüllt alle Anforderungen für Kategorie 3 und PL d.

Berechnung der Ausfallwahrscheinlichkeit

Es wird nur die Ausfallwahrscheinlichkeit der Not-Halt-Funktion berechnet.

- Das Not-Halt-Gerät S3 ist mit zwei Öffnerkontakten S3.1 und S3.2 ausgestattet. Für die Blöcke S3.1 und S3.2 gibt der Hersteller jeweils einen B_{10D} = 127 500 Zyklen an. Bei einer jährlichen Betätigung und einem n_{op} = 1 Zyklus/Jahr ergibt sich für jeden Kontakt eine $MTTF_D$ = 1 275 000 Jahre. Das Not-Halt-Sicherheitsschaltgerät K4 liegt als geprüftes Sicherheitsbauteil vor. Seine Ausfallwahrscheinlichkeit beträgt $3{,}0 \cdot 10^{-7}$/Stunde [H] und wird am Ende der Berechnung addiert.

Für die Ausfallwahrscheinlichkeit der nachfolgenden zweikanaligen Struktur gilt:

- $MTTF_D$: Die SPS K5 hat eine $MTTF_D$ = 10 Jahre [N]. Der Frequenzumrichter hat eine $MTTF_D$ = 35 Jahre [H]. Der Kondensator C1 geht mit $MTTF_D$ = 45 662 Jahren [D] in die Berechnung ein. Für K1 und K2 ergibt sich bei einem B_{10D}-Wert von 5 000 000 Zyklen [H] und einer Schalthäufigkeit von täglichem Einschalten an 240 Arbeitstagen eine $MTTF_D$ von 208 333 Jahren. Für K3 ergibt sich bei einem B_{10D}-Wert von 2 000 000 Zyklen [H] und bei 240 Arbeitstagen, 16 Arbeitsstunden und 3 Minuten Zykluszeit eine n_{op} = 76 800 Zyklen/Jahr eine $MTTF_D$ von 260 Jahren. Für Q1 ergibt sich bei einem $B1_{0D}$-Wert von 600 000 Zyklen [H] und bei 240 Arbeitstagen, 16 Arbeitsstunden und 3 Minuten Zykluszeit eine n_{op} = 76 800 Zyklen/Jahr eine $MTTF_D$ von 7,8 Jahren. Diese Werte ergeben eine symmetrisierte $MTTF_D$ des Kanals von 60 Jahren („hoch“).

- DC_{avg}: Eine ausreichende Testhäufigkeit der Not-Halt Geräte ist gewährleistet (siehe Hinweise in den Abschnitten 6.2.14 und D.2.5.1). Die Fehlererkennung der Blöcke S3.1 und S3.2 erfolgt durch einen Kreuzvergleich in K4 (*DC* = 90 %). Fehlererkennung durch den Prozess bei Ausfall der Ansteuerung der Bremsrampe führt auf *DC* = 60 % für K5. Für T1 ergibt sich *DC* = 60 % ebenfalls aus der Fehlererkennung durch den Prozess. K1 und K2 zeigen *DC* = 99 % durch in K4 integrierte Fehlererkennung und für K3 gilt *DC* = 99 % wegen Fehlererkennung durch K5. Für C1 gilt *DC* = 60 % durch Testung des Zeitglieds bei spannungsfreiem FU über die Abfallzeit von Hilfsschütz K3 in der SPS. Für Q1 folgt *DC* = 99 % durch direkte Überwachung in K5. Die Mittelungsformel für DC_{avg} ergibt 64,5 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte): Trennung (15), Diversität (20), FMEA (5) und Umgebungsbedingungen (25 + 10)
- Die zweikanalige Kombination der Steuerungselemente entspricht Kategorie 3. Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 3{,}9 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Die Gesamtausfallwahrscheinlichkeit wird durch Addition der Wahrscheinlichkeit gefährlicher Ausfälle von K4 und S3 ermittelt und ergibt $7{,}4 \cdot 10^{-7}$/Stunde. Dies entspricht dann ebenfalls PL d.
- Das verschleißbehaftete Schütz Q1 sollte nach ca. 7,8 Jahren (T_{10D}) ausgetauscht werden.

Weiterführende Literatur

- *Apfeld, R.; Zilligen, H; Köhler, B.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 7/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2013. ▸ www.dguv.de/ifa, Webcode: d639540
- IEC 61800-5-2:2016-04: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional. IEC Central Office, Switzerland CH-1211 Geneva 2016

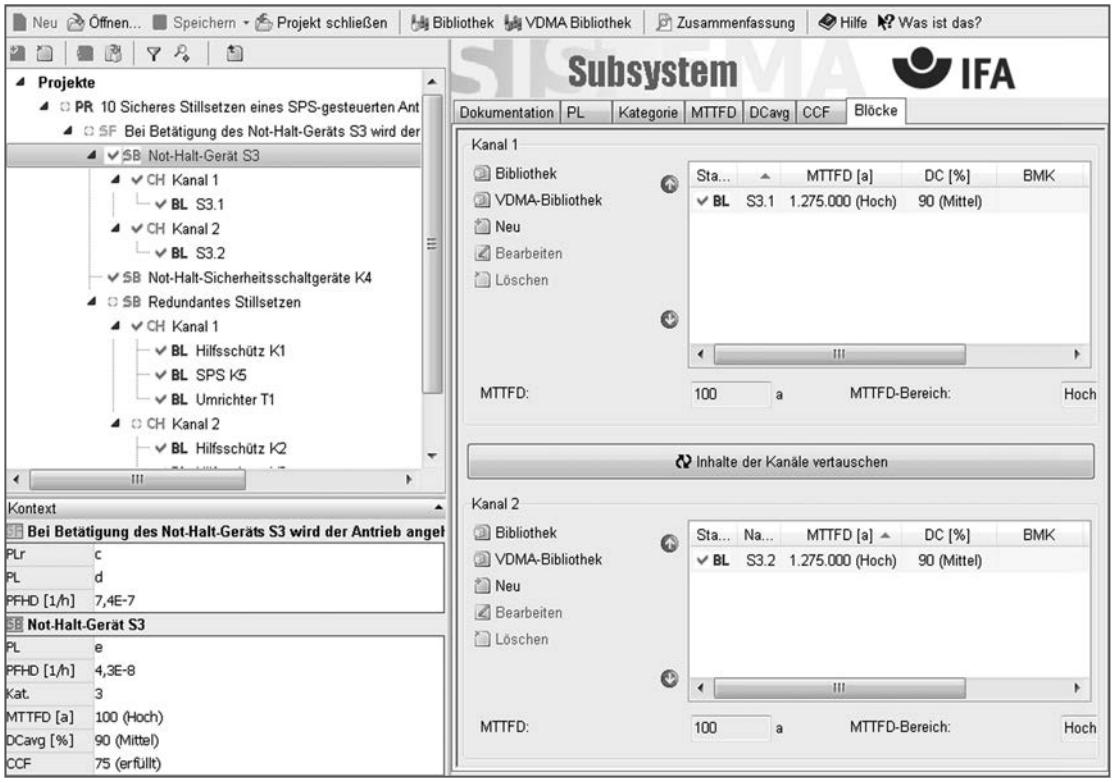


Abbildung 8.20: PL-Bestimmung mithilfe von SISTEMA

8.2.11 Getestetes pneumatisches Ventil (Subsystem) – Kategorie 2 – PL d (Beispiel 11)

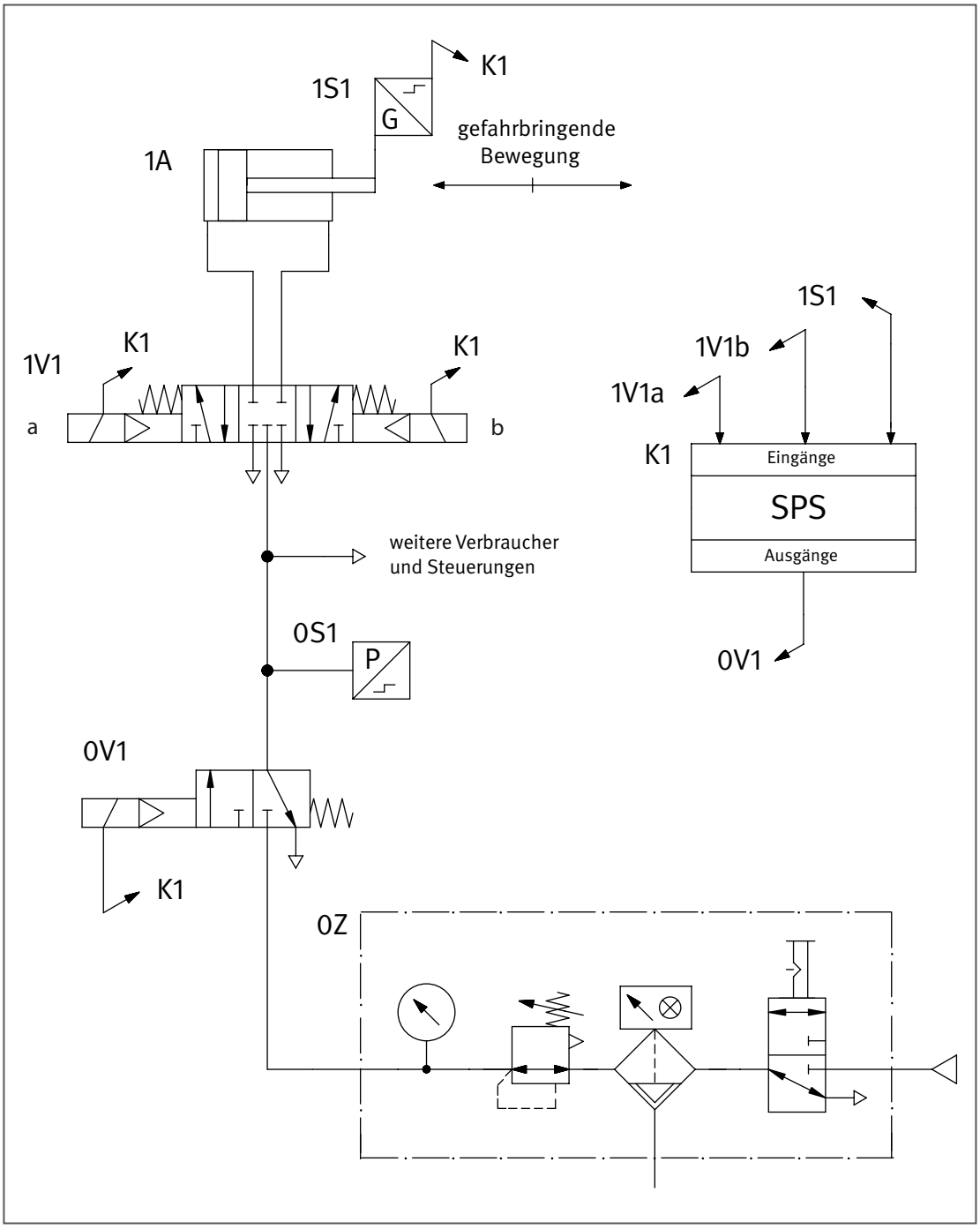
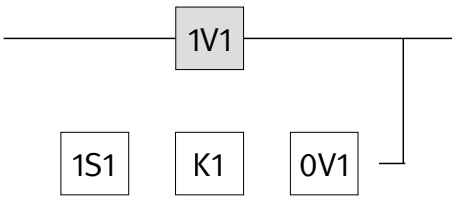


Abbildung 8.21: Pneumatisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen



Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage, realisiert durch SSC und bei erkannten Fehlern (Ausfallerkennung) durch SDE
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch ein Wegeventil 1V1 gesteuert.
- Der Ausfall des Wegeventils 1V1 zwischen den Funktionstests kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion über die SPS K1 mithilfe eines Wegmesssystems 1S1 in geeigneten Zeitabständen und beim Anfordern der Sicherheitsfunktion. Das Erkennen des Ausfalls von 1V1 führt zum Abschalten des Entlüftungsventils 0V1.
- Das Unterbrechen der gefahrbringenden Bewegung über das Entlüftungsventil 0V1 ergibt in der Regel einen verlängerten Nachlaufweg. Der Abstand zum Gefahrenbereich muss auf den verlängerten Nachlaufweg ausgelegt sein.
- Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.
- Wenn durch eingesperrte Druckluft eine weitere Gefährdung auftreten kann, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V1 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Testung erfolgt z. B. durch Überprüfung des Weg-/Zeitverhaltens (Wegmesssystem 1S1) der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einer SPS (K1).
- Die elektrische Ansteuerung von 1V1 darf nicht aus K1 erfolgen.
- In geeigneten Zeitabständen, z. B. täglich, wird zur Verhinderung eines systematischen Ausfalls die übergeordnete Abschaltfunktion (in diesem Beispiel auf das Entlüftungsventil 0V1 wirkend) überprüft.
- Für den Einsatz in Anwendungen mit seltenem Eingriff in den Gefahrbereich vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2 erfüllt werden. Die Anforderung besagt, dass die Testung unmittelbar bei Anforderung der Sicherheitsfunktion erfolgt und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand, beispielsweise unter Berücksichtigung des Nachlaufweges, der u. a. von der Entlüftungszeit und den Schaltzeiten der Ventile abhängt (hier wird über das Ventil 0V1 übergeordnet entlüftet), kürzer ist als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855 und vgl. Abschnitt 6.2.14).
- Der Einsatz der Standardkomponente K1 erfolgt entsprechend den Hinweisen in Abschnitt 6.3.10.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL c (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$ des Funktionskanals: Für das Wegeventil 1V1 wird ein B_{10D}-Wert von 20 000 000 Schaltspielen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 5 Sekunden Zykluszeit ist n_{op} = 2 764 800 Schaltspiele/Jahr und $MTTF_D$ = 72,3 Jahre. Dies ist gleichzeitig der $MTTF_D$-Wert für den Funktionskanal.
- $MTTF_D$ des Testkanals: Für das Wegmesssystem 1S1 wird ein $MTTF_D$-Wert von 150 Jahren [G] angenommen. Für die SPS K1 wird ein $MTTF_D$-Wert von 50 Jahren [G] angenommen. Für das Entlüftungsventil 0V1 gilt ein B_{10D}-Wert von 20 000 000 Zyklen [N]. Bei täglichem Einschalten an 240 Arbeitstagen ergibt sich für 0V1 ein $MTTF_D$-Wert von 833 333 Jahren. Damit beträgt die $MTTF_D$ des Testkanals 37,5 Jahre.
- DC_{avg}: DC = 60 % für 1V1 gründet sich auf den Vergleich des Weg-/Zeit-Verhaltens der gefahrbringenden Bewegung in Verbindung mit dem Schaltzustand des Wegeventils. Dies ist gleichzeitig der DC_{avg} („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_D$ (72,3 Jahre) und niedrigem DC_{avg} (60 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}6 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer. Das verschleißbehaftete Element 1V1 sollte nach jeweils ca. sieben Jahren (T_{10D}) ausgetauscht werden.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (08.16). Beuth, Berlin 216

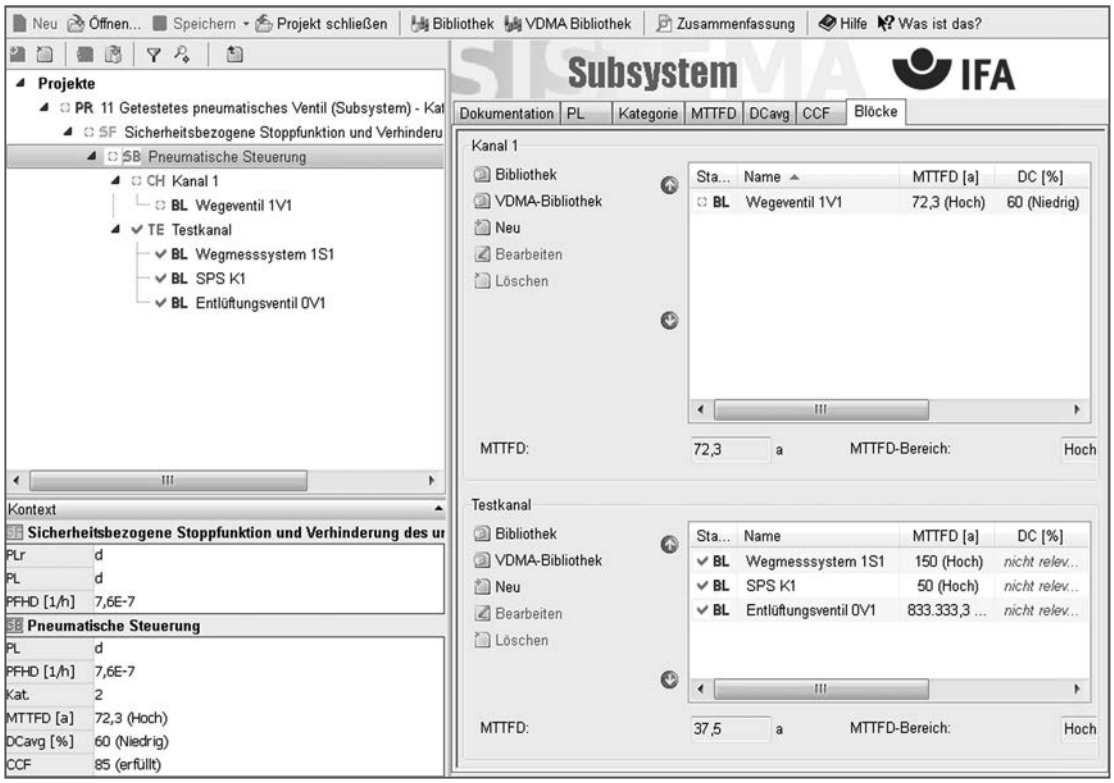


Abbildung 8.22: PL-Bestimmung mithilfe von SISTEMA

8.2.12 Getestetes hydraulisches Ventil (Subsystem) – Kategorie 2 – PL d (Beispiel 12)

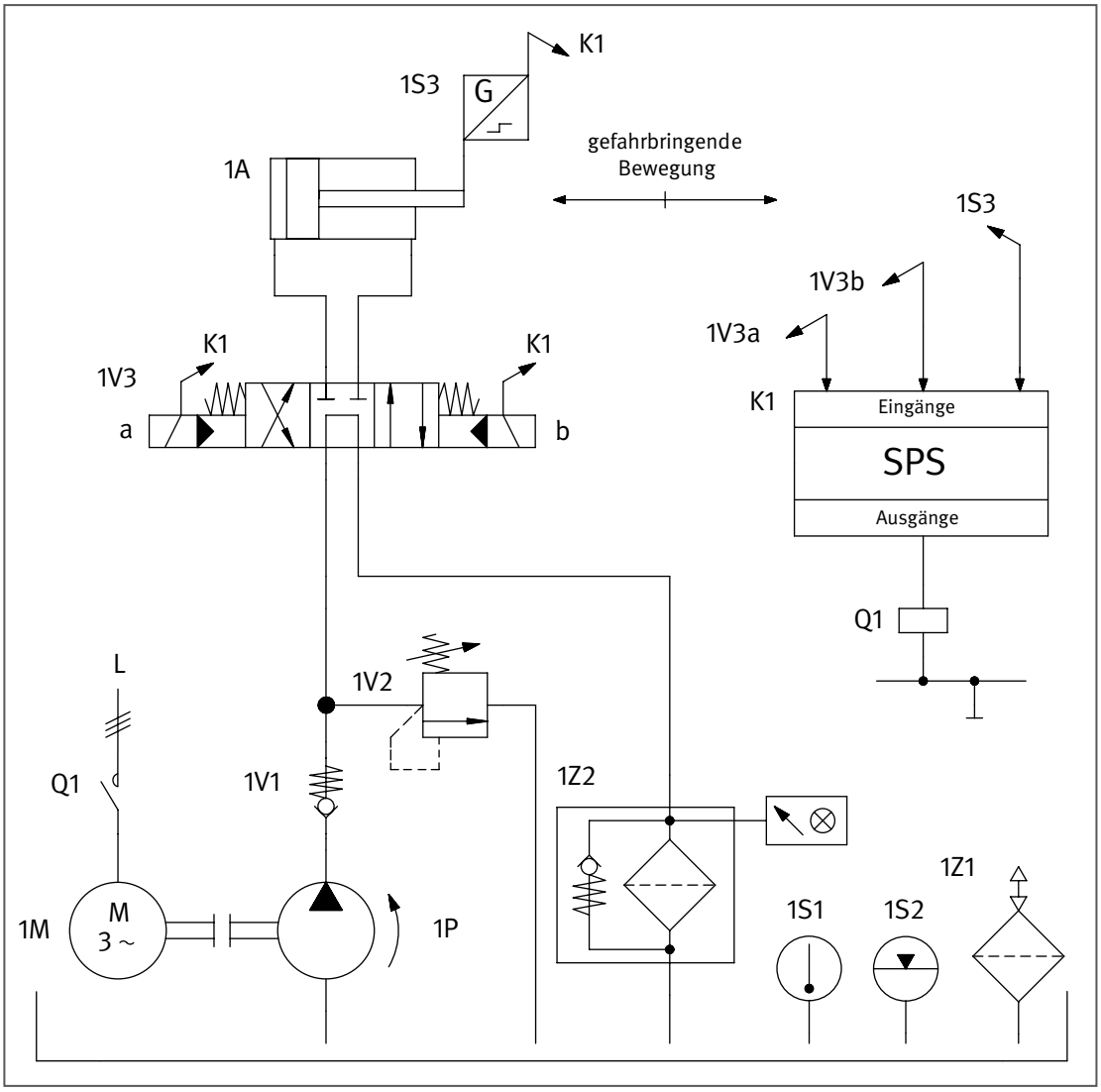
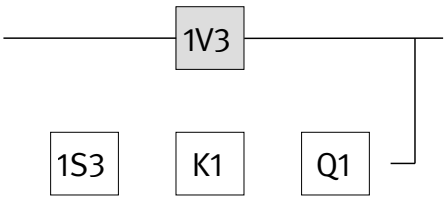


Abbildung 8.23: Hydraulisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere, sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.



Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch das Wegeventil 1V3 gesteuert.
- Der Ausfall des Wegeventils 1V3 zwischen den Funktionstests kann zum Verlust der Sicherheitsfunktion führen. Die Ausfallwahrscheinlichkeit hängt von der Zuverlässigkeit des Wegeventils ab.
- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion über die SPS K1 mithilfe eines Wegmesssystems 1S3 in geeigneten Zeitabständen und beim Anfordern der Sicherheitsfunktion. Das Erkennen des Ausfalls von 1V3 führt zum Abschalten der Hydraulikpumpe 1M bzw. 1P mittels Leistungsschütz Q1.
- Das Unterbrechen der gefahrbringenden Bewegung über die Hydraulikpumpe ergibt in der Regel einen verlängerten Nachlaufweg. Der Abstand zum Gefahrenbereich muss auf den verlängerten Nachlaufweg ausgelegt sein.
- Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V3 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Testung erfolgt z. B. durch Überprüfung des Weg-/Zeitverhaltens (Wegmesssystem 1S3) der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einer SPS (K1). Die elektrische Ansteuerung von 1V3 darf nicht aus K1 erfolgen.
- In geeigneten Zeitabständen, z. B. täglich, wird zur Verhinderung eines systematischen Ausfalls die übergeordnete Abschaltfunktion (in diesem Beispiel auf die Hydraulikpumpe wirkend) überprüft.
- Für den Einsatz in Anwendungen mit seltenem Eingriff in den Gefahrbereich vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2 erfüllt werden. Die Anforderung besagt, dass die Testung unmittelbar bei Anforderung der Sicherheitsfunktion erfolgt und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand, beispielsweise unter Berücksichtigung des Nachlaufweges, kürzer ist als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855 und vgl. Abschnitt 6.2.14).
- Der Einsatz der Standardkomponente K1 erfolgt entsprechend den Hinweisen in Abschnitt 6.3.10.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$ des Funktionskanals: Für das Wegeventil 1V3 wird eine $MTTF_D$ von 150 Jahren angenommen [H]. Dies ist gleichzeitig der $MTTF_D$-Wert für den Funktionskanal, der zunächst auf 100 Jahre gekürzt wird.
- $MTTF_D$ des Testkanals: Für das Wegmesssystem 1S3 wird ein $MTTF_D$-Wert von 91 Jahren [H] angenommen. Für die SPS K1 wird ein $MTTF_D$-Wert von 50 Jahren [G] angenommen. Für das Leistungsschütz Q1 gilt ein B_{10D}-Wert von 1300 000 Zyklen [N]. Bei täglichem Einschalten an 240 Arbeitstagen ergibt sich ein $MTTF_D$-Wert für Q1 von 54 166 Jahren. Damit beträgt die $MTTF_D$ des Testkanals 32,3 Jahre. Die $MTTF_D$ des Funktionskanals muss deshalb nach dem zugrunde liegenden Berechnungsmodell auf 64,5 Jahre gekürzt werden.
- DC_{avg}: DC = 60 % für 1V3 gründet sich auf den Vergleich des Weg-/Zeitverhaltens der gefahrbringenden Bewegung in Verbindung mit dem Schaltzustand des Wegeventils. Dies ist gleichzeitig der DC_{avg} („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_D$ (75 Jahre) und niedrigem DC_{avg} (60 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $8{,}7 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

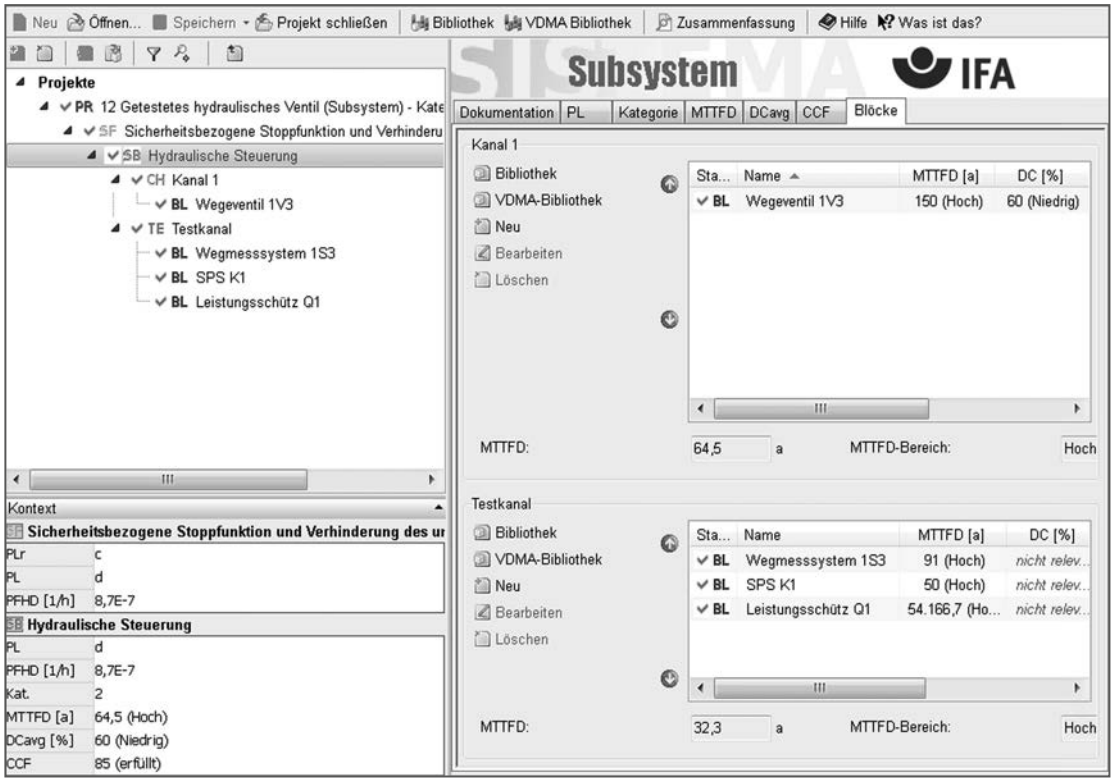


Abbildung 8.24: PL-Bestimmung mithilfe von SISTEMA

8.2.13 Unterlasterkennung für Leuchtenhänger – Kategorie 2 – PL d (Beispiel 13)

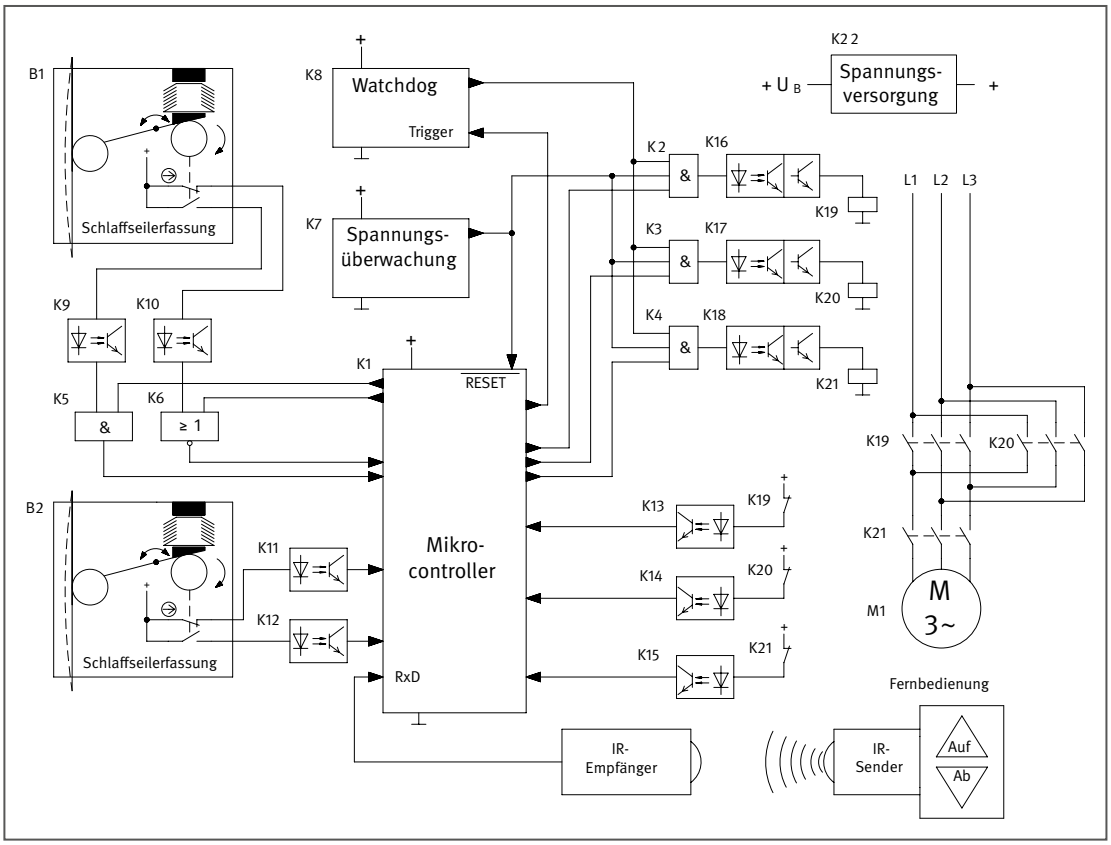


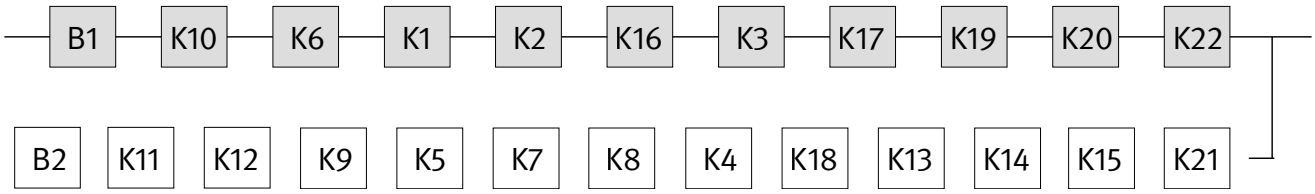
Abbildung 8.25: Kombinierte elektromechanische und programmierbare elektronische Steuerung zur Verhinderung der Unterlast von Leuchtenhängern

Sicherheitsfunktion

- Unterlast- bzw. Schlaffseilerkennung: Bei Erkennung der Unterlast eines Leuchtenhängers (schlaffes Tragmittel/Seil) wird die Abwärtsbewegung gestoppt (STO – sicher abgeschaltetes Moment).

Funktionsbeschreibung

- In der Studio- und Bühnentechnik werden zahlreiche elektromotorisch betriebene Leuchtenhänger eingesetzt. Bei der Abwärtsbewegung besteht die Gefahr, dass Unterlast (d. h. das Tragmittel wird schlaff) durch Verklemmen oder Verkanten der geführten Last oder durch Aufsetzen auf andere Gegenstände auftritt. Hierbei besteht die Gefahr, dass z. B. das Hindernis plötzlich nachgibt, die Last durchschlägt und in der Folge Personen in diesem Bereich gefährdet werden.
- Auf- und Abwärtsbewegungen des Leuchtenhängers können z. B. über eine Infrarot-Fernbedienung gesteuert werden. Diese Funktion wird hier nicht bewertet, sie ist aber immer sicherheitsgerichtet auszuführen.
- Um einen Absturz des Leuchtenhängers durch Reißen eines Tragmittels zu vermeiden, wird die Last von zwei Tragmitteln getragen. An jedem Tragmittel befindet sich ein Schlaffseilschalter B1 bzw. B2 mit einer Öffner-Schließer-Kombination.
- Der Mikrocontroller K1 wertet die Schaltzustände der Schlaffseilschalter B1 und B2 aus. Weiterhin steuert K1 über Logikgatter K2/K3 und optoentkoppelte Transistorverstärker K16/K17 die Hilfsschütze K19 und K20 für die Auf- bzw. Abwärtsbewegung des Leuchtenhängers an.
- Die Schaltzustände der Kontakte der Schlaffseilschalter B1 und B2 werden vom Mikrocontroller K1 ausgewertet und auf Plausibilität geprüft. Zur Testung der verwendeten Eingänge des Mikrocontrollers werden die Signale des Schlaffseilschalters B1 zwangsdynamisiert. Hierzu erzwingt der Mikrocontroller über Logikgatter K5 und K6 einen kurzzeitigen Wechsel der Signale, um festzustellen, ob die Eingänge den Signalwechsel noch übertragen können. Die Zwangsdynamisierung der Signale eines Schlaffseilschalters ist ausreichend.



- Im Mikrocontroller K1 werden Selbsttests der integrierten Einheiten wie Recheneinheit, Arbeits- und Festwertspeicher durchgeführt. Die Spannungsüberwachung K7 überwacht die mit K22 erzeugte Versorgungsspannung. Fehler im Mikrocontroller werden durch eine zeitliche Programmlaufüberwachung im Watchdog K8 erkannt. Die Bauteile K19 bis K21 zur Steuerung der Auf- bzw. Abwärtsbewegung des Leuchtenhängers werden mithilfe einer Rücklesung – entkoppelt durch Optokoppler K13 bis K15 – im Mikrocontroller überwacht. Im Falle eines erkannten Fehlers erfolgt eine übergeordnete Abschaltung über das Hilfsschütz K21 – angesteuert durch Logikgatter K4 und entkoppelt durch Optokoppler K18 – durch das fehlererkennende Bauteil. Wird der Watchdog K8 nicht rechtzeitig vom Mikrocontroller K1 retriggert, erfolgt ausgehend von K8 über alle Logikgatter K2 bis K4 ein Stillsetzen der Bewegung des Leuchtenhängers.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Die Erkennung einer Unterlast erfolgt redundant über beide Tragmittel mithilfe der beiden Schlaffseilschalter B1 und B2. Diese enthalten zwangsöffnende Positionsschalter entsprechend DIN EN 60947-5-1, Anhang K.
- Ein stabiler Aufbau der Betätigungsmechanik der Schlaffseilschalter ist sichergestellt.
- K19 bis K21 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Programmierung der Software (SRESW) von K1 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.

Bemerkungen

- DIN 56950-2 fordert in Abschnitt 5.2.1 zwei Tragmittel, um den Absturz eines Leuchtenhängers und seiner Last zu verhindern.
- In geeigneten Zeitabständen sind Sichtprüfungen bzw. Wartungen der Tragmittel vorzunehmen.
- Die gezeigte Schaltungsstruktur ist in Teilen nicht explizit dazu ausgelegt, mögliche Gefährdungen durch unerwartete Bewegungen des Leuchtenhängers zu verhindern.
- Die verwendete Schaltungsstruktur erreicht für die betrachtete Sicherheitsfunktion – wie die Berechnung der Ausfallwahrscheinlichkeit zeigt – PL d. Die Anwendung des Risikographen zur Bestimmung der erforderlichen Performance Level PL_r mit den Parametern S2, F1 und P1 führt nach DIN 56950-2, Abschnitt A.1.2.3.3, unter der Voraussetzung, dass der Betrieb mit Beaufsichtigung erfolgt und dass die Leuchtenhänger nur von Fachleuten betrieben werden, auf einen PL_r = c. Ist dies nicht der Fall, ist PL_r = d erforderlich.

Berechnung der Ausfallwahrscheinlichkeit

- Zur besseren Übersicht werden in Abbildung 8.25 Bauteile zu Blöcken zusammengefasst. K9 bis K15 enthalten je einen Optokoppler und zwei Widerstände. K16 bis K18 enthalten zusätzlich je einen Transistor zur Ansteuerung der nachfolgenden Hilfsschütze.
- Zur Anwendung des vereinfachten Verfahrens für die Abschätzung des erreichten PL werden die Bauteile der Schaltung wie folgt den Blöcken der vorgesehenen Architektur für Kategorie 2 zugewiesen:
  I: B1
  L: K10, K6, K1, K2, K16, K3, K17, K22
  O: K19, K20
  TE: B2, K11, K12, K9, K5, K7, K8, K4, K18, K13, K14, K15
  OTE: K21
- $MTTF_D$: Die für die Berechnung benötigten $MTTF_D$-Werte stammen vorrangig aus DIN EN ISO 13849-1 [N], SN 29500-2 und SN 29500-14 [D]. Für B1 und B2 werden folgende Kennwerte angesetzt: B_{10D} = 100 000 Zyklen [G], n_{op} = 10 Zyklen/Jahr. Für die Hilfsschütze K19 bis K21 gilt: B_{10D} = 400 000 Zyklen [N], n_{op} = 10 Zyklen/Tag an 365 Arbeitstagen. Für den Mikrocontroller K1 wird eine $MTTF_D$ von 1 142 Jahren [D] angesetzt. Für die elektronischen Bauteile werden folgende $MTTF_D$-Werte angesetzt [D]: 4 566 Jahre für Watchdog K8, 5 707 Jahre für die Optokoppler K9 bis K18, 22 831 Jahre für die Logikgatter K2 bis K6, 38 052 Jahre für die Spannungsüberwachung K7 und 45 662 Jahre für Transistoren bzw. 228 310 Jahre für Widerstände. Für die Spannungserzeugung K22 wird eine $MTTF_D$ von 228 Jahren [G] angenommen. Durch Aufsummierung der Ausfallraten aller Bauteile des funktionalen Kanals (Blöcke I, L und O) ergibt sich eine $MTTF_D$ von 128 Jahren. Diese wird gemäß den Anforderungen der Norm auf 100 Jahre beschnitten („hoch“).

- Die $MTTF_D$ des Testkanals ergibt sich durch Aufsummierung der Ausfallraten aller Bauteile der Blöcke TE und OTE. Sie beträgt 389 Jahre und ist damit größer oder gleich der Hälfte der $MTTF_D$ des funktionalen Kanals.
- DC_{avg}: DC = 60 % für B1, K10 und K6 durch Kreuzvergleich von B1 und B2 in K1 mit geringer Anforderungsrate der Sicherheitsfunktion. DC = 60 % für K1 durch zeitliche Programmlaufüberwachung und Selbsttests einfacher Wirksamkeit. DC = 99 % für K2, K3, K16, K17, K19 und K20 durch direkte Überwachung über zwangsgeführte Kontakte. Für K22 ist DC = 99 %. Die Mittelungsformel für DC_{avg} ergibt 93 % („mittel“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_D$ des Funktionskanals (100 Jahre) und mittlerem DC_{avg} (93 %). Damit ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls PFH_D von $2{,}3 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN 56950-2: Veranstaltungstechnik – Maschinentechnische Einrichtungen – Teil 2: Sicherheitstechnische Anforderungen an bewegliche Leuchtenhänger (09.14). Beuth, Berlin 2014
- DGUV Information 215-310: Sicherheit bei Veranstaltungen und Produktionen – Leitfaden für Theater, Film, Hörfunk, Fernsehen, Konzerte, Shows, Events, Messen und Ausstellungen (bisher BGI 810). Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2016. ▸ http://publikationen.dguv.de/dguv/pdf/10002/215-310.pdf
- SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Hrsg.: Siemens AG, Corporate Technology, Technology & Innovation Management, München 2004-2014

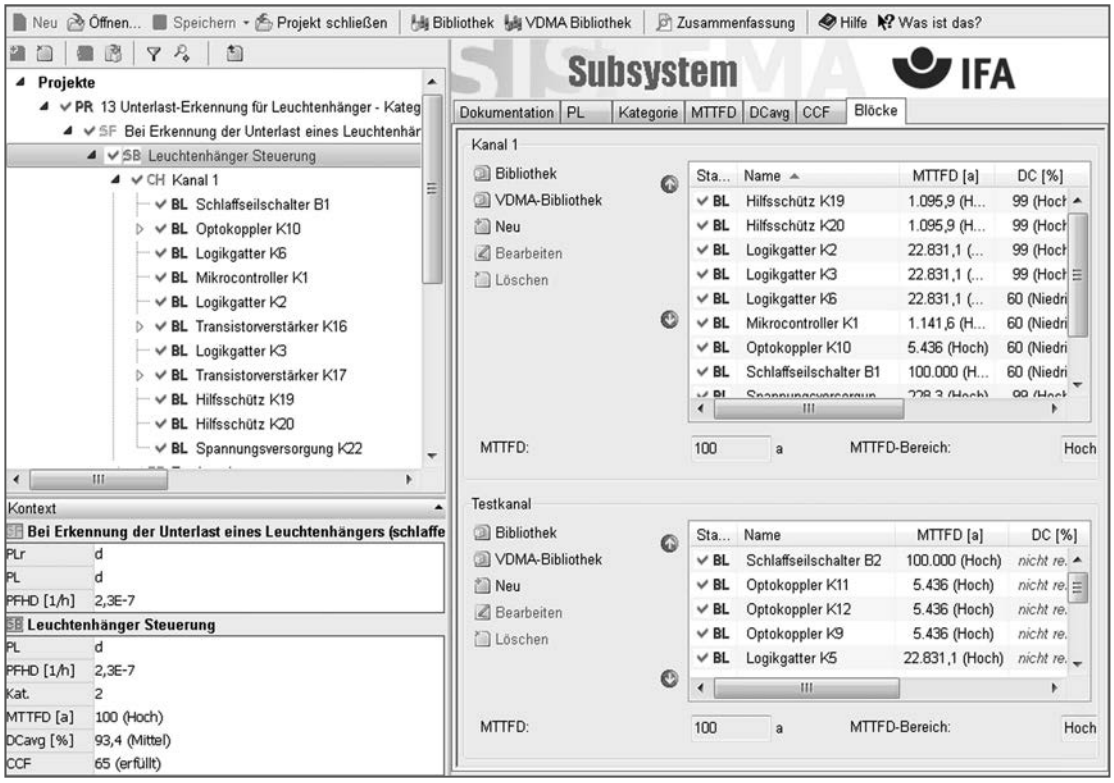


Abbildung 8.26: PL-Bestimmung mithilfe von SISTEMA

8.2.14 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 3 – PL d (Beispiel 14)

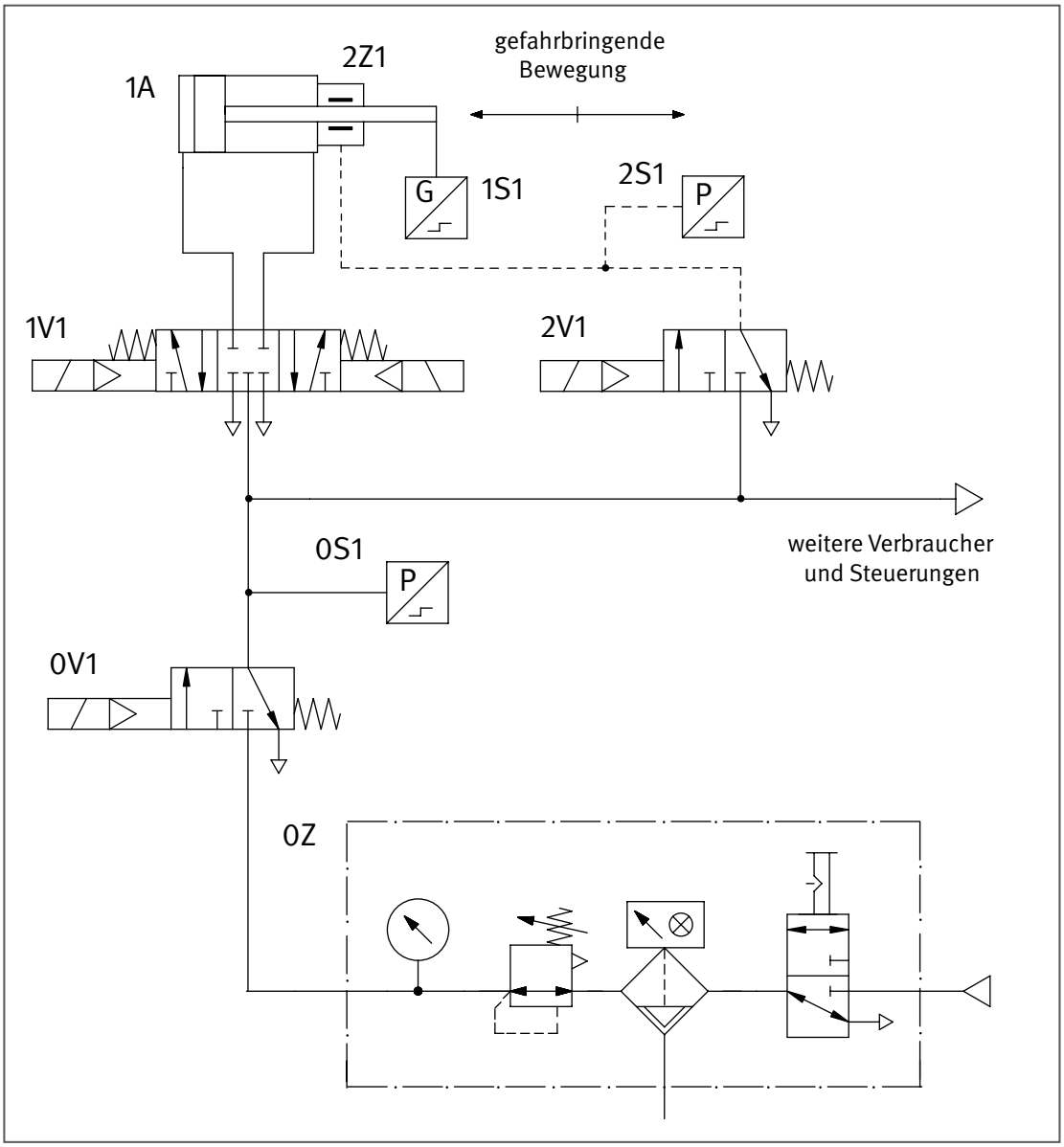
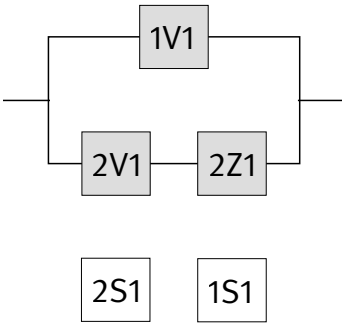


Abbildung 8.27: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage, realisiert durch SSC und SBC
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.



Funktionsbeschreibung

- Gefahrbringende Bewegungen werden redundant durch ein Wegeventil 1V1 und eine Bremse 2Z1 an der Kolbenstange gesteuert bzw. stillgesetzt. Die Bremse 2Z1 wird durch ein Steuerventil 2V1 angesteuert.
- Der einzelne Ausfall eines der genannten Ventile oder der Bremse führt nicht zum Verlust der Sicherheitsfunktion.
- Wegeventil und Bremse werden im Prozess zyklisch angesteuert.
- Die Funktion des Steuerventils 2V1 wird durch einen Druckschalter 2S1 überwacht. An dem nicht überwachten Wegeventil 1V1 und der nicht überwachten Bremse 2Z1 werden einige Fehler im Arbeitsprozess erkannt. Zusätzlich wird der Nachlaufweg (Weg-/Zeitverhalten) beim Bremsvorgang (dynamisch) oder/und bei Start der Maschine (statisch) mithilfe eines Wegmesssystems 1S1 an der Kolbenstange überwacht. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.
- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion in geeigneten Zeitabständen, z. B. mindestens alle acht Arbeitsstunden.
- Durch den Ausfall der Bremse darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zum Ausfall der Bremse führen.
- Kann durch eingesperrte Druckluft eine weitere Gefährdung auftreten, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Das Wegeventil 1V1 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung der Drucküberwachung 2S1 und des Wegmesssystems 1S1 erfolgt z. B. in der vorgeschalteten elektrischen Logik (nicht dargestellt).

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für die Ventile 1V1 und 2V1 werden B_{10D}-Werte von 20 000 000 Zyklen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 15 Sekunden Zykluszeit ist n_{op} = 921 600 Zyklen/Jahr. Für 1V1 und 2V1 ergibt sich damit eine $MTTF_D$ = 217 Jahre. Für die mechanische Bremse an der Kolbenstange 2Z1 wird ein B_{10D}-Wert von 5 000 000 Schaltspielen [H] eingesetzt. Das ergibt für die mechanische Bremse $MTTF_D$ = 54 Jahre. Insgesamt ergibt sich ein symmetrisierter $MTTF_D$-Wert pro Kanal von 75 Jahren („hoch“).
- DC_{avg}: DC = 99 % für das Steuerventil 2V1 ergibt sich aus der Drucküberwachung des Steuersignals für die Bremse. DC = 60 % für das Wegeventil 1V1 aus der Fehlererkennung über den Prozess. DC = 75 % für 2Z1 folgt aus einer Anlauftestung der mechanischen Bremse. Durch Mittelung ergibt sich damit ein DC_{avg} von 76,5 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (75 Jahre) und niedrigem DC_{avg} (76,5 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.
- Die verschleißbehaftete Bremse 2Z1 sollte nach jeweils ca. fünf Jahren (T_{10D}) ausgetauscht werden.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (08.16). Beuth, Berlin 2016

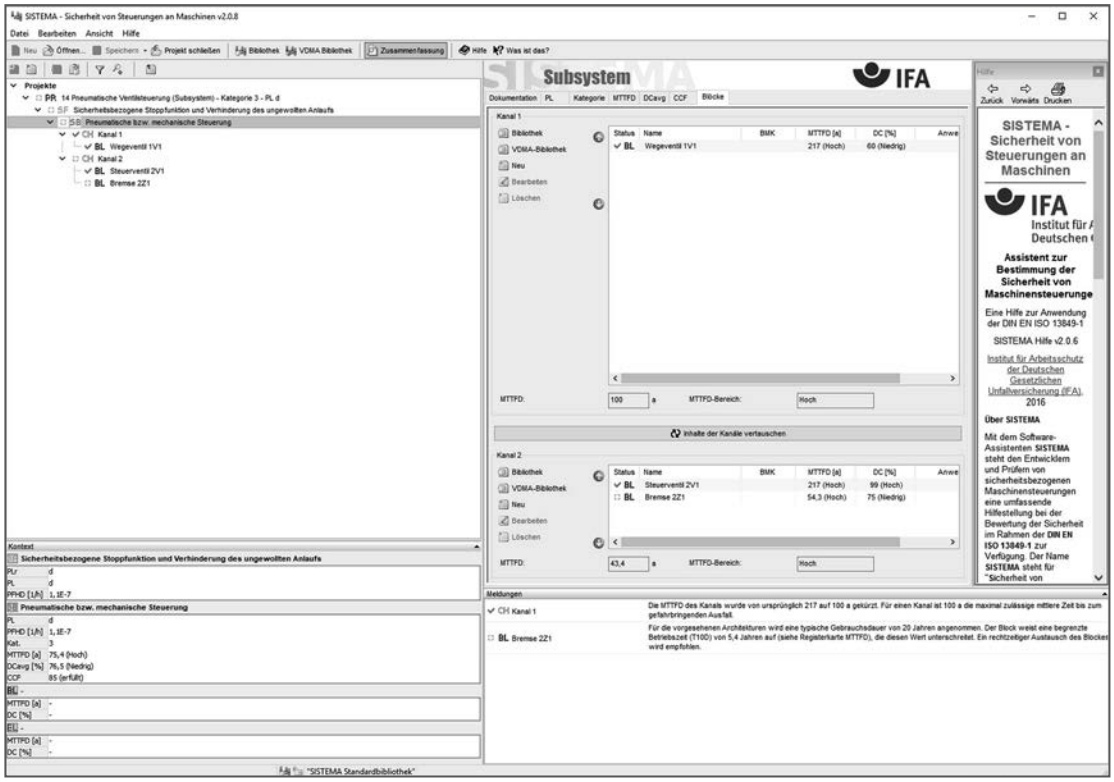


Abbildung 8.28: PL-Bestimmung mithilfe von SISTEMA

8.2.15 Schutzeinrichtung und SPS-gesteuerte Hydraulik – Kategorie 3 – PL d (Beispiel 15)

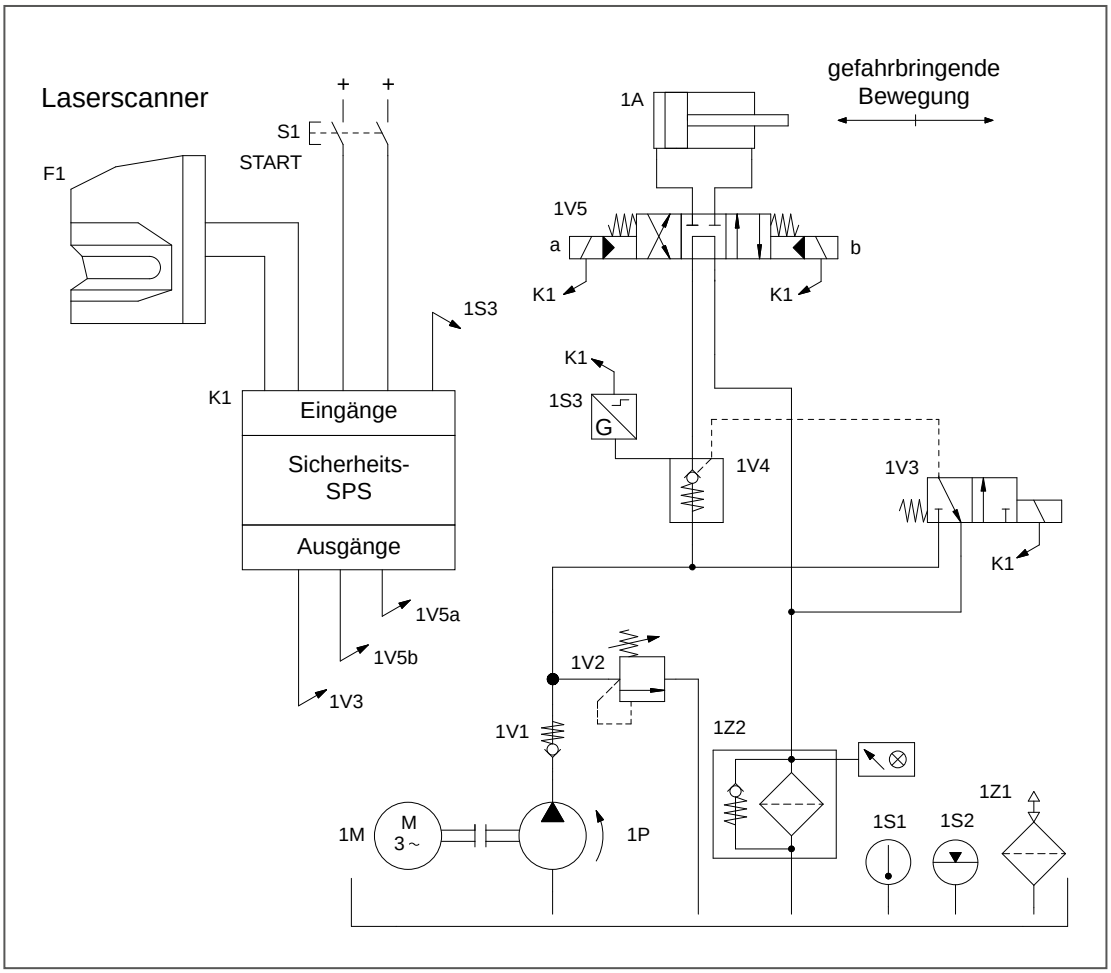


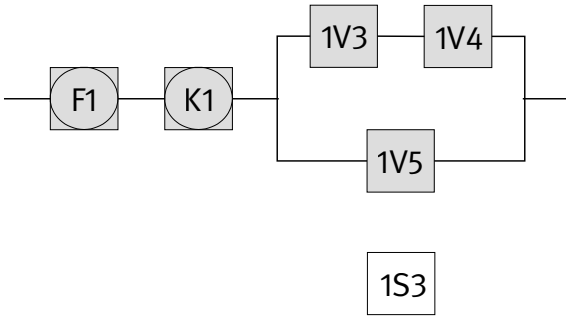
Abbildung 8.29: Schutzfeld-Überwachung durch Laserscanner mit elektrohydraulischer Abschaltung der gefahrbringenden Bewegung

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Ein Eindringen in das Schutzfeld des Laserscanners führt zu einem Stillsetzen der gefahrbringenden Bewegung.

Funktionsbeschreibung

- Der Laserscanner F1 überwacht mit seinem Schutzfeld den Bereich, in dem die Bewegung des Zylinders 1A für die Bedienperson gefährlich werden kann. Das Ausgangssignal des Laserscanners wird zweikanalig in die Sicherheits-SPS K1 eingelesen. Nach jeder Schutzfeldverletzung muss eine erneute Bewegung durch die Betätigung eines in K1 ausgewerteten Start-Tasters S1 freigegeben werden (Wiederanlaufsperre). K1 steuert mithilfe des hydraulischen Steuerungsteils die Bewegung von 1A.
- Der hydraulische Steuerungsteil ist zweikanalig aufgebaut. Der erste Kanal besteht aus dem Wegeventil 1V3, das auf das entsperrbare Rückschlagventil 1V4 wirkt. In gesperrter Stellung blockiert 1V4 Bewegungen von 1A. Der zweite Kanal besteht aus dem Richtungsventil 1V5, das in Sperr-Mittelstellung ebenfalls eine Bewegung von 1A verhindert.
- 1V5 wird zyklisch im Prozess angesteuert, 1V3 und 1V4 schließen nur bei einer Verletzung des Schutzfeldes (Anforderung der Sicherheitsfunktion), jedoch mindestens einmal pro Schicht.
- Als Maßnahme zur Fehlererkennung ist an 1V4 eine direkte Stellungsüberwachung 1S3 vorgesehen, die in K1 ausgewertet wird. Fehler in 1V5 können funktionsbedingt über den Prozess erkannt werden. Die Anhäufung unentdeckter Fehler im hydraulischen Steuerungsteil kann zum Verlust der Sicherheitsfunktion führen.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Fehler in den Anschlussleitungen von F1 und K1 dürfen sich nicht gefährlich auswirken. Hierzu werden auftretende Fehler erkannt und der sichere Zustand eingeleitet. Alternativ muss ein Fehlerausschluss für Leitungskurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4, möglich sein.
- Bei dem Laserscanner F1 und der Sicherheits-SPS K1 handelt es sich um geprüfte Sicherheitsbauteile für den Einsatz in PL d, die der Kategorie 3 und den jeweiligen Produktnormen entsprechen.
- Das Wegeventil 1V5 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung. 1V4 ist mit elektrischer Stellungsüberwachung ausgeführt, da 1V4 nicht zyklisch geschaltet wird.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.
- Es wird davon ausgegangen, dass die Ausgänge der Sicherheits-SPS jeweils von beiden Verarbeitungskanälen der SPS angesteuert werden. Sollte dies nicht der Fall sein, werden die Ausgänge, die 1V3 und 1V4 ansteuern, von einem Kanal und der Ausgang, der 1V5 ansteuert, von dem anderen Kanal der SPS angesteuert.

Berechnung der Ausfallwahrscheinlichkeit

- Da der Laserscanner F1 und die Sicherheits-SPS K1 als käufliche Sicherheitsbauteile vorliegen, werden deren Ausfallwahrscheinlichkeiten am Ende der Berechnung addiert (F1: $PFH_D = 8{,}0 \cdot 10^{-8}$/Stunde [H], K1: $PFH_D = 2{,}5 \cdot 10^{-9}$/Stunde [H]). Für den hydraulischen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_D$: Für die Ventile 1V3 bis 1V5 werden Werte von 150 Jahren [H] angenommen. Damit ergibt sich insgesamt ein symmetrisierter $MTTF_D$-Wert von 88 Jahren („hoch“) für die beiden Kanäle.
- DC_{avg}: DC = 99 % für 1V4 ergibt sich durch die direkte Überwachung in K1 mithilfe der Stellungsüberwachung 1S3. Wegen der engen Kopplung von 1V3 und 1V4 wird 1V3 dadurch mit einem DC von 99 % indirekt mit überwacht. DC = 60 % für 1V5 gründet sich auf die Fehlererkennung im Prozess bei zyklischer Ansteuerung. Durch Mittelung ergibt sich damit ein DC_{avg} von 86 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (90 Punkte): Trennung (15), Diversität (20), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente im hydraulischen Teil entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (88 Jahre) und niedrigem DC_{avg} (86 %). Damit ergibt sich für die Hydraulik eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}2 \cdot 10^{-8}$/Stunde.
- Insgesamt beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $PFH_D = (8{,}0 + 0{,}25 + 6{,}2) \cdot 10^{-8}$/Stunde = $1{,}4 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- *Bömer, T.:* Hinweise zum praktischen Einsatz von Laserscannern (Kennzahl 310 243). In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2. Aufl. 36. Lfg. XII/99. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin. Erich Schmidt, Berlin 2003 – Losebl.-Ausg. ▶ www.ifa-handbuchdigital.de/310243

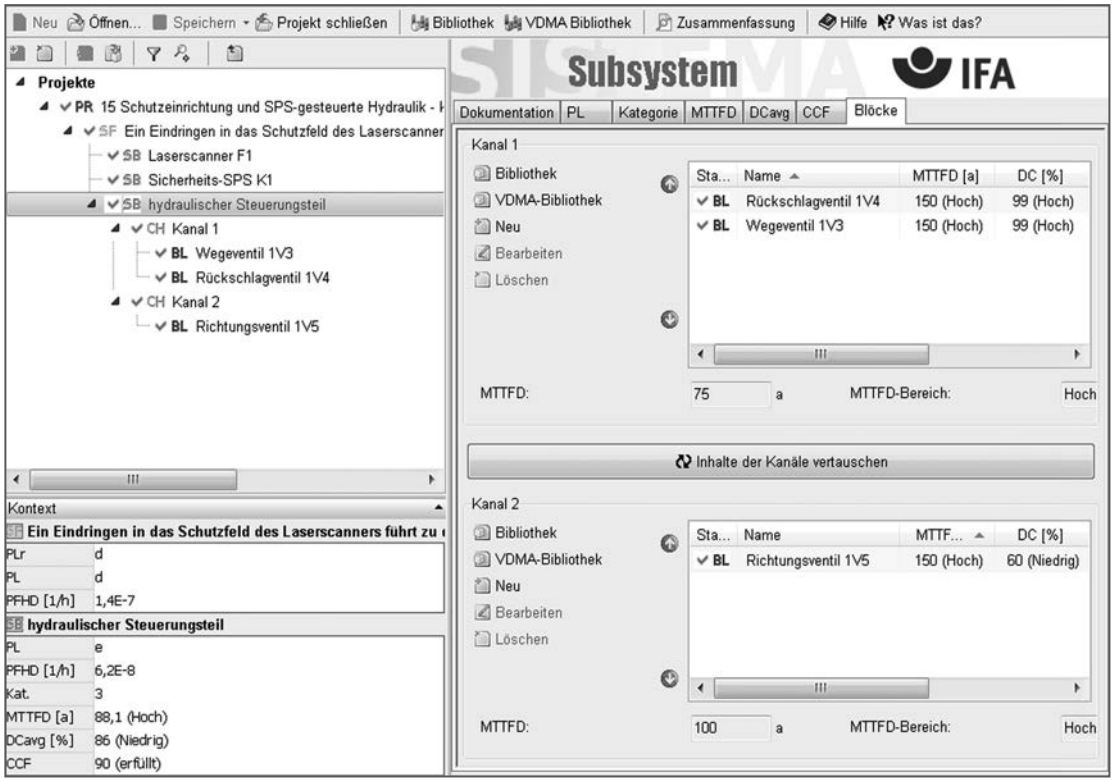


Abbildung 8.30: PL-Bestimmung mithilfe von SISTEMA

8.2.16 Erdbaumaschinensteuerung mit Bussystem – Kategorie 2 bzw. 3 – PL d (Beispiel 16)

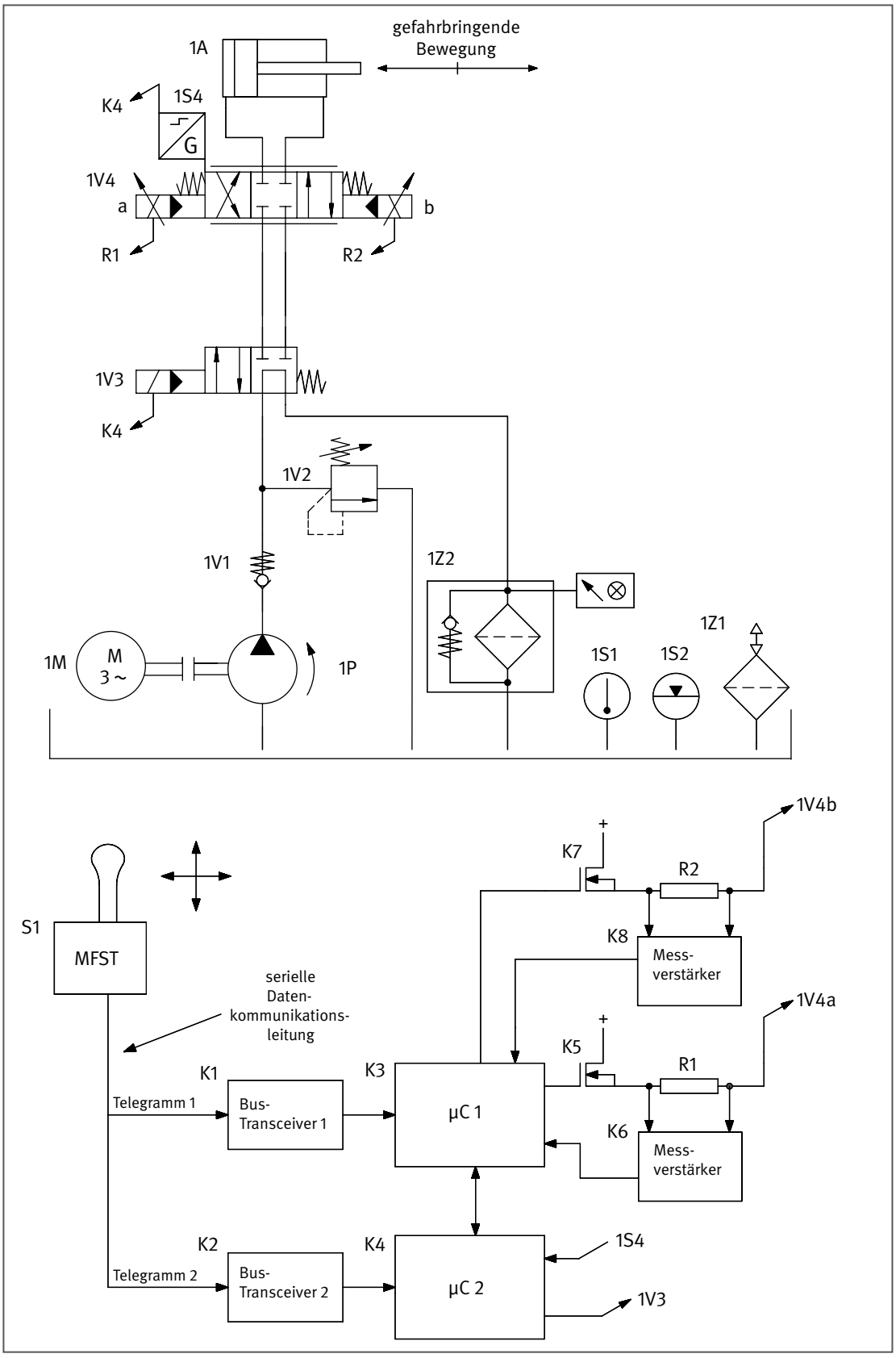
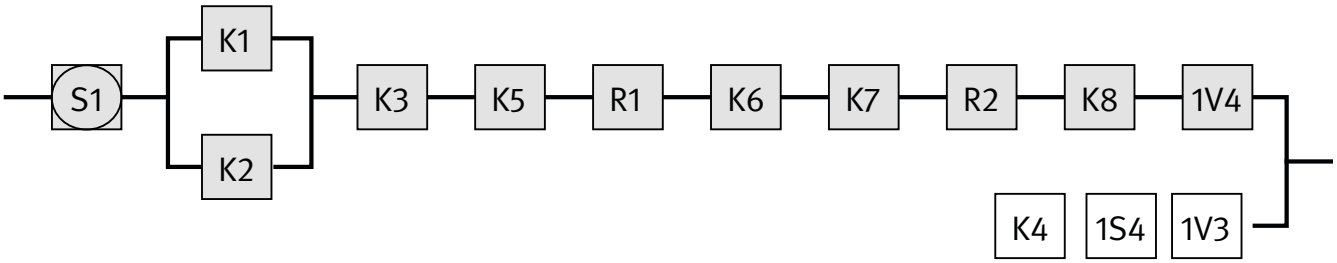


Abbildung 8.31: Ansteuerung von gefahrbringenden Bewegungen einer Erdbaumaschine



Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage der Arbeitsgeräte von Erdbaumaschinen
- Weitere sicherheitsrelevante Funktionen wie z. B. Verhinderung der Anwahl einer fehlerhaften Bewegungsrichtung der Arbeitsgeräte der Erdbaumaschine sind in diesem Beispiel nicht betrachtet.

Funktionsbeschreibung

- Das Multifunktionsstellteil (MFST) S1 wandelt die vom Bediener ausgeführte manuelle Auslenkung des MFST in elektronische Datentelegramme um. Es sendet diese Telegramme zyklisch über eine serielle Datenkommunikationsleitung (Bussystem) zur Logiksteuerung, die Ansteuersignale für die Hydraulik zur Ausführung der von der Bedienperson vorgesehenen Arbeitsbewegung der Erdbaumaschine erzeugt.
- Das vom MFST S1 gesendete Telegramm 1 gelangt über den Bus-Transceiver K1 in den Mikrocontroller K3. Dieser erzeugt aus Telegramm 1 gemäß den in der Software abgelegten Algorithmen die erforderlichen analogen Signale zur Ansteuerung des Proportionalventils 1V4. Die Widerstände R1/R2 und die Messverstärker K6/K8 dienen zur Regelung der Ausgangsströme für das Proportionalventil. Der Mikrocontroller K4 erhält ein redundantes Telegramm 2 von S1 über den Bus-Transceiver K2. K4 überprüft die korrekte Auslenkung des Proportionalventils 1V4 über das in 1V4 integrierte Wegmesssystem 1S4 innerhalb der Reaktionszeit bzw. Prozesssicherheitszeit auf Plausibilität gegen die aus Telegramm 2 ermittelte Sollstellung. Bei erkannten Fehlern schaltet K4 übergeordnet über das Wegeventil 1V3 den hydraulischen Druck ab und bringt das System in den sicheren Zustand.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Bei dem MFST handelt es sich um ein für den Einsatz in PL d geeignetes Sicherheitsbauteil, das der Kategorie 3 entspricht.
- Gemäß der Funktionsbeschreibung erfolgen die Verarbeitung der Steuerinformationen und die Ansteuerung der Ventile in einer Kategorie-2-Struktur. Dabei bilden K4 und 1S4 den Testkanal mit 1V3 als Abschaltelement des Testkanals.
- Aufgrund der kontinuierlichen Überwachung von 1V4 durch K4 über 1S4 kann ein Ausfall von 1V4 erkannt werden, sobald die Sicherheitsfunktion angefordert wird. 1V3 muss innerhalb der Reaktionszeit die sicherheitsgerichtete Reaktion ausführen, damit die Struktur der Steuerung der Kategorie 2 entspricht. Ein abruptes übergeordnetes Schalten von 1V3 darf nicht zu Gefährdungen führen.
- Das Proportionalventil 1V4 und das Wegeventil 1V3 haben eine Sperrstellung bzw. Sperr-Mittelstellung, Federrückstellung bzw. Federzentrierung und eine ausreichend positive Überdeckung.
- Die Programmierung der Software (SRESW) von K3 und K4 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.
- Die Datenübertragung vom MFST zur Logiksteuerung ist nach GS-ET-26 bzw. DIN EN 61784-3 abgesichert. Das verwendete Datenkommunikationsprotokoll enthält redundante Telegramme mit Vergleich zwischen K3 und K4 und Maßnahmen, um folgende Übertragungsfehler zu erkennen: Wiederholung, Verlust, Einfügung, falsche Abfolge, Verfälschung, Verzögerung und Maskerade (siehe auch Abschnitt 6.2.18). Die Restfehlerrate Λ ist geringer als $1 \cdot 10^{-8}$/Stunde und trägt damit wie von den Beurteilungsgrundlagen vorgesehen weniger als 1% zur maximal zulässigen Ausfallwahrscheinlichkeit der Sicherheitsfunktion bei. Die Modellierung erfolgt in Kategorie 4, der sich ergebende Anteil in der Berechnung der Gesamtausfallwahrscheinlichkeit ist vernachlässigbar.

Bemerkung

- Eine eventuell erforderliche Notlauffunktion der Erdbaumaschine ist hier nicht dargestellt und übergeordnet zu realisieren.

Berechnung der Ausfallwahrscheinlichkeit

- Das MFST S1 liegt als handelsübliches Sicherheitsbauteil vor. Die zugehörige Ausfallwahrscheinlichkeit wird am Ende der Berechnung addiert ($PFH_D = 3{,}0 \cdot 10^{-7}$/Stunde [G]). Für den übrigen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_D$ der Datenkommunikation: Für die Bus-Transceiver K1 und K2 wird eine $MTTF_D$ von 11416 Jahren [D] angesetzt. Diese wird in Kategorie 4 auf den Maximalwert von 2500 Jahren begrenzt.
- DC_{avg} der Datenkommunikation: $DC = 99\,\%$ für K1 und K2 durch Kreuzvergleich der Telegramme in den Mikrokontrollern K3 und K4.
- Die Ausfallwahrscheinlichkeit der Datenkommunikation ergibt sich zu $PFH_D = 9{,}1 \cdot 10^{-10}$/Stunde.
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10). Diese Betrachtung gilt auch für die nachfolgenden Steuerungsteile.
- $MTTF_D$ des Funktionskanals der Logik- und Hydrauliksteuerung: Für den Mikrocontroller K3 einschließlich seiner Peripherie wird nach SN 29500-2 eine $MTTF_D$ von 878 Jahren [D] berücksichtigt. Für die weiteren elektrischen Bauteile werden folgende Kenndaten angesetzt [D]: 45662 Jahre für die Schalttransistoren K5 und K7, 228311 Jahre für die Widerstände R1 und R2 und 1142 Jahre für die Messverstärker K6 und K8. Für das Proportionalventil 1V4 wird eine $MTTF_D$ von 150 Jahren [N] angenommen. Damit beträgt der $MTTF_D$-Wert des Funktionskanals 104 Jahre.
- $MTTF_D$ des Testkanals der Logik- und Hydrauliksteuerung: Für den Mikrocontroller K4 einschließlich seiner Peripherie wird nach SN 29500-2 eine $MTTF_D$ von 878 Jahren [D] berücksichtigt. Für das Wegmesssystem 1S4 wird eine $MTTF_D$ von 75 Jahren [G] angenommen. Für das Wegeventil 1V3 wird eine $MTTF_D$ von 150 Jahren [N] angenommen. Damit beträgt der $MTTF_D$-Wert des Testkanals 47 Jahre. Für das in der Norm beschriebene vereinfachte Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL ist eine Bedingung, dass die $MTTF_D$ des Testkanals größer als die Hälfte der $MTTF_D$ des Funktionskanals ist. Daher wird der $MTTF_D$-Wert des Funktionskanals auf 94 Jahre reduziert.
- DC_{avg} des Funktionskanals der Logik- und Hydrauliksteuerung: $DC = 60\,\%$ für K3 durch Kreuzvergleich mit K4 und Selbsttests einfacher Wirksamkeit durch Software; $DC = 90\,\%$ für die restlichen elektrischen Bauteile durch Fehlererkennung in K4 mittels Wegmesssystem 1S4. $DC = 99\,\%$ für 1V4 durch direkte Überwachung des Weges über 1S4 in K4. Die Mittelungsformel für DC_{avg} ergibt 93 % („mittel“).
- Die Logik- und Hydrauliksteuerung entspricht Kategorie 2 mit hoher $MTTF_D$ pro Kanal (94 Jahre) und mittlerem DC_{avg} (93 %). Damit ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls von $PFH_D = 2{,}5 \cdot 10^{-7}$/Stunde.
- Die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion ergibt sich durch Addition der Anteile des MFST, der Datenkommunikation sowie der Logik- und Hydrauliksteuerung und beträgt $PFH_D = 5{,}5 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- ISO 15998: Erdbaumaschinen – Maschinensteuerungssysteme (MSS) auf der Basis von elektronischen Bauteilen – Anforderungen und Prüfungen (04.08). Beuth, Berlin 2008
- DIN EN 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (02.11). Beuth, Berlin 2011
- Grundsätze für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“ (GS-ET-26) (03.14). Hrsg.: Fachbereich Energie Textil Elektro Medienerzeugnisse, Köln 2014
  ▶ www.dguv.de, Webcode: d14884
- SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Hrsg.: Siemens AG, Corporate Technology, Technology & Innovation Management, München 2004-2014

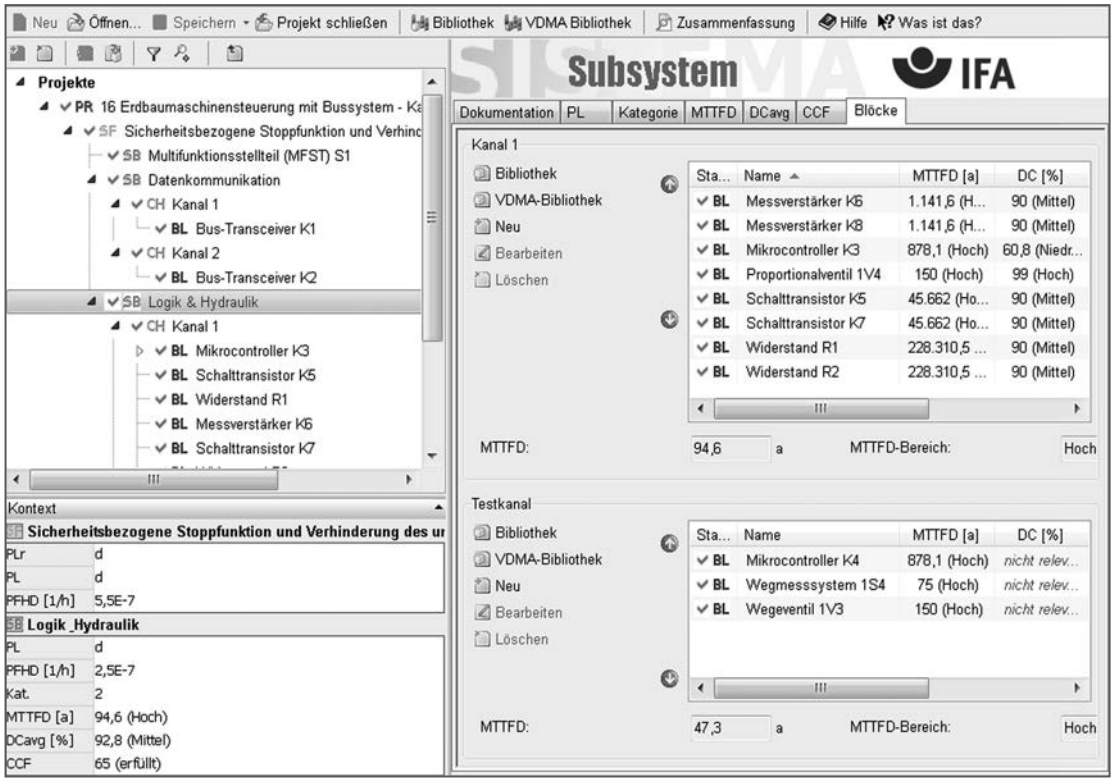


Abbildung 8.32:
PL-Bestimmung mithilfe von SISTEMA

8.2.17 Kaskadierung von Schutzeinrichtungen mittels Sicherheitsschaltgeräten – Kategorie 3 – PL d (Beispiel 17)

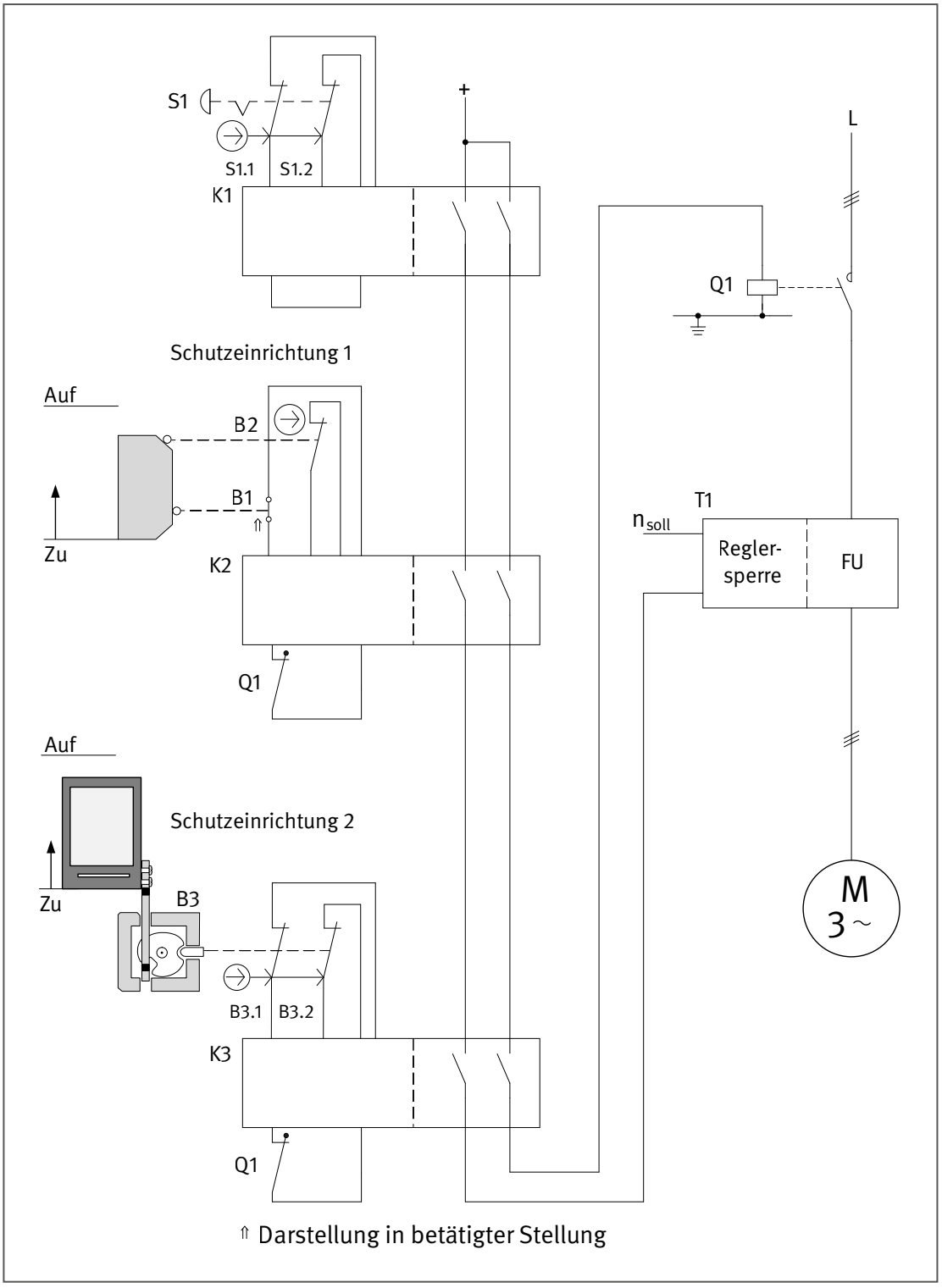
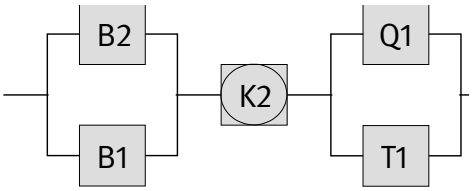


Abbildung 8.33: Kaskadierung von Schutzeinrichtungen mittels Sicherheitsschaltgeräten (Not-Halt-Funktion, STO)



Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein:
  Schutzeinrichtung 1 mit Positionsschaltern Bauart 1 (Beladen)
  Schutzeinrichtung 2 mit Positionsschalter Bauart 2 (Entnahme)
- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Gerätes S1 mit zwei zwangsöffnenden Kontakten über das Sicherheitsschaltgerät K1 redundant durch Unterbrechung der Steuerspannung von Schütz Q1 und Anwahl der Reglersperre des Frequenzumrichters T1 abgeschaltet.
- Zusätzlich erfolgt die Sicherung einer Gefahrenstelle mit zwei beweglichen trennenden Schutzeinrichtungen (z. B. jeweils für Beladung und Entnahme). Das Öffnen der Schutzeinrichtung 1 wird durch zwei Positionsschalter B1/B2 in Öffner-Schließer-Kombination erfasst und in einem Sicherheitsschaltgerät K2 ausgewertet. Dieses kann in gleicher Weise wie K1 gefahrbringende Bewegungen oder Zustände unterbrechen bzw. verhindern. Die Überwachung der Schutzeinrichtung 2 erfolgt durch einen Positionsschalter der Bauart 2 mit den Kontakten B3.1 und B3.2 und einem Sicherheitsschaltgerät K3, der ebenfalls auf Q1 und T1 wirkt.
- Bei Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten.
- Die meisten Bauteilausfälle werden erkannt und führen zur Betriebshemmung. Die Positionsschalter B1 und B2 an Schutzeinrichtung 1 werden im zugehörigen Sicherheitsschaltgerät, das auch über interne Diagnosemaßnahmen verfügt, auf Plausibilität überwacht.
- Die elektrischen Kontakte B3.1 und B3.2 werden im zugehörigen Sicherheitsschaltgerät K3, das ebenfalls über interne Diagnosemaßnahmen verfügt, auf Plausibilität überwacht.
- Fehler im Schütz Q1 werden über Spiegelkontakte und deren Rücklesung in K2 und K3 erkannt. Eine zusätzliche Rücklesung in K1 ist nicht erforderlich, da die Not-Halt-Funktion viel seltener angefordert wird. Ein Teil der Fehler in T1 wird durch den Prozess erkannt. Einige wenige Fehler werden von der Steuerung nicht erkannt.
- Durch organisatorische Maßnahmen wird sichergestellt, dass das Not-Halt-Gerät mindestens einmal pro Jahr betätigt wird.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtungen zur Betätigung der Positionsschalter ist sichergestellt.
- Das Not-Halt-Gerät S1 mit den zwangsöffnenden Kontakten S1.1 und S1.2 entspricht DIN EN ISO 13850.
- Die Kontakte der Positionsschalter B2 und B3 sind zwangsöffnend entsprechend DIN EN 60947-4-1, Anhang F.
- Die Zuleitungen zu den Positionsschaltern B1, B2 und B3 sind getrennt oder geschützt verlegt.
- Das Schütz Q1 besitzt Spiegelkontakte entsprechend DIN EN 60947-5-1, Anhang L.
- Die Sicherheitsschaltgeräte K1, K2 und K3 erfüllen alle Anforderungen für Kategorie 4 und PL e.
- Der Frequenzumrichter T1 verfügt über keine integrierte Sicherheitsfunktion.

Bemerkungen

- Die Not-Halt-Funktion ist eine ergänzende Schutzmaßnahme nach DIN EN ISO 12100 2011.

Berechnung der Ausfallwahrscheinlichkeit

- Die drei Sicherheitsfunktionen lassen sich in jeweils drei Subsystemen darstellen. Das sicherheitsbezogene Blockdiagramm zeigt die sicherheitsbezogene Stoppfunktion beispielhaft für eine der Schutzeinrichtungen, da zu einem Zeitpunkt immer nur eine Schutzeinrichtung geöffnet wird. Für die zweite Schutzeinrichtung gilt eine vergleichbare Sicherheitsfunktion mit nahezu identischer Berechnung der Ausfallwahrscheinlichkeit. Es ist für den Betätiger des Positionsschalters B3 ein Fehlerausschluss für das Brechen zu begründen.
  Für die Subsysteme wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- Bei S1 handelt es sich um ein handelsübliches Not-Halt-Gerät nach DIN EN ISO 13850. Es kann für Not-Halt-Geräte, unabhängig von der Last, ein B_{10D}-Wert von 100 000 Schaltspielen für jeden Kontakt angesetzt werden [N]. Für n_{op} wird von drei Betätigungen im Jahr ausgegangen. Hinsichtlich der Gesamtschaltungen von Q1 durch die Betätigung der Schutzeinrichtungen wird dieser Wert bei der weiteren Berechnung für beide Sicherheitsfunktionen nicht in Ansatz gebracht.
- $MTTF_D$ (Schutzeinrichtung 1, Beladen): Bei dem Schalter B1 handelt es sich um einen Positionsschalter mit Schließerkontakt. Der B_{10D} beträgt $1 \cdot 10^5$ Schaltspiele [H]. Für den zwangsöffnenden Positionsschalter B2 mit Rollenbetätigung beträgt der $B_{10D} = 20 \cdot 10^6$ Schaltspiele [H]. Bei 220 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 21120 Zyklen/Jahr und $MTTF_D$ beträgt 47,3 Jahre für B1 und 9 469 Jahre für B2.
  Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Da Q1 an beiden sicherheitsbezogenen Stoppfunktionen beteiligt ist, folgt mit dem Doppelten des oben angenommenen Wertes für n_{op} eine $MTTF_D$ von 473 Jahren. Für den Frequenzumrichter T1 beträgt die $MTTF_D$ 20 Jahre [H]. Insgesamt ergibt sich im Subsystem Q1/T1 ein symmetrisierter $MTTF_D$-Wert pro Kanal von 68,9 Jahren („hoch“). Der Positionsschalter B1 weist eine begrenzte Betriebszeit von 4,7 Jahren auf. Ein rechtzeitiger Austausch wird empfohlen.
- $MTTF_D$ (Schutzeinrichtung 2, Entnahme): Für den Positionsschalter B3 mit getrenntem Betätiger und den zwangsöffnenden Kontakten B3.1 und B3.2 ist für jeden Kontakt jeweils ein B_{10D}-Wert von 4 000 000 Zyklen [H] angegeben. Bei 220 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 21120 Zyklen/Jahr und $MTTF_D$ beträgt 1893 Jahre. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringender Ausfälle ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Da das Schütz Q1 an beiden sicherheitsbezogenen Stoppfunktionen (Beladen und Entnahme) beteiligt ist, folgt mit dem Doppelten des angenommenen Wertes für n_{op} eine $MTTF_D$ von 473 Jahren. Für den Frequenzumrichter T1 beträgt die $MTTF_D$ 20 Jahre [H]. Insgesamt ergibt sich im Subsystem Q1/T1 ein symmetrisierter $MTTF_D$-Wert pro Kanal von 68 Jahren („hoch“).
- DC_{avg}: DC = 99 % für B1 und B2 bzw. B3 beruht auf der Plausibilitätsüberwachung in K2 bzw. K3. Dies entspricht dem DC_{avg} für das Subsystem. DC = 99 % für das Schütz Q1 ergibt sich aus der Rücklesung der Kontaktstellung in den Sicherheitsschaltgeräten. Für den Frequenzumrichter T1 folgt DC = 60 % aus der Fehlererkennung durch den Prozess. Durch Mittelung ergibt sich damit für das Subsystem Q1/T1 ein DC_{avg} von 62 % („niedrig“). Eine ausreichende Testhäufigkeit des Not-Halt-Gerätes ist gewährleistet (siehe Hinweise in den Abschnitten 6.2.14 und D.2.5.1).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Subsystemen S1.1/S1.2, B2/B1, B3.1/B3.2 bzw. Q1/T2 (65, 70 bzw. 85 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10), in B2/B1 bewährte Bauteile (5), in Q1/T1 Diversität (20)
- Die Subsysteme B1/B2 und B3.1/B3.2 entsprechen Kategorie 4 mit hoher $MTTF_D$ und hohem DC_{avg} (99 %). Damit ergibt sich jeweils eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $3{,}3 \cdot 10^{-8}$/Stunde und $2{,}5 \cdot 10^{-8}$/Stunde. Das Subsystem Q1/T1 entspricht Kategorie 3 mit hoher $MTTF_D$ (68,9 Jahre) und niedrigem DC_{avg} (62 %). Damit ergibt sich für die SF „Stellungsüberwachung verriegelter trennender Schutzeinrichtungen (Schutzeinrichtung 1, Beladen)“ eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}8 \cdot 10^{-7}$/Stunde.
- Für die Sicherheitsfunktion „Stellungsüberwachung verriegelter trennender Schutzeinrichtungen (Schutzeinrichtung 2, Entnahme)“ ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}1 \cdot 10^{-7}$/Stunde. Dies entspricht in beiden Fällen PL d.
- Für die Not-Halt-Funktion ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}0 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

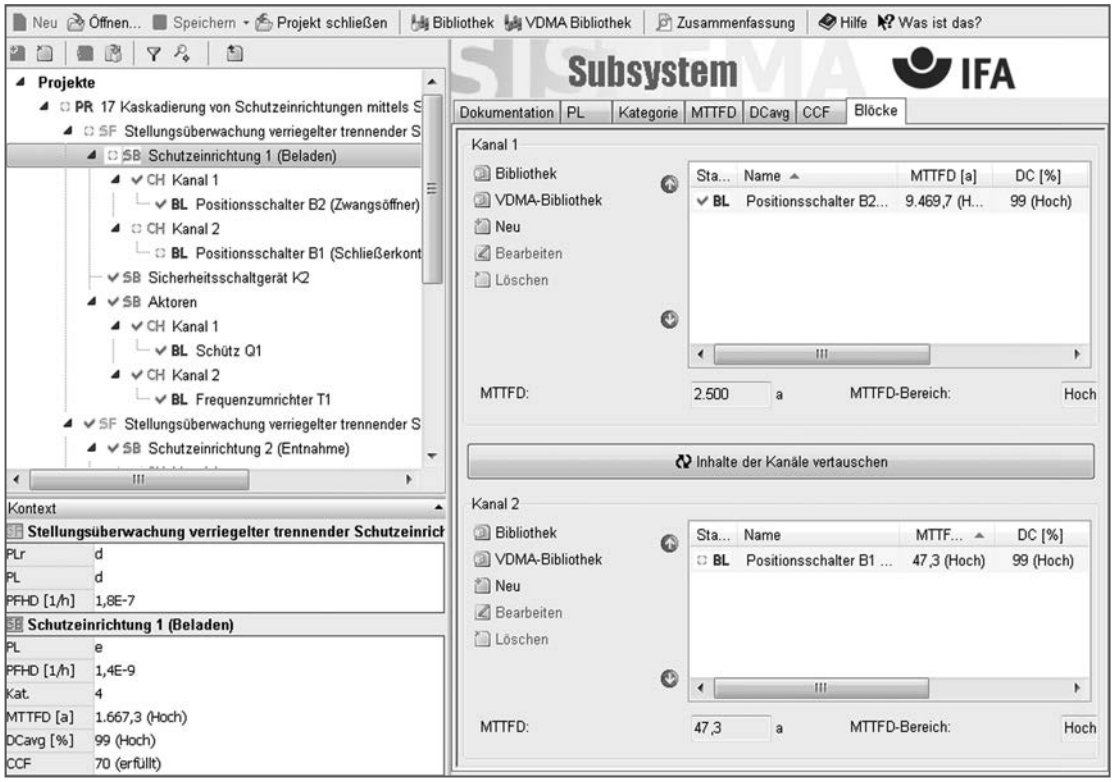


Abbildung 8.34:
PL-Bestimmung mithilfe von SISTEMA

8.2.18 Stellungsüberwachung verriegelter trennender Schutzeinrichtungen – Kategorie 3 – PL d (Beispiel 18)

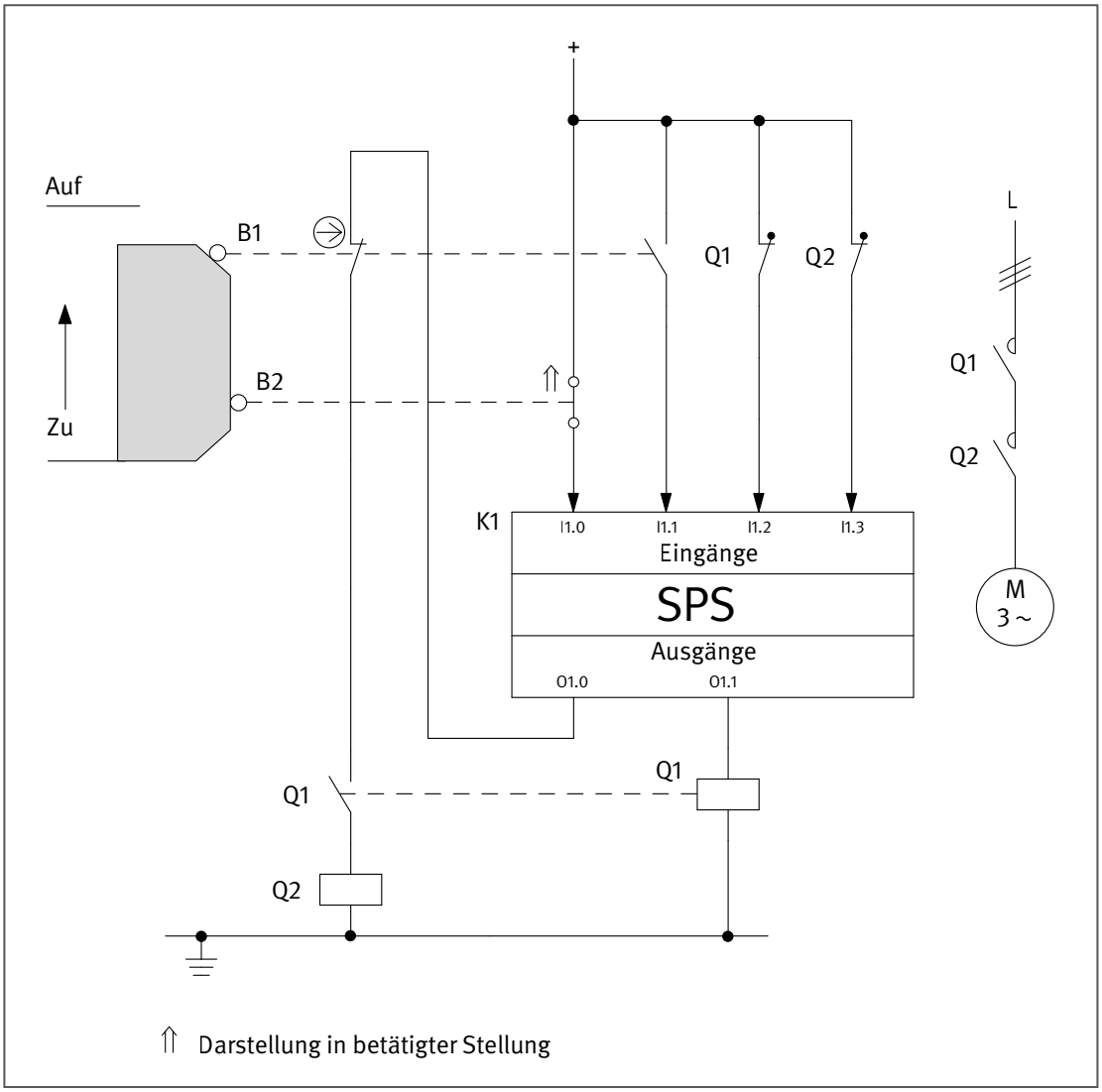
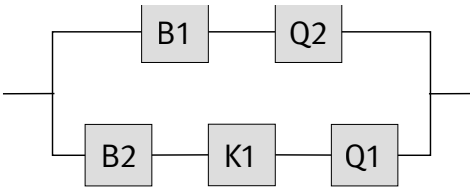


Abbildung 8.35: Redundante Stellungsüberwachung verriegelter trennender Schutzeinrichtung in diversitärer Technologie (elektromechanisch und programmierbar elektronisch)



Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der verriegelten trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der verriegelten trennenden Schutzeinrichtung (z. B. Schutzgitter) wird durch zwei Positionsschalter B1 und B2 in Öffner-Schließer-Kombination erfasst. Der Positionsschalter B1 mit zwangsöffnendem Kontakt steuert ein Schütz Q2 an, durch dessen Abfallen gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert werden. Der Positionsschalter B2 mit Schließerkontakt wird von einer Standard-SPS K1 eingelesen, die über die Ansteuerung eines zweiten Schützes Q1 die gleiche Abschaltreaktion bewirken kann.
- Beim Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten.
- Die Schaltstellung von B1 wird über einen Schließerkontakt ebenfalls in die SPS K1 eingelesen und auf Plausibilität mit der Schaltstellung von B2 verglichen. Die Schaltstellung der Schütze Q1 und Q2 wird ebenfalls über Spiegelkontakte in K1 überwacht. Bauteilausfälle in B1, B2, Q1 und Q2 werden durch K1 erkannt und führen durch das Abfallen von Q1 und Q2 zur Betriebshemmung. Fehler in der SPS K1 werden nur über die Funktion erkannt (Fehlererkennung durch den Prozess).

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern sind getrennt verlegt oder es erfolgt eine geschützte Leitungsverlegung.
- Störungen im Anfahr- und Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschieden betätigten Positionsschaltern (Öffner und Schließer) erkannt.
- Q1 und Q2 besitzen Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F. Die programmierbare SPS K1 erfüllt die normativen Anforderungen gemäß Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Der Positionsschalter B1 mit Rollenbetätigung weist einen B_{10D} von $20 \cdot 10^6$ Schaltspiele auf [H]. Für den Positionsschalter B2 (Schließer) beträgt B_{10D} = 100 000 Schaltspiele [H]. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Stunde Zykluszeit ist für diese Komponenten n_{op} = 5 840 Zyklen/Jahr und $MTTF_D$ beträgt 34 246,6 Jahre für B1 bzw. 171 Jahre für B2. Für die Schütze Q1 und Q2 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 300 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} ergibt sich für Q1 und Q2 eine $MTTF_D$ von 4 452 Jahren. Für die SPS wird ein MTTF-Wert von 15 Jahren [H] angesetzt, aus dem sich durch Verdoppelung ein $MTTF_D$-Wert von 30 Jahren ergibt. Die Kombination von B1 und Q2 ergibt $MTTF_D$ = 3 940 Jahre für den ersten Kanal, B2, K1 und Q2 tragen zur $MTTF_D$ = 25,4 Jahre im zweiten Kanal bei. Insgesamt ergibt sich über beide Kanäle ein symmetrisierter $MTTF_D$-Wert pro Kanal von 70 Jahren („hoch“). Der Positionsschalter B2 weist eine begrenzte Betriebszeit von 17,1 Jahren auf. Ein rechtzeitiger Austausch wird empfohlen.
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung beider Schaltzustände in der SPS K1. DC = 99 % für die Schütze Q1 und Q2 ergibt sich aus der Rücklesung über Spiegelkontakte ebenfalls in K1. Für K1 wird wegen der möglichen Fehlererkennung durch den Prozess DC = 60 % angenommen. Durch Mittelung ergibt sich damit ein DC_{avg} von 66,2 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ (70 Jahre) und niedrigem DC_{avg} (66,2 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}6 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

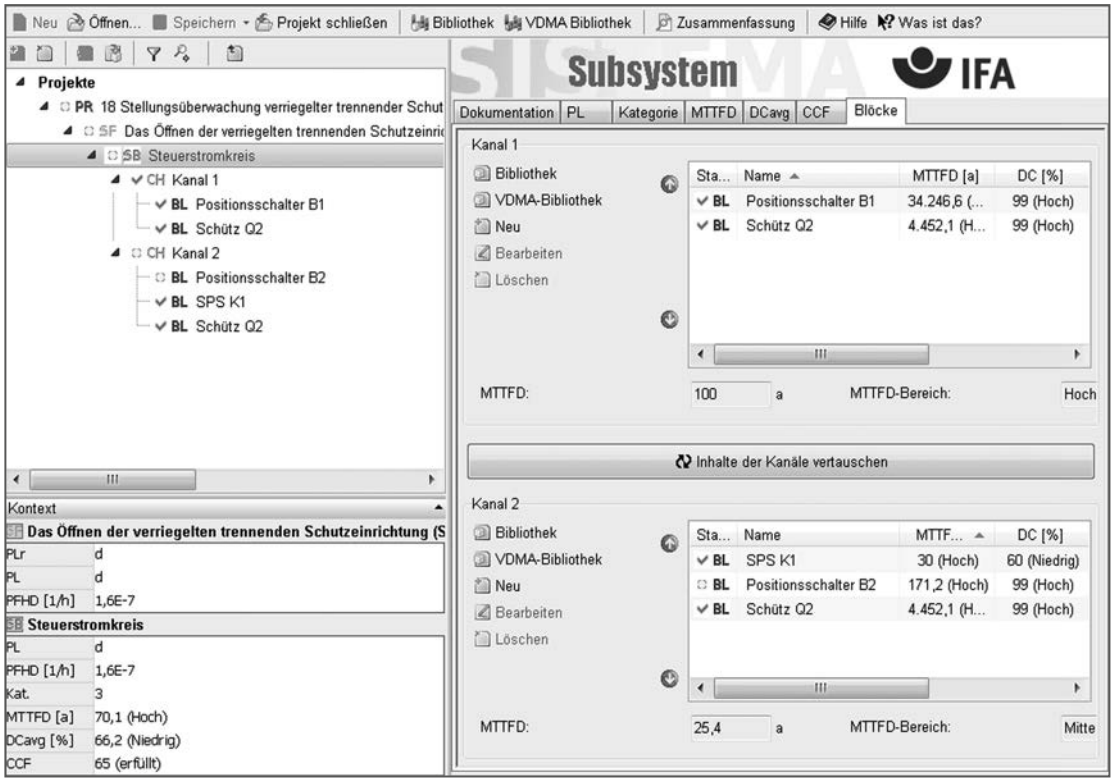


Abbildung 8.36: PL-Bestimmung mithilfe von SISTEMA

8.2.19 Verriegelungseinrichtung mit Zuhaltung – Kategorie 3 – PL d (Beispiel 19)

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):
Das Beispiel wurde grundsätzlich überarbeitet.

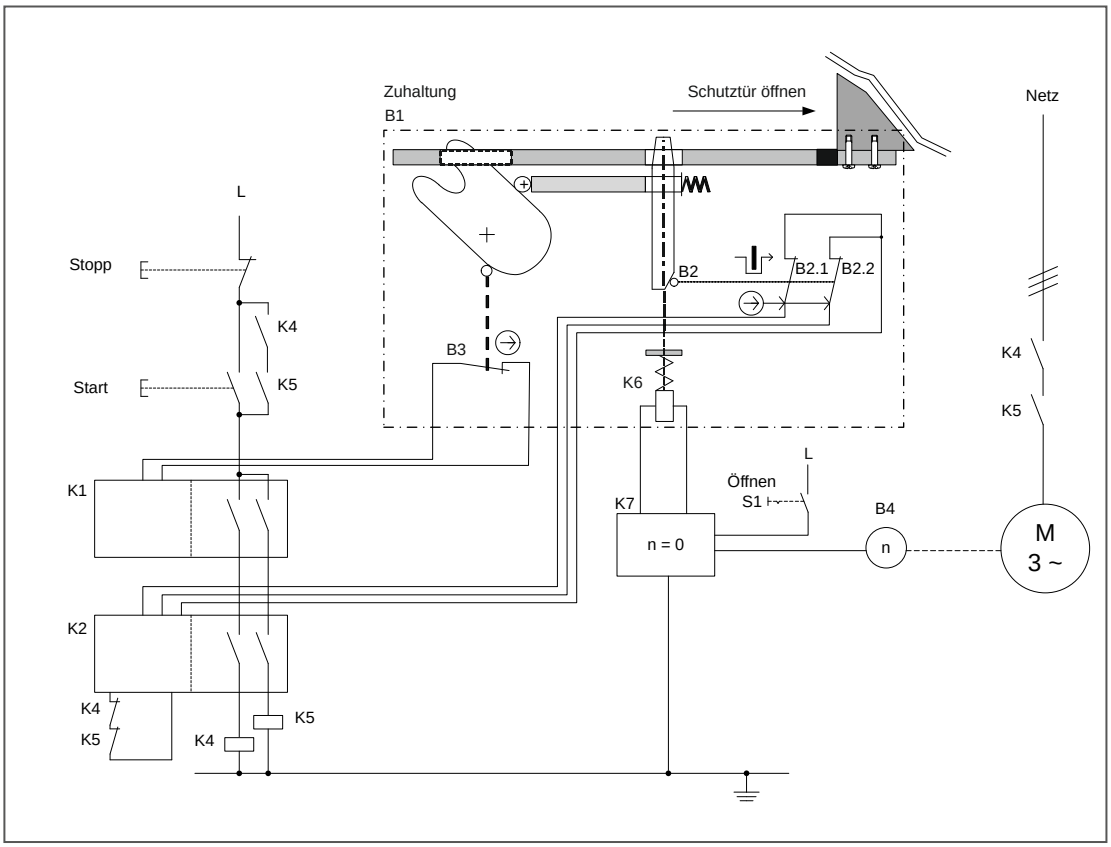


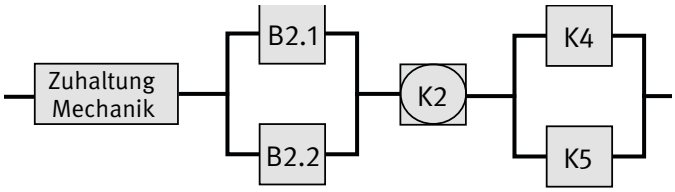
Abbildung 8.37: Stellungsüberwachung einer verriegelten trennenden Schutzeinrichtung mit Zuhaltung

Sicherheitsfunktionen

- Zuhaltung (PL d): Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung verhindert.
- Entsperren der Zuhaltung: Ein Öffnen der Schutzeinrichtung ist nur möglich nach Erreichen des Stillstands des Motors.

Funktionsbeschreibung

- Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung solange verhindert, bis die Bewegung zum Stillstand gekommen ist (Sicherheitsfunktion Zuhaltung). Die Tür wird durch einen federkraftbetätigten Bolzen (Sperrmittel) eines Hubmagneten zugehalten, der ein Herausziehen des Betätigers aus dem Schalterkopf verhindert, bis die Ansteuerung des Zuhaltemagneten erfolgt.
- Die Zuhaltung besitzt gemäß Herstellerangabe eine Fehlschließsicherung.
- Bei geöffneter Schutztür wird der unerwartete Anlauf des Motors zweikanalig durch die Sicherheitsfunktion Verriegelung verhindert (nicht dargestellt).
- Der Bolzen des Sperrmittels wirkt direkt auf die zwangsöffnenden Kontakte B2.1 und B2.2, die an ein Sicherheitsschaltgerät K2 angeschlossen sind.
- Die gefahrbringende Bewegung kann nur bei geschlossener und zugehaltener Schutztür in Gang gesetzt werden, da die Freigaben von K1 und K2 in Reihe geschaltet sind.
- Mit Betätigen der Stopp-Taste fallen die Hilfsschütze K4 und K5 ab. Nach Stillstand des Motors kann die Zuhaltung durch Betätigen des rastenden Schalters S1 geöffnet werden (Sicherheitsfunktion Entsperren der Zuhaltung). Der Stillstand des Motors wird über eine zweikanalige Überwachung B4, K7 ermittelt.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- B1 ist eine elektromechanische Zuhaltung mit Fehlschließsicherung.

  Für die Mechanik der Zuhaltung einschließlich Bruch des Sperrmittels und des Betätigers kann ein Fehlerausschluss angenommen werden, wenn die folgenden Bedingungen erfüllt sind:
  - Anwendung entsprechend der Betriebsanleitung, insbesondere Montageanleitung und technische Daten (z. B. Betätigungsradius, Betätigungsgeschwindigkeit)
  - Verhinderung des Selbstlockerns
  - die statischen Kräfte auf die Zuhaltung sind geringer als die im Datenblatt angegebene Zuhaltekraft
  - es treten keine dynamischen Kräfte auf, da die Bestromung des Entriegelungsmagneten bei geschlossener Schutztür erfolgt; siehe hierzu auch DGUV Information 203-079 „Auswahl und Anbringung von Verriegelungseinrichtungen“
  - keine Verwendung als mechanischer Endanschlag
  - unlösbare Befestigung des Betätigers
  - regelmäßige Wartung
  - Formschluss nach Montage
  - ausreichende mechanische Festigkeit aller Träger- und Funktionselemente
  - ein Absenken der Tür führt nicht dazu, dass der Betätiger außerhalb des vom Hersteller spezifizierten Bereichs eingesetzt wird
  - Schäden, die durch vorhersehbare äußere Einflüsse (z. B. Eindringen von Schmutz, Staub und mechanische Erschütterung) entstehen könnten, werden durch die Art der Montage ferngehalten oder sind aufgrund der Einsatzbedingungen nicht zu erwarten.
- B2.1 und B2.2 sind Schaltelemente der Zuhaltung mit zwangsöffnenden Kontakten entsprechend DIN EN 60947-5-1 Anhang K. Für die Berechnung gibt der Hersteller einen B_{10D}-Wert an.
- B3 ist ein zwangsöffnender Kontakt entsprechend DIN EN 60947-5-1, Anhang K, und dient zur Überwachung der Türstellung.
- K4 und K5 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Sicherheitsschaltgeräte K1 und K2 erkennen Quer- und Erdschlüsse und erfüllen die Anforderungen der Kategorie 4, PL d der DIN EN ISO 13849-1.
- Die Stillstandsüberwachung besteht aus dem Sin-/Cos-Geber B4 und dem Stillstandswächter K7. Beide erfüllen jeweils die Anforderungen der Kategorie 4, PL e.

Berechnung der Ausfallwahrscheinlichkeit

- Für die Mechanik der Zuhaltung B1 wird ein Fehlerausschluss angenommen.
  Hinweis: Bei Zuhaltungen mit „Fehlschließsicherung“ ist ein Fehlerausschluss nur entsprechend Angabe des Herstellers möglich.
- Für die Schaltelemente B2.1 und B2.2 gibt der Hersteller einen B_{10D}-Wert von jeweils 3 000 000 Zyklen [H] an. Bei einer Betätigung alle 10 Minuten ist n_{op} = 17 520 Zyklen/Jahr und $MTTF_D$ = 1712 Jahre.
- Die Hilfsschütze K4 und K5 haben einen B_{10D}-Wert von 1 000 000 Zyklen [H]. Bei einer Betätigung alle 10 Minuten ist n_{op} = 17 520 Zyklen/Jahr und $MTTF_D$ = 570 Jahre.
- Für das Sicherheitsschaltgerät K2 gibt der Hersteller $PFH_D = 3{,}0 \cdot 10^{-9}$/Stunde [H] an.
- DC_{avg} : DC = 99 % für die Kontakte B2.1 und B2.2 ergibt sich durch die direkte Überwachung in K2. DC = 99 % für K4 und K5 begründet sich durch die direkte Überwachung in K2 mittels zwangsgeführter Kontakte. Durch Mittelung ergibt sich damit ein DC_{avg} von 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Für die Sicherheitsfunktion „Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung verhindert“ beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $PFH_D = 5{,}2 \cdot 10^{-8}$/Stunde. Dies entspricht PL e; da jedoch der Positionsschalter (B2) für die Sperrmittelüberwachung und die zugehörige Anfahrmechanik nur einmal vorhanden ist, wird der PL auf d beschränkt.
- Für die Sicherheitsfunktion „Entsperren der Zuhaltung: Ein Öffnen der Schutzeinrichtung ist nur möglich nach Erreichen des Stillstands des Motors“ wird die Ausfallwahrscheinlichkeit nur vom Sin-/Cos-Geber B4 und vom Stillstandswächter K7 bestimmt. Gemäß Herstellerangabe beträgt für den Sin/Cos-Geber B4 der $PFH_D = 1{,}2 \cdot 10^{-8}$/Stunde. Für den Stillstandswächter K7 wird eine $PFH_D = 2{,}0 \cdot 10^{-8}$/Stunde angegeben [H]. Die *PFH* dieser Sicherheitsfunktion beträgt $3{,}2 \cdot 10^{-8}$/Stunde.

Weiterführende Literatur

- DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen 203-079 (12/2015). Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2015
  ▸ http://publikationen.dguv.de/dguv/pdf/10002/203-079.pdf
- Grundsätze für die Prüfung und Zertifizierung von Verriegelungseinrichtungen mit Zuhaltung (GS-ET-19) (5/2015). Hrsg.: Fachbereich Energie Textil Elektro Medienerzeugnisse, Köln 2015
  ▸ www.bgetem.de, Webcode: 12700341

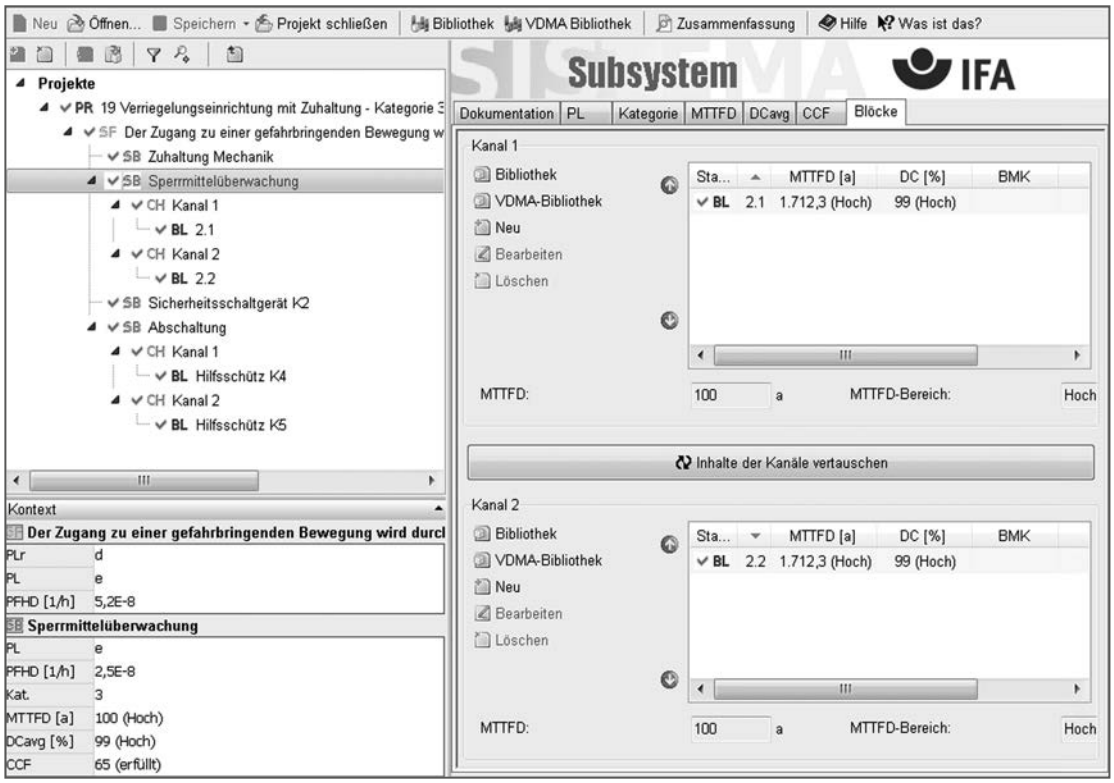
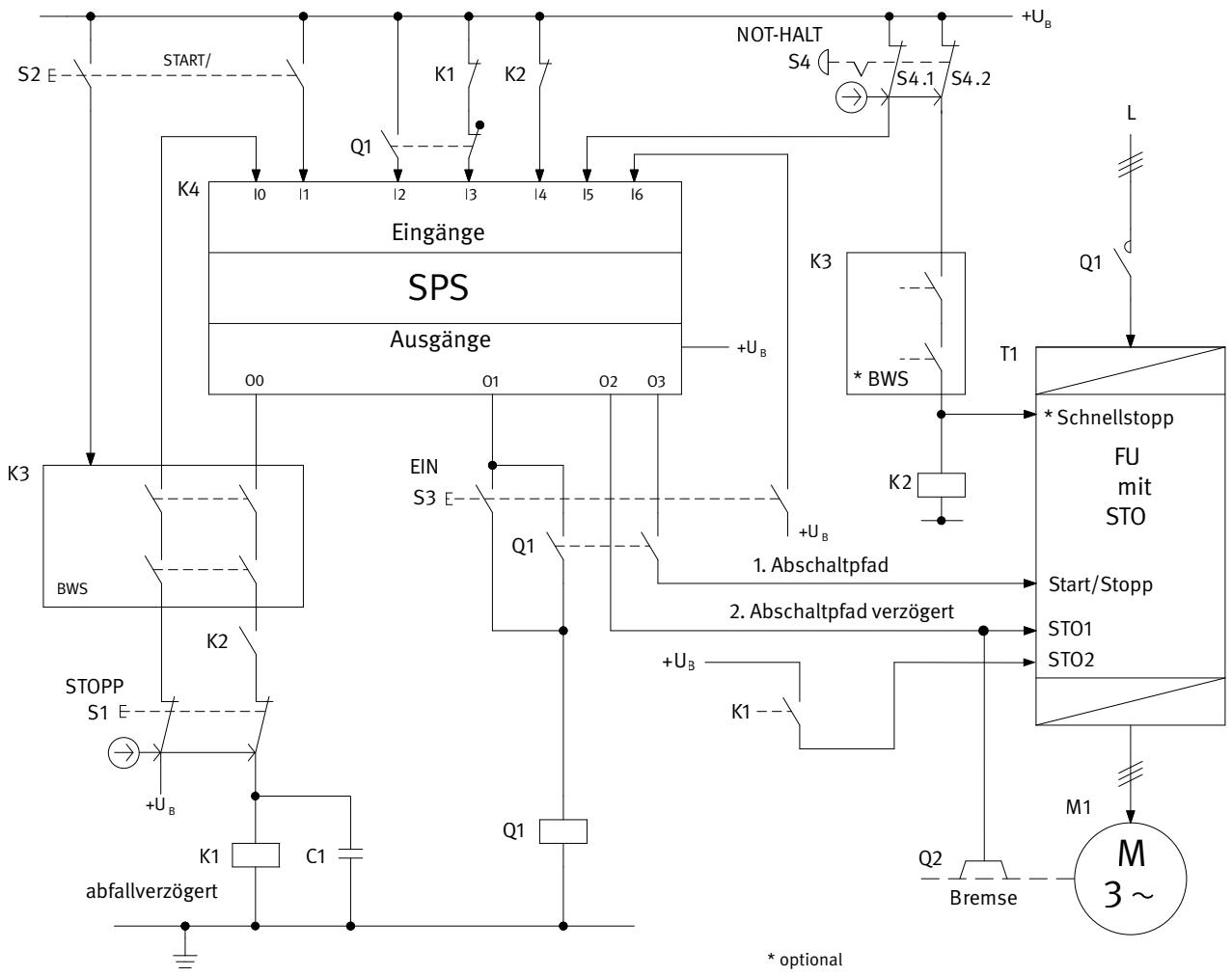


Abbildung 8.38: PL-Bestimmung mithilfe von SISTEMA

8.2.20 Sicheres Stillsetzen eines SPS-gesteuerten Antriebs – Kategorie 3 – PL d (Beispiel 20)

Abbildung 8.39:
Sicheres Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung (hier: BWS)

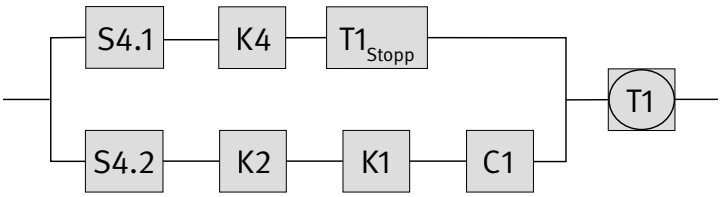


Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion: Nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung wird der Antrieb angehalten (SS1-t – Sicherer Stopp 1, STO wird zeitverzögert aktiviert).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird redundant unterbrochen, falls entweder die Stopp-Taste S1 oder die Schutzeinrichtung K3 – im Schaltbild als berührungslos wirkende Schutzeinrichtung (BWS) dargestellt – aktiviert wird. Das Stillsetzen des Antriebs im Notfall erfolgt nach Betätigung des Not-Halt-Gerätes S4. In allen drei Fällen wird über den Ausgang O3 der SPS K4 durch Deaktivierung des Eingangs „Start/Stopp“ am Frequenzumrichter (FU) T1 der Stopp ausgelöst. Redundant dazu wird über das Entregen des Hilfsschützes K1 (abfallverzögert mithilfe des Kondensators C1) der Eingang „STO2“ an T1 deaktiviert. Über den Ausgang O2 der SPS K4 existiert ein weiterer Abschaltpfad auf den Eingang „STO1“ an T1, der auch die Bremse Q2 einfallen lässt. Der erste Abschaltpfad wird also über die SPS K4 unmittelbar realisiert, wohingegen der zweite Abschaltpfad verzögert kontaktbehaftet abschaltet. Die Zeitvorgaben für O2 im SPS-Programm und für K1 sind so gewählt, dass auch unter ungünstigen Betriebsbedingungen der Stillstand der Maschinenbewegung erreicht wird.



- Steht ein Eingang „Schnellstopp“ mit besonders kurzer Geschwindigkeitsabsteuerung am FU zur Verfügung, kann eine BWS optional – wie im Schaltbild gekennzeichnet – eingebunden werden. Diese Variante wird im Folgenden nicht weiter betrachtet.
- Bei einem einzelnen Versagen der SPS K4, der Umrichtereingänge „Start/Stopp“, „STO1“ oder „STO2“, des abfallverzögerten Hilfsschützes K1 oder des Hilfsschützes K2 wird trotzdem das Stillsetzen des Antriebs sichergestellt, weil immer zwei voneinander unabhängige Abschaltpfade vorhanden sind. Das Nichtabfallen der Hilfsschütze K1 oder K2 wird wegen der vorhandenen Rückführung der zwangsgeführten Öffnerkontakte in die SPS-Eingänge I3 und I4 spätestens vor einem erneuten Ingangsetzen der Maschinenbewegung aufgedeckt.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Durch die Verwendung eines FU mit STO ist der Einsatz des Leistungsschützes Q1 zum Abschalten der Versorgungsspannung nicht unbedingt erforderlich. Der FU muss zum Antreiben und Bremsen geeignet sein.
- Für den Vergleich der Absteuerung der Eingänge „STO1/STO2“ im FU wird eine ausreichend große Zeitspanne gewählt, um die Varianz der Abfallverzögerung von K1 zu berücksichtigen.
- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Kontakte der Stopp-Taste S1 und des Not-Halt-Gerätes S4 sind zwangsöffnend ausgeführt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Standardkomponente K4 wird entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL c (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.10.
- Ist die Bremse Q2 nur aus funktionalen Gründen vorhanden und somit an der Ausführung der Sicherheitsfunktion nicht beteiligt, wird sie – wie in diesem Beispiel – bei der Berechnung der Ausfallwahrscheinlichkeit nicht berücksichtigt. Diese Vorgehensweise setzt voraus, dass ein Austrudeln des Antriebs bei einem Versagen der Stoppfunktion und somit bei alleiniger Abschaltung über STO nicht mit einem verbleibenden inakzeptabel hohen Risiko verbunden ist. Die Beteiligung einer Bremse bei der Ausführung der Sicherheitsfunktion im Zusammenhang mit dem Einsatz eines FU ist im Beispiel 23 (Karusselltürsteuerung) beschrieben.
- Die BWS K3 erfüllt, z. B. als Lichtgitter, die Anforderungen für Typ 4 nach DIN EN 61496-1 und DIN EN 61496-2 sowie für PL e.

Berechnung der Ausfallwahrscheinlichkeit

- Es wird die Ausfallwahrscheinlichkeit PFH_D des sicheren Stillsetzens ausgelöst durch das Not-Halt-Gerät S4 bzw. durch die BWS berechnet. Die Funktion „Schnellstopp“ des FU und die Möglichkeit einer Abschaltung der Spannungsversorgung für den FU über Q1 werden bei der Berechnung der Ausfallwahrscheinlichkeit der Sicherheitsfunktion nicht berücksichtigt.
- Der FU T1 mit STO liegt als käufliches Sicherheitsbauteil vor, dessen Ausfallwahrscheinlichkeit am Ende der Berechnung addiert wird ($1{,}5 \cdot 10^{-8}$/Stunde [H]). Die Stopp-Funktion des FU wird im ersten Kanal des Blockdiagramms modelliert (T1Stopp). Der FU mit STO würde eigentlich im zweiten Kanal des Blockdiagramms modelliert. Ein Modell mit einem fertigen Sicherheitsbauteil inklusive PFH_D in nur einem Kanal kennt die Norm jedoch nicht. Deshalb wird der FU T1 mit seiner STO-Funktion als einzelnes Subsystem betrachtet. Diese Betrachtung ist eine Abschätzung in die sichere Richtung.

Sicheres Stillsetzen ausgelöst durch das Not-Halt-Gerät S4:

- $MTTF_D$: Folgende $MTTF_D$-Werte werden geschätzt: 50 Jahre für K4 und 100 Jahre für die Stoppfunktion T1Stopp des FU [G]. Für S4.1 und S4.2 ergibt sich bei einem B_{10D}-Wert von jeweils 100 000 Zyklen [N] und n_{op} = 12 Zyklen/Jahr eine $MTTF_D$ von 83 333 Jahren. Für K1 ergibt sich bei einem B_{10D}-Wert von 400 000 Zyklen [N] bei 240 Arbeitstagen, 8 Arbeitsstunden und 6 Minuten Zykluszeit eine n_{op} = 19 200 Zyklen/Jahr und eine $MTTF_D$ von 208 Jahren. Für K2 ergibt sich bei einem B_{10D}-Wert von 400 000 Zyklen [N] und täglichem Einschalten an 240 Arbeitstagen eine $MTTF_D$ von 16 667 Jahren. Der Kondensator C1 geht mit $MTTF_D$ = 45 662 Jahre [D] in die Berechnung ein. Diese Werte ergeben eine symmetrisierte $MTTF_D$ pro Kanal von 72 Jahren („hoch“).

- DC_{avg}: Fehlererkennung durch den Prozess führt auf DC = 60 % für T1Stopp und in Kombination mit internen Selbsttests auf DC = 60 % für K4. Testung des Zeitglieds bei spannungsfreiem FU führt auf DC = 99 % für K1. Für C1 führt die Testung des Zeitglieds bei spannungsfreiem FU in Kombination mit der Fehleraufdeckung durch Vergleich im FU bei Anforderung der Sicherheitsfunktion auf DC = 90 %. Für S4.1, S4.2 sowie K2 gilt DC = 99 % durch Plausibilitätstest in K4. Eine ausreichende Testhäufigkeit des Not-Halt-Gerätes ist gewährleistet (siehe Hinweise in den Anschnitten 6.2.14 und D.2.5.1). Die Mittelungsformel für DC_{avg} ergibt 65 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (72 Jahre) und niedrigem DC_{avg} (65 %). Zuzüglich des FU T1 ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls PFH_D von $1{,}7 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Sicheres Stillsetzen ausgelöst durch die BWS K3:

- Die BWS K3 liegt als geprüftes Sicherheitsbauteil vor. Ihre Ausfallwahrscheinlichkeit PFH_D beträgt $3{,}0 \cdot 10^{-8}$/Stunde [H] und wird am Ende der Berechnung addiert.
- Für die zweikanalige Struktur „SPS/Elektromechanik“ wird die Ausfallwahrscheinlichkeit mit den gleichen $MTTF_D$- und DC-Werten wie oben berechnet. Das Bauteil K2 ist an der Ausführung dieser Sicherheitsfunktion jedoch nicht beteiligt. Es ergeben sich folgende Werte: $MTTF_D$ eines Kanals = 72 Jahre („hoch“) und DC_{avg} = 65 % („niedrig“). Für Kategorie 3 ergibt dies eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls PFH_D von $1{,}5 \cdot 10^{-7}$/Stunde. Die Gesamtausfallwahrscheinlichkeit wird durch Addition ermittelt und führt zu $PFH_D = 2{,}0 \cdot 10^{-7}$/Stunde. Dies entspricht ebenfalls PL d.

Weiterführende Literatur

- *Apfeld, R.; Zilligen, H.; Köhler, B.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 7/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin 2013
  ▶ www.dguv.de/ifa, Webcode: d639540
- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (05.14) und Berichtigung 1 (08.15). Beuth, Berlin 2014 und 2015
- DIN EN 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (06.14). Beuth, Berlin 2014
- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (2017). Beuth, Berlin 2017

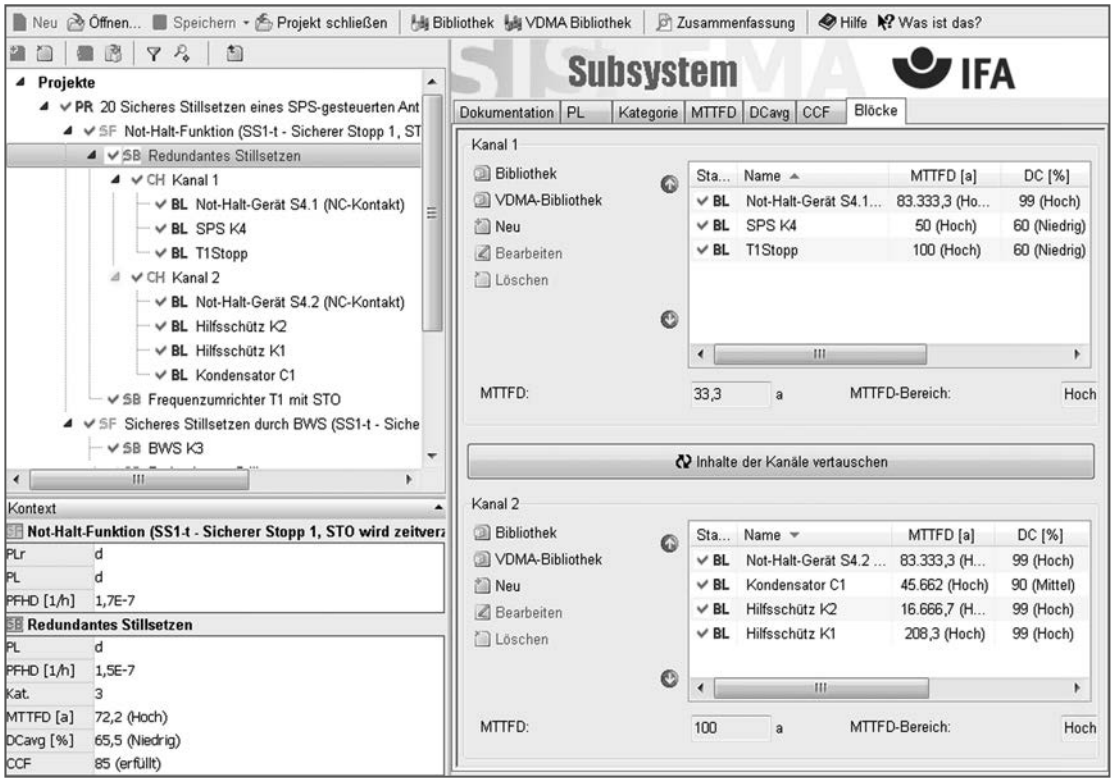


Abbildung 8.40: PL-Bestimmung mithilfe von SISTEMA

8.2.21 Sicher begrenzte Geschwindigkeit – Kategorie 3 – PL d (Beispiel 21)

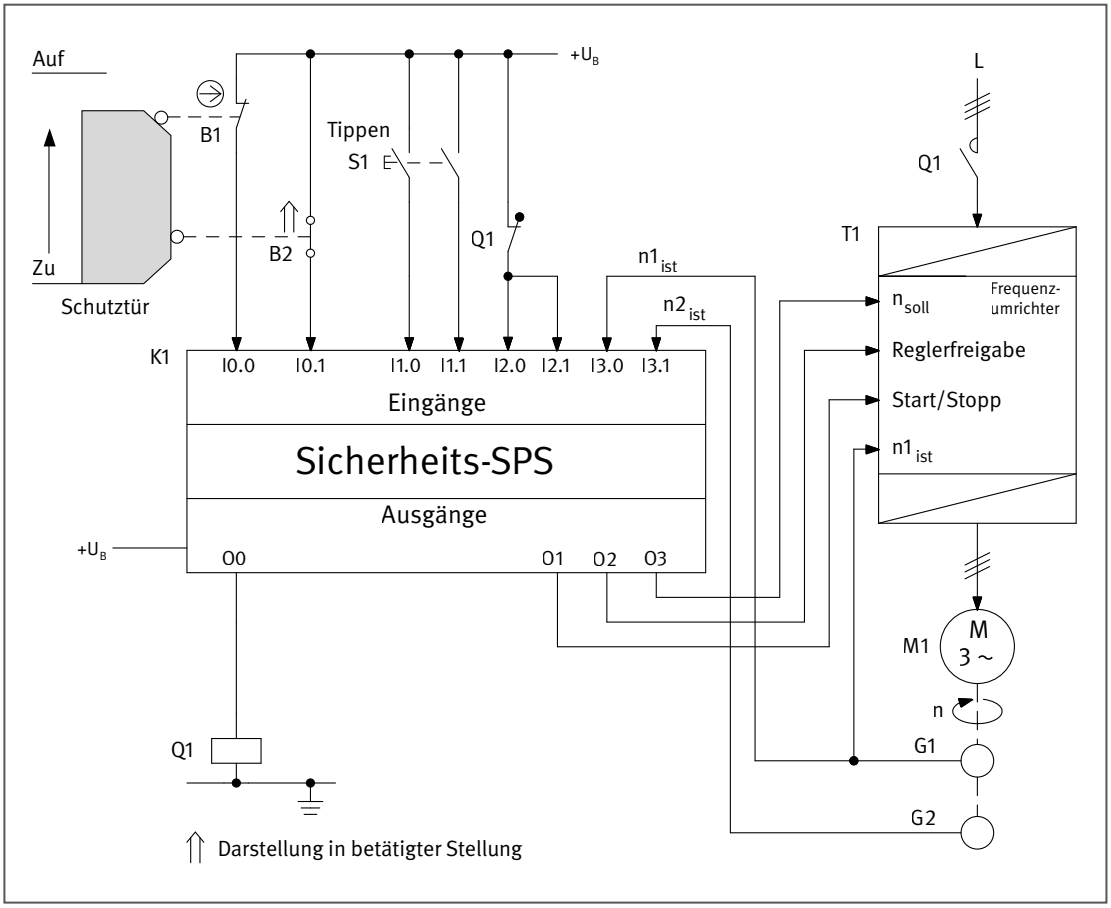


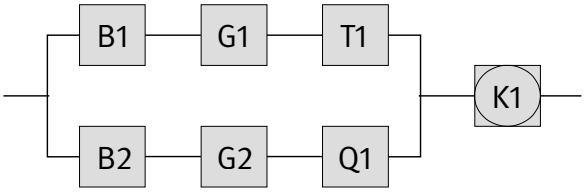
Abbildung 8.41: Sicher begrenzte Geschwindigkeit bei geöffneter Schutztür, mit Soll-/Ist-Vergleich und Drehzahl-Grenzwertvorgabe innerhalb einer Sicherheits-SPS

Sicherheitsfunktion

- Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür wird das Überschreiten einer zulässigen Drehzahl verhindert.

Funktionsbeschreibung

- Dieses Beispiel zeigt die Realisierung der Sicherheitsfunktion SLS mit einem Frequenzumrichter ohne integrierte Sicherheitsfunktionen. Die Sicherheitsfunktion SLS wird z. B. für den Tippbetrieb im Rahmen von Serviceaufgaben genutzt.
- Eine gefahrbringende Bewegung wird bei geöffneter Schutztür sicher verhindert oder unterbrochen. Das Öffnen der Schutztür wird über zwei Positionsschalter B1 und B2 in Öffner-Schließer-Kombination erfasst. Bei betätigtem Taster S1 wird mithilfe der Sicherheits-SPS K1 eine Bewegung mit sicher begrenzter Geschwindigkeit (Tippbetrieb) ausgelöst. Beide Verarbeitungskanäle innerhalb der SPS verarbeiten einen fest hinterlegten Sollgrenzwert. Die Überwachung der Istdrehzahl der begrenzten Geschwindigkeit an den Eingängen I3.0 und I3.1 von K1 erfolgt über zwei separate Drehgeber G1 und G2. Jeder Kanal der SPS führt unabhängig den Soll-/Ist-Vergleich durch. Schlägt die über T1 geregelte Reduzierung der Drehzahl auf den begrenzten Wert fehl, so kann K1 über Sperrung des Start-/Stopp-Signals und der Reglerfreigabe am Frequenzumrichter einen Stillstand einleiten. Zusätzlich wird über das Netzschütz Q1 die Energieversorgung zu T1 nach Ablauf einer programmierten Zeit getrennt.
- Die zweikanalige Sicherheits-SPS K1 führt eine interne Fehlererkennung durch. Versagt ein Verarbeitungskanal, so erfolgt die Abwärtssteuerung des Frequenzumrichters T1 sowie des Netzschützes Q1 jeweils durch den anderen noch funktionierenden Verarbeitungskanal. Ein Versagen des Frequenzumrichters, das z. B. zum unerwarteten Anlaufen, zum Weiterlaufen oder zu einer Erhöhung der Drehzahl führen kann, wird über die getrennte Erfassung der Drehzahl durch die Drehgeber G1 und G2 in beiden Verarbeitungskanälen erkannt. Das Nichtabfallen des Netzschützes Q1 wird über den in beide Verarbeitungskanäle geführten Öffnerkontakt (Eingänge I2.0 und I2.1 von K1) bemerkt und führt sowohl zur Sperrung des Start-/Stopp-Signals als auch der Reglerfreigabe am Frequenzumrichter durch beide Verarbeitungskanäle.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.
- Der Positionsschalter B1 ist zwangsöffnend entsprechend DIN EN 60947-5-1, Anhang K, ausgeführt. Der Positionsschalter B2 entspricht ebenfalls DIN EN 60947-5-1.
- Das Schütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F.
- Die Anschlussleitungen der Positionsschalter sind entweder getrennt oder gegen mechanische Beschädigung geschützt verlegt.
- Für die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit“ wird ein Fehlerausschluss für den Fehler Geberwellenbruch (G1/G2) angenommen. Einzelheiten zur Möglichkeit eines Fehlerausschlusses geben z. B. DIN EN 61800-5-2, Tabelle D.8, und GS-IFA-M21.
- Die Standardkomponenten G1 und G2 (soweit für die Drehgeber zutreffend) und T1 werden entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.
- Das Sicherheitsbauteil K1 erfüllt alle Anforderungen für Kategorie 3 und PL d. Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.10.
- Es wird davon ausgegangen, dass die Ausgänge der Sicherheits-SPS jeweils von beiden Verarbeitungskanälen der SPS angesteuert werden und der analoge Ausgang 03 zweikanalig überwacht wird.

Berechnung der Ausfallwahrscheinlichkeit

- Der SRP/CS wird in die beiden Subsysteme Sensor/Aktor und SPS unterteilt. Für das Teilsystem SPS wird eine geprüfte, für PL d taugliche Sicherheits-SPS eingesetzt, deren Ausfallwahrscheinlichkeit $1{,}5 \cdot 10^{-7}$/Stunde [G] am Ende der Berechnung für das Subsystem Sensor/Aktor addiert wird. Zur Aufstellung des Blockdiagramms siehe auch Abbildung 6.14 und entsprechende Hinweise im zugehörigen Text. Nachfolgend wird die Ausfallwahrscheinlichkeit für das Teilsystem Sensor/Aktor berechnet.
- $MTTF_D$: Bei 240 Arbeitstagen, 8 Arbeitsstunden und einer Stunde Zykluszeit beträgt n_{op} = 1920 Zyklen/Jahr. Für den Positionsschalter B1 wird aufgrund der Zwangsöffnung ein B_{10D}-Wert von 20 000 000 Zyklen [N] angenommen, der zugehörige $MTTF_D$-Wert beträgt 104 166,7 Jahre. Für B2 wird aufgrund des definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) ein B_{10D}-Wert von 100 000 Zyklen [G] für den durch Federkraft geöffneten Schließerkontakt angenommen (siehe auch Tabelle D.2) und damit eine $MTTF_D$ = 520 Jahre. Das Schütz Q1 mit B_{10D}-Wert von 400 000 Zyklen schaltet betriebsmäßig nur einmal täglich, entsprechend n_{op} = 240 Zyklen/Jahr und $MTTF_D$ = 16 667 Jahre. Folgende Herstellerangaben liegen vor: für T1 $MTTF_D$ = 100 Jahre und für G1/G2 $MTTF_D$ = 190 Jahre [H]. Diese Werte ergeben eine symmetrisierte $MTTF_D$ pro Kanal von 84 Jahren („hoch“).
- DC_{avg}: Für die verwendeten Komponenten wird jeweils ein DC = 99 % angenommen. Dieser basiert für die Positionsschalter und die Drehgeber auf einem Kreuzvergleich von Eingangssignalen in K1. Für den Frequenzumrichter T1 erfolgt eine Drehzahlüberwachung über die zwei Drehgeber in der Sicherheits-SPS und eine Fehlererkennung durch den Prozess, für das Netzschütz Q1 erfolgt eine direkte Überwachung über die SPS. Diese Werte ergeben einen DC_{avg} von 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Das Subsystem Sensor/Aktor entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (84 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls PFH_D von $3{,}0 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Der PL_r = d wird übertroffen, was bei erforderlicher zweikanaliger Ausführung der Hardware mit wenigen Bauteilen und der Verwendung von B_{10D}-Werten nach Norm, einem DC von „hoch“ sowie einer „moderaten“ Schalthäufigkeit nahezu immer der Fall sein wird.
- Die Gesamtausfallwahrscheinlichkeit wird durch Addition der Wahrscheinlichkeit gefährlicher Ausfälle von K1 ($1{,}5 \cdot 10^{-7}$/Stunde) ermittelt und beträgt $PFH_D = 1{,}8 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (2017). Beuth, Berlin 2017
- Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit (GS-IFA-M21). Hrsg.: Institut für Arbeitsschutz der DGUV, Prüf- und Zertifizierungsstelle im DGUV Test, Sankt Augustin 2015 ▸ www.dguv.de, Webcode: d11973
- DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Allgemeine Anforderungen (6/2011). Beuth, Berlin 2011

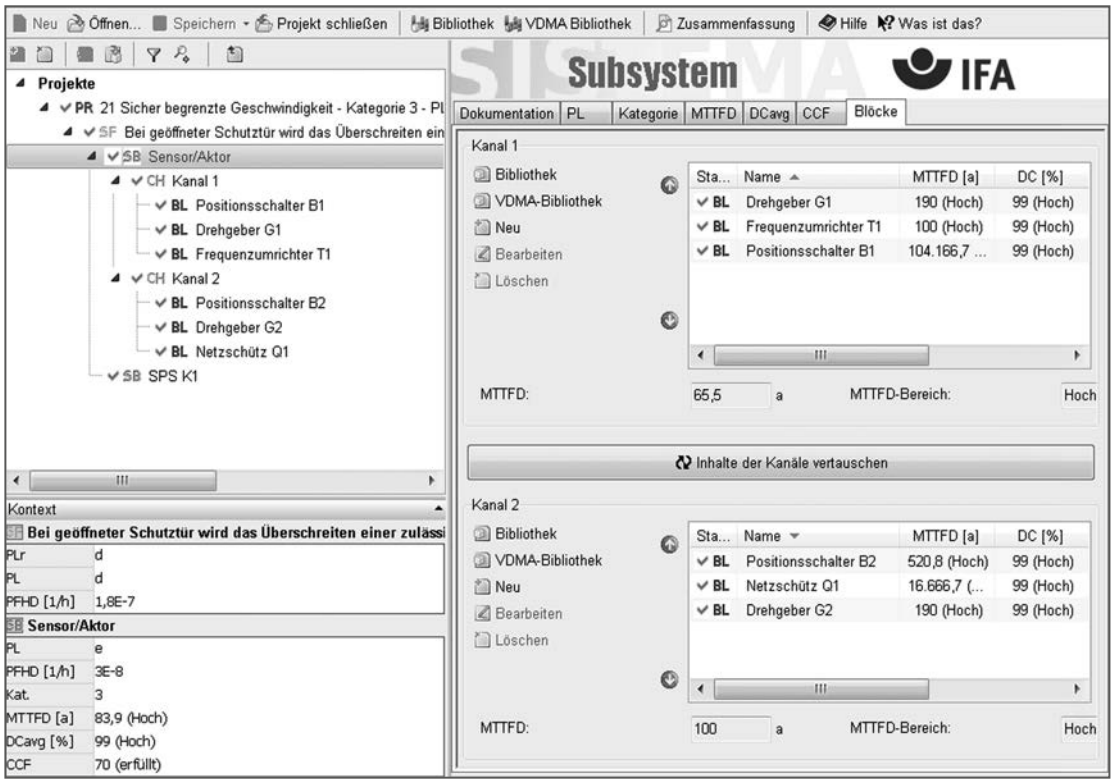


Abbildung 8.42: PL-Bestimmung mithilfe von SISTEMA

8.2.22 Muting einer Schutzeinrichtung – Kategorie 3 – PL d (Beispiel 22)

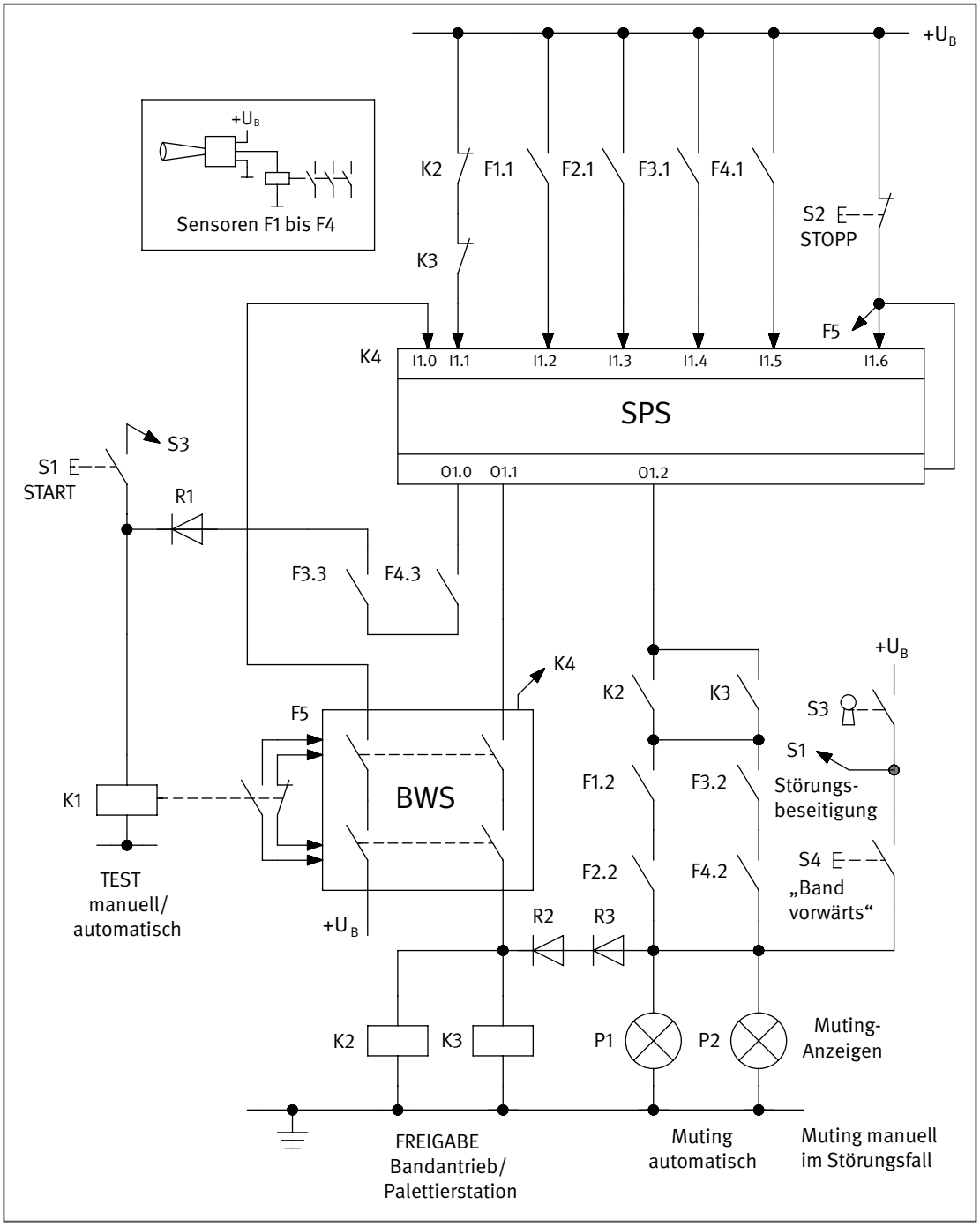
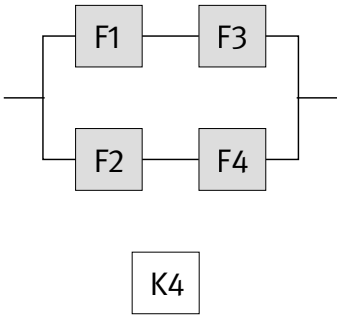


Abbildung 8.43: Überbrückung einer Schutzeinrichtung am Auslauf einer SPS-gesteuerten Palettieranlage

Sicherheitsfunktion

- Mutingfunktion: Zeitlich begrenzte, prozessabhängige Überbrückung einer Schutzeinrichtung. Weitere Sicherheitsfunktionen wie zum Beispiel die Absicherung des Zugangs zur Palettieranlage oder die Anlauf-/Wiederanlaufsperre sind im Folgenden nicht detailliert behandelt.



Funktionsbeschreibung

- Der Zugang am Auslauf der Palettieranlage wird durch eine dreistrahlige Lichtschranke (BWS) F5 des Typs 4 nach DIN EN 61496 abgesichert. Diese enthält die zusätzlichen Funktionen Anlaufsperre und Wiederanlaufsperre, die mithilfe von zwei antivalenten Eingängen realisiert sind. Das Aufheben der Anlaufsperre der Lichtschranke ist an den Startbefehl des Bandantriebs bzw. an das Einschalten der Palettierstation gekoppelt und wird ausgelöst durch den Anzug und nachfolgenden Abfall des Hilfsschützes K1 entsprechend dem Betätigen und Loslassen des Starttasters S1. Voraussetzung für einen gültigen Startbefehl ist das Abgefallensein der Hilfsschütze K2 und K3 (abgefragt über Eingang I1.1) und die Aufhebung der Anlaufsperre (abgefragt über Eingang I1.0). Als Folge wird Ausgang O1.1 gesetzt.
- Zur Steuerung des Überbrückungsvorgangs sind vier Infrarot-Lichttaster F1 bis F4 (zur Anordnung siehe auch Abbildung 8.44) eingebunden. Über die Eingänge I1.2 bis I1.5 überwacht die SPS die Betätigungsabfolge der vier Infrarot-Lichttaster über deren Kontakte F1.1 bis F4.1 unter Berücksichtigung von zwei hinterlegten Zeitvorgaben. Die Überbrückungsfunktion ist allein im Ausgangsstromkreis der SPS (Ausgang O1.2) realisiert, unabhängig vom Ausgangsstromkreis der Lichtschranke F5. Die in Reihe geschalteten Überbrückungskontakte F1.2 und F2.2 sowie F3.2 und F4.2 sind jeweils über die Dioden R2 und R3 mit der über die Hilfsschütze K2 und K3 realisierten „Freigabe“ durch ODER-Verknüpfung verbunden.
- R2 und R3 bewirken die korrekte Anzeige der Mutingfunktion und trennen den aktivierten Freigabeausgang von den Mutinganzeigen P1/P2 bei nicht aktiver Überbrückungsfunktion. Fehler in R2 oder R3 können nicht zu einem unerwarteten Muting (d. h. gefährlichem Ausfall der Mutingfunktion) führen.

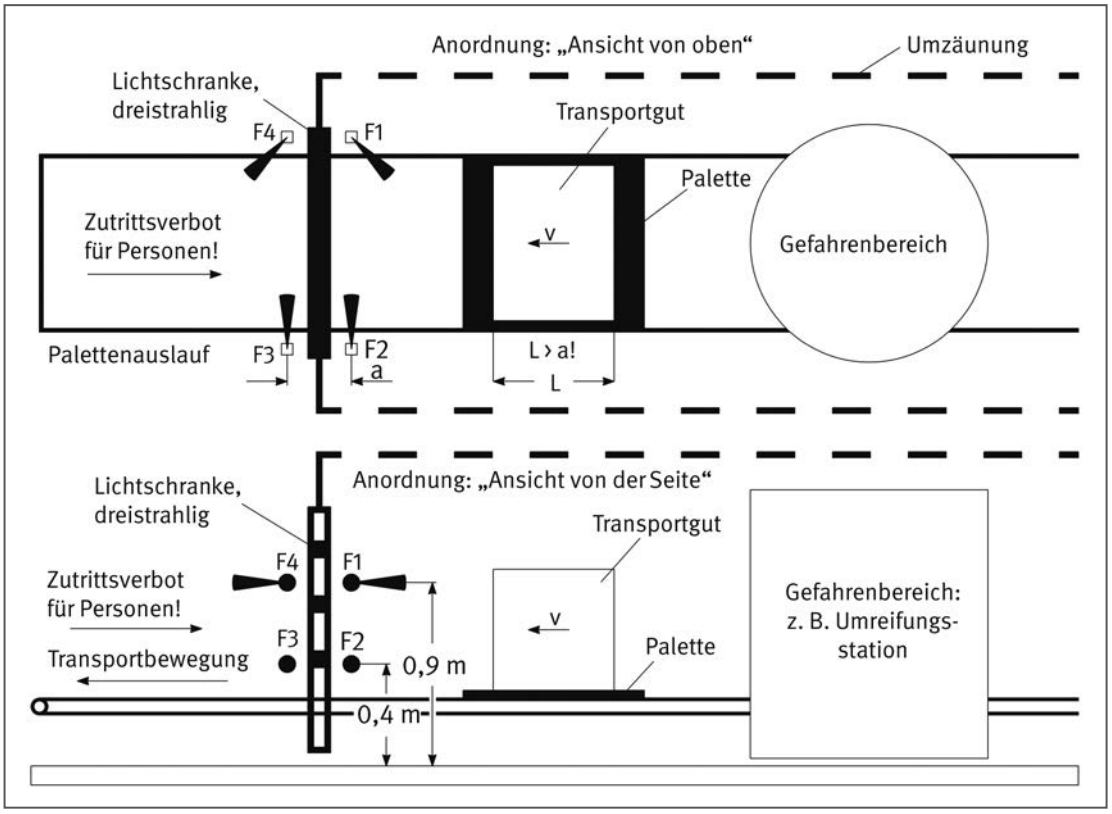


Abbildung 8.44: Automatisch gesteuerte Palettierstation – Prinzip der Absicherung des Palettenauslaufs mit Lichtschranke und Anordnung der Überbrückungssensoren F1 bis F4

- Bei Spannungsausfall mit anschließender Wiederkehr oder bei unterbrochener Lichtschranke F5 und nicht aktiver Überbrückungsfunktion werden die Hilfsschütze K2 und K3 entregt. Die jetzt nicht vorhandene Selbsthaltung verhindert deren Wiederanzug bei einem Wiederschließen der Überbrückungsstromkreise. Ein erneutes Ingangsetzen der Anlage kann nur über das Aufheben der Wiederanlaufsperre, d. h. durch willentliche Betätigung und Entlastung des Starttasters S1 erfolgen.
- Für das bestimmungsgemäße Ingangsetzen bzw. Wiederingangsetzen, z. B. nach einer Störung der Anlage, muss der Schlüsselschalter S3 betätigt werden. Mithilfe des Tipp-Tasters S4 kann die Bedienperson im Störfall eine Palette aus dem Detektionsbereich der Lichtschranke und der Überbrückungssensoren herausfahren.
  Für einen störungsfreien Ablauf des Palettentransportes durch die Auslassöffnung hindurch müssen zwei Zeitvorgaben im SPS-Programm auf die Geschwindigkeit der Transportbewegung abgestimmt werden:
  – Die Zeitvorgabe T1 bestimmt die maximale Zeitspanne, innerhalb derer – nach Aktivierung des Sensors F1 – die Aktivierung des Sensors F2 und damit das Einleiten der Überbrückungsfunktion durch das Transportgut zu erfolgen hat.
  – Die Zeitvorgabe T2 wird mit dem Wiederfreiwerden des Sensors F2 gestartet. Sie muss so gewählt werden, dass K1 bei wieder frei gewordenem Schutzfeld der Lichtschranken erregt und wieder entregt wird, noch bevor Sensor F3 durch das Transportgut deaktiviert wird und damit die Überbrückungsfunktion beenden wird.
- Das Nichtabfallen der Hilfsschütze K2 und K3 wird wegen der vorhandenen Rückführung der zwangsgeführten Öffnerkontakte in den SPS-Eingang I1.1 spätestens vor einem erneuten Ingangsetzen des Bandantriebs bzw. der Palettieranlage aufgedeckt. Ein Versagen von K1 wird mit dem nächsten Auslass einer Palette aufgedeckt.
- Ein selbsttätiger unbeabsichtigter Anlauf des Bandantriebs bzw. der Palettieranlage bei einem Energieausfall mit anschließender Wiederkehr oder bei einem Versagen der Standard-SPS wird durch die Funktion der Anlauf- bzw. Wiederanlaufsperre verhindert. Die SPS kann die Wiederanlaufsperre nur direkt, nachdem die Palette die Lichtschranke passiert hat, also bei noch aktivierten Sensoren F3 und F4, aufheben.
- Das Versagen einzelner Überbrückungssensoren wird vom Programm der SPS entweder unmittelbar aufgedeckt (wegen Überwachung auf korrekten Ablauf von Aktivierung und Deaktivierung) oder macht sich während des Palettendurchlaufs betriebshemmend bemerkbar.
- Ein Versagen des Totmann-Tasters S4, der nur zur Störbeseitigung verwendet wird (Muting manuell), unterliegt einer unmittelbaren Erkennung durch die Bedienperson.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Die Hilfsschütze K1 bis K3 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Zuleitungen zur Lichtschranke F5 und zum Totmann-Taster S4 sind so verlegt, dass Kurzschlüsse einzelner Leitungen untereinander (auch zur Versorgungsspannung) ausgeschlossen werden können.
- Die Befehlsgeber S1 bis S4 sind außerhalb des Gefahrenbereichs und mit Einblick in den Gefahrenbereich angeordnet.
- Der Überbrückungszustand wird gut erkennbar für den Bediener am Zugang zum Gefahrenbereich von zwei Leuchtmeldern angezeigt.
- Die Überbrückungssensoren F1 bis F4 sind Standardkomponenten und in Elektronik ohne Software aufgebaut.

Bemerkungen

- Beispiel für die Ermöglichung einer automatischen Materialabfuhr bei der Absicherung der Zugänge von Palettierern und Depalettierern, Umsetzstationen, Umreifungs- oder Umwickelungsmaschinen. Das gleiche Prinzip lässt sich für Zugänge mit Materialzufuhr verwenden.
- Beim Einsatz von Überbrückungssensoren, die Mikrocontroller und Software ohne Sicherheitsbewertung durch den Hersteller enthalten (d. h. die Anforderungen für sicherheitsbezogene Embedded-Software sind nicht erfüllt), müssen im angestrebten PL = d in den beiden Kanälen Bauteile mit diversitären Technologien zur Anwendung kommen.
- Nach DIN EN 415-4 kann vorausgesetzt werden, dass ein unbemerkter Zutritt von Personen durch Einlauf- bzw. Auslauföffnungen ausreichend sicher verhindert ist, wenn u. a. folgende Anforderungen eingehalten sind:
  – Verwendung einer zwei- bis dreistrahligen Lichtschranke unter Beachtung der erforderlichen Montagehöhen (bei offenem Zugang bzw. vorhandener Leerpalette im Zugang) oder
  – bei überbrückter Schutzfunktion der Lichtschranke durch die beladene Palette mit seitlichen Öffnungsweiten < 0,2 m sowie einsetzender Überbrückung durch die Palettenladung erst unmittelbar vor dem Unterbrechen der Lichtstrahlen (ohne größere zeitliche und geometrische Lücken)

Berechnung der Ausfallwahrscheinlichkeit

Für die Ausgangsrelais der Überbrückungssensoren F1 bis F4 wird in der folgenden Berechnung ein DC von 0 % angenommen, da die zum Muting verwendeten Kontakte keiner automatischen Fehlererkennung unterliegen. Aus diesem Grunde ist eine manuelle periodische Überprüfung vorgesehen, die sich mit einfachen Mitteln realisieren lässt.

- $MTTF_D$: Für den Sensorteil der Mutingsensoren F1 bis F4 wird jeweils eine $MTTF_D$ von 100 Jahren [G] angenommen. Für die Ausgangsrelais von F1 bis F4 gilt ein B_{10D}-Wert von 2 000 000 Zyklen [G]. Bei 300 Arbeitstagen, 16 Arbeitsstunden und 200 Sekunden Zykluszeit ist für diese Elemente n_{op} = 86 400 Zyklen/Jahr und $MTTF_D$ = 232 Jahre. Die $MTTF_D$ des Kanals ergibt sich zu 35 Jahren („hoch“).
- DC_{avg}: DC = 90 % für den Sensorteil der Mutingsensoren F1 bis F4 wird durch die SPS-Überwachung erreicht. Der DC für die Ausgangsrelais wird zur sicheren Seite mit 0 % abgeschätzt. Der daraus ermittelte DC_{avg}-Wert beträgt 63 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (35 Jahre) und niedrigem DC_{avg} (63 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle PFH_D von $5{,}2 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN EN 415-4: Sicherheit von Verpackungsmaschinen – Teil 4: Palettierer und Depalettierer (08.97) und Berichtigung 1 (03.03). Beuth, Berlin 1997 und 2003
- DIN EN 415-10: Sicherheit von Verpackungsmaschinen – Teil 10: Allgemeine Anforderungen (07.14). Beuth, Berlin 2014
- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (05.14) und Berichtigung 1 (08.15). Beuth, Berlin 2014 und 2015
- DIN EN 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (06.14). Beuth, Berlin 2014
- DIN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zum Erkennen von Personen (Normentwurf) (04.13). Beuth, Berlin 2013
- DIN EN ISO 13855: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (10.10). Beuth, Berlin 2010

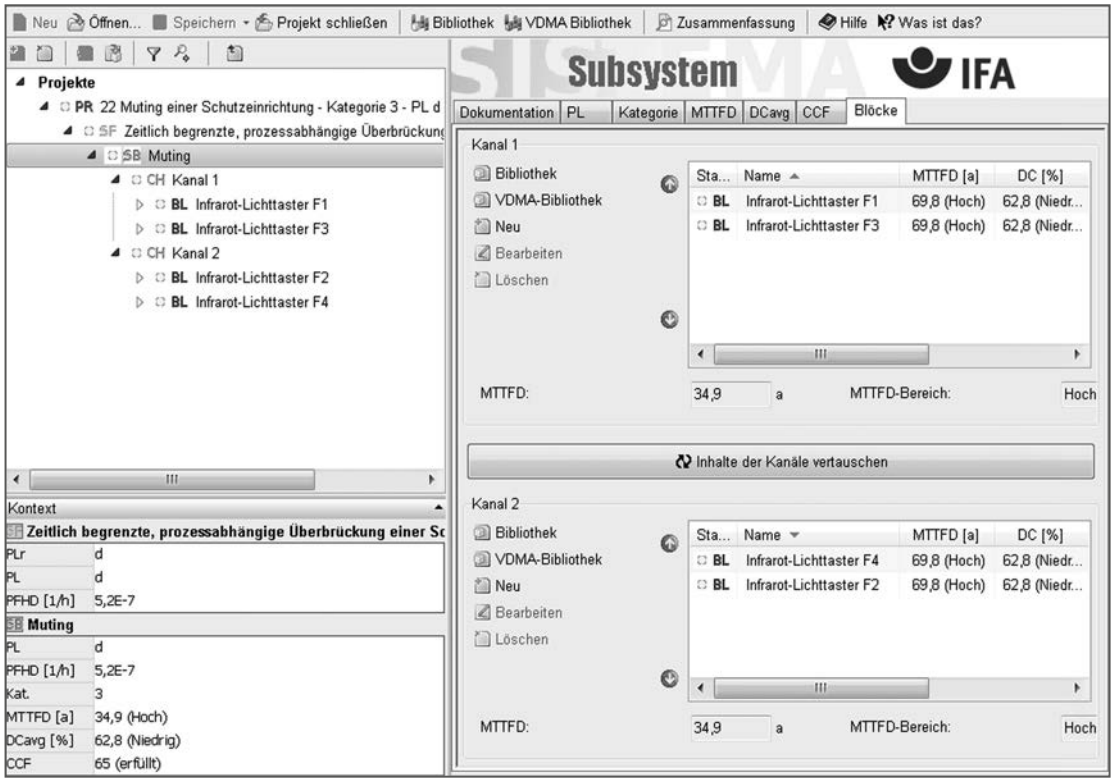


Abbildung 8.45: PL-Bestimmung mithilfe von SISTEMA

8.2.23 Karusselltürsteuerung – Kategorie 3 – PL d (Beispiel 23)

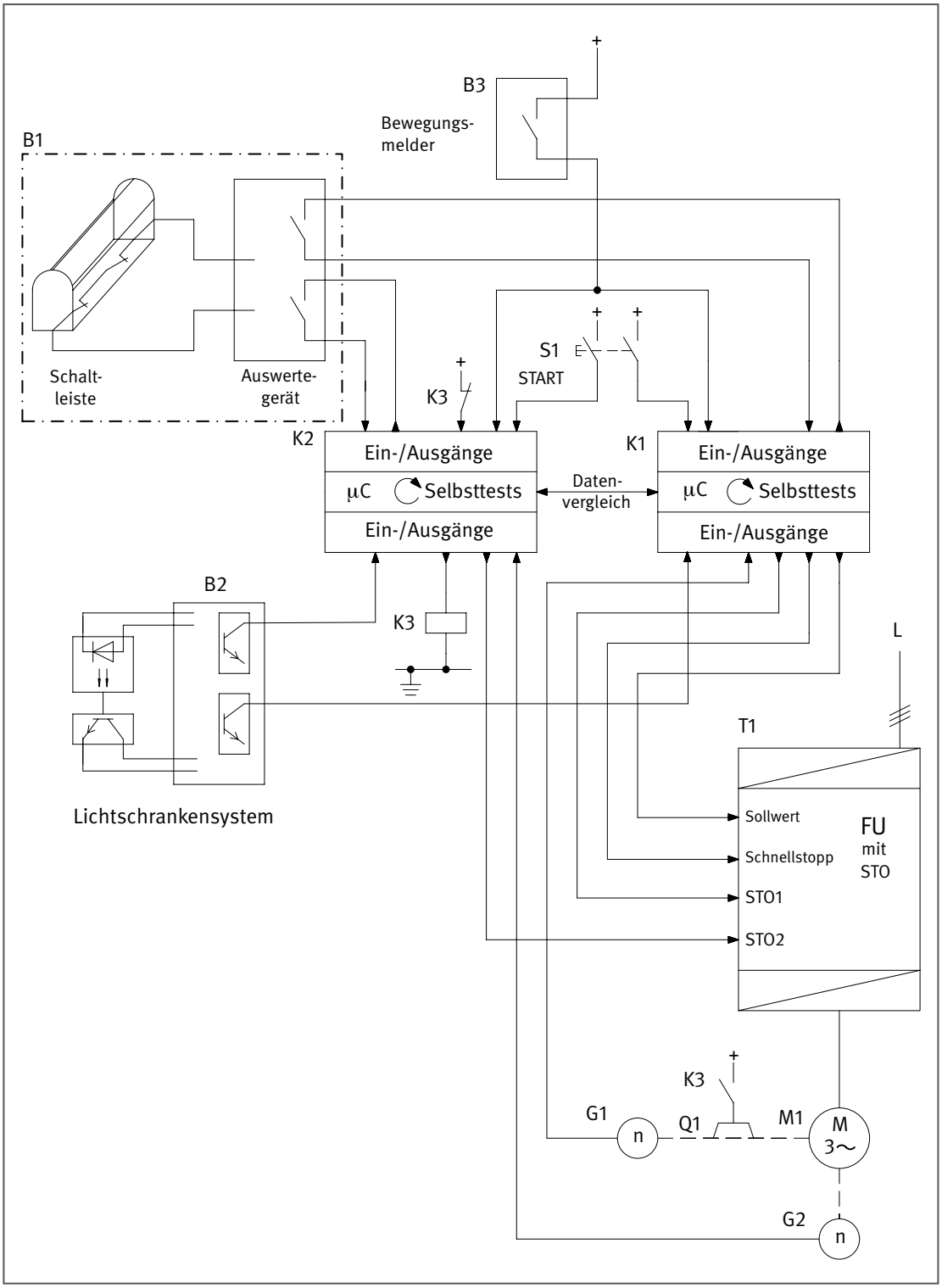
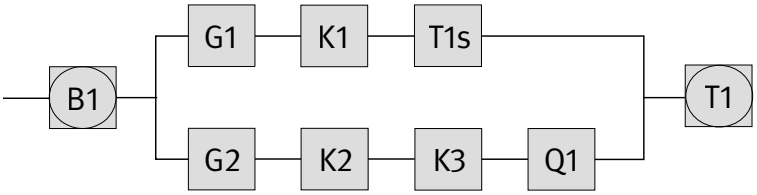


Abbildung 8.46: Karusselltür-steuerung mit Mikrocontrollern



Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Bei Betätigung der Schaltleiste wird die Drehbewegung der Karusselltür stillgesetzt (SS1-r – Sicherer Stopp 1 mit Rampenüberwachung). Diese Sicherheitsfunktion ist im sicherheitsgerichteten Blockdiagramm dargestellt.
- Sicher begrenzte Geschwindigkeit (SLS): Bei Detektion einer Person oder eines Gegenstandes durch die Lichtschranke wird die Geschwindigkeit der Karusselltür reduziert und sicher begrenzt.

Funktionsbeschreibung

- Die Drehbewegung der Karusselltür wird erstmals nach dem Einschalten der Steuerung durch den Taster S1 eingeleitet. Im Normalbetrieb erfolgt die Anforderung zur Drehung über den an der Tür befindlichen Bewegungsmelder B3. Der Frequenzumrichter T1 wird gemeinsam durch die beiden Mikrocontroller K1 und K2 angesteuert. Jeder Mikrocontroller (µC) beinhaltet einen Mikroprozessor (CPU) als Recheneinheit sowie Arbeits- (RAM) und Festwertspeicher (ROM). K1 steuert die Funktionen der Sollwertvorgabe, von STO1 sowie des Schnellstopps (T1s). Durch K2 wird STO2 angesteuert und die Bremse Q1 kann mithilfe des Hilfsschützes K3 gelöst werden. Die Drehgeber G1 und G2 übermitteln die Motordrehzahl an K1 bzw. K2. Die redundante Drehzahlüberwachung wird für beide Sicherheitsfunktionen (für die Rampenüberwachung und für die SLS) benötigt und dient auch zur Überwachung des Frequenzumrichters T1.
- Fehler in der Schaltleiste bzw. der Lichtschranke werden in den zugehörigen Auswertegeräten erkannt. Dies gilt auch für Fehler in den Auswertegeräten, die durch interne Überwachung erkannt werden. Fehler in den Komponenten der Mikrocontroller werden über Selbsttests bzw. durch Datenvergleich erkannt. Aufgedeckte Fehler führen, gesteuert über K1 und/oder K2, zur Stillsetzung der Türdrehbewegung durch T1 und/oder Q1. Zur Befreiung eingeschlossener Personen können die Türflügel von Hand geklappt werden.
- Durch redundante Verarbeitungskanäle führt ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktionen. Die Kombination unerkannter Fehler kann zum Verlust der Sicherheitsfunktionen führen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Die Schaltleiste dient der Absicherung von Quetsch-, Scher- und Einzugsstellen. Die Schaltleiste und das Auswertegerät werden als eine Einheit (B1) betrachtet. Das Teilsystem B1 erfüllt die Anforderungen nach DIN EN ISO 13856-2 in Kategorie 3 und nach DIN EN ISO 13849-1 für PL d. Fehler im Signalgeber der Schaltleiste bzw. in den Zuleitungen müssen ausgeschlossen oder über das Auswertegerät erkannt werden können (es können Schaltleisten, die nach dem Öffner- oder Schließer-Prinzip arbeiten, verwendet werden). Nach Entlastung einer zuvor betätigten Schaltleiste erfolgt ein automatischer zeitverzögerter Wiederanlauf der Drehbewegung. Die Schaltleiste verfügt über einen hinreichenden Verformungsweg und einen ausreichenden Wirkbereich.
- Die Lichtschranke dient der voreilenden, berührungslos wirkenden Absicherung von Gefahrstellen. Das Lichtschrankensystem B2 erfüllt die Anforderungen für Typ 4 nach DIN EN 61496-1 und DIN EN 61496-2 sowie für PL e nach DIN EN ISO 13849-1. Die nach der Detektion einer Person oder eines Gegenstandes durch die Lichtschranke eingenommene reduzierte, sicher begrenzte Geschwindigkeit wird nach einer voreingestellten Zeit wieder auf Normaldrehgeschwindigkeit erhöht. Die Zuleitungen zu Sender und Empfänger sind getrennt oder geschützt verlegt.
- Während des ersten Anlaufs der Türdrehbewegung werden Einschalttests durchgeführt. Dabei werden unter anderem die Blöcke der Mikrocontroller (Mikroprozessor, Arbeits- und Festwertspeicher) getestet, Ein- und Ausgangstests durchgeführt sowie die Ansteuerung des Motors über den Frequenzumrichter überprüft (u. a. Test der Funktionen Schnellstopp sowie STO1/STO2). Ebenfalls findet ein Bremsentest statt, bei dem der Frequenzumrichter gegen die eingefallene Bremse arbeiten muss.
- Im Rahmen des Datenvergleichs zwischen den beiden Controllern erfolgt der Austausch von Sollwerten und Zwischenergebnissen unter Einbeziehung der zyklisch durchgeführten Selbsttests.
- Durch die Verwendung eines Frequenzumrichters mit STO ist der Einsatz eines Schützes zum Abschalten der Versorgungsspannung nicht erforderlich. Der Frequenzumrichter ist zum Antreiben und Bremsen geeignet.
- K3 besitzt zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Die Schaltstellung des Öffnerkontaktes wird vom Mikrocontroller K2 zur Fehleraufdeckung überwacht.

- Bei dem Beispiel wird davon ausgegangen, dass zur Bremsung der Karusselltür die Regelung über den Frequenzumrichter T1 hinreichend ist. Nach Erreichen des Stillstandes wird zur Vermeidung des unerwarteten Anlaufes STO aktiviert. Bremszeit und Bremsweg werden von der Steuerung überwacht (Rampenüberwachung). Die Bremse Q1 im zweiten Kanal ist im Fehlerfall erforderlich, damit es nach einem Fehler, wenn T1 den Schnellstopp T1S nicht mehr ausführen kann, zu keiner Gefährdung durch eine unerwartete Bewegung kommen kann. Q1 arbeitet nach dem Ruhestromprinzip.
- Programmierung der Software (SRESW) in K1 und K2 entsprechend den Anforderungen für PL d nach Abschnitt 6.3.
- Die Standardkomponenten G1, G2 (soweit für die Drehgeber zutreffend) und T1 werden entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.
- Für die betrachteten Sicherheitsfunktionen wird ein Fehlerausschluss für den Fehler Geberwellenbruch (G1/G2) angenommen. Einzelheiten zur Möglichkeit eines Fehlerausschlusses siehe z. B. DIN EN 61800-5-2, Tabelle D.8, bzw. GS-IFA-M21.

Bemerkungen

- Das Schaltungsbeispiel ist einsetzbar zur Realisierung der Sicherheitsfunktionen „Sicherheitsbezogene Stoppfunktion“ und „Sicher begrenzte Geschwindigkeit“ in einer Steuerung für drei- und vierflügelige Karusselltüren mit Break-Out-Funktion (Türflügel können im Notfall von Hand geklappt werden) für den Einsatz im öffentlichen und gewerblichen Bereich.
- Eine regelmäßige manuelle Überprüfung der Schaltleiste ist erforderlich. Zum einen muss die Funktionsfähigkeit überprüft werden und zum anderen ist eine optische Begutachtung der Schaltleiste notwendig, um Beschädigungen frühzeitig erkennen zu können.

Berechnung der Ausfallwahrscheinlichkeiten

Die detaillierte Berechnung der Ausfallwahrscheinlichkeit wird für die Sicherheitsfunktion „Sicherheitsbezogene Stoppfunktion (SS1-r)“, die auch im Blockdiagramm dargestellt ist, durchgeführt:

- Da die Schaltleiste mit zugehörigem Auswertegerät als käufliches Sicherheitsbauteil vorliegt, wird deren Ausfallwahrscheinlichkeit am Ende der Berechnung addiert ($3{,}0 \cdot 10^{-7}$/Stunde [G]).
- Der Frequenzumrichter T1 mit STO liegt ebenfalls als käufliches Sicherheitsbauteil vor, dessen Ausfallwahrscheinlichkeit am Ende der Berechnung addiert wird ($1{,}5 \cdot 10^{-8}$/Stunde [H]). Die Schnellstopp-Funktion T1s wird im ersten Kanal des Blockdiagramms modelliert.
- $MTTF_D$: Die sicherheitsrelevanten Bauteile von K1 und K2 einschließlich ihrer Peripherie werden nach Anwendung des „Parts Count“-Verfahrens mit einem Wert von 878 Jahren [G] berücksichtigt. Für G1 und G2 fließt ein Wert von 190 Jahren [H] in die Berechnung ein. Für T1s wird ein Wert von 100 Jahren [H] angesetzt. Für K3 wird ein B_{10D}-Wert von 400 000 Zyklen [N] angesetzt. Bei einer Betätigung pro Tag ergeben sich n_{op} = 365 Zyklen/Jahr und eine $MTTF_D$ = 10 959 Jahre. Für Q1 wird ein B_{10D}-Wert von 1 000 000 Zyklen [H] angesetzt, was zu einer $MTTF_D$ von 27 397 Jahren führt. Die Bremse Q1 ist nur im Fehlerfall erforderlich und unterliegt keinem betriebsmäßigen Verschleiß. Insgesamt ergibt sich ein symmetrisierter $MTTF_D$-Wert von 82 Jahren („hoch“) für die beiden Kanäle.
- DC_{avg}: Für K1 und K2 ergibt sich aufgrund interner Selbsttests und Vergleichs ein *DC* von 60 %. Interne Selbsttests der Komponenten der Mikrocontroller werden durchgeführt. Für den Block T1s resultiert aus der Rampenüberwachung ein *DC* von 99 %. G1 und G2 werden aufgrund des Vergleichs über K1 und K2 mit einem *DC* von 99 % bemessen. K3 wird entsprechend der direkten Überwachung eines zurückgelesenen zwangsgeführten Kontaktes mit einem *DC* = 99 % bemessen. Aufgrund des durchgeführten statischen Einschalttests wird für Q1 ein *DC* = 30 % angesetzt. Durch Mittelung ergibt sich damit ein DC_{avg} von 95 % („mittel“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ (82 Jahre) und mittlerem DC_{avg} (95 %). Es ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls PFH_D von $4{,}3 \cdot 10^{-8}$/Stunde. Zuzüglich der Sensoreinheit B1 – bestehend aus Schaltleiste und Auswertegerät – und dem Frequenzumrichter T1 beträgt die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls der Steuerung für diese Sicherheitsfunktion insgesamt $3{,}6 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Berechnung der Ausfallwahrscheinlichkeit für die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit (SLS)“

- Für diese Berechnung wird die Sensoreinheit B1 aus der ersten Beispielberechnung durch das Lichtschrankensystem B2 mit einer Ausfallwahrscheinlichkeit von $1{,}5 \cdot 10^{-9}$/Stunde [G] ersetzt. Durch Addition ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls der Steuerung für diese Sicherheitsfunktion von $6{,}0 \cdot 10^{-8}$/Stunde. Die Realisierung der Sicherheitsfunktion SLS entspricht PL d.

Weiterführende Literatur

- DIN EN ISO 13856-2: Sicherheit von Maschinen – Druckempfindliche Schutzeinrichtungen – Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltleisten und Schaltstangen (08.13). Beuth, Berlin 2013
- DIN 18650-1: Automatische Türsysteme – Teil 1: Produktanforderungen und Prüfverfahren (06.10). Beuth, Berlin 2010
- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (04.10). Beuth, Berlin 2010
- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (05/2014) und Berichtigung 1 (08.15). Beuth, Berlin 2014 und 2015
- DIN EN 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (06.14). Beuth, Berlin 2014
- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (2017). Beuth, Berlin 2017
- Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit (GS-IFA-M21). Hrsg.: Institut für Arbeitsschutz der DGUV, Prüf- und Zertifizierungsstelle im DGUV Test, Sankt Augustin 2015
  ▶ www.dguv.de, Webcode: d11973

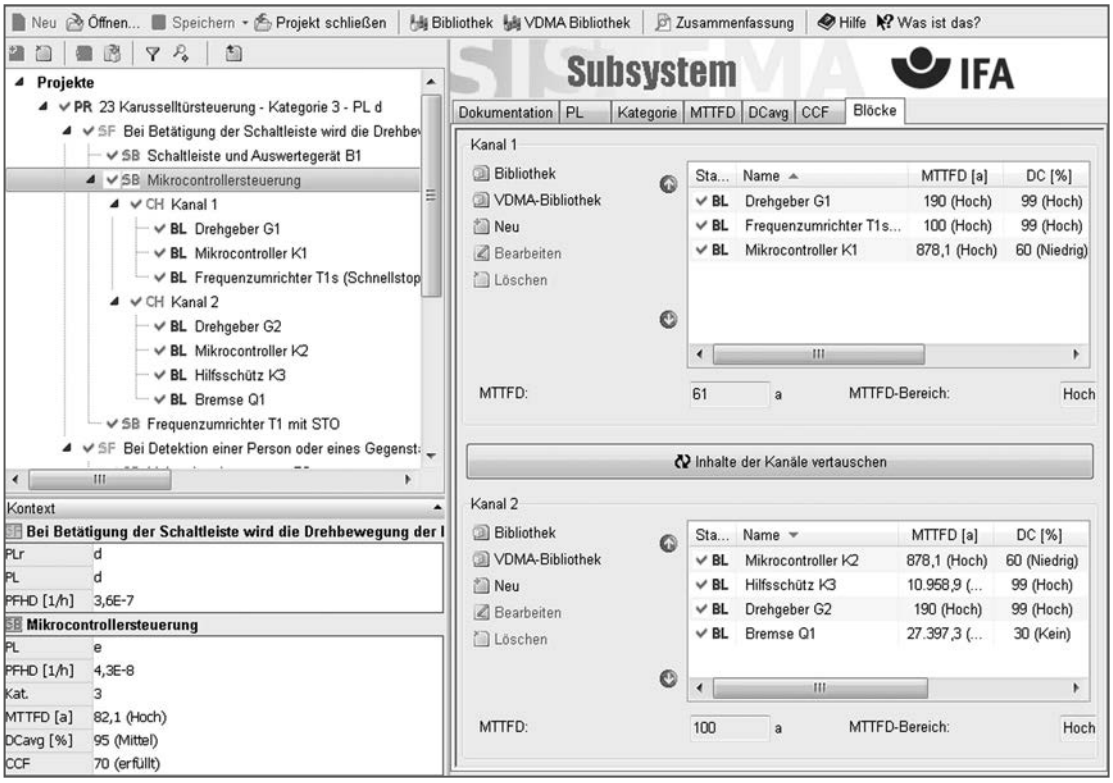
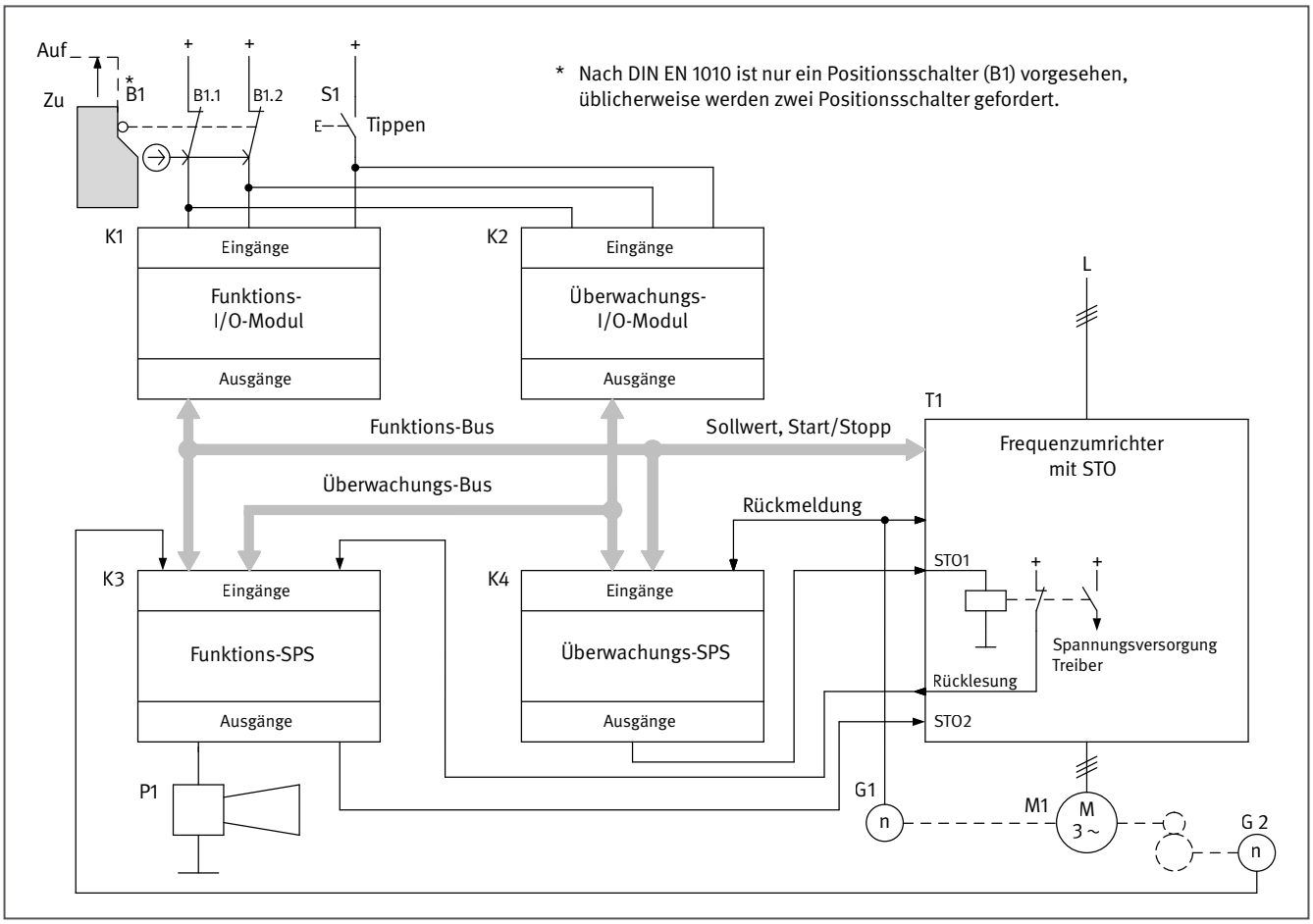


Abbildung 8.47:
PL-Bestimmung mithilfe von SISTEMA

8.2.24 Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine – Kategorie 3 – PL d bzw. c (Beispiel 24)

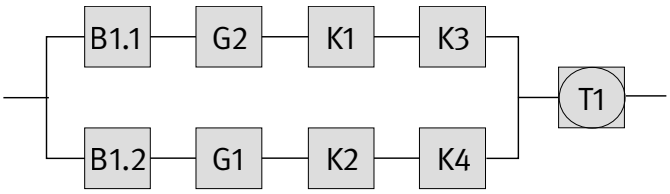
Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):
- B1 wurde durch eine Variante mit zwei zwangsöffnenden Kontakten ersetzt (statt Öffner-Schließer-Kombination).
- Ein zweiter Geber G2 auf der Maschinenwelle wurde zum vorhandenen Geber G1 auf der Motorwelle hinzugefügt.
- Der Frequenzumrichter T1 wurde durch eine Variante mit integrierter Sicherheitsfunktion STO ersetzt.
- Das Kategorie-3-Subsystem B1 wurde mit dem nachfolgenden Kategorie-3-Subsystem aus G1, G2 und K1 bis K4 zusammengefasst.

Abbildung 8.48:
Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine durch eine zweikanalige Rechnersteuerung



Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Beim Öffnen der Schutztür soll der Antrieb anhalten (SS1-r – Sicherer Stopp 1, Überwachung Bremsrampe und STO nach Stillstand).
- Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür dürfen Maschinenbewegungen nur mit begrenzter Drehzahl erfolgen.
- Tippbetrieb: Bei geöffneter Schutztür sind Bewegungen nur während der Betätigung eines Tipptasters möglich.



Funktionsbeschreibung

- Das dezentrale I/O-Modul K1 erfasst die Zustände des an der Schutzeinrichtung befestigten Positionsschalters mit Personenschutzfunktion B1 und des Tipptasters S1 und stellt diese auf dem Funktionsbus als Information zur Verfügung. Diese Information wird durch die Funktions-SPS K3 ausgewertet und führt beim Öffnen der Schutztür zur Einleitung der Stoppfunktion am Frequenzumrichter T1. Dazu wird über den Funktionsbus ein Signal zum schnellstmöglichen Stillsetzen gegeben. Redundant zu K1 und K3 arbeiten das I/O-Modul K2 und die Überwachungs-SPS K4, die über einen eigenen Überwachungsbus kommunizieren. Die Bremsrampe wird in der Funktions-SPS K3 über den Geber G2 und in der Überwachungs-SPS K4 über den Geber G1 kontrolliert. Nach Stillstand oder im Falle eines erkannten Fehlers beim Stillsetzen wird durch K3 und K4 über die beiden STO-Eingänge STO1 und STO2 von T1 die integrierte Sicherheitsfunktion STO ausgelöst.
- Der offene Zustand der Schutzeinrichtung wird über B1, K1 und K2 wie oben beschrieben in K3 und K4 erfasst. K3 und K4 sorgen dann redundant zueinander mittels G2 bzw. G1 für eine Überwachung der spezifizierten begrenzten Geschwindigkeit (SLS). Falls diese überschritten wird, leiten K3 und K4 unabhängig voneinander wie oben beschrieben den SS1-r ein.
- Bei betätigtem B1 ist nur ein Tippbetrieb über S1 mit sicher begrenzter Geschwindigkeit erlaubt. Das Loslassen von S1 wird redundant in K1 bis K4 erfasst und führt, wie oben für die sicherheitsbezogene Stoppfunktion und SLS beschrieben, zum Sicheren Stopp 1 des Antriebs (SS1-r).
- Entsprechend DIN EN 1010-1 ist ein einziger Positionsschalter B1 ausreichend. Die meisten Fehler in S1 werden durch einen besonderen Betätigungsablauf, der einen Signalwechsel erzwingt, aufgedeckt und beherrscht: Nach erstmaliger Betätigung von S1 erfolgt eine akustische Warnung (Signalgeber P1), erst nach Loslassen und erneutem Betätigen das verzögerte Anlaufen des Antriebs.
- Fehler in K1 und K2 werden durch Zustandsvergleich in K4 erkannt. K4 überwacht auch K3 durch Mithören der Eingangs- und Ausgangsinformationen. Ein Teil der Fehler in K3 wird zusätzlich durch Fehler im Prozess offenbart. In K4 finden Selbsttests (z. B. zeitliche Programmlaufüberwachung durch internen Watchdog) statt, außerdem benutzt K3 K4 zur regelmäßigen Anwahl von STO1 und überwacht das Rücklesesignal von T1.
- Der Frequenzumrichter T1 bildet mit dem Sin/Cos-Geber G1 ein Regelsystem, in dem Fehler durch den hochsynchronen Produktionsprozess offenbart werden (Fehldruck, Papierriss). Die Gebersignale von G1 auf der Motorwelle werden auch in K4 eingelesen und in T1 auf Plausibilität der Sin/Cos-Information (Sin2 + Cos2 = 1) überwacht. Redundant dazu werden die Signale eines diversitären Gebers G2 auf der Maschinenwelle ausgewertet. Obwohl beide Geber nicht auf derselben Welle sitzen, können ihre in K4 bzw. K3 eingelesenen und in Papiergeschwindigkeiten umgerechneten Werte in K4 miteinander verglichen werden und führen so zu einer Fehlererkennung für G1 und G2. Fehlererkennung für STO1 in T1 erfolgt durch ein bereitgestelltes Rücklesesignal, das in K3 ausgewertet wird. Die korrekte Abarbeitung von STO2 wird durch T1-interne Testmaßnahmen überwacht, die im Fehlerfall einen Stillstand einleiten.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Die Öffner von B1 entsprechen DIN EN 60947-5-1, Anhang K, und B1 ist in Übereinstimmung mit der DGUV Information 203-079 „Auswahl und Anbringung von Verriegelungseinrichtungen“ installiert. Maßnahmen zur Verhinderung der Lageänderung und der vernünftigerweise vorhersehbaren Manipulation sind realisiert (siehe DIN EN 14119). Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.
- S1 entspricht DIN EN 60947-5-1, sodass der Kurzschluss von benachbarten Kontakten, die voneinander isoliert sind, ausgeschlossen werden kann. Trotz Anlaufwarnung und Dynamisierung kann S1 während des Tippbetriebs hängen bleiben. Daher muss in Reichweite der Bedienperson zusätzlich ein Not-Halt-Gerät installiert sein.
- Für die Anschlussleitungen von S1 müssen die Bedingungen eines Fehlerausschlusses für Leitungskurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4, eingehalten werden. Fehler in den Anschlussleitungen von B1 werden durch eine Überwachung in K4 erkannt.
- Die programmierbaren Komponenten K1 bis K4 erfüllen die normativen Anforderungen gemäß Abschnitt 6.3.
- G1 ist in den Regelkreis eingebunden (Gewinnung der Kommutierung). Der diversitäre Geber G2 dient zur Fehlererkennung.
- Der Einsatz der Standardkomponenten G1 und G2 erfolgt entsprechend den Hinweisen aus Abschnitt 6.3.10.

- T1 besitzt eine integrierte Sicherheitsfunktion STO, die alle Anforderungen für Kategorie 3 und PL d erfüllt. Die erforderliche Fehlererkennung wird durch ein bereitgestelltes und extern überwachtes Rücklesesignal für STO1 und interne Überwachungsmaßnahmen für STO2 erreicht.
- Der Einsatz der Bussysteme (Funktionsbus, Überwachungsbus) erfolgt entsprechend den Hinweisen aus Abschnitt 6.2.18.

Bemerkungen

- Dieses Beispiel beschreibt die Absicherung von Einzugsstellen an Rotationsdruckmaschinen. Die Anwendung der DIN EN 1010-1 erfordert für nicht zyklischen Eingriff in den Gefahrenbereich, d. h. weniger als einen Eingriff pro Stunde, nur einen Positionsschalter für die Stellungsüberwachung der trennenden Schutzeinrichtung. Das Kriterium der Fehlertoleranz für Kategorie 3 erfordert für vergleichbare Maschinensteuerungen üblicherweise die Verwendung von zwei Positionsschaltern.
- Für den Tippbetrieb unter der Voraussetzung bereits gewährleisteter sicher begrenzter Geschwindigkeit kann unter bestimmten Bedingungen von der Möglichkeit zur Vermeidung der Gefährdung ausgegangen werden. Siehe zur Risikobeurteilung auch Beispiel 4 in Anhang A.

Berechnung der Ausfallwahrscheinlichkeit

- Die drei Sicherheitsfunktionen unterscheiden sich nur in der Sensorebene. B1, G1 und S1 werden daher separat beschrieben.
- Die beiden zwangsöffnenden Kontakte von B1 sind in die nachfolgende Kategorie-3-Struktur eingebunden. Pro Kontakt wird ein B_{10D}-Wert von 20 000 000 Zyklen [N] angenommen. Bei wöchentlich 10-facher Betätigung ist n_{op} = 520 Zyklen/Jahr und $MTTF_D$ = 384 615 Jahre. Unter den besonderen Anforderungen der DIN EN 1010-1 an B1 (siehe konstruktive Merkmale) wird ein *DC* von 60 % (Kreuzvergleich von Eingangssignalen ohne dynamischen Test, seltener Signalwechsel durch die Anwendung) unterstellt.
- G1 und G2 sind ebenfalls in je einen Kanal der nachfolgenden Kategorie-3-Struktur eingebunden. Sie gehen mit 30 Jahren $MTTF_D$ pro Kanal [H], 90 % *DC* für G2 durch Plausibilitätsprüfung und 99 % *DC* für G1 durch Überwachung auf $Sin^2 + Cos^2 = 1$, Plausibilitätsprüfung und Fehlererkennung im Prozess in die Bestimmung der PFH_D ein.
- S1 besitzt einen B_{10D}-Wert von 100 000 Zyklen [H]. Bei wöchentlich 10-facher Betätigung ist n_{op} = 520 Zyklen/Jahr und $MTTF_D$ = 1923 Jahre. Wegen erzwungenen Signalwechsels und Anlaufwarnung wird S1 als ein Kategorie-2-Subsystem modelliert und ein *DC* von mindestens 60 % angenommen (ein Hängenbleiben nach wiederholtem Tippen wird aber nicht erkannt). Die Testung erfolgt in K1 und K3, deren Ausfallwahrscheinlichkeit bereits in das nachfolgende Kategorie-3-Subsystem eingeht und daher nicht zusätzlich im Testkanal berücksichtigt werden muss. Um keine Fehlermeldung in SISTEMA zu provozieren, wird im Testkanal ein $MTTF_D$-Wert von 100 Jahren eingesetzt. Da die Testung unmittelbar bei der Anforderung der Sicherheitsfunktion erfolgt, ist eine ausreichende Testhäufigkeit gegeben. S1 erreicht damit als separates Subsystem eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}3 \cdot 10^{-7}$/Stunde. Da es nicht praktikabel ist, dass die Steuerung bei einem Hängenbleiben des Tippschalters automatisch den sicheren Zustand herbeiführt und der PL_r nicht größer als c ist, ist auch die Einbindung der Bedienperson erlaubt (siehe Abschnitt 6.2.5).
- K1 und K3 sowie K2 und K4 gehen in zwei Kanälen eines Kategorie-3-Subsystems in alle drei betrachteten Sicherheitsfunktionen ein. Hinsichtlich $MTTF_D$ werden 100 Jahre [H] für K1 und K2, 50 Jahre [H] für K4 und 30 Jahre [H] für K3 in Rechnung gestellt. *DC* = 99 % für K1 und K2 ergibt sich durch den direkten Vergleich der bereitgestellten Zustandsinformationen in K4. *DC* = 99 % für K3 gründet sich auf die parallele Verarbeitung aller sicherheitsrelevanten Informationen in K4 und den dortigen direkten Vergleich mit den von K3 gebildeten Zwischenergebnissen und Ausgangssignalen. Die in K4 umgesetzten Selbsttests plus partielle Überwachung durch die von K3 zurückgelesene Anwahl von STO1 führen für K4 auf einen *DC* von 60 %.
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- T1 geht mit seiner integrierten Sicherheitsfunktion STO als gekapseltes Subsystem mit Kategorie 3, PL d und einer PFH_D von $1{,}5 \cdot 10^{-10}$/Stunde ein.
- Die sicherheitsbezogene Stoppfunktion und die sicher begrenzte Geschwindigkeit werden durch ein durchgängiges Kategorie-3-Subsystem aus B1.1/B1.2, G2/G1 und K1 bis K4 realisiert, das mit T1 als gekapseltem Kategorie-3-Subsystem kombiniert wird. Für das erste Subsystem ergibt sich mit einer mittleren $MTTF_D$ pro Kanal von 14,5 Jahren und mittlerem DC_{avg} von 91 % eine PFH_D von $7{,}1 \cdot 10^{-7}$/Stunde. Durch Kombination mit T1 ($PFH_D = 1{,}5 \cdot 10^{-10}$/Stunde) ergibt sich für beide Sicherheitsfunktionen eine PFH_D von $7{,}1 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.
- Der Tippbetrieb wird durch eine Kombination des Kategorie-2-Subsystems S1 ($PFH_D = 5{,}3 \cdot 10^{-7}$/Stunde) mit den beiden Kategorie-3-Subsystemen aus T1 ($PFH_D = 1{,}5 \cdot 10^{-10}$/Stunde) und G2/G1 mit K1 bis K4 umgesetzt. Das zweite Kategorie-3-Subsystem erreicht mit einer mittleren $MTTF_D$ pro Kanal von 14,5 Jahren und mittlerem DC_{avg} von 91 % eine PFH_D von $7{,}1 \cdot 10^{-7}$/Stunde. Die Kombination der drei Subsysteme ergibt eine PFH_D von $1{,}2 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Gemeinsame Anforderungen (11.06). Beuth, Berlin 2011
- Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitungsmaschinen. Mechanik. Hrsg.: Berufsgenossenschaft Druck und Papierverarbeitung, Wiesbaden 2004
  ▸ http://dp.bgetem.de/pages/service/download/medien/BG_220-1_DP.pdf
- *Apfeld, R.; Zilligen, H; Köhler, B.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 7/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Sankt Augustin 2013
  ▸ www.dguv.de/ifa, Webcode: d639540
- Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit (GS-IFA-M21). Hrsg.: Institut für Arbeitsschutz der DGUV, Prüf- und Zertifizierungsstelle im DGUV Test, Sankt Augustin 2015
  ▸ www.dguv.de, Webcode: d11973
- DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015
  ▸ http://publikationen.dguv.de/dguv/pdf/10002/203-079.pdf

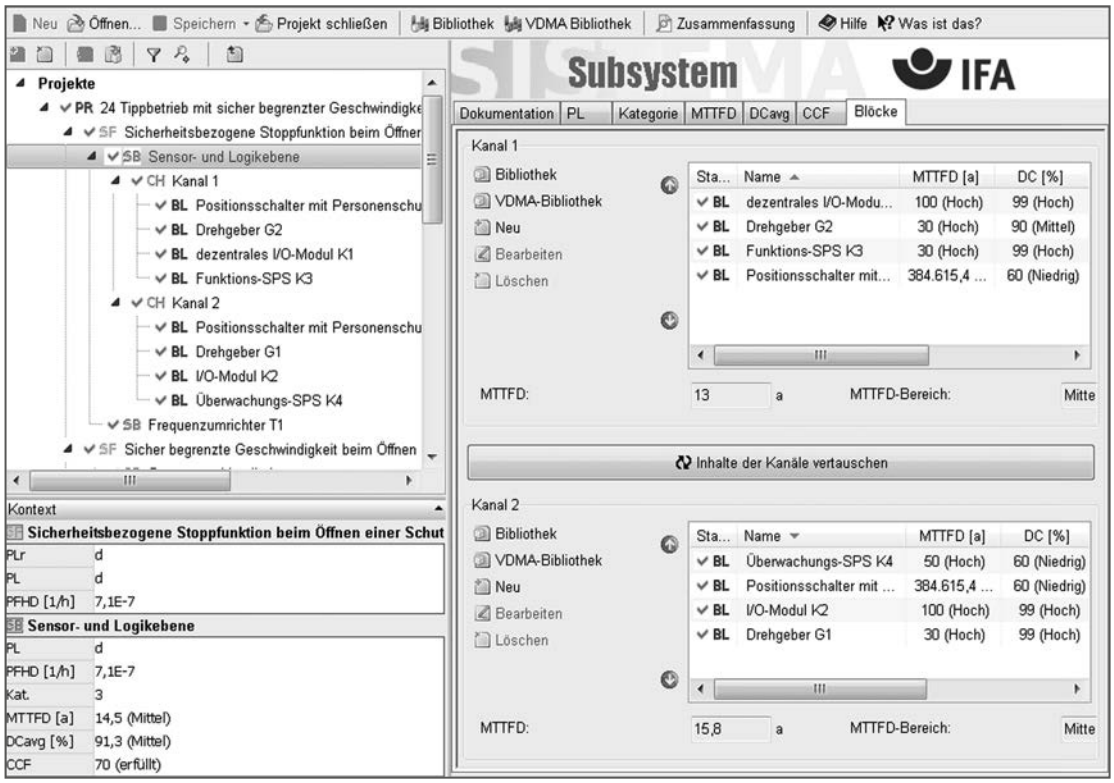


Abbildung 8.49: PL-Bestimmung mithilfe von SISTEMA

8.2.25 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 3 – PL e (Beispiel 25)

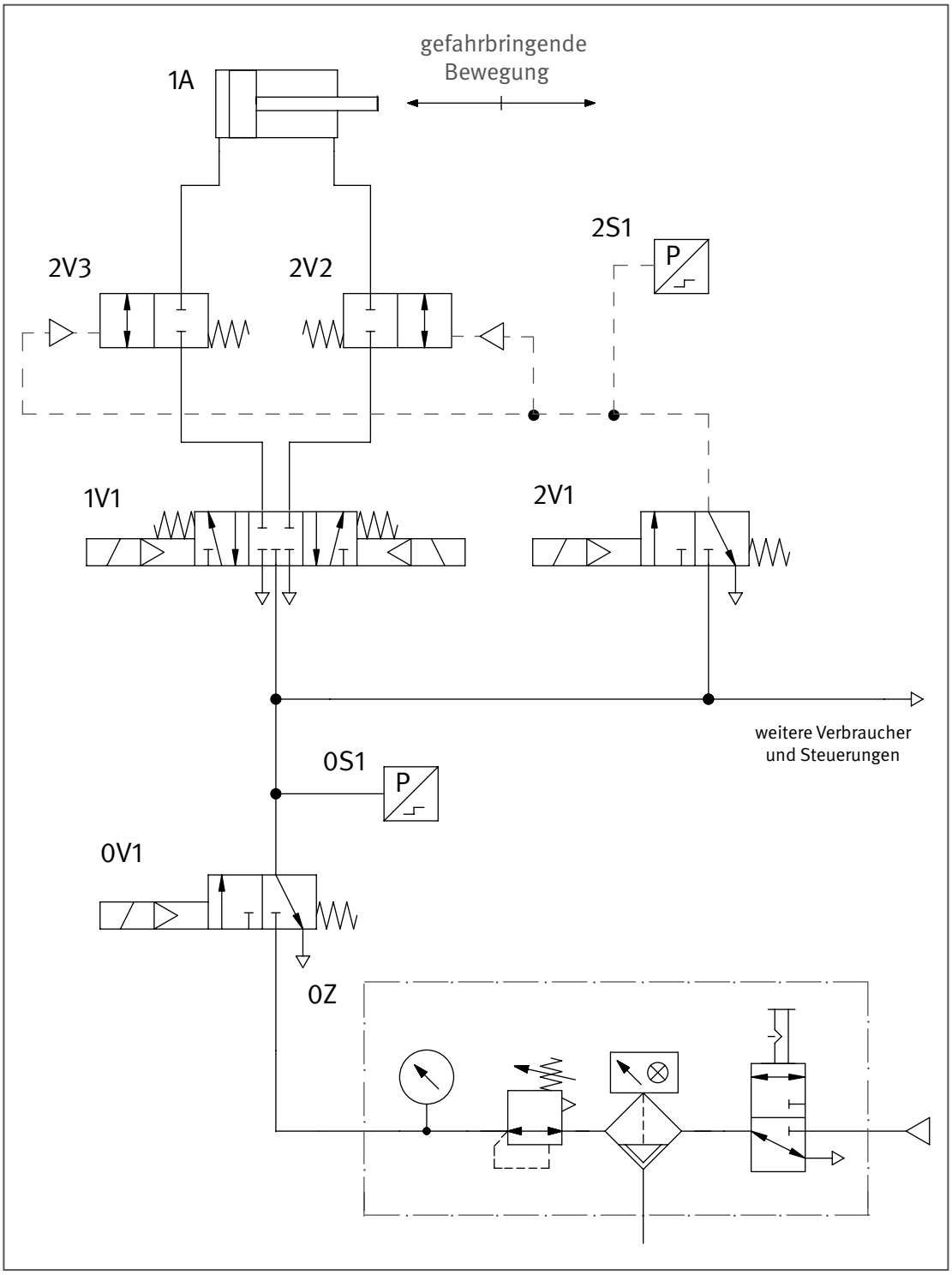
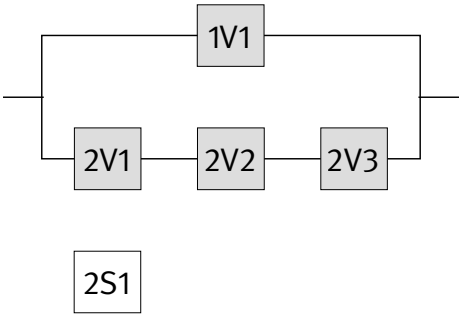


Abbildung 8.50: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen



Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage, realisiert durch SSC
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden redundant durch Wegeventile gesteuert. Ein Stillsetzen kann entweder durch das Wegeventil 1V1 oder durch die Wegeventile 2V2 und 2V3 erfolgen. Letztere werden durch das Steuerventil 2V1 angesteuert.
- Der alleinige Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- Alle Wegeventile werden zyklisch im Prozess angesteuert.
- Die Funktion des Steuerventils 2V1 wird durch einen Druckschalter 2S1 überwacht. An den nicht überwachten Ventilen werden einige Fehler im Arbeitsprozess erkannt. Die Ventile 2V2 und 2V3 sollten eine Stellungsüberwachung aufweisen oder – da diese noch nicht Stand der Technik ist – es muss eine regelmäßige Überprüfung der Funktion durchgeführt werden. Eine Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.
- Kann durch eingesperrte Druckluft eine weitere Gefährdung auftreten, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Das Wegeventil 1V1 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung.
- Die Sperrventile 2V2 und 2V3 sind möglichst im Zylinder eingeschraubt und vorgesteuert über das Ventil 2V1.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung der Drucküberwachung 2S1 erfolgt z. B. in einer einkanaligen SPS.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für die Ventile 1V1, 2V1, 2V2 und 2V3 werden B_{10D}-Werte von 20 000 000 Zyklen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 20 Sekunden Zykluszeit ist n_{op} = 691 200 Zyklen/Jahr. Damit beträgt die $MTTF_D$ für 1V1, 2V1, 2V2 und 2V3 289 Jahre. Nach Kürzen beider Kanäle auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_D$-Wert pro Kanal von 98 Jahren („hoch“).
- DC_{avg}: DC = 99 % für 2V1 ergibt sich aus der Drucküberwachung des Steuersignals für die Sperrventile. DC = 60 % für 1V1 ergibt sich aus der Fehlererkennung über den Prozess und DC = 60 % für 2V2 bzw. 2V3 aus der regelmäßigen Überprüfung der Funktion. Durch Mittelung ergibt sich damit ein DC_{avg} von 69,8 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ (98,2 Jahre) und niedrigem DC_{avg} (69,8 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $8{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMV Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (08.16). Beuth, Berlin 2016
- *Uppenkamp, J.*: Teil-Sicherheitsfunktionen nach VDMA-Einheitsblatt 24584 – Beispiele zweikanaliger elektropneumatischer Steuerungen. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (DGUV), Sankt Augustin 2017. ► www.dguv.de/ifa, Webcode: d1029520

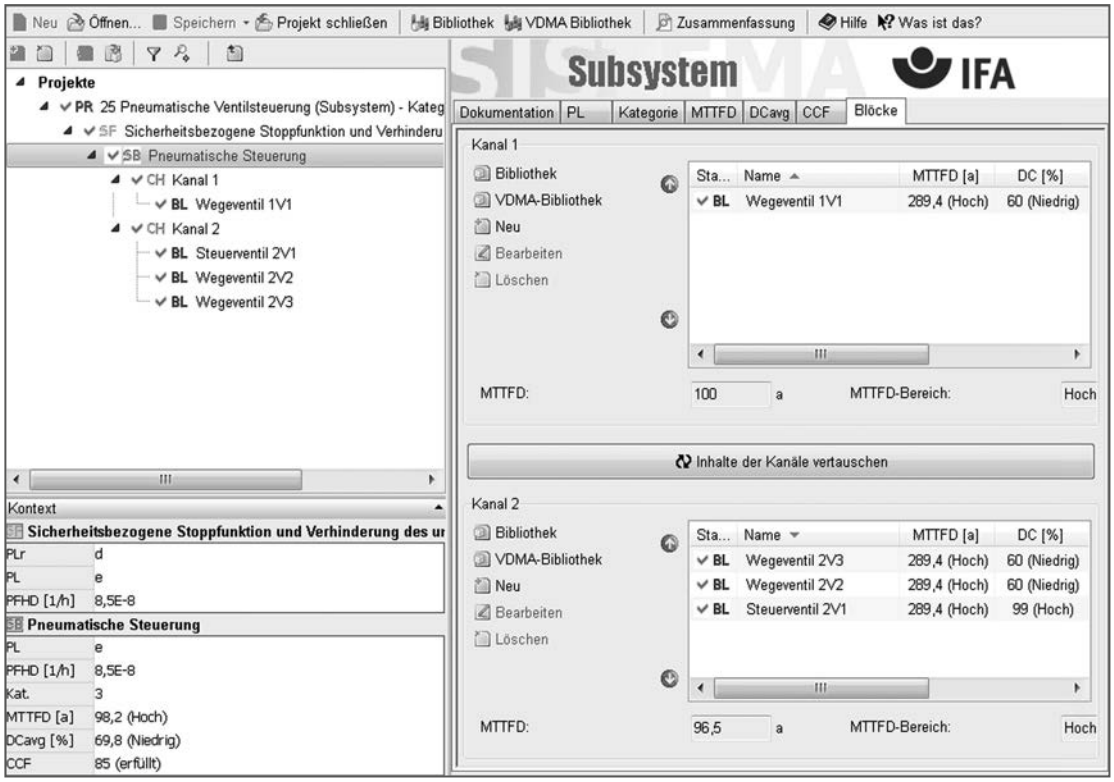


Abbildung 8.51: PL-Bestimmung mithilfe von SISTEMA

8.2.26 Pneumatische Ventilsteuerung – Kategorie 3 – PL e (Beispiel 26)

Dieses Beispiel entfällt, da es technologisch nicht mehr relevant ist.

8.2.27 Hydraulische Ventilsteuerung (Subsystem) – Kategorie 3 – PL e (Beispiel 27)

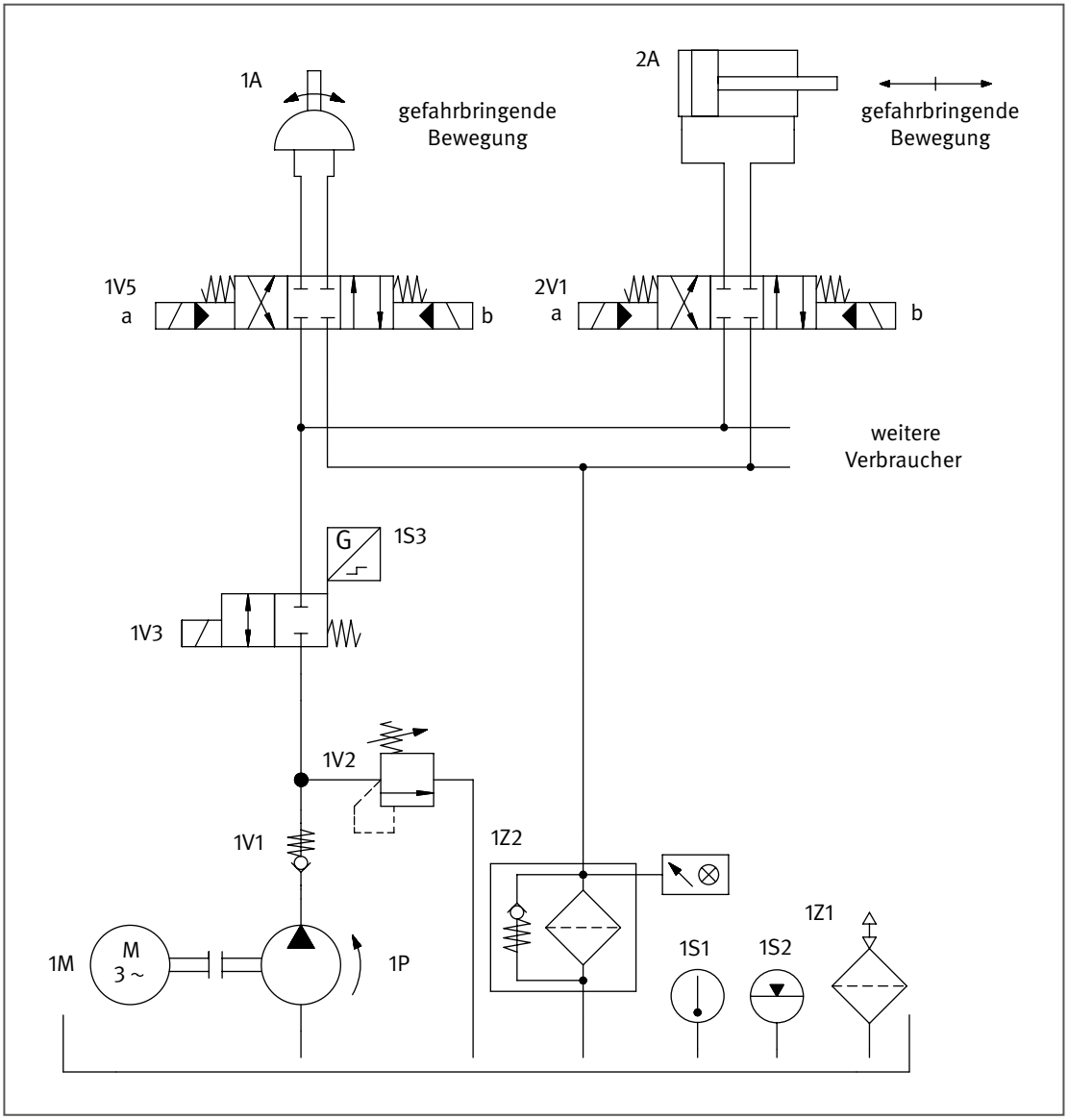


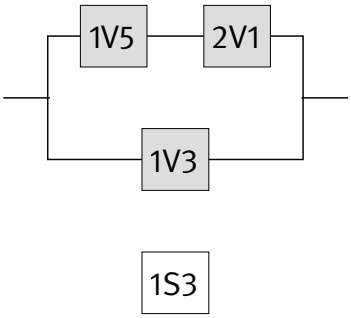
Abbildung 8.52: Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch zwei Aktoren 1A und 2A in demselben Gefahrenbereich ausgeführt. Ein Stillsetzen beider Bewegungen kann entweder durch die beiden Wegeventile 1V5 und 2V1 oder übergeordnet durch das Wegeventil 1V3 erfolgen.
- Der alleinige Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- 1V5 und 2V1 werden zyklisch im Prozess angesteuert, 1V3 schließt nur bei Anforderung der Sicherheitsfunktion, jedoch mindestens einmal pro Schicht.
- Eine technische Maßnahme zur Fehlererkennung ist nur an 1V3 vorgesehen (Stellungsüberwachung 1S3). An den nicht überwachten Ventilen werden einige Fehler im Arbeitsprozess erkannt. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Die Wegeventile 1V5 und 2V1 haben eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung. 1V3 ist mit elektrischer Stellungsüberwachung ausgeführt, da 1V3 nicht zyklisch geschaltet wird.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals (elektrisch bzw. hydraulisch) erreicht.
- Die Signalverarbeitung der elektrischen Stellungsüberwachung erfolgt z. B. in einer einkanaligen SPS.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für die Wegeventile 1V3, 1V5 und 2V1 wird eine $MTTF_D$ von 150 Jahren angenommen [H]. Nach Kürzen des zweiten Kanals (1V3) auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_D$-Wert von 88 Jahren („hoch“).
- DC_{avg}: DC = 99 % für 1V3 beruht auf der direkten Überwachung des Schaltzustandes durch 1S3. DC = 60 % für die Wegeventile 1V5 bzw. 2V1 beruht auf der indirekten Überwachung durch den Prozess. Durch Mittelung ergibt sich damit ein DC_{avg} von 73 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der hydraulischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ (88 Jahre) und niedrigem DC_{avg} (73 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $9{,}4 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

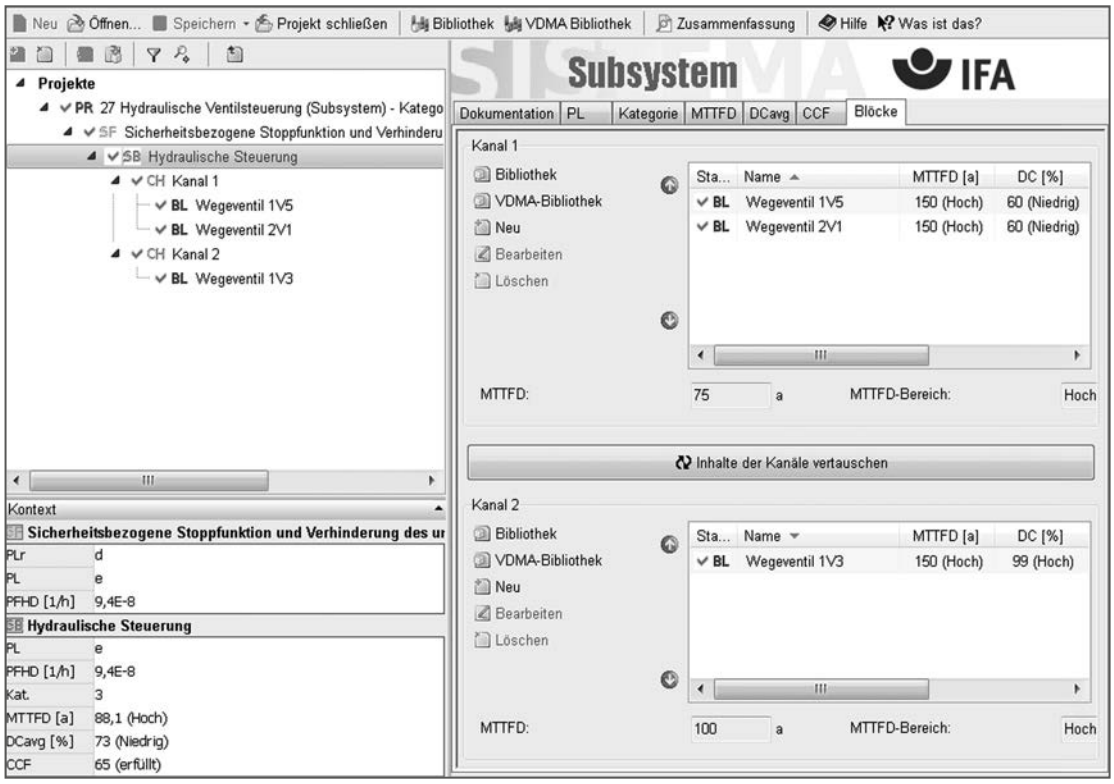


Abbildung 8.53: PL-Bestimmung mithilfe von SISTEMA

8.2.28 Stellungsüberwachung verriegelter trennender Schutzeinrichtungen – Kategorie 4 – PL e (Beispiel 28)

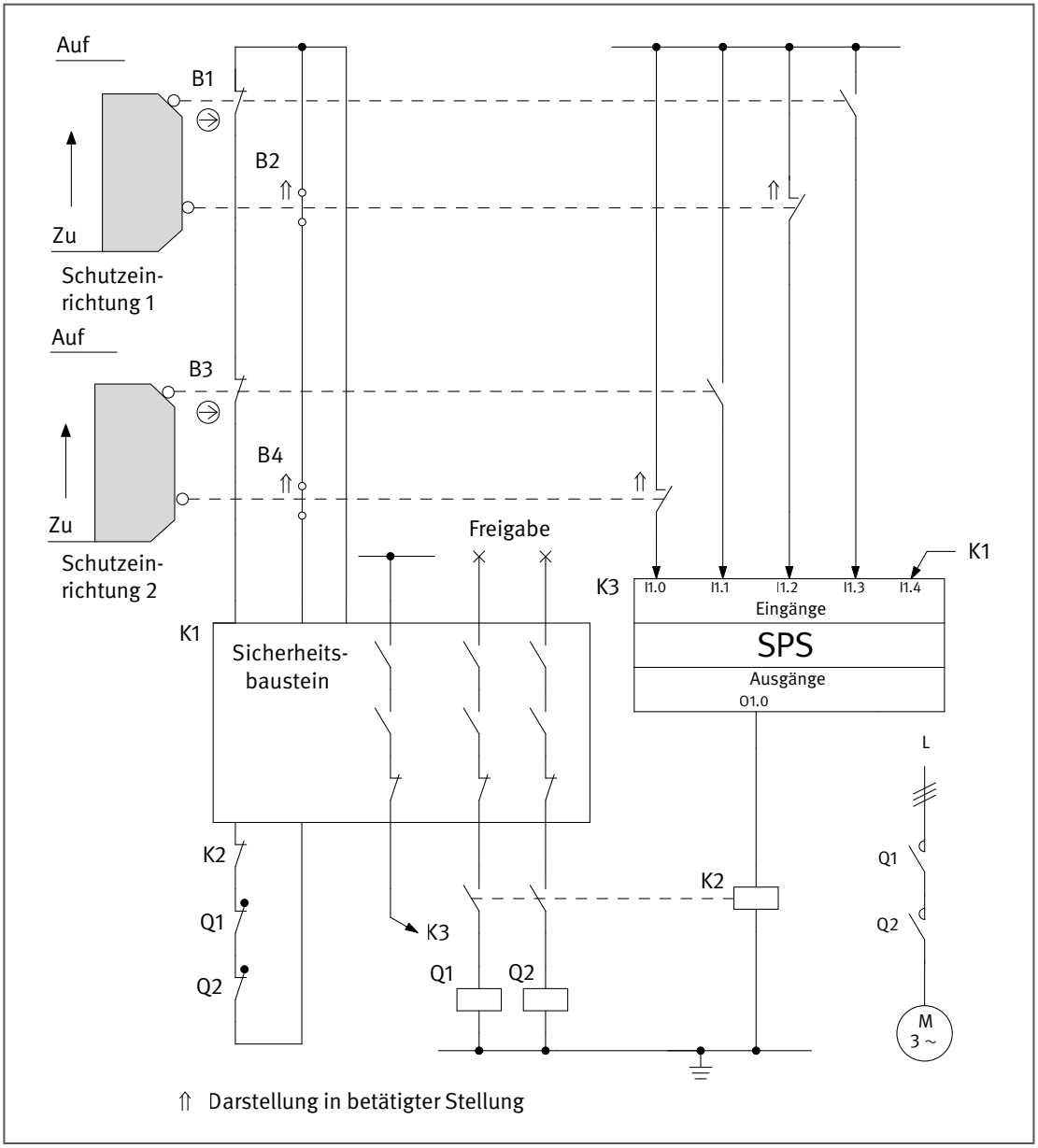


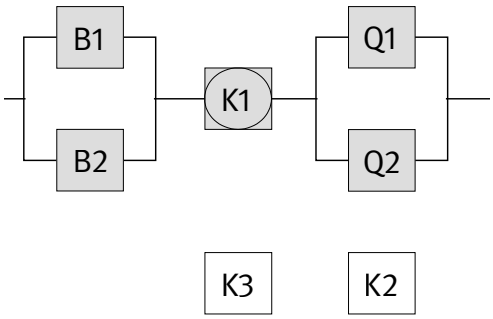
Abbildung 8.54: Stellungsüberwachung verriegelter trennender Schutzeinrichtungen zur Verhinderung von gefahrbringenden Bewegungen

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen einer verriegelten trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit zwei verriegelten trennenden Schutzeinrichtungen (Schutzgittern). Das Öffnen jedes Schutzgitters wird durch zwei Positionsschalter B1/B2 bzw. B3/B4 in Öffner-Schließer-Kombination erfasst und in einem zentralen Sicherheitsschaltgerät K1 ausgewertet. Dieser steuert zwei Schütze Q1 und Q2 an, durch deren Abfallen gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert werden.
- Alle Positionsschalter werden zur Fehlererkennung durch einen zweiten Kontakt in eine handelsübliche SPS K3 eingelesen, die hauptsächlich der Funktionssteuerung dient. Über ein Hilfsschütz K2 kann diese im Fehlerfall unabhängig von K1 die Schütze Q1 und Q2 abschalten. Fehler in K2, Q1 und Q2 werden durch das Sicherheitsschaltgerät K1 erkannt. Beim Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten. Die meisten Bauteilausfälle werden erkannt und führen zur Betriebshemmung. Eine Anhäufung von unerkannten Fehlern führt nicht zum Verlust der Sicherheitsfunktion.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtungen zur Betätigung der Positionsschalter ist sichergestellt.
- B1 und B3 sind Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern sind getrennt oder geschützt verlegt.
- Störungen im Anfahr- und Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschieden betätigten Positionsschaltern (Öffner-Schließer-Kombination) erkannt.
- Es können mehrere Schutzeinrichtungen hintereinander geschaltet werden. Durch diese Kaskadierung ist die Fehlererkennung durch K1 eingeschränkt (siehe Anhang E). Die Positionsschalter werden jedoch zusätzlich durch K3 überwacht und auf diesem Weg erfolgt auch bei Kaskadierung die Fehlererkennung.
- Das Sicherheitsschaltgerät K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Das Schütz K2 besitzt zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Schütze Q1 und Q2 sind mit Spiegelkontakten entsprechend DIN EN 60947-4-1, Anhang F, ausgestattet.
- Die programmierbare SPS K3 erfüllt die normativen Anforderungen gemäß Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- Die Schaltung lässt sich in drei Subsysteme aufteilen, wie im sicherheitsbezogenen Blockdiagramm gezeigt. Die Ausfallwahrscheinlichkeit des Sicherheitsschaltgeräts K1 wird am Ende der Berechnung addiert ($2{,}3 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für die übrigen Subsysteme wird die Ausfallwahrscheinlichkeit im Folgenden berechnet. Da jede Schutztür Bestandteil einer eigenen Sicherheitsfunktion ist, wird hier stellvertretend die Berechnung für die Schutzeinrichtung 1 gezeigt.
- $MTTF_D$: Für den zwangsöffnenden Positionsschalter B1 mit Rollenbetätigung beträgt der B_{10D} $20 \cdot 10^6$ Schaltspiele [H]. Für den Positionsschalter B2 (Schließerkontakt) beträgt der B_{10D} $1 \cdot 10^5$ Schaltspiele [H]. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 1 Stunde Zykluszeit ist für diese Komponenten n_{op} = 5 840 Zyklen/Jahr. Für B1 beträgt $MTTF_D$ 34 246 Jahre und für B2 171 Jahre. Für die Schütze Q1 und Q2 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} folgt für Q1 und Q2 eine $MTTF_D$ von 3 424 Jahren pro Kanal. Insgesamt ergibt sich in beiden Subsystemen ein symmetrisierter $MTTF_D$-Wert pro Kanal von 100 Jahren („hoch“). Der Positionsschalter B2 weist eine begrenzte Betriebszeit von 17,1 Jahren auf. Ein rechtzeitiger Austausch wird empfohlen.
- DC_{avg}: $DC = 99$ % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in K1 und K3. $DC = 99$ % für die Schütze Q1 und Q2 ergibt sich aus der Überwachung bei jedem Einschalten von K1. Die genannten DC-Werte entsprechen dem DC für das jeweilige Subsystem.
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Subsystemen B1/B2 und Q1/Q2 (70 Punkte): Trennung (15), bewährte Bauteile (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

  Die Subsysteme B1/B2 und Q1/Q2 entsprechen jeweils Kategorie 4 mit hoher $MTTF_D$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von jeweils $2{,}3 \cdot 10^{-9}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $4{,}6 \cdot 10^{-9}$/Stunde. Dies entspricht PL e.

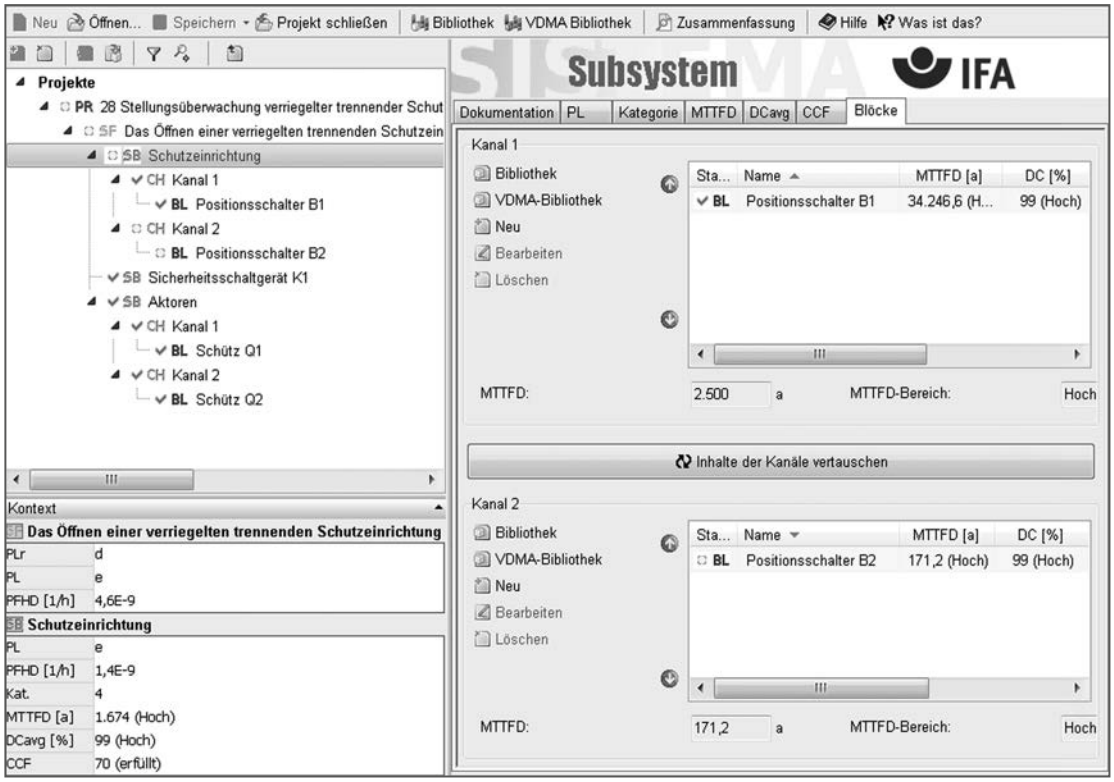


Abbildung 8.55: PL-Bestimmung mit SISTEMA

8.2.29 Kaskadierung von Not-Halt-Geräten mittels Sicherheitsschaltgerät– Kategorie 3 – PL e (Beispiel 29)

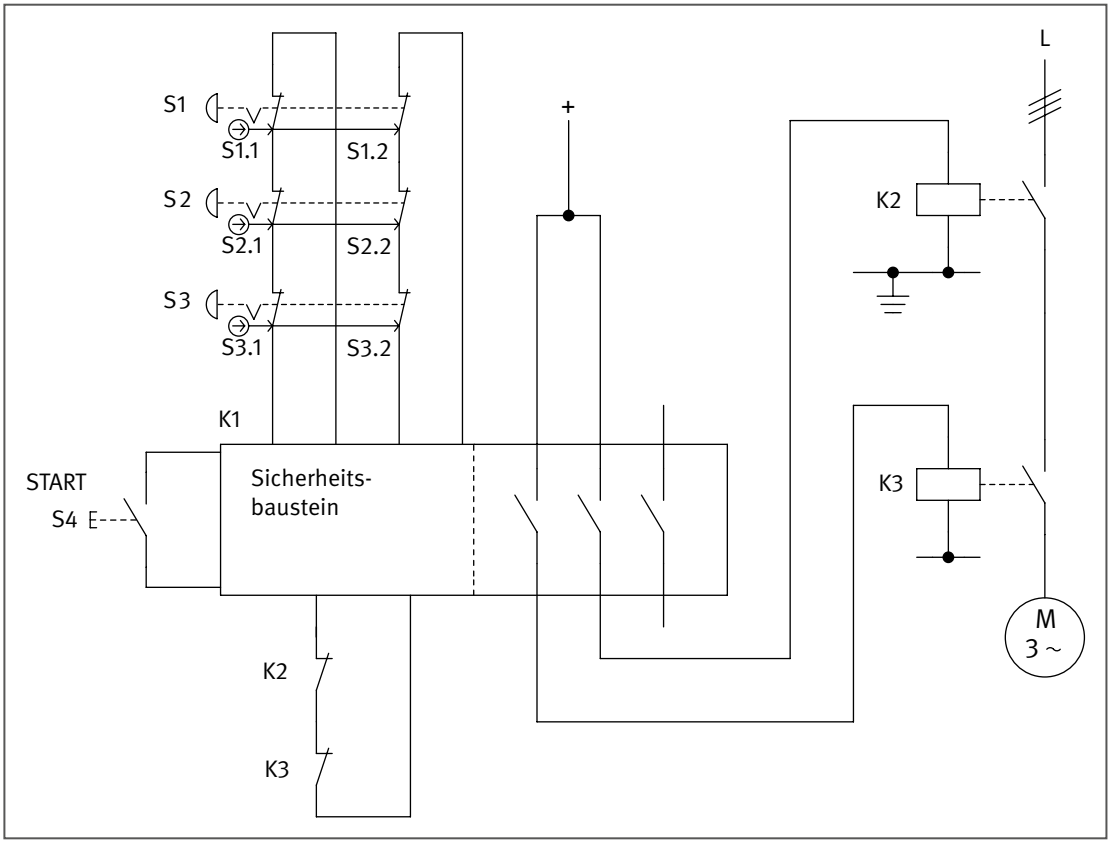


Abbildung 8.56: Kaskadierung von Not-Halt-Geräten mittels Sicherheitsschaltgerät (Not-Halt-Funktion, STO)

Sicherheitsfunktion

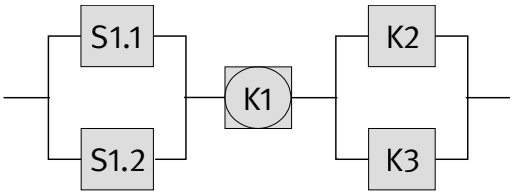
- Not-Halt-Funktion, STO durch Betätigung eines Not-Halt-Gerätes

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden durch Betätigung eines Not-Halt-Gerätes unterbrochen bzw. verhindert. Entsprechend Beispiel 3 in Abschnitt 5.3.2 löst jedes Not-Halt-Gerät eine eigene Sicherheitsfunktion aus. Stellvertretend wird im Folgenden nur S1 betrachtet. Die Auswertung von S1 erfolgt in einem Sicherheitsschaltgerät K1, das zwei redundante Hilfsschütze K2 und K3 ansteuert.
- Die Not-Halt-Geräte werden zur Fehlererkennung redundant in das Sicherheitsschaltgerät K1 eingelesen. Dieses verfügt außerdem über interne Testmaßnahmen. Die Hilfsschütze K2 und K3 werden mithilfe zwangsgeführter Rücklesekontakte ebenfalls in K1 überwacht. Ein Schalten von K2 und K3 erfolgt bei jedem Startbefehl durch den Schalter S4, ca. zweimal pro Monat. Eine Fehlerhäufung von mehr als zwei Fehlern zwischen zwei aufeinander folgenden Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen.
- Es wird nicht unterstellt, dass mehr als ein Not-Halt-Gerät gleichzeitig betätigt wird.
- Durch organisatorische Maßnahmen wird sichergestellt, dass jedes Not-Halt-Gerät mindestens einmal pro Jahr betätigt wird.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Bei den Not-Halt-Geräten S1, S2 und S3 handelt es sich um Schaltgeräte mit zwangsöffnenden Kontakten entsprechend DIN EN 60947-5-1, A1
- Die Zuleitungen zu den Schaltgeräten sind geschützt verlegt.
- Das Sicherheitsschaltgerät K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- K2 und K3 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.



Bemerkung

- Die Not-Halt-Funktion ist eine ergänzende Schutzmaßnahme nach DIN EN ISO 12100:2011.

Berechnung der Ausfallwahrscheinlichkeit

- Bei S1, S2 und S3 handelt es sich um handelsübliche Not-Halt-Geräte nach DIN EN ISO 13850. Bei der zweikanaligen Modellierung wird für jeden Kontakt eines Not-Halt-Gerätes jeweils ein B_{10D} von 100 000 Schaltspielen [N] angesetzt. Die Ausfallwahrscheinlichkeit des fertigen Sicherheitsschaltgerätes K1 wird am Ende der Berechnung addiert ($2{,}3 \cdot 10^{-9}$/Stunde [H], geeignet für PL e).
- $MTTF_D$: Für die Hilfsschütze K2 und K3 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Bei jährlich zwölf Anforderungen der Not-Halt-Funktion und 24 Startbefehlen ist n_{op} = 36 Zyklen/Jahr und $MTTF_D$ beträgt 55 556 Jahre. Dies ist gleichzeitig die symmetrisierte $MTTF_D$ für den Kanal, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg}: DC = 90 % für K2 und K3 sowie S1.1 und S1.2. Der DC beruht auf der Testung und Querschlusserkennung durch das Sicherheitsschaltgerät K1. Dies ist gleichzeitig DC_{avg} („mittel“). Eine ausreichende Testhäufigkeit der Not-Halt-Geräte ist gewährleistet (siehe Hinweise in den Abschnitten 6.2.14 und D.2.5.1).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), bewährte Bauteile (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Für das Not-Halt-Gerät S1 ergibt sich bei jährlich zwölf Anforderungen der Not-Halt-Funktion eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle PFH_D zu $4{,}3 \cdot 10^{-8}$/Stunde.
- Das Subsystem K2/K3 entspricht Kategorie 3 mit hoher $MTTF_D$ (100 Jahre) und mittlerem DC_{avg} (90 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}3 \cdot 10^{-8}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $8{,}8 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Damit ist der PL_r = d übertroffen.

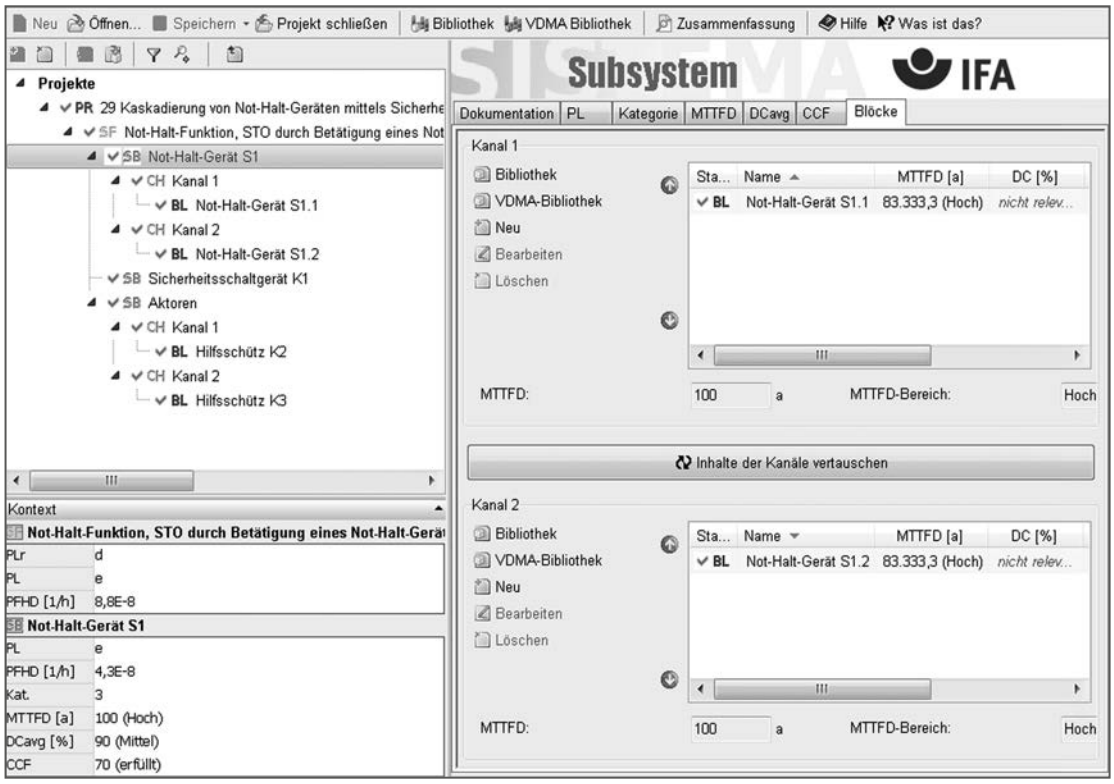


Abbildung 8.57: PL-Bestimmung mithilfe von SISTEMA

8.2.30 Schützüberwachungsbaustein – Kategorie 3 – PL e (Beispiel 30)

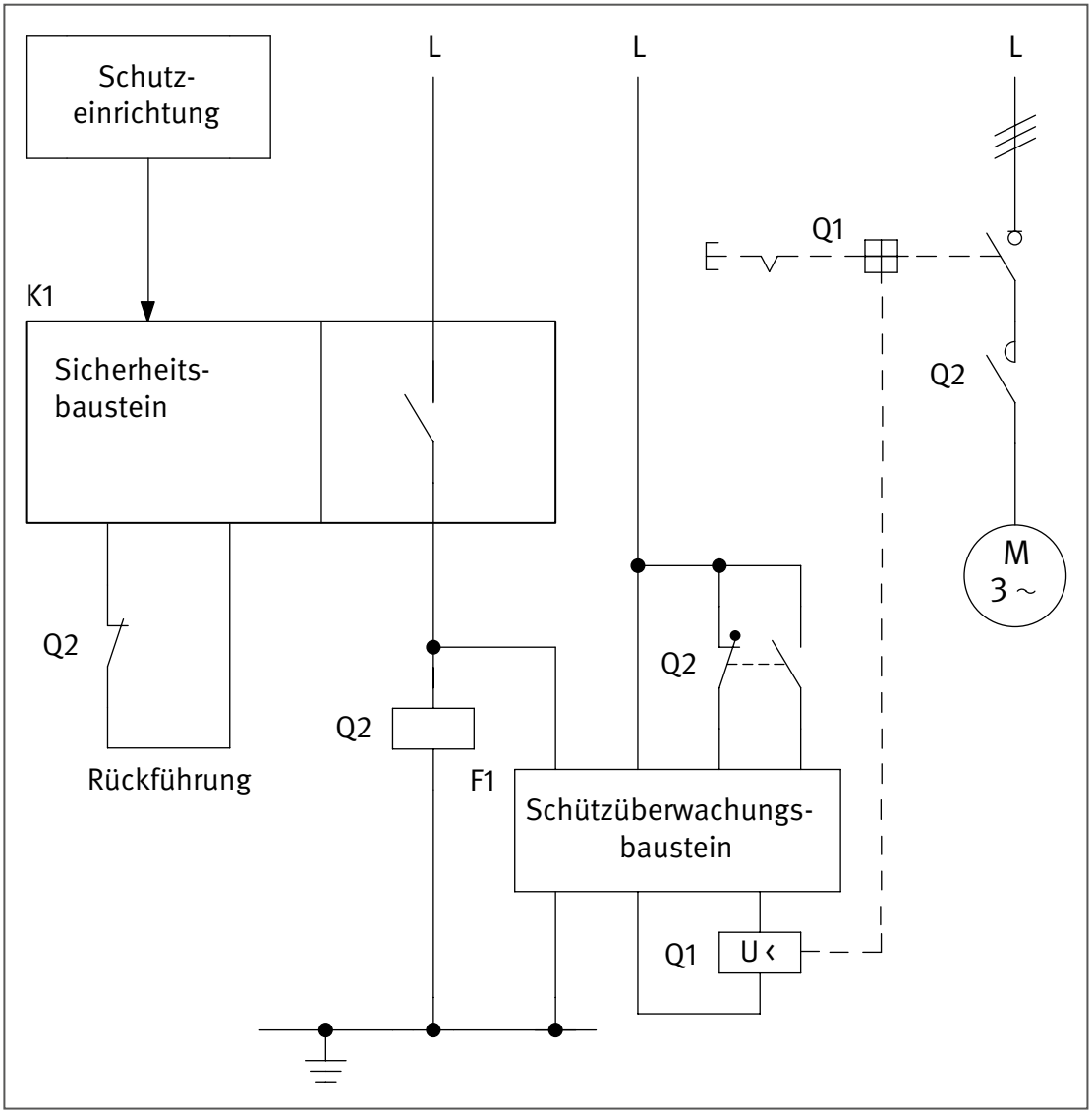


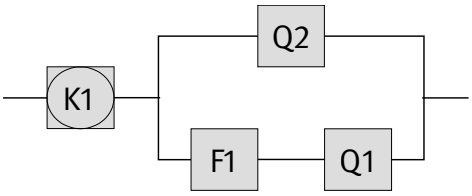
Abbildung 8.58: Einleitung des STO – Sicher abgeschaltetes Moment mittels Sicherheitsschaltgerät und Schützüberwachungsbaustein

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der verriegelten trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit einer Schutzeinrichtung, deren Öffnen durch ein Sicherheitsschaltgerät K1 detektiert wird. Dieses steuert ein Leistungsschütz Q2 und eine Kombination aus einem Schützüberwachungsbaustein F1 und einer Unterspannungsauslösung Q1 an. Das Abfallen von Q2 unterbricht gefahrbringende Bewegungen bzw. verhindert gefahrbringende Zustände. Der Schützüberwachungsbaustein F1 hat die Funktion, die Hauptkontakte von Leistungsschütz Q2 auf Verschweißen zu überwachen. Fällt Q2 nicht ab, löst F1 den vorgeordneten Leistungsschalter oder Motorstarter Q1 über dessen Unterspannungsauslösung aus. Dieser schaltet dann den Motor ab.
- Bei Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten.
- Eine Fehlerhäufung zwischen zwei aufeinander folgenden Betätigungen kann zum Verlust der Sicherheitsfunktion führen.



Konstruktive Merkmale

- Der Leistungsschalter Q1 wird über eine manuell zu implementierende Testfunktion regelmäßig geprüft. Die Zeit zwischen den Tests sollte ein Hundertstel der $MTTF_D$ von Q1 nicht überschreiten und könnte z. B. bei Maschinenwartung erfolgen. Das Schütz Q2 wird durch den Schützüberwachungsbaustein ständig getestet. Ein Verlust der Sicherheitsfunktion zwischen den Tests – wie es bei Kategorie 2 möglich ist – kann nicht vorkommen. Die Einfehlersicherheit ist damit gewährleistet und die Anforderungen der Kategorie 3 sind erfüllt.
- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Aus Vereinfachungsgründen wurde bei der Darstellung auf Details zur Schutzeinrichtung verzichtet.
- Die Schutzeinrichtung wirkt auf ein Sicherheitsschaltgerät K1, das alle Anforderungen für Kategorie 3 oder 4 und PL e erfüllt.
- Die Hilfskontakte von Schütz Q2 sind zwangsgeführt entsprechend DIN EN 60947-5-1, Anhang L.
- Die Fehlerbetrachtung für Q2 (mit Spiegelkontakten) und für das interne Relais des Schützüberwachungsbausteins F1 erfolgt wie bei zwangsgeführten Kontakten.

Bemerkung

- Die Reaktionszeit durch den Schützüberwachungsbaustein F1 hinsichtlich des Abfalls von Q1 ist zu berücksichtigen.

Berechnung der Ausfallwahrscheinlichkeit

- Die Sicherheitsfunktion lässt eine Aufteilung in zwei Subsysteme zu. Das Subsystem aus Schutzeinrichtung und Sicherheitsschaltgerät K1 wird in diesem Beispiel nicht berücksichtigt.
- $MTTF_D$: Für den Schützüberwachungsbaustein F1 beträgt die $MTTF_D$ 125 Jahre bei maximaler n_{op} = 350 400 Zyklen/Jahr [H]. Bei induktiver Last (AC3) ergibt sich für Q1 ein B_{10D}-Wert von 10 000 Schaltspielen und für Q2 ein B_{10D}-Wert von 1 300 000 Schaltspielen. Bei einer angenommenen täglichen Betätigung an 365 Arbeitstagen ist für Q1 n_{op} = 365 Zyklen/Jahr und die $MTTF_D$ beträgt 274 Jahre. Bei 365 Arbeitstagen, 16 Arbeitsstunden und einer Minute Zykluszeit ist für Q2 n_{op} = 350 400 Zyklen/Jahr und die $MTTF_D$ beträgt 37 Jahre. Für den aus F1 und Q1 bestehenden Kanal folgt eine $MTTF_D$ von 85 Jahren. Insgesamt ergibt sich ein symmetrisierter $MTTF_D$-Wert pro Kanal von 64 Jahren („hoch“).
- DC_{avg}: DC = 99 % für Q2 beruht auf der Testung über den Schützüberwachungsbaustein F1. DC = 99 % für F1 wird durch Fehler erkennende Maßnahmen innerhalb des Schützüberwachungsbausteins realisiert. Der Leistungsschalter Q1 wird über die zu implementierende manuelle Prüffunktion getestet, woraus sich DC = 90 % ableitet. Für F1 wird eine DC = 99 % angesetzt. Durch Mittelung ergibt sich damit ein DC_{avg} von 98 % („mittel“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Das Subsystem, bestehend aus Q1, Q2 und F1, entspricht Kategorie 3 mit hoher $MTTF_D$ (64 Jahre) und mittlerem DC_{avg} (98 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von 4,4 · 10–8/Stunde. Dies entspricht PL e. Nach Hinzufügen des Subsystems, bestehend aus Schutzeinrichtung und Sicherheitsschaltgerät K1, wird der PL unter Umständen geringer.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Element Q2 ein T_{10D}-Wert von 3,7 Jahren für den vorgesehenen Austausch.

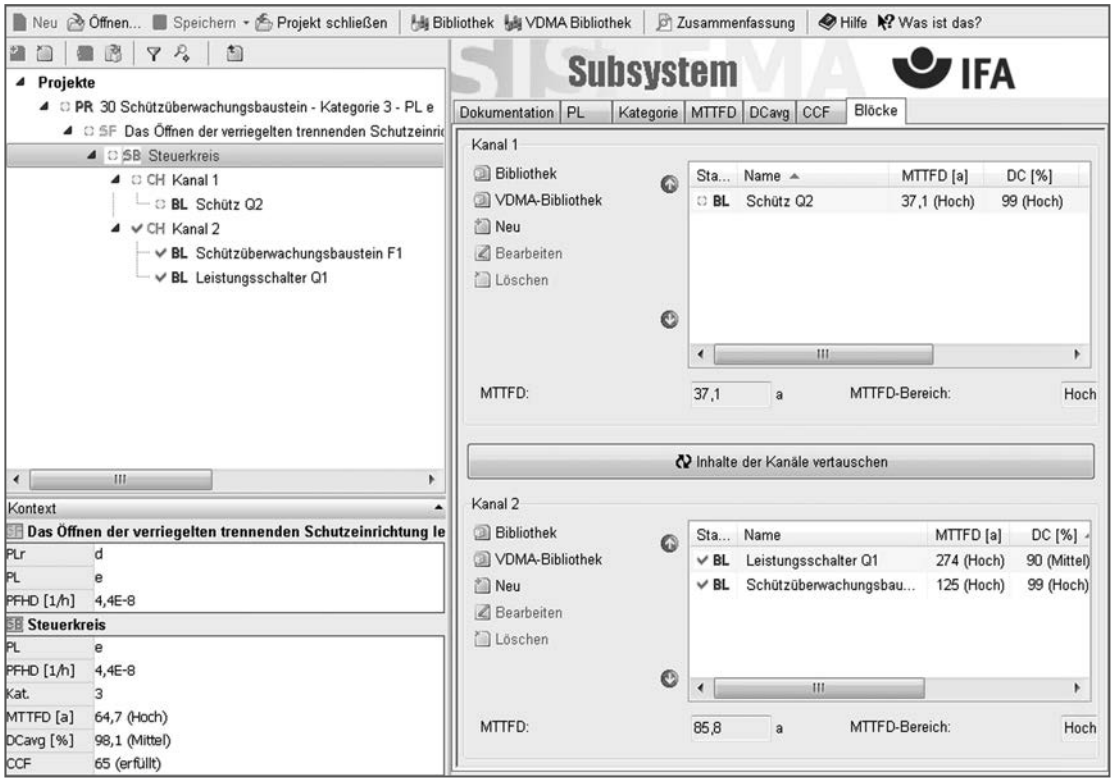


Abbildung 8.59: PL-Bestimmung mithilfe von SISTEMA

8.2.31 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 4 – PL e (Beispiel 31)

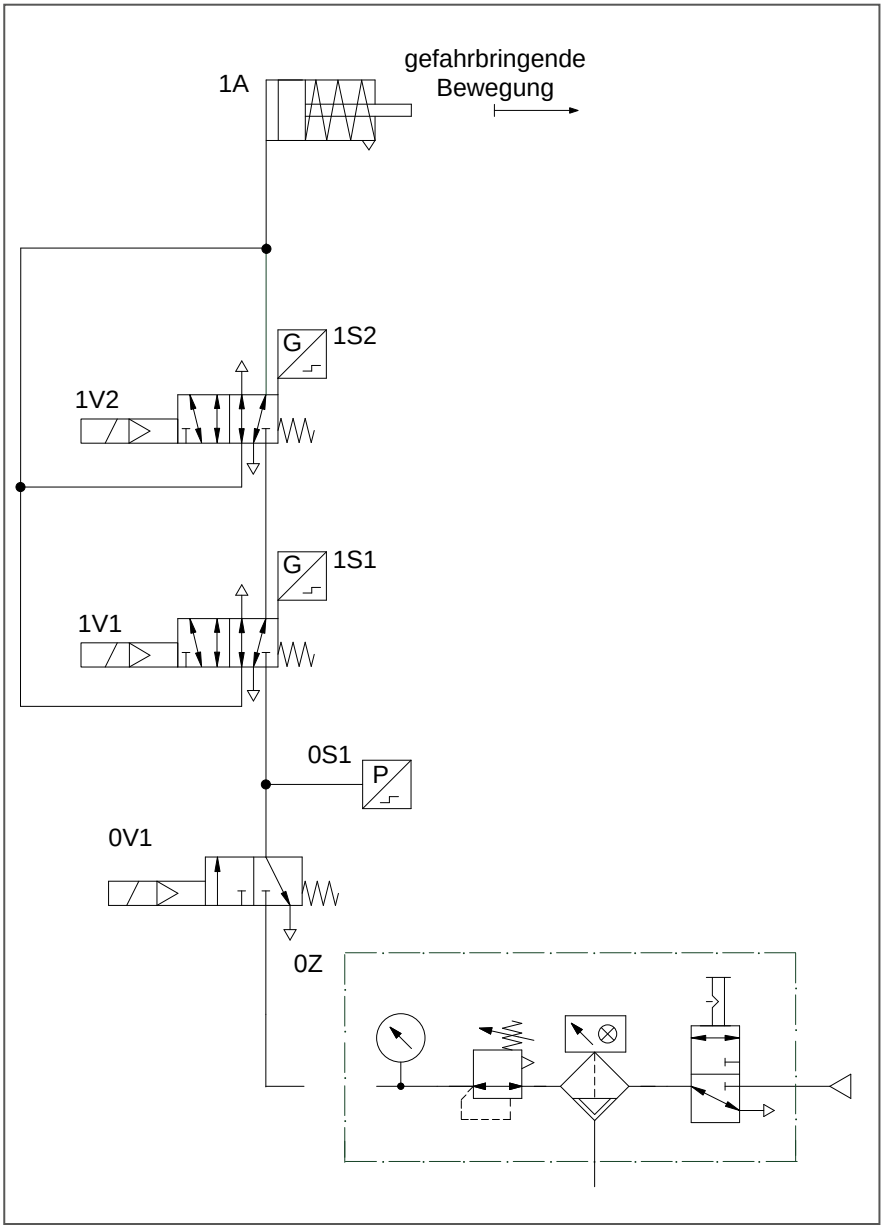


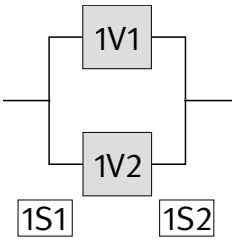
Abbildung 8.60:
Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage, realisiert durch SDE
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Eine gefahrbringende Bewegung des Zylinders wird redundant durch die Ventile 1V1 und 1V2 gesteuert. Ein Stillsetzen der Bewegung kann entweder durch das Wegeventil 1V1 oder 1V2 erfolgen.
- Der alleinige Ausfall eines der beiden Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- Nach Wegnahme mindestens eines Steuersignals wird die Kolbenseite des Zylinders entlüftet.
- Der einzelne Fehler eines Ventils wird bei Wegnahme der Ansteuerung durch die integrierte Stellungsüberwachung erkannt; nach einem Fehler wird das Einleiten der nächsten gefahrbringenden Bewegung verhindert.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- 1V1 und 1V2 sind Wegeventile mit ausreichend positiver Überdeckung, Federrückstellung sowie elektrischer Stellungsüberwachung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme der Steuersignale erreicht.
- Die Signalverarbeitung der elektrischen Stellungsüberwachung erfüllt entsprechende Anforderungen zur Beherrschung von Ausfällen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für die Wegeventile wird ein B_{10D}-Wert von 20 000 000 Zyklen [H] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 20 Sekunden Zykluszeit ist n_{op} = 691 200 Zyklen/Jahr und $MTTF_D$ = 289 Jahre („hoch“). Dies ist gleichzeitig der $MTTF_D$-Wert pro Kanal.
- DC_{avg}: DC = 99 % für 1V1 und 1V2 ergibt sich aus der direkten Überwachung der Schaltzustände. Damit ergibt sich ein DC_{avg} von ebenfalls 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_D$ (289 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $8{,}1 \cdot 10^{-9}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (08.16). Beuth, Berlin 2016

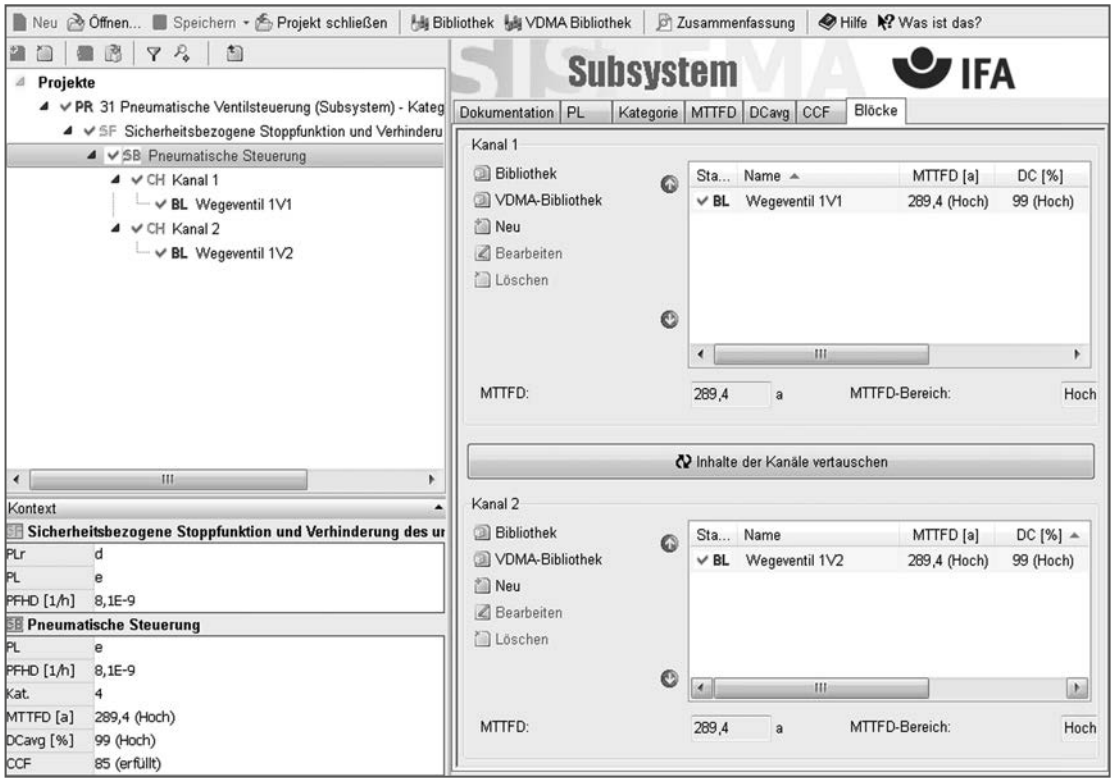


Abbildung 8.61: PL-Bestimmung mithilfe von SISTEMA

8.2.32 Hydraulische Ventilsteuerung (Subsystem) – Kategorie 4 – PL e (Beispiel 32)

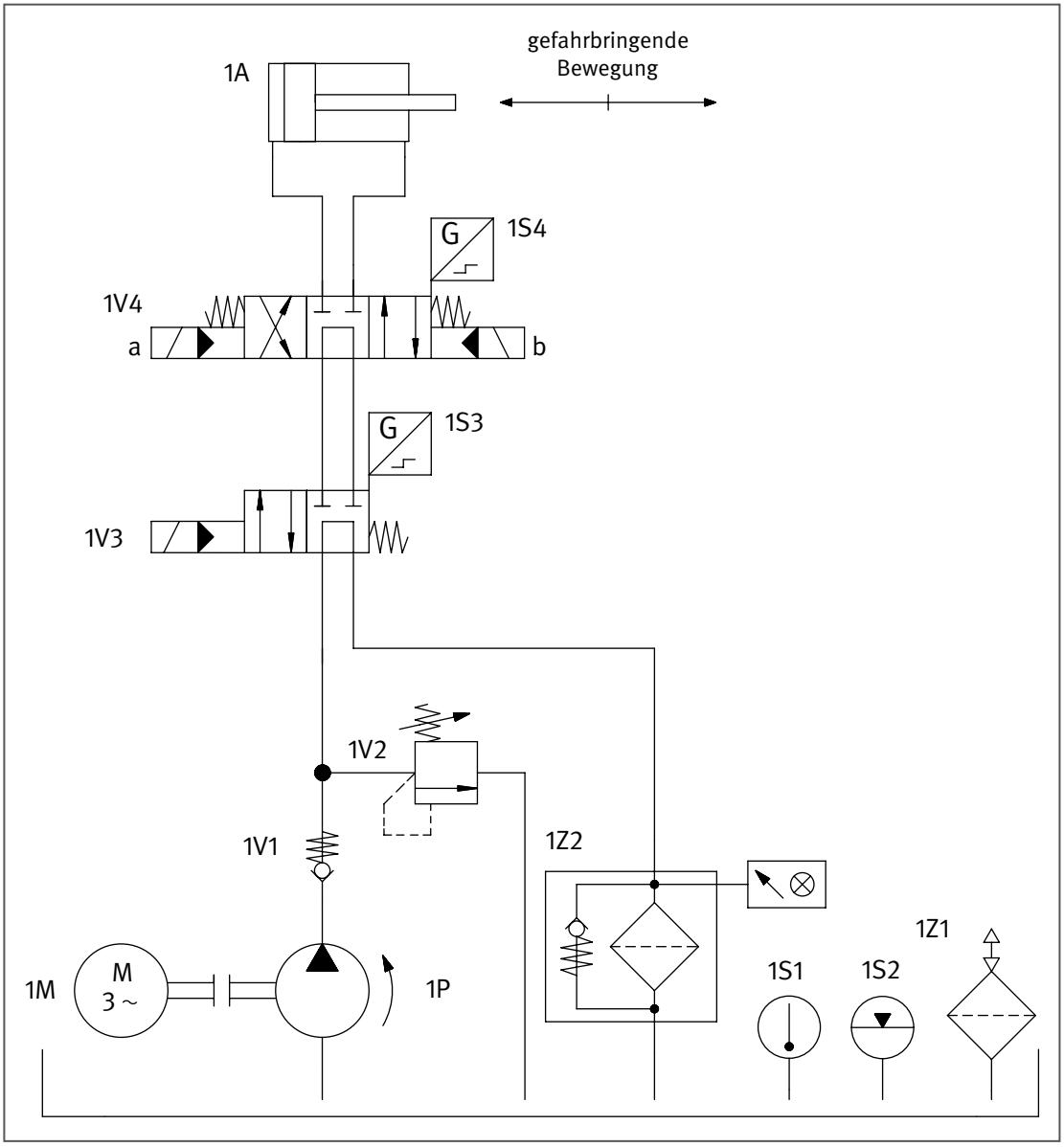


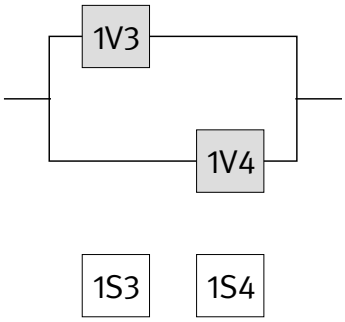
Abbildung 8.62: Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch zwei Wegeventile (1V3 und 1V4) gesteuert.
- Der einzelne Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- Beide Wegeventile werden zyklisch angesteuert.
- An beiden Wegeventilen ist jeweils eine direkte Stellungsüberwachung (1S3 und 1S4) vorgesehen. Der Ausfall jedes der beiden Wegeventile wird erkannt; nach einem Fehler wird das Einleiten der nächsten gefahrbringenden Bewegung verhindert.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Die Wegeventile 1V3 und 1V4 haben eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung sowie eine elektrische Stellungsüberwachung.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung der elektrischen Stellungsüberwachung erfüllt entsprechende Anforderungen zur Beherrschung von Ausfällen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für die Wegeventile 1V3 und 1V4 wird eine $MTTF_D$ von 150 Jahren angenommen [H].
- DC_{avg}: DC = 99 % für die Wegeventile 1V3 und 1V4 beruht auf der direkten Überwachung der Schaltzustände. Durch Mittelung ergibt sich damit ein DC_{avg} von ebenfalls 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der hydraulischen Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_D$ und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}6 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

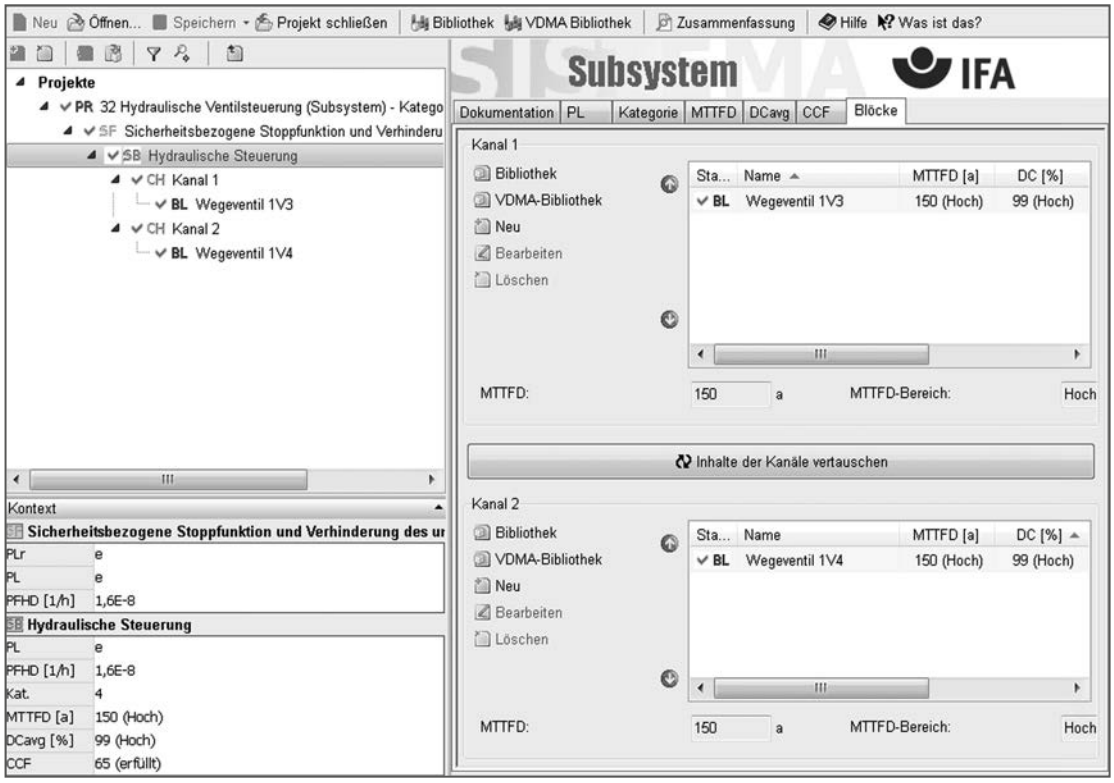


Abbildung 8.63:
PL-Bestimmung mithilfe von SISTEMA

8.2.33 Elektrohydraulische Pressensteuerung – Kategorie 4 – PL e (Beispiel 33)

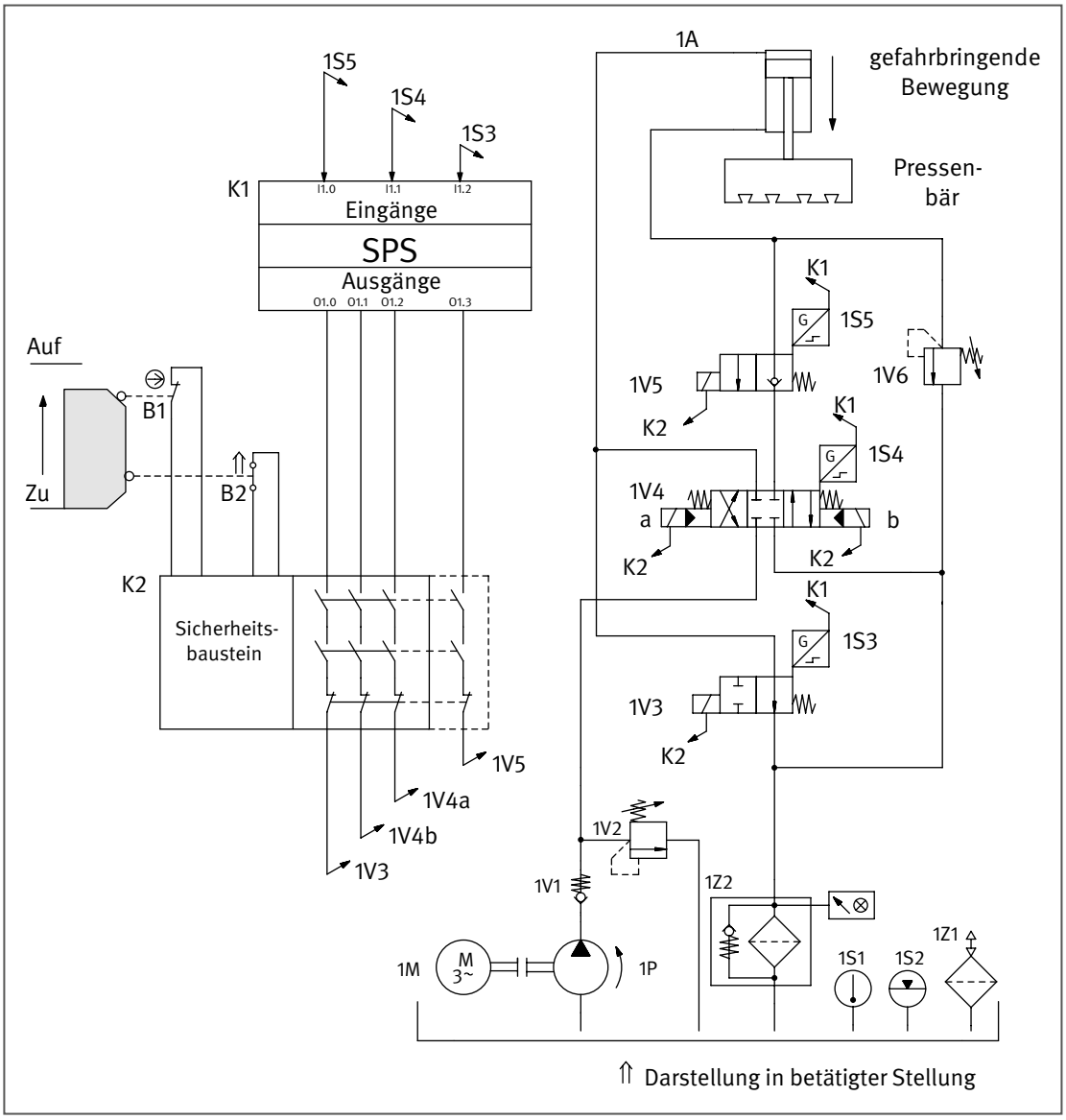
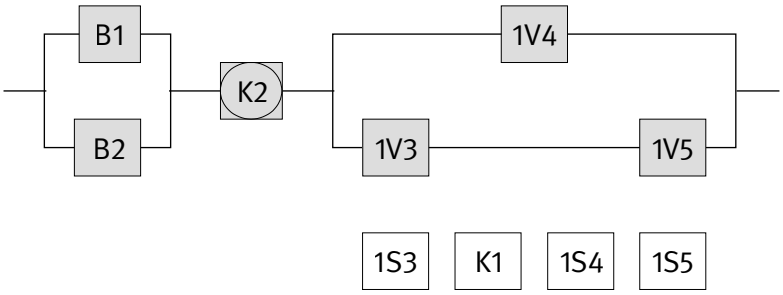


Abbildung 8.64: Pressensteuerung, elektrische Überwachung einer beweglichen trennenden Schutzeinrichtung mit hydraulischem Stillsetzen der gefahrbringenden Bewegung

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Stillsetzen der gefahrbringenden Bewegung



Funktionsbeschreibung

- Der Gefahrenbereich ist mittels einer verriegelten trennenden Schutzeinrichtung gesichert, deren Stellung von zwei Positionsschaltern B1 und B2 in Öffner-Schließer-Kombination erfasst wird. Die Signale werden in ein handelsübliches Sicherheitsschaltgerät K2 eingelesen, der in den Freigabepfad der elektrischen Vorsteuerung K1 (herkömmliche SPS) für die hydraulischen Aktoren eingeschleift ist. Gefahrbringende Bewegungen oder Zustände werden aktorseitig durch drei Wegeventile (1V3, 1V4 und 1V5) gesteuert. Bei Anforderung der Sicherheitsfunktion werden alle Ventile durch K2 stromlos geschaltet und gehen aufgrund der vorhandenen Rückstellfedern in die Sperr-Mittelstellung (1V4) bzw. in die Sperr-Stellung (1V3 und 1V5). Dabei wird der Ölrückfluss von der Kolbenunterseite des Zylinders zum Tank durch die Ventile 1V4 und 1V5 gleichzeitig unterbrochen. Bei dem Ventil 1V5 handelt es sich um ein Sitzventil, das aufgrund seiner Konstruktion den Volumenstrom leckagefrei absperrt. Ventil 1V4, das auch die Bewegungsrichtung des Zylinders steuert, ist ein Wegeventil in Schieberbauweise, das auch in der Sperr-Mittelstellung eine gewisse Leckage aufweist. Obwohl das Ventil 1V3 nur mittelbar an der Stoppfunktion beteiligt ist, kann es die Sicherheitsfunktion in gefährlicher Weise beeinträchtigen. Würden 1V3 und 1V4 gleichzeitig hängen bleiben, so würde auf der Kolbenoberseite Druck aufgebaut, während die Kolbenunterseite durch 1V5 abgesperrt bleibt. Wegen der Druckübersetzung im Zylinder würde dann das Druckbegrenzungsventil 1V6 öffnen und der Pressenbär absinken.
- Der Ausfall eines Ventils führt nicht zum Verlust der Sicherheitsfunktion. Alle Ventile werden zyklisch angesteuert.
- An allen Ventilen ist jeweils eine Stellungsabfrage 1S3, 1S4 bzw. 1S5 zur Fehlererkennung vorgesehen. Der Ausfall jedes der drei Ventile wird in der herkömmlichen SPS K1 erkannt, die nach einem Fehler das Einleiten der nächsten gefahrbringenden Bewegung verhindert.
- Ein einzelner Fehler in einer sicherheitstechnischen Komponente führt nicht zum Verlust der Sicherheitsfunktion. Darüber hinaus werden einzelne Fehler bei oder vor der nächsten Anforderung erkannt. Eine Anhäufung von unerkannten Fehlern führt nicht zum Verlust der Sicherheitsfunktion.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B werden eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Das Sicherheitsschaltgerät K2 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Zuleitungen zu den Positionsschaltern sind getrennt oder geschützt verlegt.
- Für K1 wird eine handelsübliche SPS ohne Sicherheitsfunktionen verwendet.
- Die Ventile 1V3, 1V4 und 1V5 haben eine Sperr-Mittelstellung bzw. Sperr-Stellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung und sind stellungsüberwacht.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Das Druckbegrenzungsventil 1V6 zum Schutz des Zylinders 1A und der darunter liegenden Bauteile gegen „Druckübersetzerwirkung“ erfüllt die Anforderungen der DIN EN 693:2001, Abschnitt 5.2.4.4.

Berechnung der Ausfallwahrscheinlichkeit

- K2 wird als Subsystem mit einer Ausfallwahrscheinlichkeit von $2{,}3 \cdot 10^{-9}$/Stunde [H] betrachtet. Der übrige Steuerungsteil wird getrennt nach Elektromechanik und Hydraulik zu zwei Subsystemen der Kategorie 4 zusammengefasst, deren Ausfallwahrscheinlichkeit im Folgenden berechnet wird.
- $MTTF_D$: Für den Positionsschalter mit Zwangsöffnung B1 beträgt B_{10D} $20 \cdot 10^6$ Schaltspiele [H]. Für den elektrischen Schließerkontakt von Positionsschalter B2 beträgt B_{10D} = 1 000 000 Schaltspiele [H]. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 35 040 Zyklen/Jahr und die $MTTF_D$ beträgt 5707 Jahre für B1 bzw. 285 Jahre für B2. Für die Ventile 1V3, 1V4 und 1V5 wird jeweils eine $MTTF_D$ von 150 Jahren [H] angenommen. Dies ergibt einen $MTTF_D$-Wert pro Kanal von 100 bzw. 88 Jahren („hoch“) für beide Subsysteme.

- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung beider Schaltzustände in K2. Der DC von 99 % für beide Ventile beruht auf der direkten Überwachung der Schaltzustände durch die SPS K1. Dies ergibt einen DC_{avg} von 99 % („hoch“) für beide Subsysteme.
- Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte) für beide Subsysteme: Trennung (15), bewährte Bauteile (5), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Der elektromechanische und der hydraulische Teil der Steuerung entsprechen Kategorie 4 mit hoher $MTTF_D$ und hohem DC_{avg} (99 %). Damit ergeben sich mittlere Wahrscheinlichkeiten gefährlicher Ausfälle von $1{,}3 \cdot 10^{-9}$/Stunde und $2{,}1 \cdot 10^{-8}$/Stunde. Für die komplette Sicherheitsfunktion ergibt sich durch Addition inklusive K2 eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}5 \cdot 10^{-8}$ / Stunde. Dies entspricht PL e.

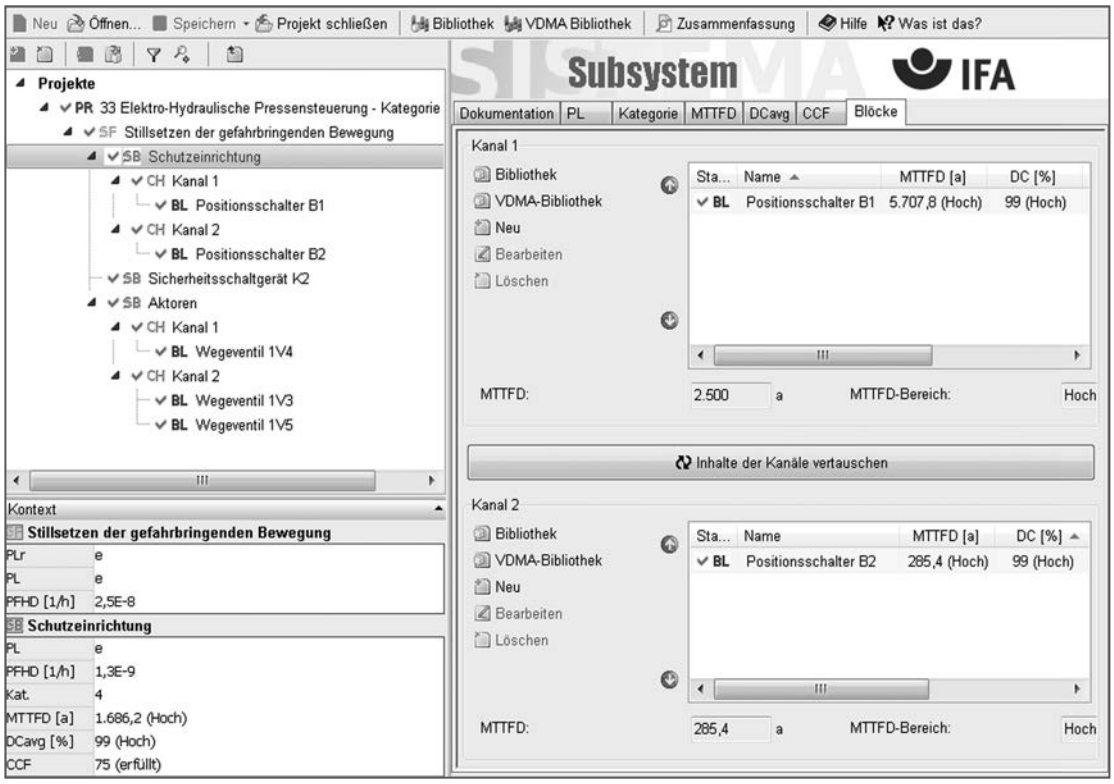


Abbildung 8.65: PL-Bestimmung mithilfe von SISTEMA

8.2.34 Stellungsüberwachung verriegelter trennender Schutzeinrichtungen – Kategorie 4 – PL e (Beispiel 34)

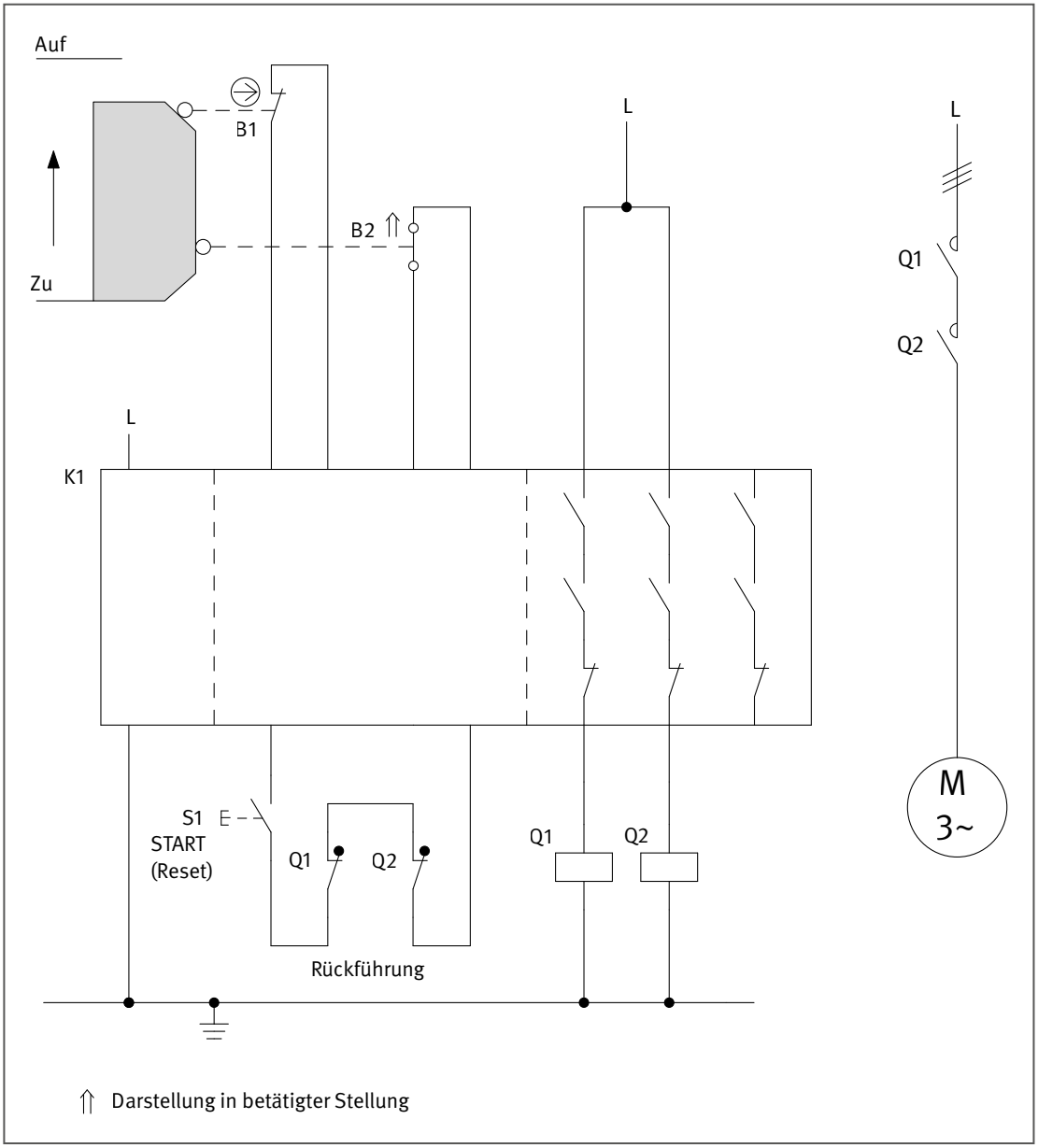


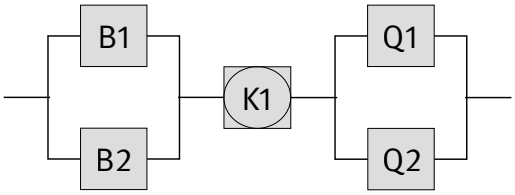
Abbildung 8.66: Stellungsüberwachung verriegelter trennender Schutzeinrichtung mittels Sicherheitsschaltgerät

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der verriegelten trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit einer verriegelten trennenden Schutzeinrichtung (Schutzgitter). Das Öffnen des Schutzgitters wird durch zwei Positionsschalter B1/B2 in Öffner-Schließer-Kombination erfasst und in einem Sicherheitsschaltgerät K1 ausgewertet. Dieses steuert zwei Schütze Q1 und Q2 an, durch deren Abfallen gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert werden.
- Die Positionsschalter werden zur Fehlererkennung in K1 auf Plausibilität überwacht. Fehler in Q1 und Q2 werden durch eine Anlauftestung in K1 erkannt. Ein Start-Befehl ist nur erfolgreich, wenn Q1 und Q2 vorher abgefallen waren. Es ist keine Anlauftestung durch Öffnen und Schließen der Schutzeinrichtung erforderlich.



- Die Sicherheitsfunktion ist auch erfüllt, wenn ein Bauteilausfall auftritt. Fehler werden während des Betriebs oder beim Betätigen (Öffnen und Schließen) der Schutzeinrichtung durch Abfall von Q1, Q2 und Betriebshemmung erkannt.
- Eine Fehlerhäufung von mehr als zwei Fehlern zwischen zwei aufeinander folgenden Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtungen zur Betätigung der Positionsschalter ist sichergestellt.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern B1 und B2 sind getrennt oder geschützt verlegt.
- Das Sicherheitsschaltgerät K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Schütze Q1 und Q2 besitzen Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F.

Bemerkung

- Kategorie 4 wird nur eingehalten, wenn nicht mehrere mechanische Positionsschalter verschiedener Schutzeinrichtungen hintereinander geschaltet werden (keine Kaskadierung), da sonst die Fehlererkennung in den Schaltern eingeschränkt ist (siehe Anhang E).

Berechnung der Ausfallwahrscheinlichkeit

- Die Schaltung lässt sich in drei Subsysteme aufteilen, wie im sicherheitsbezogenen Blockdiagramm gezeigt. Die Ausfallwahrscheinlichkeit des handelsüblichen Sicherheitsschaltgerätes K1 wird am Ende der Berechnung addiert ($2{,}3 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für die übrigen Subsysteme wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_D$: Für die Positionsschalter B1 mit Rollenbetätigung beträgt der B_{10D} $20 \cdot 10^6$ Schaltspiele [H]. Für den Positionsschalter B2 (Schließerkontakt) beträgt B_{10D} $1 \cdot 10^5$ Schaltspiele [H]. Bei 365 Arbeitstagen, 16 Arbeitsstunden und einer Stunde Zykluszeit ist für diese Komponenten n_{op} = 5 840 Zyklen/Jahr und $MTTF_D$ beträgt 1674 Jahre für B1 und B2. Für die Schütze Q1 und Q2 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} folgt für Q1 und Q2 eine $MTTF_D$ von 3 424 Jahren pro Kanal.
  Der Positionsschalter B2 weist eine begrenzte Betriebszeit von 17,1 Jahren auf. Ein rechtzeitiger Austausch wird empfohlen.
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in K1. DC = 99 % für die Schütze Q1 und Q2 ergibt sich aus der regelmäßigen Überwachung durch K1 beim Start. Die genannten DC-Werte entsprechen dem DC_{avg} für das jeweilige Subsystem.
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Subsystemen B1/B2 und Q1/Q2 (85 bzw. 70 Punkte): Trennung (15), Diversität (20, nur B1/B2), bewährte Bauteile (5, nur Q1/Q2), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Subsysteme B1/B2 und Q1/Q2 entsprechen jeweils Kategorie 4 mit hoher $MTTF_D$ (1 674 und 2 500 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}4 \cdot 10^{-9}$/Stunde und 9,1 10E-10 /Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $4{,}6 \cdot 10^{-9}$/Stunde. Dies entspricht PL e.

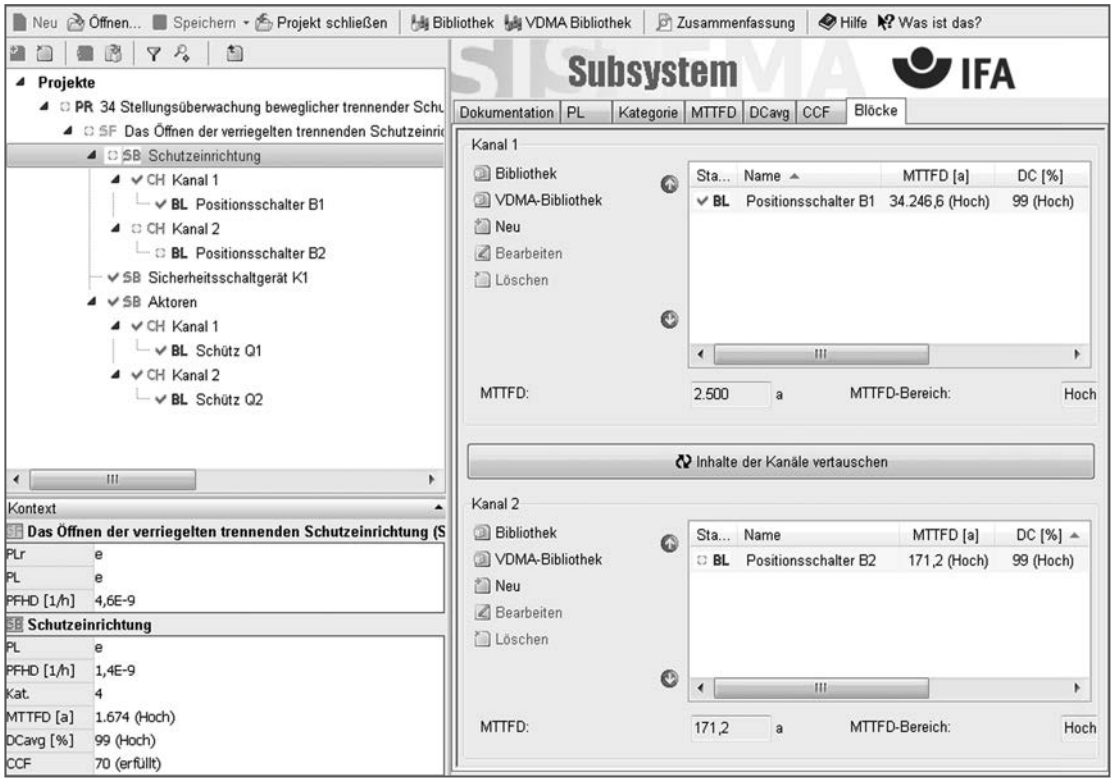


Abbildung 8.67: PL-Bestimmung mithilfe von SISTEMA

8.2.35 Zweihandschaltung – Kategorie 4 – PL e (Beispiel 35)

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):
Der PFH_D-Wert für die Logikeinheit K1 und die B_{10D}-Werte für die Taster S1 und S2 wurden an realistische Herstellerwerte angepasst.

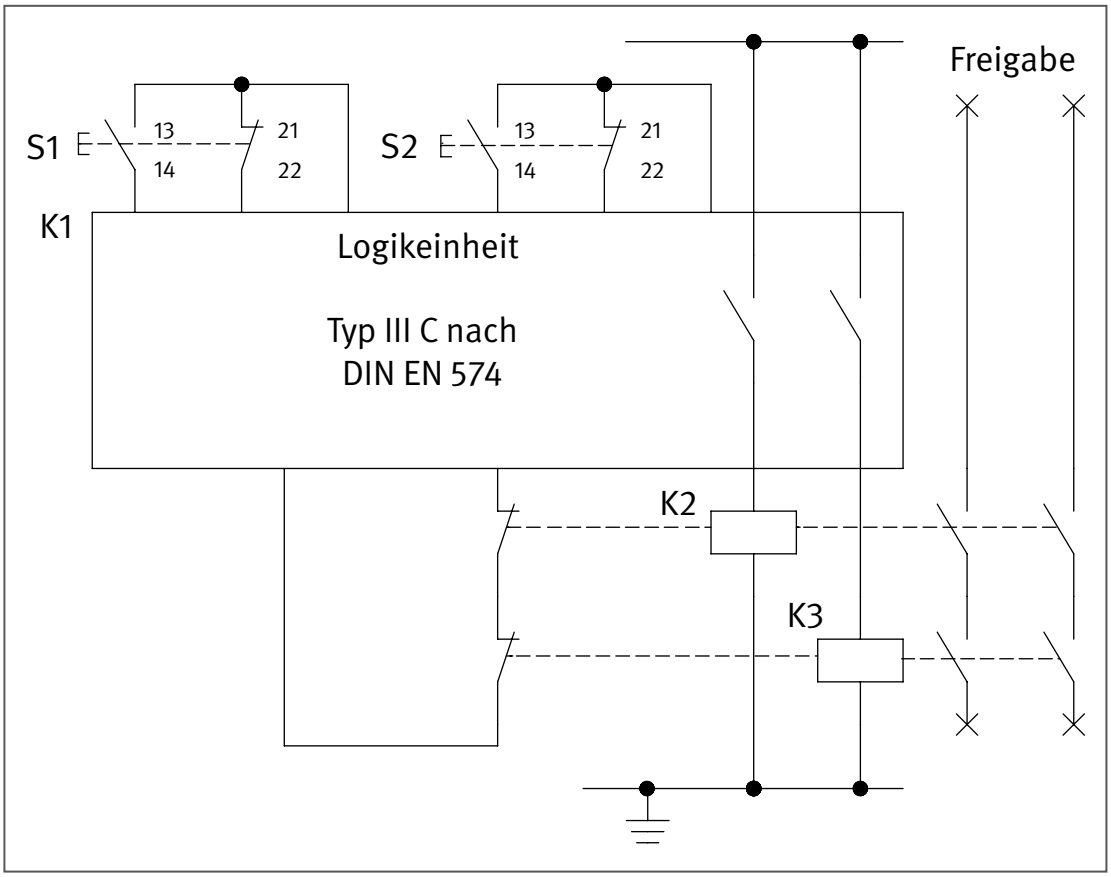


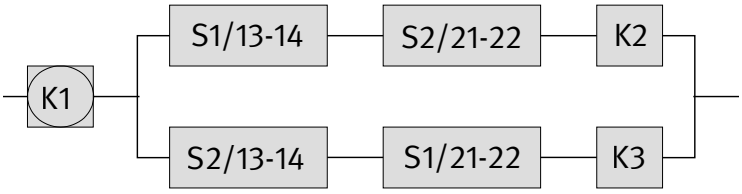
Abbildung 8.68: Zweihandschaltung, Signalverarbeitung durch eine Logikeinheit mit nachgeschalteten Hilfsschützen

Sicherheitsfunktion

- Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung: Beim Loslassen mindestens eines der beiden Taster S1/S2 wird die Freigabe aufgehoben und solange blockiert, bis beide Taster entlastet und erneut synchron betätigt werden.

Funktionsbeschreibung

- Die Logikeinheit K1 überwacht die Betätigung der Stellteile (Taster) S1 und S2. Nur wenn beide aus dem entlasteten Zustand synchron (d. h. innerhalb einer festgelegten Zeitvorgabe von maximal 500 ms nach DIN EN 574) betätigt werden, ziehen die Hilfsschütze K2 und K3 an und die Freigabe erfolgt. Beim Loslassen mindestens eines der Taster S1/S2 heben K2/K3 die Freigabe auf.
- Durch K2 und K3 erfolgt eine Kontaktvervielfachung/Lastanpassung. Die eigentliche Verhinderung der gefahrbringenden Bewegung, z. B. durch Trennung der elektrischen oder hydraulischen Energie, ist anwendungsabhängig und hier nicht dargestellt.
- Störungen im Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschiedenen Kontakten (Öffner-Schließer-Kombination) in S1/S2 weitestgehend erkannt. Nach der Recommendation for Use (RfU) CNB/M/11.033/R/E Rev 06 können mechanische Fehler der Stellteile ausgeschlossen werden, wenn diese DIN EN 60947-5-1 entsprechen.



- Fehler in S1/S2 und in K2/K3 (mit Öffnerkontakten im Rückführkreis) werden in K1 erkannt und führen zum dauerhaften Abschalten über K2 und K3. Alle Einzelfehler werden bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt.
- Eine häufige Betätigung der elektromechanischen Elemente sorgt für eine ausreichend hohe Testrate (Dynamisierung).

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) wie in Abschnitt 8.1 beschrieben sind vorgesehen.
- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1. Daher können nach RfU CNB/M/11.033/R/E Rev 06 mechanische Fehler ausgeschlossen werden.
- Fehler in den Anschlussleitungen von S1 und S2 werden in der Logikeinheit erkannt. Wäre dies nicht möglich, so müssten die Bedingungen für einen Fehlerausschluss für Leitungskurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4, eingehalten werden. Wegen der geringen Ströme werden Taster mit Goldauflage empfohlen.
- Zum Anbau der Taster und zu Maßnahmen zur Vermeidung von versehentlicher Betätigung und von Umgehen siehe DIN EN 574, Abschnitte 8 und 9. Der Sicherheitsabstand zum Gefährdungsbereich muss ausreichend groß sein.
- Die Logikeinheit K1 entspricht Typ III C gemäß DIN EN 574 mit Selbstüberwachung und Erkennung interner Fehler. K1 ist ein geprüftes Sicherheitsbauteil für den Einsatz in Kategorie 4 und PL e.
- Die Hilfsschütze K2 und K3 besitzen zur Rücklesung zwangsgeführte Öffnerkontakte entsprechend DIN EN 60947-5-1, Anhang L.

Bemerkung

- Das dargestellte Beispiel eignet sich für die Anwendung z. B. an mechanischen Pressen (DIN EN 692).

Berechnung der Ausfallwahrscheinlichkeit

- K1 wird als Subsystem mit einer Ausfallwahrscheinlichkeit von $3{,}0 \cdot 10^{-9}$/Stunde [H] betrachtet. Der übrige Steuerungsteil wird zu einem Subsystem der Kategorie 4 zusammengefasst, dessen Ausfallwahrscheinlichkeit im Folgenden berechnet wird.
- Da S1 und S2 unabhängig voneinander beim Loslassen eine Abschaltung auslösen müssen, sind sie logisch in Reihe geschaltet. Dazu wurde je ein Schließerkontakt 13-14 und ein Öffnerkontakt 21-22 einem Steuerungskanal zugeordnet. Das sicherheitsgerichtete Blockdiagramm unterscheidet sich hier deutlich vom funktionalen Schaltplan. Wenn Zuverlässigkeitsdaten nur für die Taster insgesamt (Betätigungsmechanik plus Öffner- und Schließerkontakt) verfügbar sind, können die Ausfallwerte der Taster als Abschätzung zur sicheren Seite für die Ausfallwerte der Kontakte (plus Betätigungsmechanik) herangezogen werden.
- $MTTF_D$: Für S1 und S2 werden wegen des durch K1 erzeugten definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) B_{10D}-Werte von je 2 000 000 Schaltspielen [H] angenommen. Bei 240 Arbeitstagen, 8 Arbeitsstunden und 30 Sekunden Zykluszeit ist für diese Komponenten n_{op} = 230 400 Zyklen/Jahr und pro Kontakt $MTTF_D$ = 86,8 Jahre. Da K2 und K3 ebenfalls Steuerströme schalten, gelten für K2 und K3 B_{10D}-Werte von je 20 000 000 Zyklen [N] und daraus resultierende $MTTF_D$-Werte von 868 Jahren. Bei höheren Anforderungen (längere Arbeitszeit oder kürzere Zykluszeit) sind unter Umständen für K2/K3 höhere, durch den Hersteller abgesicherte B_{10D}-Werte erforderlich. Insgesamt ergibt sich ein $MTTF_D$-Wert pro Kanal von 41 Jahren („hoch“).
- DC_{avg}: DC = 99 % für S1 und S2 ergibt sich durch die direkte Überwachung mithilfe der Öffner-Schließer-Kombinationen in K1. DC = 99 % für K2 und K3 gründet sich auf dem Rücklesen der zwangsgeführten Öffnerkontakte im Rückführkreis von K1. Die hohe Betätigungsdynamik in der Anwendung führt zu einer häufigen Testung (siehe Abschnitt 6.2.14). Durch Mittelung ergibt sich damit ein DC_{avg} von 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_D$ pro Kanal (41 Jahre) und hohem DC_{avg} (99 %). Für die Kombination von S1, S2, K2 und K3 ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}7 \cdot 10^{-8}$/Stunde. Wird ein Wert von $3{,}0 \cdot 10^{-9}$/Stunde [G] für K1 hinzuaddiert, so ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}0 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Unter Umständen ist zur Komplettierung der Sicherheitsfunktion zusätzlich die Ausfallwahrscheinlichkeit nachgeordneter Leistungselemente zu addieren.
- Die verschleißbehafteten Elemente S1 und S2 sollten nach jeweils ca. acht Jahren (T_{10D}) ausgetauscht werden.

Weiterführende Literatur

- DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte – Gestaltungsleitsätze (12.08). Beuth, Berlin 2008 (vorgesehener Ersatz durch ISO 13851)
- Recommendation for Use. Hrsg.: Vertikalgruppe 11 (VG 11) im europäischen Erfahrungsaustausch notifizierter Prüfstellen ▸ http://ec.europa.eu/DocsRoom/documents/14265/attachments/1/translations/en/renditions/native CNB/M/11.033/R/E Rev 06, S. 181, November 2015

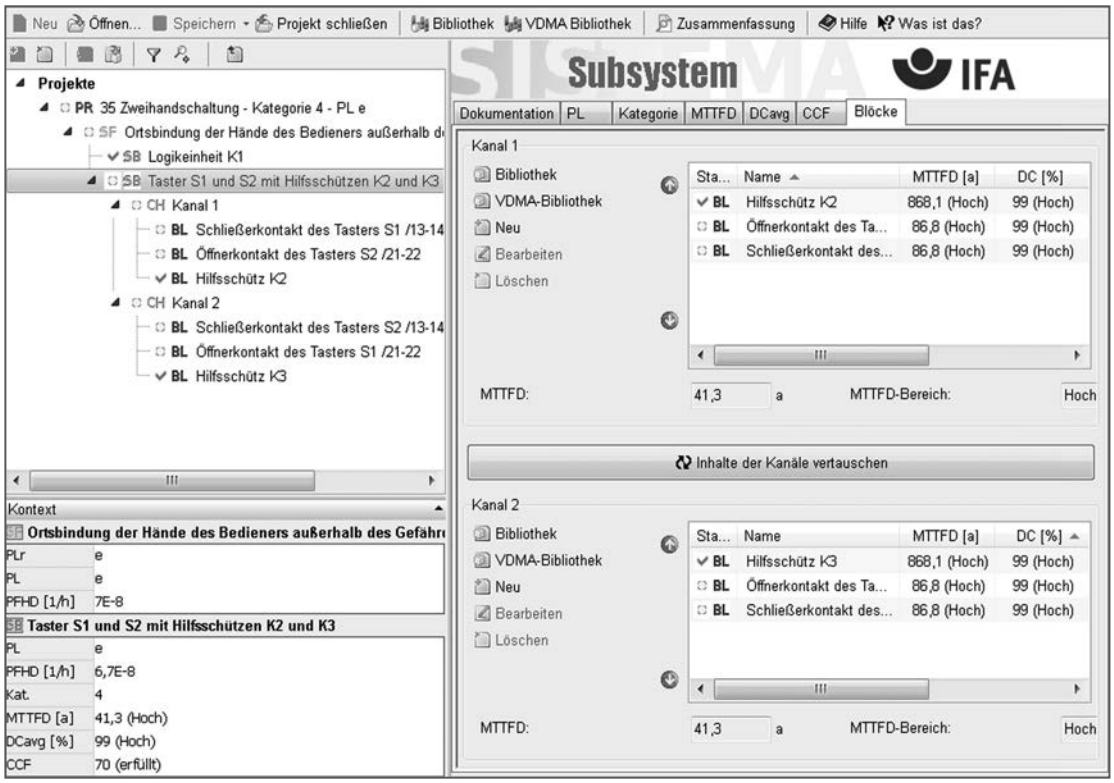


Abbildung 8.69: PL-Bestimmung mithilfe von SISTEMA

8.2.36 Verarbeitung von Signalen einer Lichtschranke – Kategorie 4 – PL e (Beispiel 36)

Dieses Beispiel entfällt, da es technologisch nicht mehr relevant ist

8.2.37 Planschneidemaschine mit programmierbarer elektronischer Logiksteuerung – Kategorie 4 – PL e (Beispiel 37)

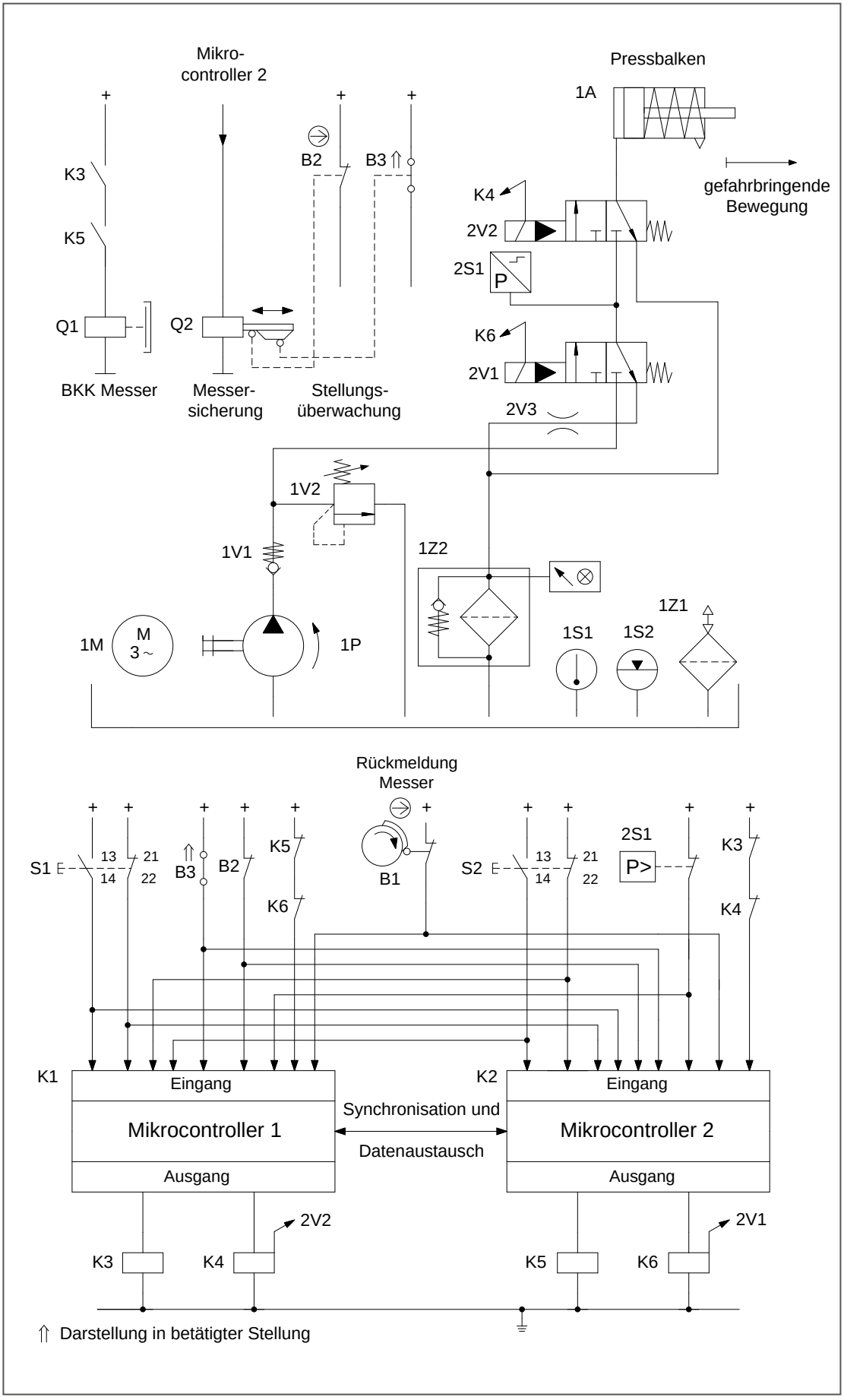
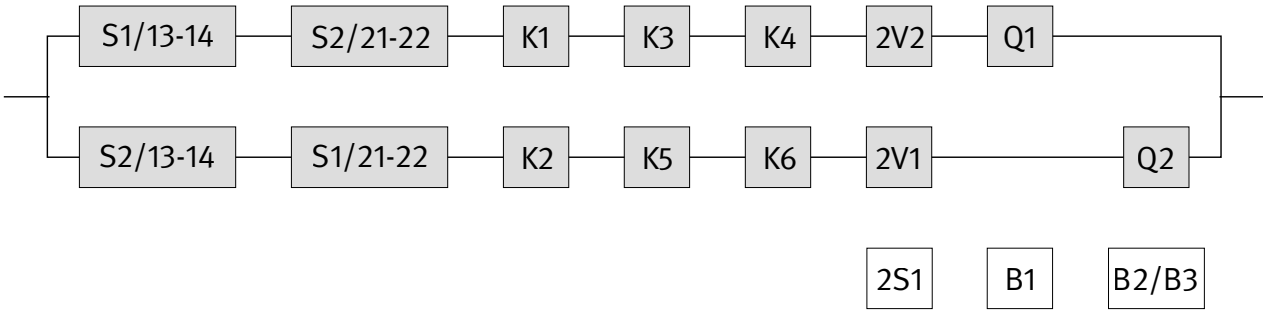


Abbildung 8.70: Ansteuerung eines elektrischen Messerantriebs und eines hydraulischen Pressbalkens



Sicherheitsfunktion

- Ortsbindung der Hände einer einzelnen Bedienperson außerhalb des Gefährdungsbereiches während der Press- und Schneidbewegung: Beim Loslassen mindestens eines der beiden Taster S1/S2 wird die Freigabe aufgehoben und so lange blockiert, bis beide Taster entlastet und erneut synchron betätigt werden.

Funktionsbeschreibung

- Die Betätigung der Zweihandschaltung (ZHS) S1 und S2 startet die gefahrbringenden Bewegungen (Bearbeitungszyklus) des Pressbalkens (Hydraulik) 1A und des Messers (Elektromechanik). Wird während eines Zyklus auch nur ein Taster S1 oder S2 losgelassen oder erfolgt ein Signalwechsel in der Peripherie der Maschine (z. B. Lichtgitter, im Schaltbild nicht dargestellt) nicht wie durch die Steuerung erwartet, stoppt der Zyklus und die Maschine verbleibt in diesem sicheren Zustand. Das Messer und der Pressbalken stellen wegen ihrer unmittelbaren räumlichen Nähe zueinander eine gemeinsame Gefahrstelle dar; die Gefährdung wiederholt sich zyklisch. Nicht explizit dargestellt ist der Antrieb des Messers durch einen Exzenterantrieb, dessen Energie aus einer kontinuierlich laufenden Schwungmasse entnommen wird. Der Pressbalken wird linear durch eine Hydraulik angetrieben, deren Pumpe an den Antrieb der Schwungmasse gebunden ist.
- Mit Drücken der Taster S1/S2 (ZHS) werden die Signalwechsel beiden Mikrocontrollern K1 und K2 zugeführt. Erfüllen diese Signale die Anforderungen an die Gleichzeitigkeit nach Norm (DIN EN 574, Typ III C) und erfüllen alle peripheren Signale eine Startbedingung, setzen K1 und K2 die Ausgänge für eine gültige Schnittanforderung. Über die Hilfsschütze K3 bis K6 kontrolliert jeder Mikrocontroller beide gefahrbringenden Bewegungen. Über zwei hydraulische Ventile 2V1 und 2V2 kann die Schließbewegung des Pressbalkens 1A unterbunden werden. Die Ansteuerung der Brems-/Kupplungskombination (BKK) Q1 kann über K3 und K5 unterbunden werden. Eine geeignet dimensionierte mechanische Konstruktion einer Messersicherung Q2 muss zusätzlich zyklisch von K2 freigegeben werden. Bei erkannten Fehlern in Q1 kann damit spätestens im Folgezyklus der Messerdurchlauf verhindert werden.
- Fehler in den Schaltern S1/S2 oder in den Hilfsschützen K3 bis K6 mit zwangsgeführten Rücklesekontakten werden durch einen Kreuzvergleich in den Mikrocontrollern erkannt. Die Funktion von 2V1/2V2 wird mithilfe des Druckschalters 2S1 überwacht. Da die Mikrocontroller während des Betriebs im Hintergrund zusätzlich Selbsttests ausführen, können hier interne Fehler und Fehler in der Peripherie rechtzeitig erkannt werden.
- Alle Maschinenzustände werden durch beide Mikrocontroller überwacht und gesteuert. Durch den zyklischen Ablauf eines Schnittes werden alle Systemzustände ebenfalls zyklisch durchlaufen und untereinander verglichen. Fehler und Abweichungen von definierten Zwischenzuständen führen spätestens nach einem durchlaufenen Zyklus zum Stopp der Maschine. Dieses Verfahren ist im Schaltbild durch „Rückmeldung Messer“ B1 und „Stellungsüberwachung“ B2/B3 der Messersicherung Q2 angedeutet.
- Die Überwachung eines Verschleißes der Bremse erfolgt mithilfe von Positionsschalter B1. Schon bei minimal erhöhtem Nachlauf wird B1 angefahren und ein weiterer Schnitt steuerungstechnisch verhindert.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1.
- B1 und B2 sind zwangsöffnende Positionsschalter entsprechend DIN EN 60947-5-1, Anhang K.
- K3 bis K6 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Anschlussleitungen der Positionsschalter sind entweder getrennt oder gegen mechanische Beschädigung geschützt verlegt.
- Die Software der homogen redundanten Rechnerstruktur entspricht den Anforderungen der DIN EN 61508-3, Abschnitt 7, für SIL 3.

- Für den Fehler „vollständiges Versagen der Brems-/Kupplungskombination“, d. h. Nicht-Auskuppeln bei zurückgezogener Schnittfreigabe nach ausgelöstem Schnitt, erfolgt ein Fehlerausschluss. Dieser begründet sich in langjähriger Erfahrung und den konstruktiven Merkmalen der Brems-/Kupplungs-Kombination mit der Möglichkeit, einen Bremsenverschleiß frühzeitig zu bemerken.
- Die Bauteile B1 und B2/B3 werden benötigt, um die in DIN EN 1010-3 geforderten Maßnahmen zu Messerstillstand und Messernachlauf umzusetzen.

Berechnung der Ausfallwahrscheinlichkeit

- Die vorgesehene Architektur für Kategorie 4 für die Ansteuerung des Messerantriebs und des Pressbalkens wird wie beschrieben durch zwei unabhängige Kanäle realisiert. Da die Kanäle nahezu identisch aufgebaut sind und mit gleichen Zahlenwerten berechnet werden, ist eine Symmetrisierung nicht erforderlich. Zur Vereinfachung wird die Ansteuerung von Q1 nur einkanalig angenommen. Die berechnete Ausfallwahrscheinlichkeit ist daher in der Realität geringfügig kleiner.
- Da S1 und S2 unabhängig voneinander beim Loslassen eine Abschaltung auslösen müssen, sind sie logisch in Reihe geschaltet. Dazu wurde je ein Schließerkontakt 13-14 und ein Öffnerkontakt 21-22 einem Steuerungskanal zugeordnet. Das sicherheitsgerichtete Blockdiagramm unterscheidet sich hier deutlich vom funktionalen Schaltplan. Als Abschätzung zur sicheren Seite wird der B_{10D}-Wert für jeden einzelnen Schaltkontakt verwendet.
- $MTTF_D$: Bei 240 Arbeitstagen, 8 Arbeitsstunden und 60 Sekunden Zykluszeit beträgt n_{op} = 115 200 Schaltspiele/Jahr. Für S1 und S2 werden, aufgrund langjähriger Erfahrung im Bau dieser Maschinen zusammen mit entsprechenden Qualitätsaufzeichnungen und konstruktiven Maßnahmen wie dem definierten Steuerstrom (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend), vom Maschinenhersteller B_{10D}-Werte von je 2 000 000 Schaltspielen [G] angenommen und damit eine $MTTF_D$ = 173 Jahre. Für die Mikrocontroller einschließlich ihrer Peripherie wird nach SN 29500-2 eine $MTTF_D$ von 878 Jahren [D] angegeben. Für die Hilfsschütze K3 bis K6 gilt bei geringer Last B_{10D} = 20 000 000 Schaltspiele [N] und damit $MTTF_D$ = 1736 Jahre. Für die Brems-/Kupplungskombination Q1 wird der $MTTF_D$-Wert von 607 Jahre aus B_{10D} = 7 000 000 Zyklen [G] errechnet. Der gleiche Wert wird für die Messersicherung Q2 im zweiten Kanal angenommen. Die Werte für die beiden Wegeventile 2V1 und 2V2 betragen 150 Jahre [N]. Diese Werte ergeben eine $MTTF_D$ eines Kanals von 45,2 Jahren („hoch“).
- DC_{avg}: *DC = 99 %* für S1/S2 basiert auf dem Kreuzvergleich von Eingangssignalen ohne dynamischen Test mit häufigem Signalwechsel. *DC = 90 %* für K1/K2 folgt aus Selbsttests durch Software und dynamischem Kreuzvergleich von Daten mit zeitlicher Erwartungshaltung. *DC = 99 %* für K3 bis K6 ergibt sich durch Plausibilitätsprüfung über zwangsgeführte Kontakte. Für 2V1/2V2 ist der *DC = 99 %* wegen indirekter und direkter Überwachung durch elektrische Drucküberwachung bei häufigem Signalwechsel. Ein Verschleiß der Kupplung führt zu einem geänderten Schnittverhalten. Dieses Verhalten wird messtechnisch erfasst und daher für Q1 ein *DC = 99 %* angenommen. Ein Ausfall von Q2 wird infolge der zyklischen Betätigung und der Überwachungselemente B1 und B3 sofort bemerkt. Damit wird ein *DC = 99 %* begründet. Diese Werte ergeben einen DC_{avg} von 98,5 % (im Toleranzbereich von „hoch“).
- Ausreichende Maßnahmen gegen Fehler gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebung (25 + 10)
- Für Kategorie 4 ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für die verschleißbehafteten Elemente S1 und S2 ein Wert von über 17 Jahren (T_{10D}) für den vorgesehenen Austausch.

Weiterführende Literatur

- DIN EN 1010-3: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 3: Schneidemaschinen (06.10). Beuth, Berlin 2010
- DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze (12.2008). Beuth, Berlin 2008
- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (04.10). Beuth, Berlin 2010

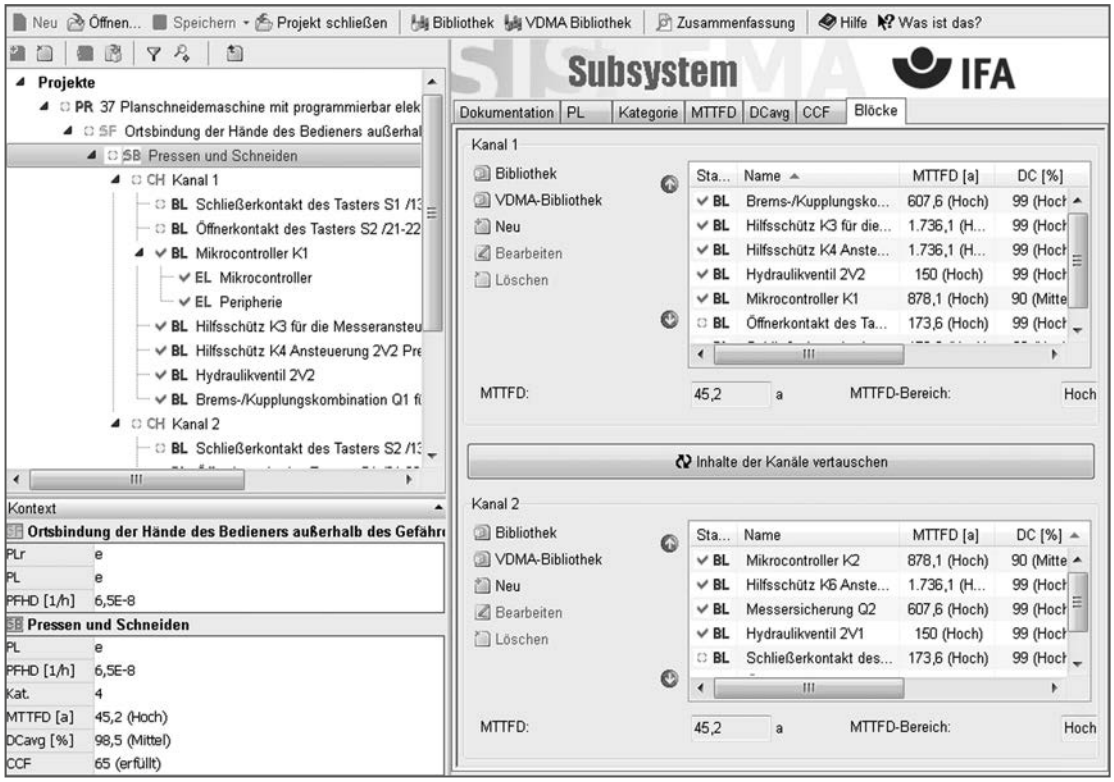
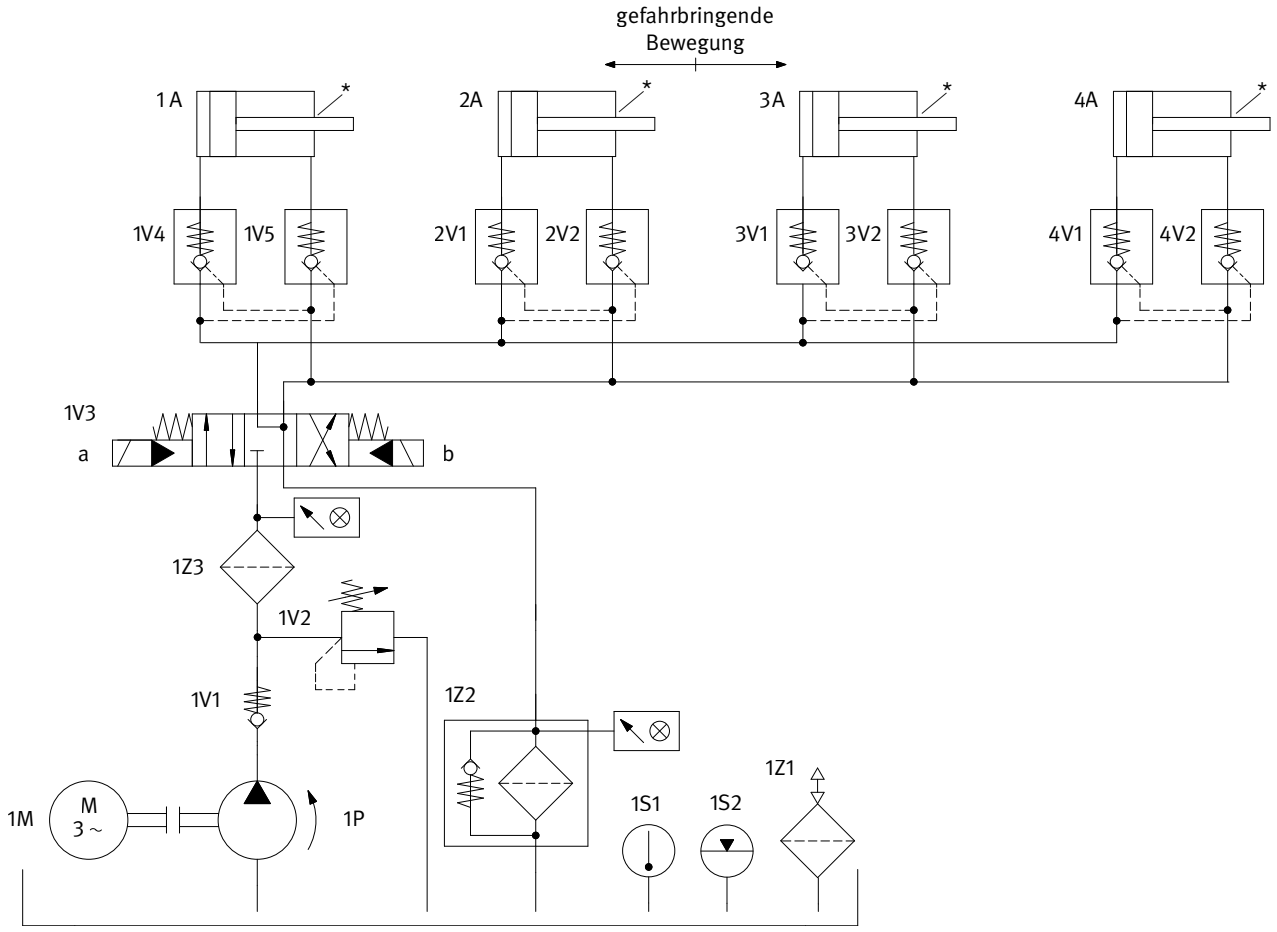


Abbildung 8.71:
PL-Bestimmung mithilfe von SISTEMA

8.2.38 Hydraulische Ventilsteuerung (Subsystem) – Kategorie 1 – PL c (Beispiel 38)

Abbildung 8.72:
Hydraulische Ventile zur Steuerung von gefahrbringenden Bewegungen

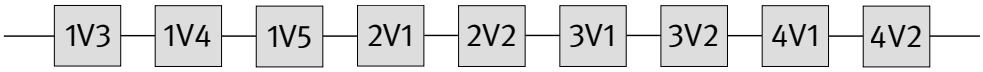


Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage
- In diesem Beispiel ist nur der hydraulische Steuerungsteil als Subsystem dargestellt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch vier Aktoren 1A bis 4A ausgeführt. Ein Stillsetzen der Bewegungen erfolgt über das sicherheitstechnisch bewährte Wegeventil 1V3 in Verbindung mit den sicherheitstechnisch bewährten entsperrbaren Rückschlagventilen.
- Der Ausfall des Wegeventils oder eines der entsperrbaren Rückschlagventile kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit der Ventile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V3 handelt es sich um ein Wegeventil mit ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- Bei den Ventilen 1V4, 1V5, 2V1, 2V2, 3V1, 3V2, 4V1 und 4V2 handelt es sich um entsperrbare Rückschlagventile.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Bestätigung für das Wegeventil und die entsperrbaren Rückschlagventile als sicherheitstechnisch bewährtes Bauteil erfolgt durch den Hersteller/Anwender.
- Als gezielte Maßnahmen zur Erhöhung der Zuverlässigkeit der Ventile sind ein Druckfilter 1Z3 vor dem Wegeventil und geeignete Maßnahmen gegen Schmutzeinzug durch die Kolbenstange am Zylinder (z. B. wirksamer Abstreifer an den Kolbenstangen, siehe * in Abbildung 8.72) vorgesehen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_D$: Für das Wegeventil und die entsperrbaren Rückschlagventile wird jeweils eine $MTTF_D$ von 600 Jahren angenommen [N], da die Schaltspielzahl der Ventile für diese Anwendung zwischen 250 000 und 500 000 pro Jahr (n_{op}) liegt.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Der hydraulische Teil der Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (66,7 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}7 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

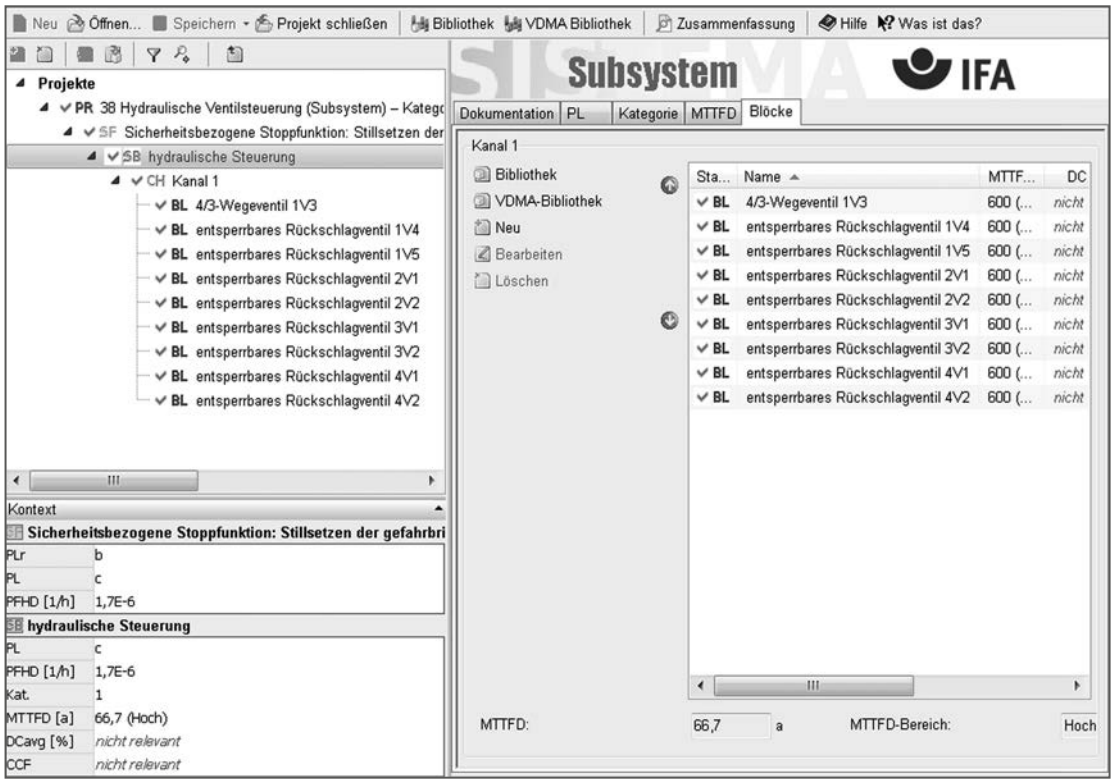


Abbildung 8.73: PL-Bestimmung mithilfe von SISTEMA

9 Literatur

[1] Richtlinie 98/37/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen. ABl. EG (1998) Nr. L 207, S. 1-46; geänd. durch Richtlinie 98/79/ EG – ABl. EG (1998) Nr. L 331, S. 1-37
▸ http://eur-lex.europa.eu

[2] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). ABl. EU (2006) Nr. L 157, S. 24-86
▸ http://eur-lex.europa.eu

[3] DIN EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (03.11). Beuth, Berlin 2011

[4] DIN ISO/TR 14121-2: Sicherheit von Maschinen – Risikobeurteilung – Teil 2: Praktische Anleitung und Verfahrensbeispiele (02.13). Beuth, Berlin 2013

[5] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (06.16). Beuth, Berlin 2016

[6] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (02.13). Beuth, Berlin 2013

[7] *Ostermann, H.-J.; von Locquenghien, D.:* Wegweiser Maschinensicherheit. Bundesanzeiger Verlagsgesellschaft, Köln 2007

[8] *Reudenbach, R.:* Sichere Maschinen in Europa – Teil 1: Europäische und nationale Rechtsgrundlagen. 8. Aufl. Technik & Information, Bochum 2007

[9] DIN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (03.97). Beuth, Berlin 1997

[10] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1 bis Teil 7 (02.11). Beuth, Berlin 2011

[11] DIN EN 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (05.16). Beuth, Berlin 2016

[12] *Bömer, T.:* Funktionale Sicherheit nach IEC 61508. In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2. Aufl. 2003. Kennzahl 330 219. Lfg. 2/14, XII/2014. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin. Erich Schmidt, Berlin 2003 – Losebl.-Ausg.
▸ www.ifa-handbuchdigital.de/330219

[13] *Hauke, M.; Schaefer, M.:* Sicherheitsnorm mit neuem Konzept. O + P Ölhydraulik und Pneumatik 50 (2006) Nr. 3, S. 142-147
▸ www.dguv.de/medien/ifa/de/pra/en13849/aenderung_1_von_en13849_1.pdf

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

[15] *Hauke, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Rempel, P.; Ostermann, B.:* Änderung der DIN EN ISO 13849-1 – Die wesentlichen Neuerungen aus 2015 im Überblick. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2015
▸ www.dguv.de/medien/ifa/de/pub/grl/pdf/2006_016.pdf

[16] *Schaefer, M.; Hauke, M.:* Performance Level Calculator – PLC. 5. Aufl. Hrsg.: Institut für Arbeitsschutz (IFA) der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V. – Fachverband Automation, Frankfurt am Main, und Verband Deutscher Maschinen- und Anlagenbau e.V. – VDMA, Frankfurt am Main 2015
▸ www.dguv.de/ifa, Webcode d3508

[17] Übersicht über die Prüfgrundsätze des DGUV Test.
▸ www.dguv.de/ifa, Webcode: d11817

[18] Summary list of titles and references of harmonised standards under Directive 2006/42/EC on Machinery. Hrsg.: European Commission
▸ http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/machinery/index_en.htm

[19] IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2. Aufl. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin. Erich Schmidt, Berlin 2003 – Losebl.-Ausg.
▸ www.ifa-handbuchdigital.de

[20] DIN EN 61800-5-2: Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (08.14). Beuth, Berlin 2017

[21] VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (08.16). Beuth, Berlin 2016

[22] *Apfeld R.; Zilligen H.; Köhler B.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA-Report 7/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2013
▸ www.dguv.de/ifa, Webcode: d639540

[23] Das SISTEMA-Kochbuch 6: Definition von Sicherheitsfunktionen – Was ist wichtig? Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2015
▸ www.dguv.de/ifa, Webcode: d109240

[24] *Apfeld, R.; Schaefer, M.:* Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachmesse und Kongress SPS/IPC DRIVES, 23.-25. November 2010, Nürnberg – Vortrag
▸ www.dguv.de/ifa, Webcode: d18471

[25] DIN EN 60204-1; VDE 0113-1:2007-06: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

[26] Interpretationspapier zum Thema „Wesentliche Veränderung von Maschinen". Bek. des BMAS vom 09.04.15 – IIIb5-39607-3. GMBl. (2015) Nr. 10, S. 183-186
▸ www.bmas.de/DE/Themen/Arbeitsschutz/Produktsicherheit/interpretationspapier-wesentliche-veraenderung-von-maschinen.html

[27] DIN EN 1010-3: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 3: Schneidemaschinen (06.10). Beuth, Berlin 2010

[28] DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Gemeinsame Anforderungen (06.11). Beuth, Berlin 2011

[29] *Apfeld, R.; Huelke, M.; Lüken, K.; Schaefer, M., et al.:* Manipulation von Schutzeinrichtungen an Maschinen. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006
▸ www.dguv.de/ifa, Webcode: d6303
▸ www.stopp-manipulation.org

[30] DGUV Information 209-068/069 (bisher: BGI/GUV-I 5048-1/2): Ergonomische Maschinengestaltung, Checkliste, Auswertungsbogen und Informationen (12.2010). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Sankt Augustin 2010
▸ www.dguv.de/ifa, Webcode d3443

[31] VDI/VDE 3850: Gebrauchstaugliche Gestaltung von Benutzungsschnittstellen für technische Anlagen. Blatt 1: Konzepte, Prinzipien und grundsätzliche Empfehlungen (04/14). Blatt 2: Interaktionsgeräte für Bildschirme (01/17). Blatt 3: Merkmale, Gestaltung und Einsatzmöglichkeiten von Benutzungsschnittstellen mit Touchscreens (11/15). Beuth, Berlin 2014/2015/2017

[32] *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 2011
▸ www.dguv.de/ifa, Webcode: d109240

[33] *Birolini, A.:* Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management. 3. Aufl. Springer, Berlin 1991

[34] *Apfeld, R.; Hauke, M.; Schaefer, M.; Rempel, P.; Ostermann, B.:* Das SISTEMA-Kochbuch – Teil 1: Vom Schaltbild zum Performance Level – Quantifizierung von Sicherheitsfunktionen mit SISTEMA – Version 1.0 (DE). Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2010
▸ www.dguv.de/ifa, Webcode: d109240

[35] DIN EN ISO 14119: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (03.14). Beuth, Berlin 2014

[36] Vertical Recommendation for Use Sheets (RfUs) – Status on November 2015, Number CNB/M/11.050/R/E Rev 05, S. 191, Hrsg.: European Co-Ordination of Notified Bodies Machinery Directive 2006/42/EC + Amendment, 2015
▸ http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery

[37] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (02.11). Beuth, Berlin 2011

[38] Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten (GS-ET-26). Hrsg.: Fachbereich Energie Textil Elektro Medienerzeugnisse, Köln 2014
▸ www.bgetem.de, Webcode: 12677093

[39] DIN EN 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2010) (02.11). Beuth, Berlin 2011

[40] *Reinert, D.; Schaefer, M.:* Sichere Bussysteme für die Automation. Hüthig, Heidelberg 2001

[41] *Huckle, T.:* Kleine BUGs, große GAUs. Vortrag zum Thema „Softwarefehler und ihre Folgen".
▸ http://www5.in.tum.de/~huckle/bugsn.pdf

[42] DIN EN 61508-3: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (02/11). Beuth, Berlin 2011

[43] *Huelke, M.; Becker, N.; Eggeling, M.:* Sicherheitsbezogene Anwendungssoftware von Maschinen – Die Matrixmethode des IFA. IFA Report 2/2016. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2016
▸ www.dguv.de/ifa, Webcode: d1023063

[44] Software-Assistent SOFTEMA: Spezifikation zur IFA-Matrixmethode bei sicherheitsbezogener Anwendungssoftware. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin
▸ www.dguv.de/ifa, Webcode: d1082520

[45] *Friedrich, J.; Kuhrmann, M.; Sihling, M.; Hammerschall, U.:* Das V-Modell XT für Projektleiter und QS-Verantwortliche kompakt und übersichtlich. Springer, Berlin 2009

[46] DIN EN 61131-3: Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (06.14). Beuth, Berlin 2014

[47] MISRA C:2012. Guidelines for the Use of the C Language in Critical Systems.
▸ www.misra.org.uk

[48] DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (02.11). Beuth, Berlin 2011

[49] SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Hrsg.: Siemens AG, Center for Quality Engineering, München 1994 bis 2005

[50] *Mai, M.; Reuß, G.:* Selbsttests für Mikroprozessoren mit Sicherheitsaufgaben. BGIA-Report 7/2006. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006
▸ www.dguv.de/ifa, Webcode: d6163

[51] DIN EN 82079-1: Erstellen von Gebrauchsanleitungen – Gliederung, Inhalt und Darstellung – Teil 1: Allgemeine Grundsätze und ausführliche Anforderungen (06.13). Beuth, Berlin 2013

[52] ISO 9355: Ergonomic requirements for the design of displays and control actuators – Part 1: Human interactions with displays and control actuators (12/99), Part 2: Displays (09/06), Part 3: Control actuators (12/99). ISO Central Office, Genf, Schweiz 1999 und 2006

[53] Leitfaden Software-Ergonomie; Gestaltung von Bedienoberflächen. VDMA Verlag, Frankfurt am Main 2004

[54] DIN EN ISO 9241-11: Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte, Entwurf 01.2017, Beuth, Berlin 2017

[55] DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze (12.08). Beuth, Berlin 2008

[56] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (04.10). Beuth, Berlin 2010

[57] *Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M., et al.:* Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849. BGIA-Report 2/2008. 2. Aufl. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2008
▸ www.dguv.de/ifa, Webcode: d18588

[58] DIN EN ISO 4413: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile (04.11). Beuth, Berlin 2011

[59] DIN EN ISO 4414: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile (04.11). Beuth, Berlin 2011

[60] DIN EN 1037: Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf (11.08), Beuth, Berlin 2008

[61] ISO 1219-1: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 1: Graphische Symbole für konventionelle und datentechnische Anwendungen (06/12). Beuth, Berlin 2012

[62] ISO 1219-2: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 2: Schaltpläne (09.12). Beuth, Berlin 2012

[63] ISO 8573-1: Druckluft – Teil 1: Verunreinigungen und Reinheitsklassen (04.10). Beuth, Berlin 2010

Anhang A:
Beispiele zur Risikobeurteilung

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Definition der Sicherheitsfunktionen erweitert
- Einschätzung der Häufigkeit und Expositionsdauer detaillierter dargestellt
- Berücksichtigung Unfallgeschehen ergänzt

Beispiel 1: Schließkantensicherung

In Abbildung A.1 ist die Risikobeurteilung für die Sicherheitsfunktion

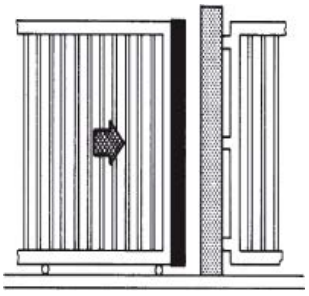
- SF1 – Unterbrechung der Schließbewegung und Reversieren bei Erkennung eines Hindernisses

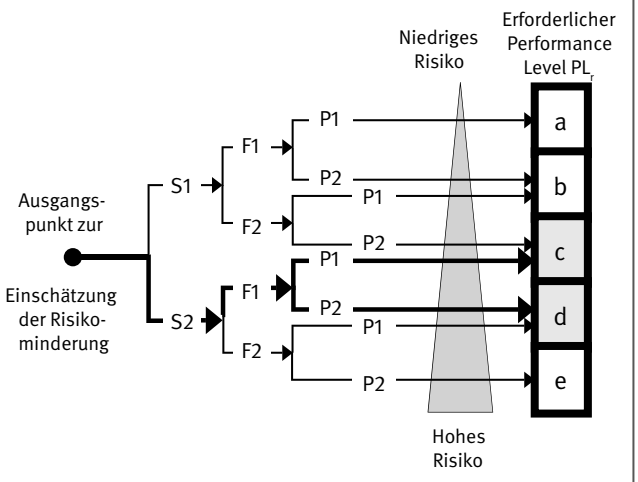
einer Schließkantensicherung[1] dargestellt. Mit der Bewegung kraftbetätigter Fenster-, Tür- und Torflügel (siehe Abbildung A.1) ist in der Regel die Bildung von Quetsch- und Scherstellen verbunden. Diese Gefahrstellen bestehen im Allgemeinen nur dann, wenn sich der Flügel seinen Endstellungen nähert. Verletzungen von Personen an derartigen Gefahrstellen lassen sich z. B. durch Schließkantensicherungen vermeiden. Schließkantensicherungen, z. B. Schaltleisten, werden auf die Schließkanten der Flügel gesetzt. Bei Erkennung eines Hindernisses wird die Schließbewegung unterbrochen und eine rückläufige Bewegung eingeleitet.

Quetsch- und Scherstellen können an kraftbetätigten Fenster-, Tür- und Torflügeln Ursache für schwere, unter Umständen tödliche Verletzungen sein, sodass als Schadensausmaß S2 angenommen werden muss. Personen halten sich im Bereich der zeitlich begrenzt auftretenden Quetsch- und Scherstellen nur selten (Häufigkeit geringer als einmal alle 15 Minuten) und auch nur für kurze Zeit (Expositionsdauer insgesamt geringer als 1/20 der gesamten Betriebsdauer) auf (F1). Normalerweise haben gefährdete Personen die Möglichkeit, sich aus dem vom bewegten Flügel gebildeten Gefahrenbereich zu entfernen (P1), damit ergibt sich ein erforderlicher Performance Level PL_r = c. Dieses Ergebnis wird durch die Produktnorm DIN EN 12453 bestätigt. Das Normungsgremium hatte offensichtlich keine Veranlassung, aufgrund des Unfallgeschehens hiervon abzuweichen. Wie man diese Sicherheitsfunktion realisieren kann, ist im Beispiel 13 in [1] beschrieben.

Bei Schnelllauftoren ist es kaum möglich, sich rechtzeitig aus dem Gefahrenbereich zu entfernen. Durch die Einschätzung P2 anstatt P1 ergibt sich daher für diese Produkte ein erforderlicher Performance Level PL_r = d.

Abbildung A.1:
Risikobeurteilung für die Schließkantensicherung an kraftbetätigten Fenstern, Türen und Toren





S2 – ernste irreversible Verletzung
F1 – seltene Exposition oder kurze Dauer
P1 – Vermeidung der Gefährdung möglich
P2 – Vermeidung der Gefährdung kaum möglich

[1] Schließkantensicherungen fielen früher unter die Bauproduktrichtlinie. Da die eingesetzten Schaltleisten jedoch Sicherheitsbauteile nach der Maschinenrichtlinie sind, werden auch Schließkantensicherungen nach dieser Richtlinie bewertet.

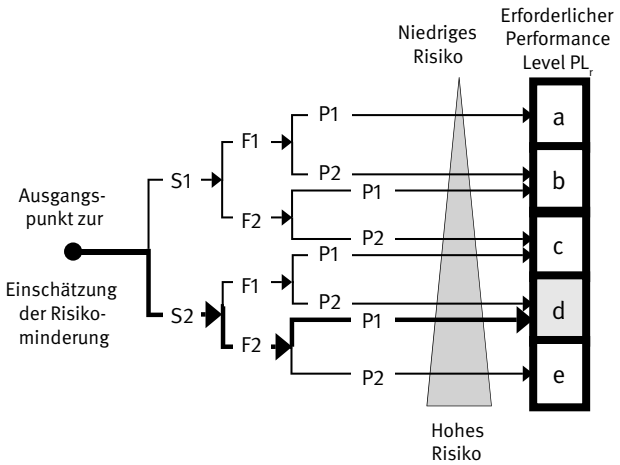
Beispiel 2: Fahrerloses Transportfahrzeug

An fahrerlosen Transportfahrzeugen wird für den Auffahrschutz die Sicherheitsfunktion

- SF1 – Stillsetzen des Transportfahrzeugs bei Annäherung an ein Hindernis

eingesetzt. Da sich ein fahrerloses Transportfahrzeug unter Umständen mit tonnenschwerer Last bewegt, ist eine schwere irreversible Verletzung bei einer Kollision mit dem Fahrzeug, wenn sie bei voller Geschwindigkeit stattfindet, wahrscheinlich (S2). Die Fahrwege des Fahrzeugs sind für Personen frei zugänglich; deshalb muss mit einem relativ häufigen Aufenthalt von Personen im Gefahrenbereich (Häufigkeit höher als einmal alle 15 Minuten) gerechnet werden (F2). Da das Fahrzeug mit recht niedriger Geschwindigkeit fährt (in der Regel 3 bis 5 km/h), hat eine Person bei Herannahen eines solchen Fahrzeugs meist die Möglichkeit auszuweichen (P1). Für SF1 ergibt sich damit ein erforderlicher Performance Level PL_r = d (siehe Abbildung A.2). Dieses Ergebnis wird durch die Produktnorm DIN EN 1525 bestätigt. Das Normungsgremium hatte offensichtlich keine Veranlassung, aufgrund des Unfallgeschehens hiervon abzuweichen.

Abbildung A.2:
Risikobeurteilung für den Auffahrschutz an einem fahrerlosen Flurförderzeug



S2 – ernste irreversible Verletzung
F2 – häufige Exposition oder lange Dauer
P1 – Vermeidung der Gefährdung möglich

Beispiel 3: Webmaschine

Webmaschinen werden zum vollautomatischen Weben von Stoffen eingesetzt. Die wesentliche Gefährdung besteht in der Quetschung zwischen Webblatt und Breithalter. Bei Kettfadenbrüchen muss die Bedienperson bei stehender Maschine in die Gefahrenstelle eingreifen, um die Kettfadenenden wieder zu verbinden. Zur Verhinderung des unerwarteten Anlaufs wird die Sicherheitsfunktion

- SF1 – Bei Eingreifen in den Gefahrenbereich Verhinderung eines unerwarteten Anlaufs durch Sicher abgeschaltetes Moment (STO – Safe Torque Off) aller Antriebe

eingesetzt. Bei einem Maschinenanlauf kann es zu Fingerquetschungen und -brüchen kommen (S2). Die Häufigkeit der Gefährdungsexposition kann mit selten (geringer als einmal alle 15 Minuten) bezeichnet werden, die gesamte Expositionsdauer ist geringer als 1/20 der gesamten Betriebsdauer (F1). Befinden sich die Hände der Bedienperson bereits im Gefahrenbereich, während es zu einem unerwarteten Anlauf kommt, ist diese Bewegung so schnell, dass ein Ausweichen kaum möglich ist (P2). Damit ergibt sich für SF1 ein erforderlicher Performance Level PL_r = d (siehe Abbildung A.3). Dieses Ergebnis wird durch die Produktnorm DIN EN ISO 11111-6 bestätigt. Das Normungsgremium hatte offensichtlich keine Veranlassung, aufgrund des Unfallgeschehens hiervon abzuweichen.

Beispiel 4: Rotationsdruckmaschine

In einer Rollenrotationsdruckmaschine wird eine Papierbahn durch eine Vielzahl von Zylindern geführt. Insbesondere für den Einsatz im Zeitungsdruck werden hohe Verarbeitungsgeschwindigkeiten und hohe Drehzahlen der Zylinder erreicht. Wesentliche Gefährdungen bestehen an den Einzugsstellen der gegenläufigen Zylinder. In diesem Beispiel wird eine Gefahrenstelle einer Druckmaschine betrachtet, an der zu Wartungsarbeiten manuelle Eingriffe bei reduzierten Maschinengeschwindigkeiten durchgeführt werden. Der Zugang zur Einzugsstelle wird durch eine Schutztür (Verschutzung) gesichert. Folgende Sicherheitsfunktionen sind vorgesehen:

- SF1 – Durch das Öffnen der Schutztür während des Betriebs werden die Zylinder bis zum Stillstand abgebremst.
- SF 2 – Bei geöffneter Schutztür dürfen Maschinenbewegungen nur mit begrenzten Drehzahlen erfolgen.
- SF 3 – Bei geöffneter Schutztür sind Bewegungen nur während der Betätigung eines Tipptasters möglich.

Ein Einzug zwischen die Zylinder führt zu schweren Verletzungen (S2). Da Tätigkeiten im Gefahrenbereich nur zu Wartungsarbeiten anfallen, kann die Häufigkeit der Gefährdungsexposition mit selten (geringer als einmal alle 15 Minuten) bezeichnet werden, die gesamte Expositionsdauer ist geringer als 1/20 der gesamten Betriebsdauer (F1). Die Möglichkeit, der gefahrbringenden Bewegung auszuweichen, ist bei Produktionsgeschwindigkeiten nicht gegeben (P2). Für die Sicherheitsfunktionen SF1 und SF2 ergibt sich daher ein erforderlicher Performance Level PL_r = d (siehe Abbildung A.4). Die Sicherheitsfunktion SF3 jedoch kann

Abbildung A.3:
Risikobeurteilung für eine Webmaschine

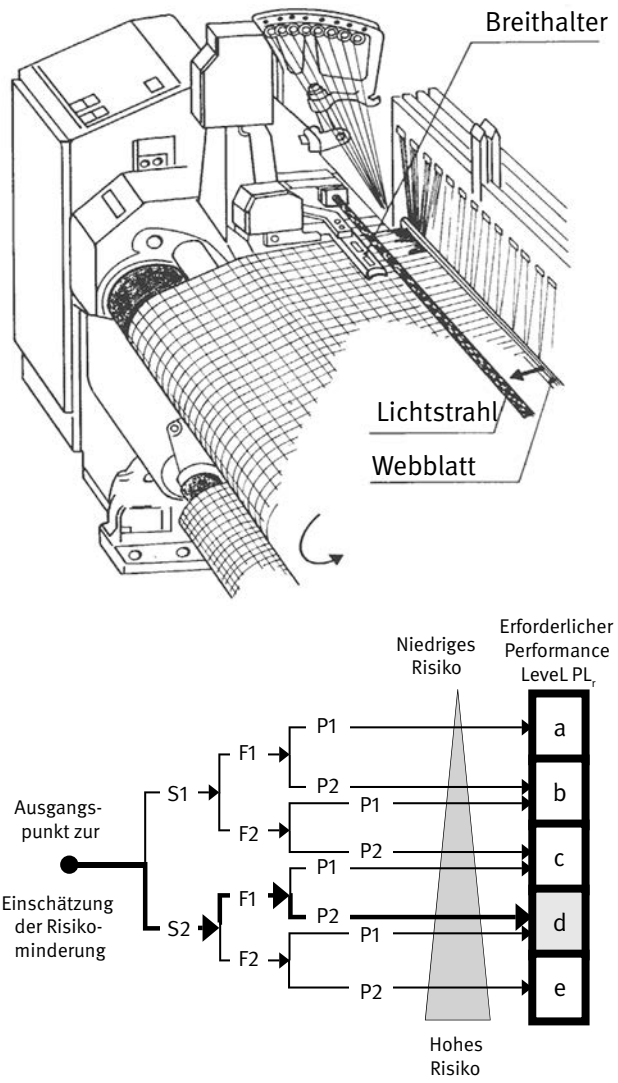
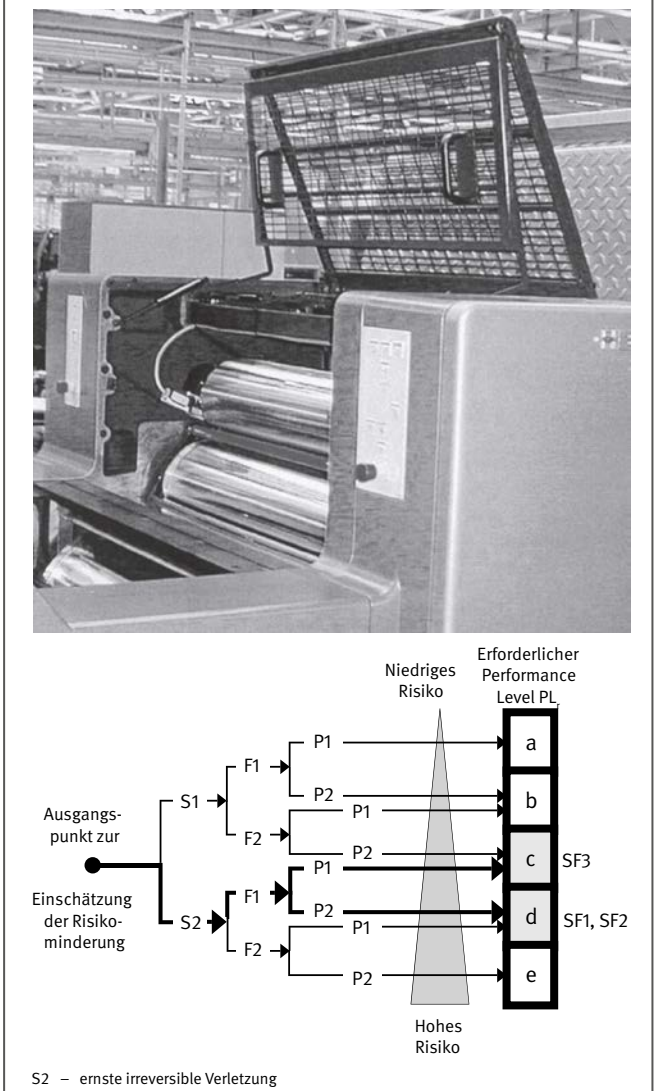


Abbildung A.4:
Risikobeurteilung an einer Rotationsdruckmaschine



nur dann verwendet werden, wenn die Druckmaschine zuvor stillgesetzt (SF1) und die zulässige Zylinderdrehzahl begrenzt wurde (SF2). Damit sind die möglichen Maschinenbewegungen für die Bedienperson überschaubar und sie kann den gefahrbringenden Bewegungen ausweichen (P1). Für SF3 ist daher ein erforderlicher Performance Level PL_r = c ausreichend (siehe Abbildung A.4). Die für diese Maschine zutreffende Produktnorm DIN EN 1010-1:2011 legt abweichend von der Anwendung des Risikographen für die Sicherheitsfunktion SF3 einen PL_r von d fest. Hierbei wurde leider die Risikominderung durch SF1 und SF2 nicht berücksichtigt.

Wie man die hier beschriebenen Sicherheitsfunktionen realisieren kann, ist in Kapitel 8 im Beispiel 24 beschrieben.

Literatur

[1] *Apfeld R.; Zilligen H.; Köhler B.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 7/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2013
► www.dguv.de/ifa, Webcode: d639540

Anhang B: Sicherheitsbezogenes Blockdiagramm und FMEA

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Schreibung von PFH_D (früher: *PFH*), $MTTF_D$, λ_S, λ_D, λ_{DD}, λ_{DU}, B_{10D}, T_{10D} an die neue Normversion (mit Großbuchstaben im Index) angepasst
- Ausführungen über die Verwendung von Ausfallartenverteilungen hinzugefügt
- Erläuterungen zur Problematik der Gewinnung von B_{10D} aus B_{10} hinzugefügt
- Abschnitt „Literatur“ aktualisiert

Zum Nachweis von Kategorie und Performance Level (PL) nach DIN EN ISO 13849-1 muss die Struktur eines sicherheitsgerichteten Systems unter dem Aspekt der zu realisierenden Sicherheitsfunktion (ggf. mehrerer Funktionen separat) analysiert werden. Für den obligatorischen quantitativen Nachweis des PL müssen Systeminformationen auf geeignete Weise aufbereitet werden, damit die quantitative Größe PFH_D (Probability of a Dangerous Failure per Hour) oder direkt der darauf basierende PL bestimmt werden kann. Zwei wichtige Schritte auf diesem Weg sind das sicherheitsbezogene Blockdiagramm und die funktionsblockweise durchgeführte Ausfalleffektanalyse FMEA (Failure Mode and Effects Analysis)[1].

B.1 Zweck und Erstellung eines sicherheitsbezogenen Blockdiagramms

Das Ergebnis der unter sicherheitstechnischem Blickwinkel erfolgenden Analyse der Systemstruktur wird zweckmäßig in Form eines Blockdiagramms dargestellt, das man als „sicherheitsbezogenes Blockdiagramm“ bezeichnen kann. Im Diagramm soll zum Ausdruck kommen, ob die Sicherheitsfunktion ganz oder teilweise ein- oder mehrkanalig ausgeführt wird und welche Diagnosemöglichkeiten bestehen, um interne Bauelementausfälle zu erkennen. Weil unter dem hier interessierenden Aspekt der Quantifizierung von Ausfallwahrscheinlichkeiten die Diagnose ein Kompensationsmittel für Bauelementausfälle ist, wird in diesem Anhang anstelle des sonst üblichen Begriffs „Fehlererkennung“ der Ausdruck „Ausfallerkennung“ verwendet.

In der Maschinensicherheit akzeptiert man meistens, dass infolge eines Steuerungsausfalls anstelle der Ausführung der ursprünglich vorgesehenen Sicherheitsfunktion eine Ersatzreaktion erfolgt, die einen sicheren Zustand herbeiführt, z. B. die Betriebshemmung mit energielosen Ausgängen (Abschaltsystem, englisch: Shutdown-System). Kategorie und PL sollen gemäß DIN EN ISO 13849-1 eine Aussage allein über die sicherheitstechnische Qualität machen und nicht über die Wahrscheinlichkeit des störungsfreien Betriebs, die „Verfügbarkeit“. Daher werden Signalpfade, die im Fehlerfall einen sicheren Zustand herbeiführen, genauso als vollwertig angesehen wie Funktionseinheiten, die eine unter Umständen komplizierte Sicherheitsfunktion ausführen. Ein solcher „einfacher Sicherheits-Signalpfad“ ist jedoch nur dann ein eigenständiger „Kanal“, wenn er ständig im Eingriff ist. Kann der Sicherheitspfad erst nach Aufdeckung eines Ausfalls im eigentlichen Haupt-Funktionspfad aktiv werden, so hängt sein Nutzen für die Sicherheit von der Qualität der Ausfallerkennung ab. Diese Qualität wird durch den Diagnosedeckungsgrad des Mechanismus zur Ausfallerkennung beschrieben. In solch einem Fall stellt der Sicherheitspfad in der Regel nur eine Testeinrichtung mit Abschaltweg zur Verfügung. Derartige Architekturmerkmale müssen im sicherheitsbezogenen Blockdiagramm korrekt zum Ausdruck kommen. Die unterschiedliche Darstellung einer echten Zweikanaligkeit und eines überwachten Einzelkanals ist gut zu erkennen, wenn man die Bilder 10 und 11 der Norm vergleicht.

Betrachtet werden muss auch, ob Bauelemente oder Schaltungsteile vorhanden sind, die zwar nicht die Sicherheitsfunktion oder die sicherheitsgerichtete Ersatzfunktion für den Fehlerfall ausführen, die aber bei bestimmten Bauteilausfällen die ordnungsgemäße Ausführung der Sicherheits- bzw. Ersatzfunktion durch andere Bauelemente verhindern können. Solche Schaltungsteile können notwendige Hilfsfunktionen wie z. B. die Spannungsversorgung oder Steuerungsfunktionen ohne (beabsichtigte) Sicherheitsbedeutung bereitstellen, jedoch mit einer Rückwirkung auf sicherheitsbezogene Teile. Bauelemente und Teilschaltungen müssen immer dann in einem Funktionsblock berücksichtigt werden, wenn von ihnen bei Ausfällen eine schädliche Wirkung auf die Sicherheitsfunktion, ihre Ersatzfunktion oder Diagnosefunktionen ausgehen kann. Beispielsweise muss bei Bauteilen zur Sicherstellung der elektromagnetischen Verträglichkeit (EMV) betrachtet werden, ob ihr Ausfall, z. B. ein Kondensatorkurzschluss, negative Auswirkung auf sicherheitsrelevante Schaltungen hat.

[1] Die hier beschriebene FMEA betrachtet auch die Erkennung von Ausfällen (Diagnose) und kann deswegen auch als FMEDA (Failure Mode, Effects and Diagnostics Analysis) bezeichnet werden.

Teilschaltungen mit definierten Ein- und Ausgängen können als Funktionsblock aufgefasst werden. Um die Anzahl der benötigten Funktionsblöcke möglichst gering zu halten, können funktional in Reihe geschaltete Teilschaltungen – also Schaltungen, die nacheinander verschiedene Schritte der Signalverarbeitung ausführen – zu einem Funktionsblock zusammengefasst werden. Bei anders angeordneten Blöcken sollte die Zusammenfassung sinnvollerweise nur so weit gehen, dass Redundanzen wie z. B. getrennte Abschaltpfade und die gegenseitige Diagnose von Funktionsblöcken noch zum Ausdruck kommen. Am Ende der Schaltungsanalyse muss ein Blockdiagramm stehen, das all jene Strukturen widerspiegelt, die sicherheitstechnisch bedeutsam sind:

- einfach vorhandene oder parallele Signalpfade („Kanäle“), die zur Ausführung der Sicherheitsfunktion dienen
- Signalpfade, die im Fehlerfall eine sicherheitsgerichtete Ersatzfunktion ausführen
- Schaltungen zur Ausfallerkennung (Diagnose)

Wenn Hilfsschaltungen, die für die Ausführung der Sicherheitsfunktion oder für eine andere sicherheitsgerichtete Aktion benötigt werden (z. B. Netzteile, Oszillatoren), nur einen Kanal beeinflussen können, so sollten sie dem oder den Funktionsblöcken dieses Kanals zugeordnet werden. Wirken diese Hilfsschaltungen auf mehrere Kanäle, dann bilden sie im sicherheitsbezogenen Blockdiagramm einen separaten einkanaligen Teil (Funktionsblock). Entsprechendes gilt für Schaltungen, die durch eine bestimmte Art ihres Ausfalls die Ausführung der Sicherheitsfunktion, einer anderen sicherheitsgerichteten Aktion oder der Diagnose verhindern können (z. B. Schaltungen zum Anwählen einer sicheren Betriebsart oder manche Bauelemente zur Sicherstellung der EMV). Über Schaltpläne und Stücklisten muss der Inhalt jedes Funktionsblocks eindeutig bestimmt sein. Wegen der Art seiner Erstellung und seines speziellen Zweckes unterscheidet sich das sicherheitsbezogene Blockdiagramm im Allgemeinen von Blockdiagrammen, die anderen Zwecken dienen, z. B. solchen, die sich an einem mechanischen Aufbau von Baugruppen orientieren.

Abbildung B.1 zeigt als Beispiel das sicherheitsbezogene Blockdiagramm einer einkanaligen Maschinensteuerung in Kategorie 2 mit

- einem Mikrocontroller,
- einer Lichtschranke zur Gefahrstellenüberwachung,
- einem „Watchdog“ zur Erkennung von einigen Controller-Fehlfunktionen,
- einer geregelten Motorantriebssteuerung (Frequenzumrichter), die vom Controller angesteuert wird und
- einem Motorabschaltorgan, das vom Watchdog betätigt werden kann (Impulssperre).

Die Sicherheitsfunktion besteht im Abschalten des Motors, sobald und solange der Lichtstrahl der Lichtschranke unterbrochen wird („Sicher abgeschaltetes Moment“ bzw. „Safe torque off“). Der Mikrocontroller und die nachgeschaltete Antriebssteuerung führen neben der Sicherheitsfunktion verschiedene andere Maschinenfunktionen aus, die hier nicht betrachtet werden, weil sie keine Sicherheitsfunktionen sind. Obwohl in diesem Beispiel die Sicherheitsfunktion allein mit elektrotechnischen Mitteln realisiert wird, gelten die beschriebenen Prinzipien für das sicherheitsbezogene Blockdiagramm und die FMEA-Technologie übergreifend.

Im sicherheitsbezogenen Blockdiagramm erscheinen nur Funktionsblöcke, die mit der Sicherheitsfunktion „Sicher abgeschaltetes Moment“ im Zusammenhang stehen, jedoch keine Bedien- und Anzeigeorgane für andere Maschinenfunktionen. Eventuell kann von einigen Bauelementen dieser Schaltungsteile im Fehlerfall eine die Sicherheitsfunktion störende Rückwirkung ausgehen. Nur dann sind diese Bauelemente denjenigen Funktionsblöcken zuzurechnen, die sie zum Ausfall bringen können.

Oftmals wird das sicherheitsbezogene Blockdiagramm wie im vorgestellten Beispiel die Gestalt einer der „vorgesehenen Architekturen“ nach der Norm DIN EN ISO 13849-1, Abschnitt 6.2.2,

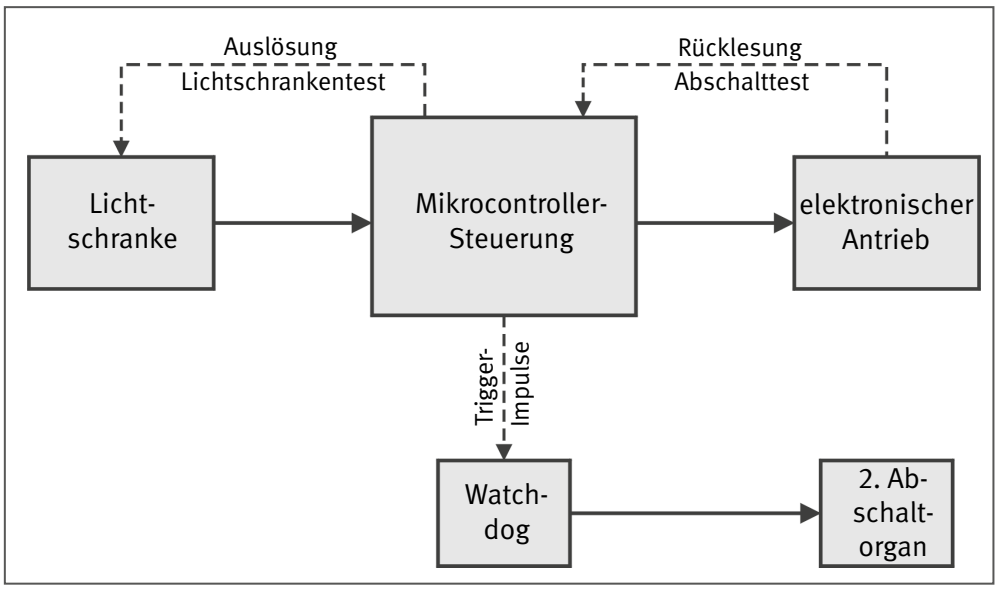


Abbildung B.1:
Beispiel für das sicherheitsbezogene Blockdiagramm einer einkanaligen Maschinensteuerung in Kategorie 2

(Abschnitte 6.2.1 bis 6.2.7 dieses Reports) haben. Dann kann das in Abschnitt 4.5.4 der Norm dargestellte Verfahren (ergänzt durch die Anhänge B, C, D, E, I und K der Norm) zur quantitativen Bestimmung des Performance Levels angewendet werden. Es ist aber nicht ratsam, eine andere Struktur „gewaltsam“ in die Form einer dieser Architekturen zu pressen. Möglicherweise lässt sich eine aktuell vorliegende Systemstruktur auch in Teile zerlegen, die jeweils stückweise einer vorgesehenen Architektur entsprechen. Gelingt eine solche Zerlegung nicht, so muss für das gegebene sicherheitsbezogene Blockdiagramm ein eigenes Modell zur quantitativen Bestimmung der sicherheitsbezogenen Zuverlässigkeit erstellt werden. Eine Einführung in geeignete Modellierungstechniken findet man beispielsweise in [1].

B.2 Zweck und Eigenart einer FMEA für die Quantifizierung

Für den quantitativen Nachweis des PL muss die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) abgeschätzt werden. Dies kann mithilfe eines eigens für das vorliegende System erstellten Rechenmodells (z. B. Markov-Modell) geschehen. Lässt aber das sicherheitsbezogene Blockdiagramm wie im Beispiel aus Abbildung B.1 formal die Gestalt einer der „vorgesehenen Architekturen“ gemäß Abschnitt 6.2.3 bis 6.2.7 erkennen, so kann das oben erwähnte Verfahren dieser Norm zur quantitativen Bestimmung des PL angewendet werden. In beiden Fällen muss von den Funktionsblöcken des sicherheitsbezogenen Blockdiagramms jeweils die Ausfallrate in die gefährliche (sicherheitstechnisch ungünstige) Richtung bzw. ihr Kehrwert, die $MTTF_D$ (Mean Time to Dangerous Failure, mittlere Zeit bis zum Ausfall in die gefährliche Richtung), und der *DC* (Diagnostic Coverage, Diagnosedeckungsgrad) bekannt sein. Zur Ermittlung dieser Daten dient die FMEA in einer speziellen Ausprägungsart, die Bauelementausfallraten als quantitative Größen einbezieht. Darin unterscheidet sich die hier verwendete besondere Form der FMEA von den meisten anderen FMEA-Spielarten, die anderen Zwecken dienen, beispielsweise der entwicklungsbegleitenden Problemfrüherkennung und Fehlervermeidung [2].

Besonderes Merkmal einer FMEA für Quantifizierungszwecke ist ihre Gliederung entsprechend den Funktionsblöcken des sicherheitsbezogenen Blockdiagramms. Im Prinzip wird für jeden dieser Funktionsblöcke eine separate FMEA durchgeführt, die nur für den jeweiligen Funktionsblock Ergebnisse liefert. Die funktionsblockbezogenen Ergebnisse werden erst nachträglich zusammengeführt, indem sie gemeinsam über ein systemspezifisches Rechenmodell oder das vereinfachte Quantifizierungsverfahren aus DIN EN ISO 13849-1 in die Ermittlung der PFH_D bzw. des PL einfließen.

B.2.1 Ausführung einer FMEA für die Quantifizierung

Im Folgenden wird die prinzipielle Vorgehensweise bei einer Quantifizierungs-FMEA am Beispiel des Funktionsblocks „Lichtschranke“ aus Abbildung B.2 demonstriert. Zu diesem Zweck wurde die Schaltung bewusst einfach gehalten. Nur die gestrichelt eingerahmten Bauelemente gehören zum Funktionsblock. Die Elemente S1 und P2 sind eine Ersatzschaltung für die reale Einbindung des Funktionsblocks innerhalb des Systems nach Abbildung B.1. Solange der Fototransistor K1 Licht von der Infrarot-LED P1 empfängt, hält er den Transistor K2 gesperrt, wodurch der Transistor K3 leitet und an Anschluss X1.2 eine positive Ausgangsspannung ansteht, die mit dem Voltmeter P2 messbar ist. Wird der Lichtstrahl unterbrochen, so sperrt K1, K2 wird leitend und K3 schaltet die Ausgangspannung ab. Der Test des Funktionsblocks „Lichtschranke“, den die Mikrocontroller-Steuerung aus Abbildung B.1 programmgesteuert durchführt, kann mit dem Taster S1 und dem Voltmeter P2 simuliert werden: Die Lichtquelle P1 wird kurzzeitig ausgeschaltet und dabei wird geprüft, ob die Ausgangsspannung ordnungsgemäß auf Null Volt absinkt. Den signalverarbeitenden Elementen des

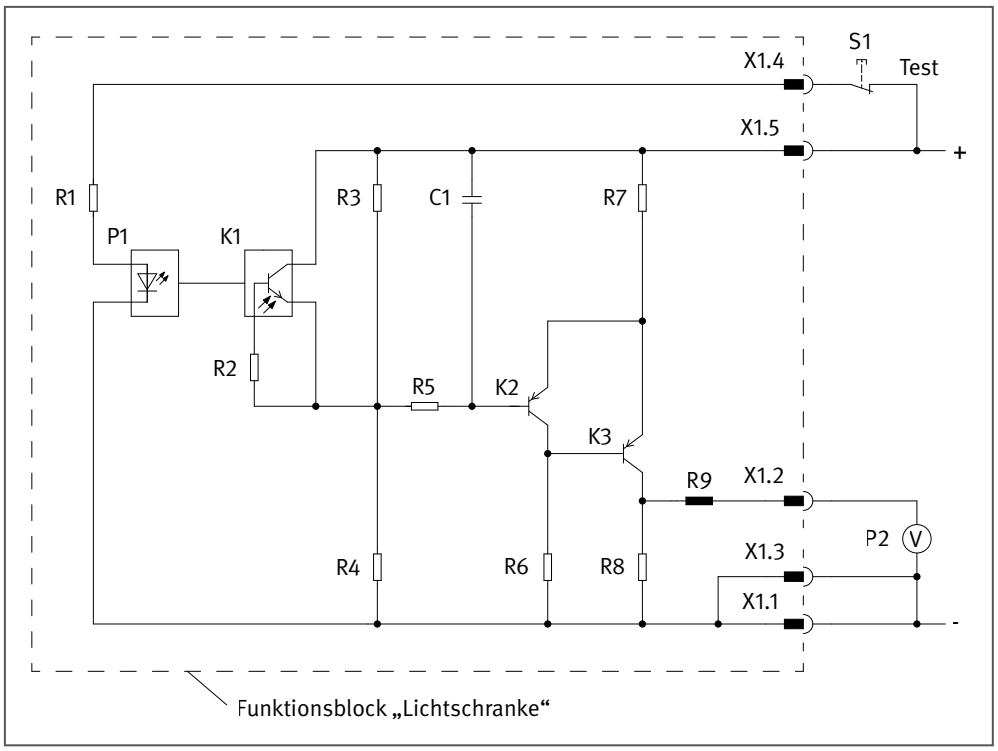


Abbildung B.2:
Angenommene Schaltung (einfaches Beispiel) des Funktionsblocks „Lichtschranke“ aus dem sicherheitsbezogenen Blockdiagramm nach Abbildung B.1

Funktionsblocks „Lichtschranke“ (K1 bis K3, R2 bis R9, C1) wird dabei dasselbe Verhalten abverlangt wie bei einer „echten“ Anforderung der Sicherheitsfunktion durch Unterbrechen des Lichtstrahls. Dieser Test wird im Folgenden als „Test 1“ bezeichnet.

B.2.2 Gefährliche Ausfallrichtung eines Funktionsblocks

Als erster Schritt muss die gefährliche Ausfallrichtung des Funktionsblocks bestimmt werden. Im Allgemeinen können nicht nur einzelne Bauelemente, sondern in der Folge auch ein ganzer Funktionsblock auf verschiedene Weise ausfallen. Als „gefährliche“ Ausfallrichtung eines Funktionsblocks gelten diejenigen Arten des Ausfalls, die aus sicherheitstechnischer Sicht ungünstig sind. Manche Ausfälle lassen das ganze System direkt gefährlich ausfallen, sodass es weder die ursprüngliche Sicherheitsfunktion noch eine sicherheitsgerichtete Ersatzaktion ausführen kann. Andere Ausfälle erhöhen die Wahrscheinlichkeit, dass dies geschieht, indem jetzt eine geringere Zahl weiterer Ausfälle ausreicht, um das System gefährlich ausfallen zu lassen. Gibt es für den ausfallenden Funktionsblock keine Redundanz, also keinen zweiten Kanal, der seine Funktion ersetzen kann, und wird nicht durch Diagnose hinreichend schnell eine Aktion ausgeführt, die einen sicheren Zustand erzeugt, so führt der gefährliche Ausfall des Funktionsblocks zum gefährlichen Ausfall des Systems. Aber auch, wenn wegen vorhandener Redundanz oder einer schnellen Ausfallreaktion anderer Schaltungsteile keine der möglichen Ausfallarten des infrage stehenden Funktionsblocks einen gefährlichen Systemausfall verursacht, kann und muss seine „gefährliche“ Ausfallrichtung festgestellt werden. Es ist diejenige Ausfallrichtung, die dazu führt, dass der Funktionsblock seinen vorgesehenen Beitrag zu einem sicheren Systemverhalten nicht mehr leistet. Mitunter müssen auch mehrere Ausfallarten, die durch unterschiedliches, aber gleichermaßen schädliches Blockverhalten gekennzeichnet sind, berücksichtigt werden (z. B. dauerhaftes Einschalten und Schwingung am Ausgang). Es ist daher am einfachsten, die gefährliche Ausfallrichtung durch den Verlust der sicherheitstechnisch geforderten Funktion des Funktionsblocks zu beschreiben. Diagnosemöglichkeiten werden erst später berücksichtigt und bleiben bei diesem Schritt zunächst außer Acht. Beim vorliegenden Beispiel (Lichtschranke, Abbildung B.2) soll die Ausgangsspannung des Funktionsblocks auf Null abfallen, solange der Fototransistor K1 kein Licht von der LED P1 empfängt, denn darin besteht der Beitrag dieses Funktionsblocks zur Ausführung der Sicherheitsfunktion „Sicher abgeschaltetes Moment bei unterbrochenem Lichtstrahl“.

Somit kann die gefährliche Ausfallrichtung des Funktionsblocks beschrieben werden als „Anliegen einer Ausgangsspannung größer als Null bei Nichtbeleuchtung des Fototransistors K1“.

B.2.3 Bauelementausfallraten

Verschiedene Datenquellen kommen für Bauelementausfallraten infrage. Beispiele für elektronische Bauelemente sind in [3 bis 6] aufgeführt. Alle diese Quellen enthalten herstellerübergreifende Daten. Auch für mechanische, pneumatische und hydraulische Bauelemente gibt es Sammlungen von Ausfallraten. Bei einzelnen Bauelementen, die nicht in den einschlägigen Verzeichnissen gelistet sind, wird man die Ausfallrate vom Hersteller einholen müssen (z. B. bei speziellen ASICs). Viele gängige Quantifizierungstechniken, auch das vereinfachte Verfahren aus DIN EN ISO 13849-1, Abschnitt 4.5.4, gehen von der zeitlichen Konstanz der Ausfallraten aus, was eine Idealisierung darstellt. Durch entsprechende Dimensionierung und notfalls vorbeugenden Austausch kann erreicht werden, dass die Bauelemente während der Gebrauchsdauer T_M (Mission Time) noch nicht in die Verschleißphase mit stark ansteigender Ausfallrate geraten.

Als schnell verfügbare Quelle für zumeist konservativ (pessimistisch) abgeschätzte Ausfallraten bietet sich DIN EN ISO 13849-1, Anhang C, an. Hier wird insbesondere ein Weg gewiesen, auf dem für zyklisch arbeitende elektromechanische, fluidtechnische und mechanische Einzelkomponenten Ausfallraten aus den sogenannten B_{10D}-Werten (siehe Tabelle D.2 dieses Reports) abgeleitet werden können.

Sofern keine konservative Abschätzung der Ausfallrate vorliegt, muss bei jedem Bauelement darauf geachtet werden, dass der verwendete Wert unter den im konkreten Anwendungsfall gegebenen Einsatzbedingungen (Temperatur, Strom, Spannung, Verlustleistung …) gilt. Auch die Eigenerwärmung ist zu berücksichtigen. Gängige Datenquellen, z. B. [3 bis 6], bieten Möglichkeiten, die unter definierten Referenzbedingungen geltenden Basisausfallraten in Werte umzurechnen, die unter davon abweichenden Bedingungen gelten. Geeignete Umrechnungsformeln, jedoch keine Basisausfallraten findet man in [7].

B.2.4 Erstellung einer funktionsblockweisen FMEA für Quantifizierungszwecke

Bei der FMEA werden die Bauelemente des Funktionsblocks zunächst einzeln bewertet und daraus die Komplettbewertung des Blocks abgeleitet. Dies geschieht zweckmäßig in Form einer Tabelle, die diesen Prozess und zugleich das Ergebnis dokumentiert. Die FMEA kann mit unterschiedlichem Exaktheitsanspruch ausgeführt werden, was sich in verschieden hohem Aufwand für die Erstellung der dazugehörigen Tabellen widerspiegelt. Eine mögliche Ausführung ist beispielsweise in [8] angegeben. Verbindliche Vorschriften existieren nicht. Die in Abbildung B.3 vorgestellte Variante stellt einen Kompromiss zwischen hohem Akkuratheitsanspruch und Aufwand einerseits sowie allzu starker Vereinfachung andererseits dar und nimmt Rücksicht auf die Genauigkeit und die Verfügbarkeit der verwendeten Daten. Die dort verwendeten Zahlen sind angenommene Beispielwerte.

Die Bauelemente des Funktionsblocks werden zeilenweise aufgelistet und mit ihren Ausfallraten versehen. Die übliche Einheit der Ausfallrate ist „FIT“ (Failures In Time); $1\ \mathrm{FIT} = 10^{-9}/\mathrm{h}$. Als einziger Gewichtsfaktor für die Basisausfallrate erscheint hier der Temperaturfaktor. Der Verzicht auf weitere Anpassungsfaktoren ist dann gerechtfertigt, wenn die Bauelemente im Mittel elektrisch tendenziell überdimensioniert sind, was häufig der Fall ist. Ihre elektrische Belastung liegt dann überwiegend unter der Referenzbelastung, für welche die Basisausfallrate gilt, sodass die entsprechenden Anpassungsfaktoren <1 sind. Somit bedeutet das Weglassen dieser Faktoren eine Abschätzung zur sicheren Seite und zugleich eine Arbeitsersparnis, weil die genauen elektrischen Betriebswerte für die Bauelemente nicht alle einzeln ermittelt werden müssen. Sobald jedoch bekannt ist, dass

Bezeichnung des Funktionsblocks:	Lichtschranke
Gefährliche Ausfallrichtung des Funktionsblocks:	Anstehen einer Ausgangsspannung größer als Null bei Nichtbeleuchtung des Fototransistors K1
Datenquelle für Ausfallraten:	XYZ-Datenbank

Referenz-bezeich-nung	Bauelement-Art	Relev. Bauelem.-Temp. (°C)	Basis-Ausfall-Rate (FIT)	Tempe-ratur-faktor	Ausf.anteil in sichere Richtung	Ausf.anteil in gefährl. Richtung	erk.bar durch Test Nr.	DC	λ (FIT)	λ_S (FIT)	λ_D (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)	Anm.
R1	Chip-Widerstand MS	55	0,5	1,20	1	0	–	–	0,60	0,60	0,00	0,00	0,00	
R2	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	1)
R3	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R4	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R5	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R6	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R7	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R8	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R9	HF-Spule SMD	50	1,8	1,12	1	0	–	–	2,02	2,02	0,00	0,00	0,00	
C1	Chip-Kond. keram.	50	1,1	1,60	0	1	1	0,5	1,76	0,00	1,76	0,88	0,88	2)
P1	Infrarot-LED	60	2,5	2,24	1	0	–	–	5,60	5,60	0,00	0,00	0,00	
K1	Fototransistor	60	3,4	1,80	0,5	0,5	1	1	6,12	3,06	3,06	3,06	0,00	
K2	Transistor SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
K3	Transistor SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
X1	Steckverb. 5-polig	50	1,5	1,00	0,5	0,5	1	1	1,50	0,75	0,75	0,75	0,00	3)
–	Leiterpl. mit 36 Lötst.	50	1,8	1,00	0,5	0,5	1	0,9172	1,80	0,90	0,90	0,83	0,07	4)
								Summen:	31,23	19,71	11,52	10,57	0,95	

$MTTF_D$ (a): 9905,9 DC (%): 91,72

Anmerkungen:

1) Bei Unterbrechung und hoher Umgebungstemperatur fließt durch K1 unter Umständen ein zu hoher Dunkelstrom.
2) Bei Unterbrechung wird die Schaltung gegenüber EM-Störungen empfindlich; Erkennbarkeit nicht gesichert.
3) Kurzschlüsse innerhalb von X1 können einen Ausfall in die gefährliche Richtung verursachen.
4) Aufteilung DD/DU wie die durchschnittliche Aufteilung von allen übrigen Elementen.

Abbildung B.3:
Sinnvolle Ausführungsform einer FMEA-Tabelle für den Funktionsblock „Lichtschranke“ aus Abbildung B.2

die Last bestimmter Bauelemente über der Referenzbelastung liegt, sollten die relevanten Anpassungsfaktoren berücksichtigt werden. Wenn die Basisausfallrate einzelner Bauelemente innerhalb des Funktionsblocks dominiert, was beispielsweise für Prozessoren und Leistungshalbleiter oft zutrifft, dann ist eine genaue Betrachtung und ggf. Berücksichtigung aller erforderlichen Anpassungsfaktoren für diese Bauelemente geboten.

Als nächstes wird die Gesamtausfallrate λ jedes Bauelementes in die Anteile λ_S („safe“ bzw. sichere Richtung) und λ_D („dangerous“ bzw. gefährliche Richtung) aufgeteilt, wozu u. a. die „gefährliche Ausfallrichtung“ des Funktionsblocks bekannt sein muss (siehe oben). Nach der „reinen Lehre“ muss dies in zwei Schritten geschehen:

Die Gesamtausfallrate wird zuerst auf die verschiedenen Ausfallarten (z. B. Unterbrechung, Kurzschluss, Drift, Funktionsänderung) verteilt. Angaben zur Ausfallartenverteilung für verschiedene Bauelemente findet man z. B. in DIN EN 61709 [7] und in IEC/TR 62380 [4]. Auch in kommerzieller FMEDA-Software sind

typischerweise Ausfallartenverteilungen hinterlegt. Die Angaben in den verschiedenen Quellen sind nicht einheitlich. Ein unnötiger Wechsel der Quelle für die Ausfallartenverteilung von Bauteil zu Bauteil ist nicht akzeptabel.

Im zweiten Schritt werden die auf jede Ausfallart entfallenden Ausfallratenanteile λ_S oder λ_D zugewiesen, je nachdem, ob die betreffende Ausfallart den Funktionsblock in dessen sichere oder gefährliche Richtung ausfallen lässt. Das unveränderte Weiterfunktionieren wird dabei wie ein Ausfall in die sichere Richtung gewertet.

In Abbildung B.3 wird ein vereinfachter pragmatischer Weg dargestellt, der ohne eine bestimmte Quelle für Ausfallartenverteilungen auskommt und bei dem nur geprüft wird, welcher der drei folgenden Fälle bei einem Bauelement vorliegt:

a) Alle Ausfallarten führen zum Ausfall des Funktionsblocks in dessen sichere Richtung oder haben keine Auswirkung auf sein Verhalten.

b) Es gibt mindestens eine Ausfallart, die den Funktionsblock in dessen sichere Richtung ausfallen lässt, und mindestens eine Ausfallart, die ihn in seine gefährliche Richtung ausfallen lässt.

c) Alle Ausfallarten führen zum Ausfall des Funktionsblocks in dessen gefährliche Richtung.

Im Fall a) wird die komplette Ausfallrate λ der Ausfallrate λ_S in die sichere Richtung zugewiesen (Beispiel: Infrarot-LED P1). Entsprechend wird im Fall c) die gesamte Ausfallrate λ der Ausfallrate λ_D in die gefährliche Richtung zugerechnet (Beispiel: Kondensator C1). Im Fall b) weist man die Gesamtausfallrate λ je zur Hälfte λ_S und λ_D zu (Beispiel: Transistor K2).

Die vereinfachte Vorgehensweise im Fall b) ist normalerweise bei Bauelementen mit einem kleinen Beitrag zur Gesamtausfallrate des Funktionsblocks gerechtfertigt, wenn dieser viele solche Elemente enthält. Einzelne Bauelemente mit einem überdurchschnittlichen Beitrag zur Gesamtausfallrate des Funktionsblocks sind ggf. gesondert zu betrachten. Bei komplexen integrierten Schaltungen wie Prozessoren kann ebenfalls eine 50-zu-50-%-Aufteilung der Ausfallrate auf λ_S und λ_D vorgenommen werden. Dasselbe gilt für Lötstellen/Leiterplatten. Vorsicht ist geboten bei diskreten oder niedrig integrierten Bauelementen mit relativ hoher Ausfallrate. Trägt z. B. ein Schütz oder ein Leistungshalbleiter wesentlich zur Gesamtausfallrate des Funktionsblocks bei, so ist im Zweifelsfall von einem überwiegenden Ausfall in die gefährliche Richtung auszugehen. Dies gilt umso mehr, wenn es sich um die den Ausgangsstrom schaltenden Elemente von Sicherheitsausgängen handelt.

Bei Bauelementen zur Ertüchtigung der Schaltung gegenüber Störeinflüssen – z. B. elektromagnetischen Störungen oder hoher Umgebungstemperatur – ist zur Bewertung des Funktionsblockverhaltens eine Unterscheidung zwischen zwei möglichen Fällen sinnvoll. Ist das Auftreten der Störphänomene lediglich „möglich“ und dient die Schaltungsmaßnahme im Wesentlichen zur Erhöhung der Geräteverfügbarkeit unter (seltenen) ungünstigen Bedingungen, so muss bei der Beurteilung des Funktionsblockverhaltens beim Bauelementeausfall das gleichzeitige Vorliegen des „Störphänomens“ nicht angenommen werden. Sieht jedoch die vorgesehene Betriebsweise des Gerätes die gelegentliche bis ständige Präsenz der Störung vor oder legt die typische Betriebsweise dies nahe (z. B. Einbau in der Reichweite bekannter elektromagnetischer Störquellen oder heißer Einbauort), so muss die Bewertung des Bauelementausfalls die Anwesenheit der Störbeaufschlagung berücksichtigen. Das gilt auch für die Beurteilung der Ausfallerkennbarkeit bei diesen Bauelementen durch Diagnosemaßnahmen.

Bei verschleißbehafteten Bauelementen wird meistens eine zeitkonstante Ersatz-Ausfallrate in die gefährliche Richtung verwendet, die mithilfe der Gleichung C.5 aus DIN EN ISO 13849-1, Anhang C.4.2, berechnet wird. Hierfür wird der Kennwert B_{10D} benötigt, der die mittlere Anzahl der Schaltspiele bis zum Ausfall in die gefährliche Richtung angibt. Idealerweise stammt der B_{10D}-Wert vom Hersteller des Bauelements, der zugleich angibt, welche Ausfallrichtung dabei als die gefährliche angenommen wurde (z. B. Nichtöffnen von Schaltkontakten), denn prinzipiell kann eine Ausfallrichtung nur im Hinblick auf eine bestimmte Applikation als gefährlich bzw. ungefährlich bewertet werden. Oftmals ist vom Hersteller nur ein B_{10}-Wert (Anzahl der Schaltspiele bis zu irgendeinem Ausfall) verfügbar. Für diesen Fall wird mitunter die Berechnung des B_{10D}-Wertes nach der Gleichung $B_{10D} = B_{10}/RDF$ empfohlen, wobei RDF der Anteil der gefährlichen Ausfälle an der Gesamtheit der Ausfälle ist („ratio of dangerous failure“). Auch DIN EN ISO 13849-1, Anhang C.4.2, Fußnote 2, folgt mit RDF = 0,5 diesem Ansatz. Diese Berechnungsmethode beruht jedoch auf vereinfachenden Annahmen, die von den tatsächlichen Verhältnissen bei den hier betrachteten Verschleißteilen deutlich abweichen können. Daher sollte B_{10D} auf das Zweifache des Wertes von B_{10} begrenzt werden, wenn B_{10D} mittels des Quotienten B_{10}/RDF ermittelt wird. Durch den Zusammenhang aus Gleichung C.3 in DIN EN ISO 13849-1, Anhang C.4.2, hat die B_{10D}-Ermittlung auch Konsequenzen für die zulässige Bauteil-Betriebszeit T_{10D} und somit eventuell auch für zu spezifizierende Bauteil-Austauschintervalle.

Der nächste Arbeitsschritt besteht in der Berücksichtigung der Diagnose. Es wird ausschließlich diejenige Diagnose berücksichtigt, die sich auf Ausfälle in die – bezogen auf den Funktionsblock – gefährliche Richtung bezieht. Daher muss nur bei solchen Bauelementen, bei denen es einen Ausfallanteil in diese gefährliche Richtung gibt, geprüft werden, ob ein Test oder ggf. mehrere Tests in der Lage sind, diese Ausfälle ganz oder teilweise zu erkennen. In entsprechenden Spalten werden der jeweils wirksame Test sowie der „bauelementbezogene“ Diagnosedeckungsgrad *DC* (Diagnostic Coverage) eingetragen, der den erkennbaren Anteil der Ausfälle in die gefährliche Richtung angibt. Handelt es sich um diskrete Bauelemente wie im Beispiel aus Abbildung B.2, so kann dem gefährlichen Ausfall eines einzelnen Elementes oft einer der DC-Werte „0“ für „nicht erkennbar“ oder „1“ für „erkennbar“ zugewiesen werden. Bei komplexen integrierten Bauelementen und bei diskreten Elementen, deren Ausfall ein solches komplexes Bauelement in der Funktion beeinträchtigen kann, muss der bauelementbezogene *DC* unter Berücksichtigung sowohl der gefährlichen Ausfallart als auch des zur Verfügung stehenden Testverfahrens geschätzt werden. Eine Hilfestellung zu dieser Schätzung bietet Tabelle E.2, in der gängigen Testverfahren DC-Werte von 0 % („kein“), 60 %

(„niedrig“), 90 % („mittel“) und 99 % („hoch“) zugemessen werden. Bei der Zuweisung eines DC zu einem Bauelement muss auch beachtet werden, dass die Bewertung als „erkennbar“ nur dann erfolgen darf, wenn das System tatsächlich in der Lage ist, die vorgesehene sicherheitsgerichtete Aktion auszuführen. So ist beispielsweise eine schaltungsinterne Ausfallerkennung nutzlos, wenn sie wegen eines bereits ausgefallenen Abschaltpfades unwirksam ist.

Im vorliegenden Beispiel brauchen die Bauelemente R1, R6 bis R9 und P1 nicht unter dem Diagnoseaspekt betrachtet zu werden, weil sie keine Ausfälle des Funktionsblocks „Lichtschranke“ in dessen gefährliche Ausfallrichtung verursachen können. Ihr Ausfallanteil in die gefährliche Richtung ist jeweils 0. Der Ausfall der Elemente R2 bis R5, K1 bis K3 und X1 in die gefährliche Richtung wird von „Test 1“ (in diesem Beispiel der einzige Test) vollständig erkannt, d. h., bei zu Testzwecken abgeschalteter LED P1 detektiert der Test eine Ausgangsspannung von > 0. Daher wird diesen Elementen der bauelementbezogene DC-Wert von „1“ zuerkannt. Anders ist dies beim Kondensator C1, der zur Unterdrückung von regelmäßig, aber nicht ständig vorkommenden elektromagnetischen Störungen dient (Annahme bei diesem Beispiel!). Driftausfälle (begrenzte Kapazitätsänderungen) sind unkritisch, aber ein Kurzschluss führt dazu, dass der Ausgang (Anschluss X1.2) nicht abgeschaltet werden kann (gefährliche Ausfallrichtung des Funktionsblocks). Ein Kurzschluss von C1 wird durch Test 1 erkannt. Bei Unterbrechung von C1 pflanzt sich die elektromagnetische Störung über K2 und K3 bis zum Ausgang des Funktionsblocks fort. Dabei ist unklar, wie die nachfolgende Schaltung dieses hochfrequente Wechselsignal interpretiert und ob das Störphänomen auch während des Tests vorliegt. Ungünstigstenfalls verhindert die nicht unterdrückte Störung, dass das mit Störungen überlagerte Ausgangssignal bei nicht beleuchtetem Fototransistor K1 von der nachfolgenden Schaltung als Anforderung der Sicherheitsfunktion interpretiert wird (= gefährlicher Ausfall des Funktionsblocks „Lichtschranke“). Wenn die Störung zum Testzeitpunkt nicht vorliegt, kann Test 1 die Kondensatorunterbrechung nicht erkennen. Da keine verlässliche Ausfallartenverteilung für den Kondensator bekannt ist, wird – unter Vernachlässigung der unkritischen Driftausfälle – angenommen, dass Kurzschlüsse und Unterbrechungen je 50 % der Ausfälle ausmachen. Beide Ausfallarten führen zum gefährlichen Funktionsblockausfall; sicher erkennbar sind jedoch nur die Kondensatorkurzschlüsse, d. h. die (geschätzte) Hälfte aller gefährlichen Kondensatorausfälle. Somit wird der bauelementbezogene Diagnosedeckungsgrad mit 50 % bzw. 0,5 abgeschätzt. Die Leiterplatte mit den Lötstellen kann Kurzschlüsse und Unterbrechungen an verschiedenen Stellen in die Schaltung einbringen. Der in Abbildung B.3 realisierte pragmatische Ansatz zur Abschätzung des DC-Wertes für Lötstellen und Leiterplatte besteht darin, ihnen jenen mittleren DC-Wert zuzuweisen, der sich für alle übrigen Bauelemente des Funktionsblocks aus der Gleichung $DC = \Sigma \lambda_{DD} / \Sigma \lambda_D$ ergibt. So wirkt sich das Einbeziehen von Leiterplatte und Lötstellen nicht auf den DC-Wert aus, der für den kompletten Funktionsblock berechnet wird.

In jeder Tabellenzeile, d. h. für jedes Bauelement gilt:

λ = Temperaturfaktor · Basisausfallrate (ggf. mit weiteren Korrekturfaktoren, s.o.)

λ_S = Ausfallanteil in die sichere Richtung · λ

λ_D = Ausfallanteil in die gefährliche Richtung · λ

$\lambda_{DD} = DC \cdot \lambda_D$

$\lambda_{DU} = (1 - DC) \cdot \lambda_D$

Für diese λ-Werte werden in der Tabelle Spaltensummen gebildet. Aus dem Summenwert λ_D bzw. aus den Summenwerten λ_D und λ_{DD} ergeben sich die $MTTF_D$, d. h. die mittlere Zeit bis zum gefährlichen Ausfall des Funktionsblocks, sowie der *DC* des Funktionsblocks:

$MTTF_D = 1/\lambda_D$

$DC = \lambda_{DD}/\lambda_D$

Um den PL bei einer der vorgesehenen Architekturen nach Abschnitt 6.2.3 bis 6.2.7 zu bestimmen, werden als Eingangsgrößen nur die Werte von $MTTF_D$ und *DC* benötigt. Im vorliegenden Beispiel ergeben sich ein $MTTF_D$-Wert von 9 905,9 Jahren und ein *DC* von 91,72 %. Wird ein anderes Quantifizierungsverfahren angewendet, können auch Werte wie λ_{DD} bzw. λ_{DU} aus der FMEA-Tabelle Verwendung finden.

B.3 „Parts Count“-Verfahren

Zur Arbeits- und Zeitersparnis kann anstelle einer FMEA ein einfacheres Verfahren angewandt werden. Verzichtet man auf die detaillierte Analyse des Schaltungsverhaltens bei den verschiedenen Ausfallarten der einzelnen Bauelemente, gelangt man zum sogenannten „Parts Count“-Verfahren (vgl. Anhang D dieses Reports). Es stammt ursprünglich aus dem MIL-Handbook 217F (Nachfolgepublikation siehe [6]) und wird in einer Variante in DIN EN ISO 13849-1, Anhang D.1, beschrieben. Bei gleichzeitiger Annahme verhältnismäßig „konservativer“ (hoher) Ausfallraten kann eine Anpassung der Ausfallraten an die realen Betriebsbedingungen entfallen. Zusätzlich wird häufig bei vielen Elementen von 50 % Ausfallanteil in die – bezogen auf den Funktionsblock – gefährliche Richtung ausgegangen. So entsteht aus der FMEA-Tabelle, wenn man nicht benötigte Spalten für die Gewichtung und Aufspaltung der Ausfallraten weglässt, eine einfachere Tabelle. Verglichen mit FMEA-Ergebnissen liefert das „Parts Count“-Verfahren normalerweise schlechtere (kleinere) $MTTF_D$-Werte, weil tendenzmäßig höhere Ausfallraten einfließen und auch Bauelemente berücksichtigt werden, die ausschließlich Funktionsblockausfälle in die sichere Richtung verursachen können.

Wendet man das „Parts Count“-Prinzip auf das oben behandelte Beispiel (Lichtschranke) an und geht man dabei von den temperaturangepassten Ausfallraten aus Abbildung B.3 sowie bei allen Elementen von generell 50 % gefährlichen Ausfällen aus, so erhält man einen $MTTF_D$-Wert von 7 310,8 Jahren. Verglichen mit dem FMEA-Ergebnis ist dieser Wert um ca. 26 % schlechter. Die Verschlechterung ist bei diesem Beispiel allein dem Verzicht auf die Schaltungsanalyse geschuldet. Wird ein DC-Wert für den Funktionsblock benötigt, so muss – wie bei der FMEA – der bauelementbezogene DC für jedes Element oder, z. B. in Anlehnung an Anhang E, der DC des gesamten Funktionsblocks geschätzt werden.

Grundsätzlich ist die in diesem Anhang des Reports am Beispiel einer elektronischen Schaltung vorgestellte FMEA-Variante für Quantifizierungszwecke als Methode auf andere Technologien übertragbar. Sie kann also in formal gleicher Weise, z. B. für mechanische, hydraulische und pneumatische Systeme, angewendet werden.

Literatur

[1] *Goble, W. M.:* Control Systems Safety Evaluation and Reliability. 3rd ed. Hrsg.: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010

[2] DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (11/2006). Beuth, Berlin 2006; IEC 60812: 2006: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[3] SN 29500: Ausfallraten Bauelemente, Erwartungswerte. Hrsg.: Siemens AG, Corporate Technology, Technology & Innovation Management, München 2004-2014 (Bestellanfragen an michaela.pabst@siemens.com oder thomas.haizmann@siemens.com)

[4] IEC/TR 62380: Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment. Hrsg.: International Electrotechnical Commission (IEC), Genf 2004

[5] Telcordia SR-332, Issue 3: Reliability Prediction Procedure for Electronic Equipment. Hrsg.: Ericsson Inc., Piscataway, New Jersey 2011

[6] Handbook of 217Plus Reliability Prediction Models. Quanterion Solutions Incorporated, Utica, New York 2015

[7] DIN EN 61709: Elektrische Bauelemente – Zuverlässigkeit – Referenzbedingungen für Ausfallraten und Beanspruchungsmodelle zur Umrechnung (1/1999). Beuth, Berlin 2012; hierzu ergänzend DIN EN 61709 Berichtigung 1:2012-07 vom selben Herausgeber

[8] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (02.11), Anhang C. Beuth, Berlin 2011

Anhang C: Fehlerlisten, Fehlerausschlüsse und Sicherheitsprinzipien

C.1 Fehlerlisten

Die bei der Validierung von SRP/CS anzunehmenden Fehler und mögliche Fehlerausschlüsse für mechanische, pneumatische, hydraulische und elektrische Bauteile finden sich in DIN EN ISO 13849-2 [1], Anhang A bis D, in sogenannten Fehlerlisten. In einzelnen Produktnormen, z. B. DIN EN 61800-5-2 [2] und DIN EN 61496-1 [3], sind ebenfalls Fehlerlisten oder Ergänzungen zu den genannten Fehlerlisten vorhanden. Der Beitrag 340 220 im IFA-Handbuch [4] erläutert Hintergründe und das Zustandekommen der Fehlerlisten.

C.2 Fehlerausschlüsse

Ohne die Annahme von Fehlerausschlüssen sind sichere Steuerungen manchmal nicht mit vertretbarem Aufwand zu realisieren. Gründe für einen Fehlerausschluss können insbesondere die physikalische Unmöglichkeit einer bestimmten Fehlerart oder die technische Unwahrscheinlichkeit des Auftretens eines Fehlers sein sowie allgemein anerkannte technische Erfahrungen (siehe auch Abschnitt 7.3 der DIN EN ISO 13849-1). Fehlerausschlüsse sind auch für neu entworfene Komponenten oder Bauelemente grundsätzlich möglich. Jeder Fehlerausschluss muss in der technischen Dokumentation genau begründet werden. DIN EN ISO 13849-2 beschreibt für einzelne Bauelemente mögliche Fehlerausschlüsse, soweit sie als zulässig erachtet werden. Angaben in den folgenden Beispielen sind, wo erforderlich, im Sinne üblicher Praxis aktualisiert.

C.2.1 Beispiele für Fehlerausschlüsse an Bauteilen

C.2.1.1 Bauteile der Fluidtechnik

Für pneumatische und hydraulische Bauteile sind häufig vergleichbare Fehlerausschlüsse formuliert. Jedoch sind auch fluidspezifische Fehlerausschlüsse vorhanden.

Beispiel für gemeinsame Fehlerausschlüsse an fluidischen Bauteilen:

- Wegeventile

  Die Fehlerannahme „Nichtschalten oder nicht vollständiges Schalten“ kann unter folgenden Voraussetzungen ausgeschlossen werden: Zwangläufige mechanische Betätigung der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist. Bei hydraulischen Wegeventilen kann für ein Patronensitzventil spezieller Bauart (siehe Anmerkungen in DIN EN ISO 13849-2, Tabelle C.3) bezogen auf das Nichtöffnen ein Fehlerausschluss formuliert werden, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert.

C.2.1.2 Elektrische Bauteile

- Optokoppler

  Die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs“ kann unter folgenden Voraussetzungen ausgeschlossen werden: Der Optokoppler ist entsprechend Überspannungskategorie III nach IEC 60664-1 gebaut. Wird eine SELV/PELV-Spannungsversorgung verwendet, genügt Verschmutzungsgrad 2/Überspannungskategorie II. Es werden Maßnahmen getroffen, um sicherzustellen, dass ein interner Fehler des Optokopplers nicht zu übermäßigem Temperaturanstieg seiner Isolierwerkstoffe führen kann.

- Leiterplatte/bestückte Leiterplatte

  Die Fehlerannahme „Kurzschluss zwischen benachbarten Leiterbahnen/Kontaktstellen“ kann nach Norm ausgeschlossen werden, sofern folgende Voraussetzungen zutreffen:
  - Als Basismaterial wird mindestens EP GC nach IEC 60893-1 verwendet.
  - Kriech- und Luftstrecken werden mindestens nach IEC 60664-5 (für Strecken von mehr als 2 mm IEC 60664-1) bemessen mit Verschmutzungsgrad 2/Überspannungskategorie III. Wenn beide Leiterbahnen über ein SELV/PELV-Netzgerät versorgt werden, gilt Verschmutzungsgrad 2/Überspannungskategorie II mit einer Mindeststrecke von 0,1 mm.
  - Die bestückte Leiterplatte ist in einem Gehäuse eingebaut, das einen Schutz von mindestens IP54 gibt und die Leiterseite ist mit einer alterungsbeständigen Lack- oder Schutzschicht versehen, die alle Leiterbahnen abdeckt.
  - In der Praxis auch akzeptiert: Die alterungsbeständige Lack- oder Schutzschicht kann aus heutiger Sicht z. B. aus einem hochwertigen Lötstopplack bestehen. Eine zusätzliche Beschichtung von Leiterplatten entsprechend IEC 60664-3 kann den zugrunde gelegten Verschmutzungsgrad und damit die erforderlichen Kriech- und Luftstrecken verringern.

  Werden bleifreie Lötverfahren und Produkte angewendet, können elektrische Kurzschlüsse durch die Bildung von Zinn-Whiskern vorkommen. Zinn-Whisker bilden sich hauptsächlich bei Oberflächen mit reiner, glänzender Zinnbeschichtung. Die nadelähnlichen Überstände können eine Länge von mehr als 1 mm erreichen (Anmerkung: in [1] wird ein sehr viel geringerer Wert genannt) und elektrische Kurzschlüsse

verursachen. Die vorherrschende Theorie lautet, dass Whisker durch Druckbelastung verursacht werden, die sich beim Verzinnen aufbaut. Diese Möglichkeit sollte beurteilt werden, insbesondere wenn ein Fehlerausschluss an einem Bauteil angewendet wird, wie z. B. Fehlerausschluss eines Kurzschlusses.

Wenn das Risiko der Zinn-Whisker-Bildung als hoch eingeschätzt wird, ist ein Fehlerausschluss für einen Kurzschluss zwischen Anschlüssen von Bauteilen auf einer Leiterplatte trotz Einhaltung der oben aufgeführten Voraussetzungen nicht möglich. Whisker an Leiterbahnen von Leiterplatten wurden bisher nicht festgestellt. Die Leiterbahnen bestehen üblicherweise aus Kupfer ohne Zinnbeschichtung. Die Literaturhinweise [5; 6] können zur Beurteilung des Phänomens hilfreich sein.

- Leitungen/Kabel

  Die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Leitern“ kann ausgeschlossen werden, wenn die Leiter
  – dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt (z. B. durch Kabelkanal, Panzerrohr) oder
  – in unterschiedlichen Mantelleitungen verlegt oder innerhalb eines elektrischen Einbauraumes verlegt oder
  – einzeln durch eine Erdverbindung geschützt sind.

  Voraussetzung ist, dass sowohl die Leitungen als auch der Einbauraum den jeweiligen Anforderungen entsprechen (siehe DIN EN 60204-1).

- Elektromechanische Positionsschalter, Handschalter

  Die Fehlerannahme „Nichtöffnen von Kontakten“ kann unter folgender Voraussetzung ausgeschlossen werden:
  – Kontakte nach EN 60947-5-1: 2004, Anhang K, öffnen sich. Es ist anzumerken, dass dieser Fehlerausschluss nur für den elektrischen Teil des Schalters gilt (es handelt sich um einen Fehlerausschluss aus der Fehlerliste zur Elektrik). Anhang D.2.5 enthält detaillierte Ausführungen zu den Themen Fehlerausschluss und Modellierung von elektromechanischen Bauteilen.

C.3 Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien werden in den Tabellen A.1, B.1, C.1 und D.1 der informativen Anhänge der DIN EN ISO 13849-2 behandelt.

C.3.1 Allgemein für alle Technologien

- Anwendung geeigneter Werkstoffe und angemessener Herstellungsverfahren

  Werkstoffe, Herstellungs- und Behandlungsverfahren werden unter Berücksichtigung von Einsatz und Beanspruchungen ausgewählt.

- Richtige Dimensionierung und Formgebung aller Bauteile

  Alle Bauteile werden so ausgewählt, dass sie den erwarteten Betriebsbedingungen genügen. Wichtige Kriterien sind z. B. Schaltvermögen, Schalthäufigkeit, Spannungsfestigkeit, Druckhöhe, dynamisches Druckverhalten, Volumenstrom, Temperatur und Viskosität der Druckflüssigkeit, Art und Zustand der Druckflüssigkeit bzw. der Druckluft.

- Alle Bauteile sind gegen Umgebungsbedingungen und relevante äußere Einflüsse beständig.

  Die SRP/CS sind so ausgelegt, dass sie ihre Funktionen auch unter für die Anwendung üblichen äußeren Einflüssen ausführen können. Wichtige Kriterien sind z. B. mechanische Einflüsse, klimatische Einflüsse, Dichtigkeit des Gehäuses und EMV-Störfestigkeit.

- Prinzip der Energietrennung (Ruhestromprinzip)

  Der sichere Zustand wird durch Wegnahme des Steuersignals (elektrische Spannung, Druck), also durch Energieabschaltung, erreicht. Wichtige Kriterien sind z. B. sicherer Zustand bei Energieunterbrechung oder wirksame Federrückstellung bei Ventilen in der Fluidtechnik.

- Schutz gegen unerwarteten Anlauf

  Der unerwartete Anlauf, z. B. verursacht durch gespeicherte Energie oder nach Wiederherstellung der Energieversorgung, wird vermieden.

C.3.2 Beispiele für grundlegende Sicherheitsprinzipien in der Fluidtechnik

- Druckbegrenzung

  Der Anstieg des Drucks in einem System oder in Teilsystemen über ein festgelegtes Niveau hinaus wird in der Regel durch ein oder mehrere Druckbegrenzungsventile verhindert. In der Pneumatik werden dazu vorwiegend Druckregelventile mit Sekundärentlüftung eingesetzt.

- Maßnahmen zur Vermeidung von Verunreinigungen des Druckmediums

  Die für die verwendeten Bauteile erforderliche Reinheitsklasse des Druckmediums wird durch eine geeignete Einrichtung, meist ein Filter, erreicht. In der Pneumatik ist auch eine entsprechende Entwässerung erforderlich.

C.3.3 Beispiele für grundlegende Sicherheitsprinzipien in der Elektrik

- Richtige Schutzleiterverbindung

  Eine Seite des Steuerstromkreises, eine Klemme jedes elektromagnetisch betätigten Geräts oder eine Klemme anderer elektrischer Geräte ist mit einem Schutzleiter verbunden. Diese Seite des Geräts wird also nicht benutzt, um z. B. die Abschaltung einer gefahrbringenden Bewegung

herbeizuführen. Ein Fehler durch Masseschluss kann daher nicht dazu führen, dass ein Abschaltpfad (unbemerkt) ausfällt.

- Unterdrückung von Spannungsspitzen

  Eine Einrichtung zur Unterdrückung von Spannungsspitzen (RC-Glied, Diode, Varistor) wird parallel zur Last (nicht parallel zu den Kontakten) geschaltet.

C.3.4 Beispiele für grundlegende Sicherheitsprinzipien in der Rechnertechnik/Software

DIN EN ISO 13849-2 beschreibt keine grundlegenden Sicherheitsprinzipien für den Einsatz von programmierbaren Systemen bzw. Software. Als solche können jedoch die sogenannten Basismaßnahmen für SRESW und SRASW nach den Abschnitten 4.6.2 und 4.6.3 der Norm verstanden werden (siehe hierzu auch Abschnitt 6.3). Ergänzend wirkt die Überwachung des Programmablaufs, um eine fehlerhafte Reihenfolge von Befehlen bzw. Softwaremodulen zu erkennen, die trotz aller Sorgfalt bei der Verifikation und Validierung auftreten können. Umgesetzt wird diese Maßnahme in der Regel mithilfe eines externen, zyklisch „retriggerten“ Watchdogs, der das SRP/CS bei fehlerhaftem Programmablauf in einen definierten sicheren Zustand bringen können muss.

C.4 Bewährte Sicherheitsprinzipien

Die Tabellen A.2, B.2, C.2 und D.2 der informativen Anhänge der DIN EN ISO 13849-2 behandeln bewährte Sicherheitsprinzipien. Ziel der Anwendung bewährter Sicherheitsprinzipien ist es, kritische Fehler oder Ausfälle zu minimieren oder auszuschließen und so die Wahrscheinlichkeit von Fehlern oder Ausfällen, die die Sicherheitsfunktion beeinflussen, zu vermindern.

C.4.1 Allgemein für alle Technologien bewährte Sicherheitsprinzipien

- Überdimensionierung/Sicherheitsfaktor

  Alle Betriebsmittel werden unter Nennwert beansprucht. Ziel ist es, die Ausfallwahrscheinlichkeit zu reduzieren.

- Zwangläufige/formschlüssige Betätigung

  Es handelt sich um eine sichere Betätigung durch starre mechanische Teile mit formschlüssigen, steifen und nicht federnden Verbindungen. Ziel ist es, eine sichere Befehlsgabe zu erreichen, z. B. beim Betätigen eines Positionsschalters das zwangläufige Öffnen auch eines verschweißten Kontaktes.

- Begrenzung elektrischer und/oder mechanischer Parameter

  Kraft-, Weg-, Zeit-, Drehzahl- oder Geschwindigkeitsbegrenzungen werden durch elektrische, mechanische oder fluidtechnische Einrichtungen auf zulässige Werte reduziert. Ziel ist die Risikominderung durch verbesserte Gefahrenabwehr.

C.4.2 Beispiele für bewährte Sicherheitsprinzipien in der Fluidtechnik

- Gesicherte Position

  Das bewegliche Element eines Bauteils wird mechanisch in einer möglichen Position gehalten (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Kraft notwendig.

- Anwendung bewährter Federn

  DIN EN ISO 13849-2 führt in Tabelle A.2 detaillierte Anforderungen zu bewährten Federn auf.

C.4.3 Beispiele für bewährte Sicherheitsprinzipien in der Elektrik

- Begrenzung elektrischer Parameter

  Begrenzung von Spannung, Strom, Energie oder Frequenz zum Vermeiden eines unsicheren Zustands

- Vermeidung undefinierter Zustände

  Undefinierte Zustände im SRP/CS sind zu vermeiden. Das SRP/CS ist so zu konstruieren, dass sein Zustand während des üblichen Betriebs und unter allen zu erwartenden Betriebsbedingungen vorherbestimmt werden kann, z. B. durch Verwendung von Bauteilen mit definiertem Ansprechverhalten (Schaltschwellen, Hysterese) und mit definierter zeitlicher Abfolge.

- Trennung von Nicht-Sicherheitsfunktionen und Sicherheitsfunktionen

  Um unvorhergesehene Einflüsse auf Sicherheitsfunktionen auszuschließen, werden diese von Nicht-Sicherheitsfunktionen getrennt realisiert.

C.4.4 Beispiele für bewährte Sicherheitsprinzipien in der Rechnertechnik/Software

DIN EN ISO 13849-2 beschreibt keine bewährten Sicherheitsprinzipien für den Einsatz von programmierbaren Systemen bzw. Software. Als solche können jedoch die sogenannten zusätzlichen Maßnahmen für SRESW und SRASW nach den Abschnitten 4.6.2 und 4.6.3 der Norm verstanden werden (siehe hierzu auch Abschnitt 6.3). Ein weiteres bewährtes Sicherheitsprinzip ist die Fehleraufdeckung in komplexen Bauelementen wie zum Beispiel Mikrocontrollern durch Selbsttests. Tabelle E.1 der Norm zur Abschätzung des Diagnosedeckungsgrades listet solche Selbsttests wie zum Beispiel Speichertests oder CPU-Tests. Informationen zur Realisierung solcher Tests enthält auch ein BGIA-Report [7]. Abhängig von der Anwendung können auch „Fehlererkennung durch den Prozess“ und „Fehlererkennung durch Vergleich zwischen Kanälen“ als bewährte Sicherheitsprinzipien gelten.

C.5 Bewährte Bauteile

Bewährte Bauteile für Mechanik und Elektrik werden in den Tabellen A.3 und D.3 der informativen Anhänge der DIN EN ISO 13849-2 behandelt. Ziel der Verwendung bewährter Bauteile ist es, kritische Fehler oder Ausfälle zu minimieren oder auszuschließen und so die Wahrscheinlichkeit von Fehlern oder Ausfällen, die die Sicherheitsfunktion beeinflussen, zu vermindern. Als allgemeine Kriterien für ein bewährtes Bauteil gelten gemäß den Ausführungen zur Kategorie 1, dass das Bauteil

a) in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet wurde oder

b) unter Anwendung von Prinzipien hergestellt und verifiziert wurde, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen zeigen.

Komplexe elektronische Bauteile (z. B. SPS, Mikroprozessor, ASIC) können im Sinne der Norm nicht als bewährt betrachtet werden. Die Einstufung als bewährtes Bauteil hängt auch von der Anwendung ab: In manchen Anwendungen kann ein Bauteil als bewährt gelten, wohingegen dies in anderen Anwendungen, z. B. aufgrund der Umgebungseinflüsse, ausgeschlossen werden muss.

C.5.1 Beispiel für ein bewährtes Bauteil in der Mechanik

- Feder

  Eine Feder gilt als bewährtes Bauteil, wenn die Angaben zu bewährten Sicherheitsprinzipien für die Anwendung bewährter Federn in DIN EN ISO 13849-2, Tabelle A.2, eingehalten und weiterhin die technischen Festlegungen für Federstähle nach ISO 4960 [8] berücksichtigt werden.

C.5.2 Beispiele für bewährte Bauteile in der Fluidtechnik

DIN EN ISO 13849-2 benennt für die Fluidtechnik keine bewährten Bauteile. Die Eigenschaft, bewährt zu sein, hängt insbesondere von der speziellen Anwendung sowie von der Einhaltung der Anforderungen zu bewährten Bauteilen der Kategorie 1 und Anforderungen aus den Normen DIN EN ISO 4413 [9] und DIN EN ISO 4414 [10] ab.

Sicherheitstechnisch bewährte Bauteile können z. B. sein:

- Wegeventile, Sperrventile und Druckventile

C.5.3 Beispiele für bewährte Bauteile in der Elektrik

- Sicherung

  Eine Sicherung ist eine Überstromschutzeinrichtung, die einen Stromkreis bei zu hoher Stromstärke, z. B. infolge eines Isolationsfehlers, unterbricht (Prinzip der Energietrennung). Zu unterscheiden sind Schmelzsicherungen sowie ersatzweise Leitungsschutzschalter. Sicherungen haben sich seit Jahrzehnten als Überstromschutzeinrichtungen bewährt. Für Sicherungen existieren umfangreiche Bestimmungen [11; 12]. Versagensfälle von Sicherungen sind bei bestimmungsgemäßem Einsatz und korrekter Dimensionierung praktisch auszuschließen.

- Not-Aus-Gerät/Not-Halt-Gerät

  Zur Einleitung von Handlungen im Notfall dienen Geräte für Not-Aus und Not-Halt nach DIN EN ISO 13850 [13]. Den Geräten gemeinsam ist die Ausrüstung mit zwangsöffnenden Hilfsstromschaltern zur Energieunterbrechung nach Anhang K in DIN EN 60947-5-1 [14]. Zwei Arten von Hilfsstromschaltern mit Zwangsöffnung werden unterschieden:
  – Typ 1: Mit nur einem Schaltglied, das als zwangsöffnender Kontakt ausgeführt ist.
  – Typ 2: Mit einem oder mehreren Öffnern und möglicherweise mit einem oder mehreren Schließern und/oder einem oder mehreren Wechslern. Alle Öffnerkontakte einschließlich der Öffnerteile der Wechsler müssen zwangläufig öffnende Schaltglieder haben.

  Zu weiteren Details, insbesondere zur Modellierung von Not-Halt-Geräten, siehe Anhang D.2.5.4.

- Schalter mit zwangläufigem Betätigungsmodus (direkt öffnend)

  Diese besondere Art der Schalter wird als Tastschalter, Positionsschalter und als Wahlschalter mit Nockenbetätigung, z. B. zur Anwahl von Betriebsarten, auf dem Markt angeboten. Die Schalter haben sich seit Jahrzehnten bewährt. Ihnen zugrunde liegt das bewährte Sicherheitsprinzip des zwangläufigen Betätigungsmodus durch zwangsöffnende Kontakte. Als bewährtes Bauteil muss der Schalter den Anforderungen der DIN EN 60947-5-1 [14], Anhang K, entsprechen.

Literatur

[1] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (02.13). Beuth, Berlin 2013

[2] DIN EN 61800-5-2: Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

[3] DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (05.14). Beuth, Berlin 2014

[4] *Bömer, T.:* Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Kennzahl 340 220. In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2. Aufl., Lfg. 1/16, VI/2016. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. Erich Schmidt, Berlin 2003 – Losebl.-Ausg.
► www.ifa-handbuchdigital.de/340220

[5] Measuring whisker growth on tin and tin alloy surface finishes, JESD22-A121A. Hrsg.: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2008

[6] Environmental acceptance requirements for tin whisker susceptibility of tin and tin alloy surface finishes, JESD201A. Hrsg.: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2008

[7] *Mai, M.; Reuß, G.:* Selbsttests für Mikroprozessoren mit Sicherheitsaufgaben oder „Quo vadis Fehler?“. BGIA-Report 7/2006. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006
▶ www.dguv.de/ifa, Webcode: d6163

[8] ISO 4960: Kaltband aus unlegierten Stählen mit Kohlenstoffgehalten über 0,25 % (12.07). Beuth, Berlin 2007

[9] DIN EN ISO 4413: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile (04.11). Beuth, Berlin 2011

[10] DIN EN ISO 4414: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile (04.11). Beuth, Berlin 2011

[11] DIN EN 60269-1: Niederspannungssicherungen – Teil 1: Allgemeine Anforderungen (05.15). Beuth, Berlin 2015

[12] DIN EN 60127-1: Geräteschutzsicherungen – Teil 1: Begriffe für die Geräteschutzsicherungen und allgemeine Anforderungen an G-Sicherungseinsätze (12.15). Beuth, Berlin 2015

[13] DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt-Funktion – Gestaltungsleitsätze (05.16). Beuth, Berlin 2016

[14] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (04.10). Beuth, Berlin 2010

Anhang D:
Mean Time to Dangerous Failure ($MTTF_D$)

Änderungen 2008 zu 2016:

- Erhöhung der Kanal-$MTTF_D$-Begrenzung auf 2500 Jahre für Kategorie 4 eingefügt
- Abschnitt D.2.4.2 und Abbildung D.3 überarbeitet, um die Verständlichkeit zu erhöhen
- In Abschnitt D.2.3 erhöhte $MTTF_D$-Werte für Hydraulikventile nach dem Verfahren guter ingenieurmäßiger Praxis eingefügt
- In Abschnitt D.2.4 Erläuterungen zum Einsatz von Schützen und zur Umrechnung von mechanischer/elektrischer Lebensdauer in B_{10D}-Werte eingefügt
- In Abschnitt D.2.5, Tabelle D.2 (Verfahren guter ingenieurmäßiger Praxis) aktualisiert, u. a. höhere $MTTF_D$-Werte für selten betätigte Hydraulikventile, verringerter B_{10D}-Wert für „Schütze mit nominaler Last“, für Not-Halt-Geräte und Druck-Taster (z. B. Zustimmungsschalter) B_{10D}-Wert statt Fehlerausschluss.
- In Abschnitt D.2.5 ausführliche Erläuterungen zur Modellierung elektromechanischer Bauteile eingefügt
- In Abschnitt D.2.6 Hinweis auf den gelöschten Sicherheitsfaktor von 10 für typische elektronische Bauteile eingefügt

D.1 Was bedeutet „$MTTF_D$“?

Die mittlere Zeit bis zum gefahrbringenden Ausfall $MTTF_D$ (Mean Time to Dangerous Failure) beschreibt die Zuverlässigkeit der in einer Steuerung verwendeten Bauteile und fließt als einer von mehreren Parametern in die Bestimmung des Performance Levels ein. In DIN EN ISO 13849-1 wird die $MTTF_D$ als „Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall“ definiert, was mehrere Aspekte betont:

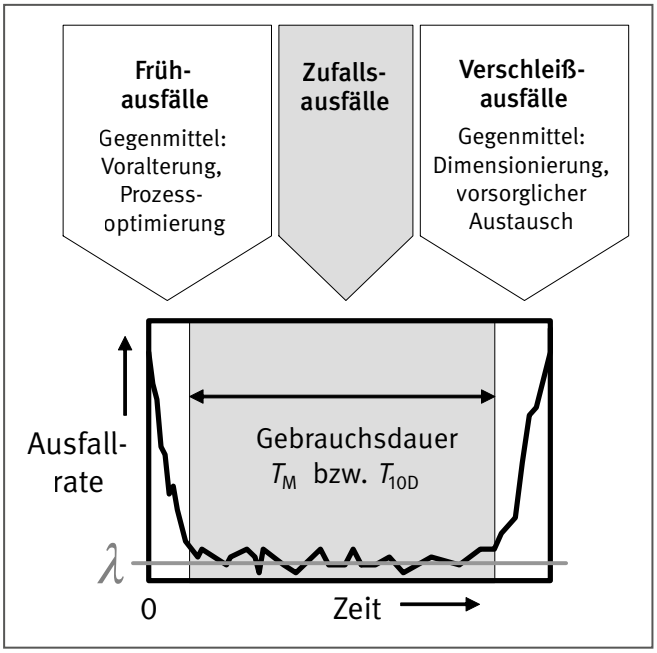
- $MTTF_D$ ist eine statistische Größe, d. h. ein empirisch entstandener Wert bzw. eine Kennzahl, die nichts mit einer „garantierten Lebensdauer“, „ausfallfreien Zeit“ oder Ähnlichem zu tun hat.
- $MTTF_D$ hat die physikalische Dimension einer Zeit und wird meist in Jahren angegeben.
- Es geht nur um Ausfälle in die gefahrbringende Richtung, d. h. solche, die die Ausführung der Sicherheitsfunktion beeinträchtigen. Führen mehrere Kanäle die Sicherheitsfunktion aus (Redundanz), so spricht man auch von einem „gefahrbringenden Ausfall“, wenn nur ein einzelner Kanal betroffen ist.

D.1.1 Badewannenkurve und konstante Ausfallrate

Eine übliche Form der Beschreibung von Bauteilzuverlässigkeiten ist die Angabe von Ausfallraten, abgekürzt λ (nur auf gefahrbringende Ausfälle bezogen entsprechend λ_D), mit der gebräuchlichen Einheit FIT (Failures In Time, d. h. Anzahl der Ausfälle in 10^9 Bauteilstunden, 1 FIT = 10^{-9}/h). Diese Ausfallrate beschreibt zu einem bestimmten Zeitpunkt die Rate, mit der funktionsfähige Bauteile gerade ausfallen. Das heißt, die Zahl der Ausfälle pro Zeit wird durch die Anzahl der zum jeweiligen Zeitpunkt noch ausfallfreien Bauteile geteilt. Das Ausfallverhalten vieler Arten von Bauteilen (speziell elektronischer Bauteile) stellt sich in Abhängigkeit von der Zeit als mehr oder weniger ausgeprägte „Badewannenkurve“ dar [1] (siehe Abbildung D.1).

Am Anfang der Gebrauchsdauer fallen in der Regel verstärkt Bauteile aus. Dies sind Frühausfälle, die aber nur für kurze Zeit dominieren. Nach Überschreiten der empfehlenswerten Gebrauchsdauer steigen die Ausfälle wieder an. Im mittleren Bereich der üblichen Gebrauchsdauer ist insbesondere bei elektronischen Bauelementen oft ein plateauähnlicher Bereich konstanter Ausfallrate zu beobachten. Dieser wird durch die sogenannten Zufallsausfälle geprägt. Selbst stärker von Verschleiß als von Zufallsausfällen dominierte Bauteile, z. B. elektro-

Abbildung D.1:
„Badewannenkurve“ der Ausfallrate



mechanische oder pneumatische, lassen sich oft im Rahmen ihrer Gebrauchsdauer durch die Annahme einer zur sicheren Seite hin abgeschätzten konstanten Ausfallrate beschreiben. Üblicherweise werden Frühausfälle vernachlässigt, da Komponenten mit ausgeprägten Frühausfällen den Verfügbarkeitsanforderungen an eine Maschinensteuerung nicht gerecht werden und daher im Markt nur eine geringe Rolle spielen. Geeignete Maßnahmen zur Reduktion von Frühausfällen sind Voralterung (Burn-In), Selektion und Optimierung der Herstellungsprozesse. Im Sinne der Einfachheit wird daher in DIN EN ISO 13849-1 grundsätzlich innerhalb der Gebrauchsdauer von konstanten Ausfallraten ausgegangen. Diese Annahme hat den Vorteil, dass sich damit die weitere mathematische Betrachtung stark vereinfacht, und sie ist Grundlage für die hinter dem Säulendiagramm bzw. dem vereinfachten Verfahren der DIN EN ISO 13849-1 stehende Markov-Modellierung der vorgesehenen Architekturen. Aus einer konstanten Ausfallrate folgen mathematisch eine mit der Einsatzzeit exponentiell abfallende Kurve der Zuverlässigkeit und ein Erwartungswert der Zeit bis zum Ausfall ($MTTF_D$), der dem Kehrwert der Ausfallrate entspricht, d. h.

$$MTTF_D = \frac{1}{\lambda_D} \qquad \text{(D.1)}$$

Bei konstanter Ausfallrate ist also die Angabe der $MTTF_D$ der Angabe einer Ausfallrate gleichwertig, ist aber viel illustrativer. Während die praktische Bedeutung eines FIT-Wertes wenig anschaulich ist, vermittelt die Angabe eines zeitlichen Erwartungswertes in Jahren eher eine Vorstellung von der Bauelementgüte. Abbildung D.2 zeigt die statistisch zu erwartende Entwicklung des Anteils gefahrbringender Ausfälle über der Einsatzzeit für vier verschiedene $MTTF_D$-Werte. Hier lässt sich ein weiterer mathematischer Zusammenhang ablesen, nämlich dass bei Erreichen der $MTTF_D$-Marke auf der Zeitachse im statistischen Mittel ca. 63 % aller anfänglich intakten Bauteile gefahrbringend ausgefallen sind (nicht 50 %, da zwar mehr Bauteile vor Erreichen der $MTTF_D$ ausfallen, dafür aber die dann noch intakten Bauteile mit Restlaufzeiten von teilweise dem Mehrfachen der $MTTF_D$ schwerer wiegen).

Das vereinfachte Quantifizierungsverfahren nach DIN EN ISO 13849-1 unterstellt eine übliche Gebrauchsdauer von maximal 20 Jahren für Bauteile in Sicherheitssteuerungen im Maschinenbau. Vor diesem Hintergrund und bei Kenntnis des zeitlichen Verlaufs der Ausfallrate (Abbildung D.1) wird verständlich, dass die Angabe eines $MTTF_D$-Wertes nur als illustrative Kennzeichnung für das Zuverlässigkeitsniveau innerhalb der Gebrauchsdauer verstanden werden sollte und weder eine Garantie für eine ausfallfreie Zeit vor Erreichen der $MTTF_D$ noch eine exakte Vorhersage für den Ausfallzeitpunkt eines Einzelbauteils bietet. Ist der Verschleißbereich erreicht, ändert sich das Ausfallverhalten grundlegend und kann nicht mehr sinnvoll durch eine konstante Ausfallrate beschrieben werden.

D.1.2 Klasseneinteilung und Begrenzung

Die Annahme einer $MTTF_D$ für jedes sicherheitsrelevante Bauteil (wenn kein Fehlerausschluss begründet werden kann) ist Voraussetzung für die nachfolgenden Schritte, die zunächst auf Block- und dann auf Kanalebene zur sogenannten $MTTF_D$ jedes Kanals führen. Auf Kanalebene schlägt DIN EN ISO 13849-1 die Einteilung in drei typische $MTTF_D$-Klassen vor (Tabelle D.1). Diese Klassen sollen kleine Unterschiede in den errechneten $MTTF_D$ -Werten nivellieren, die ohnehin innerhalb der statistischen Unsicherheit untergehen. Auch soll damit die Gleichwertigkeit mit den anderen Parametern (fünf Kategorien, vier DC-Stufen) gewahrt bleiben und die notwendige Vereinfachung für die Darstellung im Säulendiagramm erreicht werden.

Tabelle D.1:
Klasseneinteilung der $MTTF_D$ für Kanäle, die die Sicherheitsfunktion ausführen

Bezeichnung der $MTTF_D$ für jeden Kanal	Bereich der $MTTF_D$ für jeden Kanal
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre

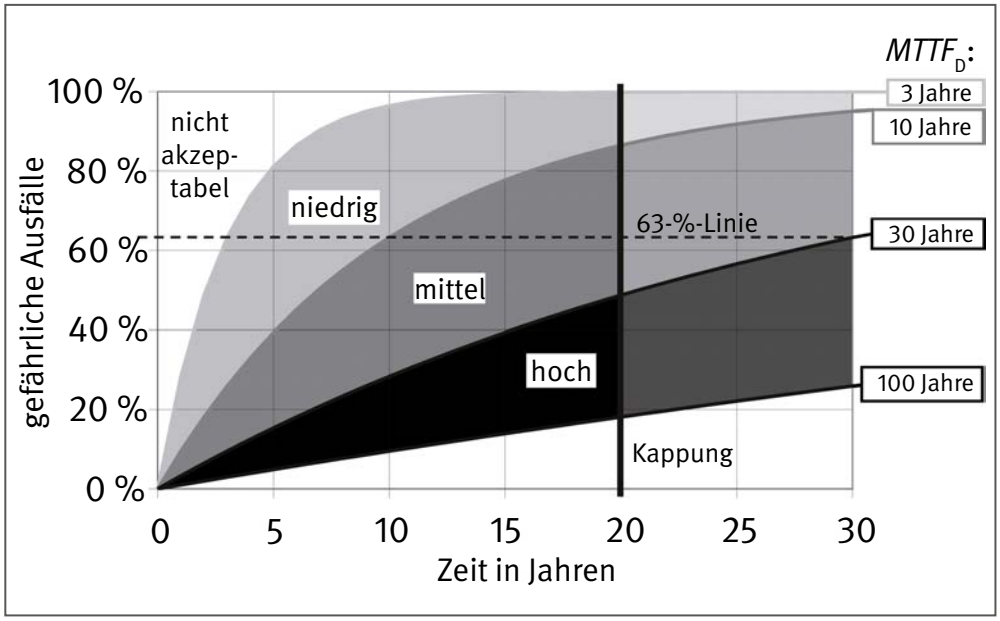


Abbildung D.2:
Illustration der $MTTF_D$

Gewünschte Nebeneffekte dieser Klassenbildung sind die Zurückweisung von $MTTF_D$-Werten jedes Kanals < 3 Jahre und die Beschränkung höherer $MTTF_D$-Werte jedes Kanals auf maximal 100 Jahre (in Kategorie 4 wird diese Beschränkung auf 2500 Jahre angehoben, auch diese Werte sind der Klasse „hoch" zuzuordnen). Abbildung D.2 macht deutlich, dass bei einer $MTTF_D$ von drei Jahren schon nach einem Jahr fast 30 % gefahrbringende Ausfälle zu erwarten sind, was für eine Sicherheitssteuerung inakzeptabel erscheint. Am anderen Ende des Spektrums erscheint ein statistisch abgesicherter Nachweis von Zuverlässigkeiten > 100 Jahre $MTTF_D$ sehr fragwürdig (in Kategorie 4 ist dies akzeptabel, da die anderen für die Zuverlässigkeit bestimmenden Parameter wie Redundanz und Fehlererkennung schon ein hohes Niveau haben). Außerdem bleibt selbst bei beliebig hohen $MTTF_D$-Zahlen eine Restwahrscheinlichkeit für einen gefahrbringenden Ausfall innerhalb der Gebrauchsdauer, der darüber hinaus auch aus anderen Gründen auftreten kann (z. B. Fehlanwendung). Daher erscheint die Absicherung hoher Performance Level alleine durch Verwendung hoch zuverlässiger Bauteile ohne entsprechende Redundanz und Fehlererkennung nicht angemessen. Im Säulendiagramm nach DIN EN ISO 13849-1 wird dies dadurch ausgedrückt, dass kein $MTTF_D$-Bereich über der hohen $MTTF_D$-Klasse dargestellt wird, auch wenn dies aufgrund der Wahrscheinlichkeitsrechnung möglich wäre. Die Rückstufung höherer $MTTF_D$-Werte auf den Maximalwert von 100 bzw. 2500 Jahren findet erst auf Kanalebene statt, d. h., für einzelne Bauteile können deutlich höhere $MTTF_D$-Werte in die Berechnung einfließen.

D.1.3 Woher kommen die Daten?

Ein mögliches Problem für die Normanwendung, besonders zum Zeitpunkt der ersten Veröffentlichung der revidierten DIN EN ISO 13849-1, waren fehlende $MTTF_D$-Angaben für im SRP/CS verwendete Bauteile [2]. Grundsätzlich schlägt die Norm in Abschnitt 4.5.2 eine Hierarchie von Datenquellen vor, die an erster Stelle Herstellerangaben ([H]) nennt, dann typische Zahlenwerte, die in der Norm selbst gelistet sind ([N]), und schließlich einen sehr konservativ abgeschätzten Ersatzwert von zehn Jahren. Da dieser Ersatzwert auf ein Bauteil bezogen ist und bei mehreren Bauteilen in einem Kanal schnell die $MTTF_D$-Untergrenze von drei Jahren erreicht wird, waren und sind die in der Norm selbst gelisteten $MTTF_D$-Werte von besonderer Bedeutung. Dies gilt zumindest noch so lange, bis die Angabe von $MTTF_D$-Werten vonseiten der Hersteller zur Selbstverständlichkeit wird – auch für Bauteile, die nicht von vorneherein für die Verwendung in SRP/CS entwickelt wurden.

D.2 Unterschiede der Technologien

Das Ausfallverhalten von Bauteilen hängt naturgemäß sehr stark von der eingesetzten Technologie ab, da die „Badewannencharakteristik" und die Bedeutung von Verschleißeffekten unterschiedlich stark ausgeprägt sein können. Bei mechanischen und hydraulischen Komponenten, die von der Konstruktion und der Anwendung auf hohe Zuverlässigkeit und geringen Verschleiß optimiert werden, kann von einer sehr hohen $MTTF_D$ ausgegangen werden. Hier spielen Zufallsausfälle (der Bereich konstanter Ausfallrate) und Verschleißausfälle eine geringere Rolle. Bei den meisten elektronischen Komponenten hingegen ist das Ausfallverhalten innerhalb der typischen Einsatzdauer vergleichsweise „billiger" industrieller Komponenten üblicherweise sehr gut durch eine konstante Ausfallrate beschrieben, da der Verschleißbereich nur bei verschärften Einsatzbedingungen erreicht wird. Ganz anders geartet wiederum ist das Ausfallverhalten von elektromechanischen oder pneumatischen Bauelementen: Hier kann der Verschleißbereich durchaus in der üblichen Einsatzdauer erreicht werden. Daher wird als Kenngröße üblicherweise auch die erreichbare Anzahl erfolgreicher Schaltzyklen bzw. Schaltspiele angegeben und nicht eine Lebensdauer als Zeit oder eine zeitbezogene Ausfallrate. Allen diesen technologieabhängigen Besonderheiten muss bei der Bestimmung des $MTTF_D$-Wertes Rechnung getragen werden, sodass die Norm hier unterschiedliche Herangehensweisen vorschlägt.

D.2.1 $MTTF_D$ mechanischer Steuerungskomponenten

Der Ansatz konstanter Ausfallraten ist für mechanische Steuerungskomponenten leider nicht sehr angemessen. Andererseits enthält fast jede Sicherheitsfunktion zumindest im Bereich der Sensoren oder Aktoren mechanische Steuerungselemente, die z. B. Bewegungen erkennen oder gefahrbringende Bewegungen stillsetzen müssen. Obwohl die Angabe einer zur sicheren Seite hin abgeschätzten $MTTF_D$ vielfach auch für diese Komponenten möglich wäre, wird hier in der Regel ein Fehlerausschluss herangezogen. Solange die Voraussetzungen für den Fehlerausschluss eingehalten und dokumentiert werden, ist dies meistens die eleganteste Methode, um die Zuverlässigkeit der mechanischen Komponenten zu berücksichtigen. Zu diesen Voraussetzungen gehört u. a. die ausreichende Widerstandsfähigkeit gegenüber den zu erwartenden Umwelteinflüssen, d. h. die Gültigkeit eines Fehlerausschlusses hängt von der gewählten Applikation ab. Eine andere Voraussetzung ist z. B. ausreichende Überdimensionierung, die sicherstellt, dass die mechanischen Komponenten z. B. im Bereich der Dauerfestigkeit belastet werden. Falls ein Fehlerausschluss nicht möglich ist, bietet eventuell die Anwendung des weiter unten genannten Verfahrens guter ingenieurmäßiger Praxis die Möglichkeit, einen $MTTF_D$-Wert abzuschätzen.

D.2.2 BIA-Report 6/2004 „Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen"

Bei hydraulischen Anlagen ist als „sicherheitsbezogener Teil der Steuerung" insbesondere der Ventilbereich zu betrachten. Dabei sind vor allem Ventile, die gefahrbringende Bewegungen oder Zustände steuern, für die Berechnung des Performance Levels von äußerster Wichtigkeit. Das Ausfallverhalten hydraulischer Ventile wird erfahrungsgemäß wenig von Zufallsausfällen und eher von Verschleißausfällen geprägt. Dabei handelt es sich in erster Linie um systematische Ursachen wie z. B. Überbeanspruchung, ungünstige Einsatzbedingungen oder fehlende Wartung. Um die Lebensdauer hydraulischer Ventile besser abschätzen zu können, initiierte das IFA (zu der Zeit noch BGIA) eine Diplomarbeit zu diesem Thema, deren Ergebnisse als BIA-Report 6/2004 „Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen" [3] vorliegen. Da es sich in der Regel bei Ventilen, die Steuerungsaufgaben übernehmen, um Wegeventile in Schieberbauweise handelt, wurden die $MTTF_D$-Werte für „hydraulische Bauteile" ersatzweise an Wegeventilen in

Schieberbauweise ermittelt. Die wichtigsten Ergebnisse dieser Untersuchung werden im Folgenden kurz vorgestellt.

Die Grundlage für die Abschätzung eines $MTTF_D$-Wertes bilden in erster Linie die Ausfallraten von hydraulischen Wege-Schieberventilen, die im Rahmen einer Untersuchung in den Instandhaltungsabteilungen zweier großer Hydraulikanwender ermittelt wurden (im Folgenden Anwender A und B genannt). Dies erfolgte durch Auswertung von EDV-Daten (Neubeschaffungsmengen von hydraulischen Wegeventilen in Schieberbauweise und Reparaturberichten) und Mitwirkung bei Instandhaltungsarbeiten. Zusätzlich zu den Ausfalldaten der Ventile wurden die Einsatzbedingungen berücksichtigt. Somit ist die Vergleichbarkeit der bei den jeweiligen Hydraulikanwendern ermittelten $MTTF_D$-Werte gegeben. Zur Absicherung und Bestätigung dieser Daten wurden darüber hinaus durch eine Umfrage unter Ventilherstellern zusätzliche Ausfalldaten gesammelt. Bei Anwender A wurden die Ausfallraten der Wegeventile in der Instandhaltungsabteilung der Getriebefertigung erfasst. Verfügbar waren die Daten aller ausgefallenen Wegeventile über einen Zeitraum von 38 Monaten, in dem es 143 Ausfälle von Wegeventilen gab. In den Maschinen der Getriebefertigung, größtenteils Werkzeugmaschinen, waren ungefähr 8 050 Wegeventile unterschiedlichen Alters im Einsatz. Wenn in dieser Zeitspanne eine konstante Ausfallrate unterstellt wird, lässt sich aus den Daten für Anwender A eine $MTTF_D$ von 178 Jahren als Kehrwert der Ausfallrate errechnen. Bei diesem Anwender wurden die Einsatzbedingungen an den Hydraulikanlagen weitgehend nach den Vorgaben der Hersteller eingehalten. Da es sich vorwiegend um neue Fertigungsstraßen handelte, erfolgte eine zustandsorientierte Instandhaltung.

Bei Anwender B wurden die Ausfalldaten für die Wegeventile ebenfalls in der Instandhaltungsabteilung der Getriebefertigung aufgenommen. Hier waren ungefähr 25 000 Wegeventile unterschiedlichen Alters im Einsatz. Verfügbar waren die Daten aller ausgefallenen Wegeventile in einem Zeitraum von vier Jahren (2000 bis 2003). Im Gegensatz zum Anwender A waren hier die Ausfalldaten für jedes Jahr einzeln abrufbar; somit war es möglich, eine $MTTF_D$ für jedes einzelne Jahr zu bestimmen. Dabei stieg die $MTTF_D$ von 195 Jahren im Jahre 2000 auf 300 im Jahre 2003. Es zeigte sich ein signifikanter Zusammenhang zwischen Ventilausfällen und Einsatz- bzw. Umgebungsbedingungen, denn Anwender B hatte seine Instandhaltungsmaßnahmen und Einsatzbedingungen im Laufe der Jahre kontinuierlich verbessert. Des Weiteren wurden gegenüber Anwender A die Einsatzbedingungen durch zusätzliche Maßnahmen verbessert, z. B. Überwachung der Öltemperatur, größere meist außerhalb der Maschine untergebrachte Öltanks, feinere Rücklauffilter sowie Abzugsanlagen zur Minderung der Verunreinigungen in der Umgebungsluft. Die Untersuchung zeigte, dass die zylindrischen Führungen der Bauteile in Ventilen, z. B. Steuerschieber, in Verbindung mit Art, Qualität und Verschmutzungsgrad der eingesetzten Druckflüssigkeit sowie Auslegung, Material und Ausführung der Zentrier-/Rückstellfeder einen wesentlichen Einfluss auf die zu erwartende Lebensdauer hydraulischer Wege-Schieberventile haben. Dabei wurde ein deutlicher Zusammenhang zwischen Qualität der Einsatzbedingungen und der erreichten Lebensdauer bis zum Ausfall über einen definierten Betrachtungszeitraum festgestellt.

D.2.3 $MTTF_D$ hydraulischer Steuerungskomponenten

Aufgrund der Ergebnisse der oben genannten Untersuchung wird in DIN EN ISO 13849-1 für hydraulische Bauteile unter bestimmten Voraussetzungen eine $MTTF_D$ von 150 bis 1 200 Jahren vorgeschlagen. Zwar wurden schwerpunktmäßig Ventile in Schieberbauweise untersucht, aufgrund des ähnlichen Ausfallverhaltens lässt sich die ermittelte Lebensdauer $MTTF_D$ aber als gute Abschätzung für alle sicherheitsrelevanten hydraulischen Ventile verwenden. Voraussetzung hierfür ist allerdings die Einhaltung der in DIN EN ISO 13849-2 aufgeführten, auf hydraulische Ventile bezogenen grundlegenden und bewährten Sicherheitsprinzipien bei Konstruktion und Herstellung. Weiterhin müssen die ebenfalls in DIN EN ISO 13849-2 aufgeführten anwendungsbezogenen grundlegenden und bewährten Sicherheitsprinzipien vom Ventilhersteller genannt (Herstellervorgaben, Einsatzbedingungen) und in der Praxis eingehalten werden.

Anhang C.2, Tabelle C.1, der DIN EN ISO 13849-2 nennt die grundlegenden Sicherheitsprinzipien für hydraulische Systeme. Zu den wichtigsten Prinzipien gehört die Anwendung geeigneter Werkstoffe und Herstellungsverfahren sowie des Prinzips der Energietrennung, Druckbegrenzung, Schutz gegen unerwarteten Anlauf und ein geeigneter Temperaturbereich (weitere Erläuterungen siehe Anhang C).

Anhang C.3, Tabelle C.2, der DIN EN ISO 13849-2 listet bewährte Sicherheitsprinzipien für hydraulische Systeme auf. Die wichtigsten Prinzipien umfassen Überdimensionierung/Sicherheitsfaktoren, Begrenzung/Verringerung der Geschwindigkeit durch einen Widerstand zum Erreichen eines definierten Volumenstroms, Begrenzung/Verringerung der Kraft, einen geeigneten Bereich für die Betriebsbedingungen, Überwachung des Zustands des Druckmediums, Verwendung bewährter Federn und eine ausreichend große positive Überdeckung in Schieberventilen (weitere Erläuterungen siehe ebenfalls Anhang C).

Die Erfahrung mit der Anwendung der zweiten Edition der Norm hat gezeigt, dass für Hydraulikventile auch die Betätigungshäufigkeit n_{op} (Anzahl der jährlichen Betätigungen, siehe Abschnitt D.2.4) ein für die Zuverlässigkeit relevanter Parameter ist. Daher werden in der dritten Edition der Norm im Rahmen des Verfahrens guter ingenieurmäßiger Praxis (siehe Abschnitt D.2.5) abhängig von n_{op} abgestufte $MTTF_D$-Werte für Hydraulikventile zwischen 150 und 1 200 Jahren angegeben (siehe Tabelle D.2).

Auch wenn die Norm unter diesen Voraussetzungen $MTTF_D$-Werte für hydraulische Ventile angibt, sollte dennoch jeder Hersteller von Ventilen für seine Bauteile möglichst eigene Ausfallzahlen ermitteln und eine eigene $MTTF_D$ angeben.

D.2.4 $MTTF_D$ pneumatischer und elektromechanischer Steuerungskomponenten

In der Fluidtechnik sowie in der Mechanik und Elektromechanik wird die Lebensdauer bzw. die Zuverlässigkeit der Komponenten in der Regel vom Verschleißverhalten der bewegten Elemente bestimmt.

Tabelle D.2:
Typische Zuverlässigkeitskennwerte, die bei guter ingenieurmäßiger Praxis als erreicht angenommen werden können

	Grundlegende und bewährte Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013	Andere relevante Normen	Typische Werte: $MTTF_D$ (Jahre) B_{10D} (Zyklen)
Mechanische Bauteile	Tabellen A.1 und A.2	—	$MTTF_D$ = 150 Jahre
Hydraulische Bauteile mit $n_{op} \geq 1000\,000$ Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 150 Jahre
Hydraulische Bauteile mit 500 000 Zyklen pro Jahr ≤ n_{op} < 1000 000 Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 300 Jahre
Hydraulische Bauteile mit 250 000 Zyklen pro Jahr ≤ n_{op} < 500 000 Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 600 Jahre
Hydraulische Bauteile mit n_{op} < 250 000 Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 1200 Jahre
Pneumatische Bauteile	Tabellen B.1 und B.2	DIN EN ISO 4414	B_{10D} = 20 000 000 Zyklen
Relais und Hilfsschütze mit geringer Last	Tabellen D.1 und D.2	DIN EN 61810-1/-2/-3 DIN EN 60947-4-1 DIN EN 60947-5-1	B_{10D}= 20 000 000 Zyklen
Relais und Hilfsschütze mit nominaler Last	Tabellen D.1 und D.2	DIN EN 61810-1/-2/-3 DIN EN 60947-4-1 DIN EN 60947-5-1	B_{10D}= 400 000 Zyklen
Näherungsschalter mit geringer Last	Tabellen D.1 und D.2	DIN EN 60947-5-3 DIN EN ISO 14119	B_{10D}= 20 000 000 Zyklen
Näherungsschalter mit nominaler Last	Tabellen D.1 und D.2	DIN EN 60947-5-3 DIN EN ISO 14119	B_{10D}= 400 000 Zyklen
Schütze mit geringer Last	Tabellen D.1 und D.2	DIN EN 60947-4-1	B_{10D}= 20 000 000 Zyklen
Schütze mit nominaler Last	Tabellen D.1 und D.2	DIN EN 60947-4-1	B_{10D}= 1300 000 Zyklen
Positionsschalter [a]	Tabellen D.1 und D.2	DIN EN 60947-5-1 DIN EN ISO 14119	B_{10D}= 20 000 000 Zyklen
Positionsschalter (mit separatem Betätiger, Zuhaltung) [a]	Tabellen D.1 und D.2	DIN EN 60947-5-1 DIN EN ISO 14119	B_{10D}= 2 000 000 Zyklen
Positionsschalter[b] **und Taster**[b] **bei ohmscher Last und Überdimensionierung (≦ 10 % der maximalen Last) bezogen auf die elektrischen Kontakte**	Tabellen D.1 und D.2	DIN EN 60947-5-1 DIN EN ISO 14119	B_{10D}= 1000 000 Zyklen
Positionsschalter[b] **und Taster**[b] **bei Überdimensionierung nach Tabelle D.2, DIN EN ISO 13849-2: 2013, bezogen auf die elektrischen Kontakte**	Tabellen D.1 und D.2	DIN EN 60947-5-1 DIN EN ISO 14119	B_{10D}= 100 000 Zyklen
Not-Halt-Geräte [a]	Tabellen D.1 und D.2	DIN EN 60947-5-5 DIN EN ISO 13850	B_{10D}= 100 000 Zyklen
Zustimmungsschalter [a]	Tabellen D.1 und D.2	DIN EN 60947-5-8	B_{10D}= 100 000 Zyklen

[a] **falls Fehlerausschluss für Zwangsöffnung möglich ist**

[b] **für Schließerkontakte und für Öffnerkontakte, falls Fehlerausschluss für Zwangsöffnung nicht möglich ist**

Bei fluidtechnischen Komponenten wie z. B. Ventilen, die meistens komplexe Einheiten mit vielen beweglichen Elementen (z. B. Schieber, Stößel, Federn in Vorsteuerstufe und Hauptstufe) darstellen, können auch die betrieblichen Umgebungsbedingungen die Lebensdauer stark beeinflussen. Hierbei sind insbesondere zu nennen:

- Qualität und Zustand des Druckmediums (Druckluft)
- Verträglichkeit von Dichtungen mit den Schmierstoffen
- Temperatureinflüsse
- Umgebungseinflüsse wie z. B. Stäube, Gase, Flüssigkeiten

Auf eine Einhaltung der vom Hersteller der Komponenten spezifizierten Anforderungen ist unbedingt zu achten, damit die bei der Ermittlung der Steuerungskategorie zugrunde gelegten Parameter bezüglich des Ausfallverhaltens der Komponente zutreffend sind.

Bei den elektromechanischen Schützen unterscheidet man zwischen Hilfsschützen und Leistungsschützen. Hilfsschütze werden zur Realisierung logischer Verknüpfungen und zur Ansteuerung von Leistungsschützen eingesetzt. Für das Schalten größerer Leistungen z. B. von Motoren > 3 kW werden

üblicherweise Leistungsschütze eingesetzt. Für Hilfsschütze gelten die Bestimmungen aus DIN EN IEC 60947-5-1 und für Leistungsschütze aus DIN EN IEC 60947-4-1.

Für die Auswahl und den Einsatz sind umfangreiche Kriterien zu beachten. Dies sind insbesondere:

- Netz- und Betriebsbedingungen
- Schaltaufgaben und -bedingungen
- Schalthäufigkeit und Lebensdauer
- Schutz bei Überstrom und Übertemperatur
- Schutz bei Überspannungen
- spezielle Einsatzbedingungen

Die Hersteller geben in speziellen Handbüchern umfassende Hinweise zur Auswahl und Projektierung.

Im Rahmen der Quantifizierung nach DIN EN ISO 13849 wird an dieser Stelle kurz auf die Auswahlkriterien zur Lebensdauer eingegangen. Man unterscheidet zwischen der mechanischen und der elektrischen Lebensdauer. Die mechanische Lebensdauer eines Schützes wird durch die Schaltspielzahl ausgedrückt, die das Schütz ohne Belastung der Strombahnen erreicht. Sie hängt vom Verschleiß der mechanisch bewegten Teile ab.

Die elektrische Lebensdauer eines Schaltgerätes wird durch die Schaltzahl festgelegt, bis zu der die elektrischen Schaltkontakte abgenutzt sind. Die elektrischen Schaltkontakte werden beim Schalten unter Last sowohl beim Einschalt- als auch beim Ausschaltvorgang beansprucht. Der dabei auftretende Kontaktabbrand verursacht den Verschleiß der Schaltstücke. Er ist abhängig von Spannung, Strom, Last (z. B. induktiv) und Zeit. Bei vollständigem Kontaktabbrand kommt es in der Regel zu einem Verschweißen der Kontakte. Dies muss in sicherheitsrelevanten Anwendungen detektiert werden, um gefahrbringende Zustände durch das Nichtöffnen zu verhindern. Für die Detektion sind Schütze mit zwangsgeführten Kontakten bei Hilfsschützen oder sogenannten Spiegelkontakten bei Leistungsschützen einzusetzen. Hierzu sind die Angaben des Herstellers zu beachten.

Die mechanische Lebensdauer und die elektrische Lebensdauer der Schaltstücke ermitteln die Hersteller in Versuchsreihen. Diese Größen sind jedoch nicht unabhängig voneinander. Die tatsächliche Lebensdauer des Schützes kann außer von der mechanischen Abnutzung auch von Leistung und Betriebsart der Last abhängen. Bei den dadurch beeinflussten Werten spricht man von der Gerätelebensdauer.

Die in Tabelle D.2 dieses Reports angegebenen sogenannten B_{10D}-Werte (siehe Abschnitt D.2.4.1) für die Gerätelebensdauer sind als Anhaltswerte zu sehen. Es sind bevorzugt die Angaben des Herstellers zu verwenden. Gibt ein Hersteller selbst keinen B_{10D}-Wert an, wohl aber Werte (Anzahl Schaltzyklen) für die mechanische und die elektrische Lebensdauer, so kann der kleinere dieser Werte (bei der elektrischen Lebensdauer in der Regel abhängig von der Last) als Schätzwert für den B_{10}-Wert angenommen werden. Durch Verdoppelung kann daraus der B_{10D}-Wert ermittelt werden (siehe Abschnitt D.2.4.1).

Sind die folgenden Merkmale erfüllt, kann der $MTTF_D$-Wert für ein einzelnes pneumatisches, elektromechanisches oder mechanisches Bauteil nach den weiter unten aufgeführten Formeln abgeschätzt werden:

- Der Hersteller des Bauteils bestätigt die Verwendung grundlegender Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabelle B.1 oder Tabelle D.1, für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).

- Der Hersteller eines Bauteils, das in einer Steuerung der Kategorie 1, 2, 3 oder 4 verwendet werden soll, bestätigt die Verwendung bewährter Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabellen B.2 oder D.2, für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).

- Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für die SRP/CS-Konstruktion und die Anwendung fest. Der SRP/CS-Konstrukteur erfüllt die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabellen B.1 oder D.1, für die Implementierung und den Betrieb des Bauteils und informiert den Anwender über seine Verantwortung, die von ihm umzusetzenden Sicherheitsprinzipien zu erfüllen. Bei den Kategorien 1, 2, 3 und 4 gilt dieselbe Verpflichtung auch hinsichtlich der Einhaltung der bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabellen B.2 oder D.2, und dies wiederum bei Implementierung und Betrieb des Bauteils.

Die hinter den grundlegenden und bewährten Sicherheitsprinzipien stehenden konkreten Maßnahmen ähneln denjenigen, die oben für hydraulische Bauelemente ausführlicher beschrieben sind.

Der $MTTF_D$-Wert ist definiert als die mittlere Zeit bis zum gefahrbringenden Ausfall. Um diese Zeit für ein Bauteil bestimmen zu können, müssen entsprechende Lebensdauermerkmale festgelegt werden. Dies können zurückgelegte Strecken für Pneumatikzylinder, Betätigungshäufigkeiten für Ventile oder elektromechanische Bauteile sowie Lastwechsel bei mechanischen Komponenten sein. In der Regel wird die Zuverlässigkeit für pneumatische oder elektromechanische Bauteile im Labor bestimmt.

D.2.4.1 Bestimmung des Lebensdauerkennwertes B_{10D}

Mit im Labor oder eventuell auch bei Felduntersuchungen ermittelten Werten kann die Ausfallhäufigkeit z. B. mithilfe der Weibull-Statistik bestimmt werden [4]. Die zweiparametrige Weibull-Verteilungsfunktion in Abbildung D.3 ist flexibler als die Exponentialverteilung, die sie als Spezialfall (b = 1) enthält. Ein Ansteigen der Ausfallrate bei Erreichen der Verschleißphase lässt sich durch b-Parameter > 1 gut beschreiben. Der T-Parameter beschreibt die charakteristische Lebensdauer, bei der 63,2 % der betrachteten Bauteile ausgefallen sind. Werden nur gefahrbringende Ausfälle betrachtet, kann dies durch den Index „D“ dargestellt werden. Als Methode zur Bestimmung der Weibull-Parameter können je nach Testverfahren verschiedene Methoden angewendet werden. Dies umfasst auch unvollständige Daten, wenn also z. B. nicht schadhafte Teile berücksichtigt werden sollen. Als Ergebnis können aus den Diagrammen die

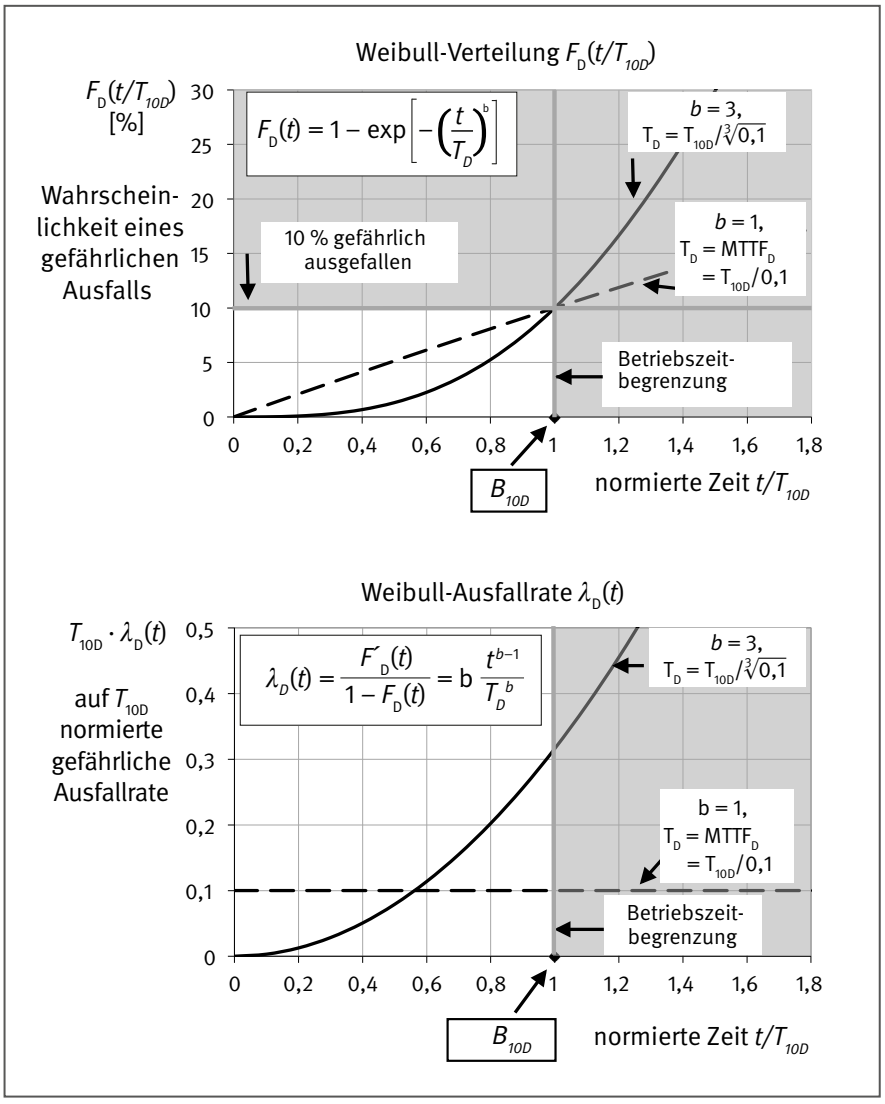


Abbildung D.3:
Illustration der Umrechnung von B_{10D} in $MTTF_D$

Kennwerte für die Parameter b und T abgelesen werden. Daraus lässt sich dann die nominale Lebensdauer T_{10} bestimmen, bei der 10 % der betrachteten Bauteile ausgefallen sind. Bei pneumatischen und elektromechanischen Bauteilen werden Lebensdauern statt in der Dimension „Zeit" in der Regel als Schaltspiele in der Pseudo-Einheit „Zyklen" angegeben. Die Umrechnung erfolgt mittels der mittleren Anzahl jährlicher Betätigungen n_{op} (in Zyklen pro Jahr, siehe Abschnitt D.2.4.2). Der B_{10}-Wert in Zyklen entspricht dabei dem T_{10}-Wert auf Zeitbasis. Der $MTTF_D$-Wert wird wie später unter Abschnitt D.2.4.2 beschrieben mit der nominalen Lebensdauer B_{10} ermittelt. Für eine Zuverlässigkeitsanalyse mithilfe der Weibull-Statistik ist Software auf dem Markt erhältlich. Die sicherheitstechnischen Zuverlässigkeitskennwerte für fluidtechnische und elektromechanische Komponenten sind vom Hersteller dieser Bauteile anzugeben. Für die Ermittlung der Zuverlässigkeit von pneumatischen Komponenten kann die Norm ISO 19973 „Pneumatik – Bewertung der Zuverlässigkeit von Bauteilen durch Prüfung" zugrunde gelegt werden. Diese Norm besteht zurzeit aus fünf Teilen:

- Teil 1: Allgemeine Verfahren
- Teil 2: Ventile
- Teil 3: Zylinder mit Kolbenstange
- Teil 4: Druckregelventile
- Teil 5: Rückschlagventile, Wechselventile (ODER-Ventile), Zweidruckventile (UND-Ventile), einstellbare Drosselrückschlagventile, Schnellentlüftungsventile

Bei der Ermittlung der Zuverlässigkeit von Pneumatikventilen wird die Lebensdauer (B_{10}-Wert) in Zyklen bis zum Ausfall angegeben. Die nominale Lebensdauer B_{10} (in einigen Literaturangaben auch t_{10}) ist die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der 10 % der betrachteten Menge ausgefallen sind. Da das Ausfallkriterium „Verfügbarkeit" bei Ventilen auch nicht sicherheitsrelevante Ausfälle umfasst (z. B. Leckage über dem definiertem Schwellwert), wurde normativ vereinbart, dass der ermittelte Wert für die nominale Lebensdauer (B_{10}) mit zwei multipliziert den B_{10D}-Wert (engl. dangerous, nominale Lebensdauer, nach der

bis 10 % der Bauteile gefahrbringend ausgefallen sind) ergeben kann:

$$B_{10D} = 2 \cdot B_{10} \qquad \text{(D.2)}$$

Der B_{10}-Wert wird in der Regel im Labor ermittelt. Dabei werden mindestens sieben Ventile von unterschiedlichen Produktionszeitpunkten einer Langzeitbelastung ausgesetzt. Die maximale Schaltfrequenz für die Langzeitbelastung wird über den Druckaufbau (Erreichen von 90 % des Prüfdruckes) und den Druckabbau (Erreichen von 10 % des Prüfdruckes) in einem angeschlossenen, nach Anschlussquerschnitten definierten Volumen ermittelt. Für eine Bewertung der Prüfergebnisse sollten mindestens fünf von sieben Ventilen ausgefallen sein. Als Verfahren zur Bestimmung der Weibull-Parameter werden in ISO 19973-1 beispielhaft die Verfahren „Maximum Likelihood“ und „Rank Regression“ genannt.

Näherungsweise gilt, dass bei einer geringen Anzahl von Prüflingen, z. B. sieben Ventilen, der Erstausfall den B_{10}-Wert bestimmt bzw. die bis zum Zeitpunkt des Erstausfalls erreichten Zyklen ungefähr dem B_{10}-Wert entsprechen. Ist der Erstausfall gefahrbringend, entspricht diese Schaltspielzahl ungefähr dem B_{10D}-Wert.

Als gefahrbringende Ausfälle bei Pneumatikventilen sind insbesondere zu nennen:

- Nichtschalten (Hängenbleiben in der End- oder Nulllage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)
- Veränderung der Schaltzeiten
- selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)

Die Betrachtung der Ausfälle bezieht sich immer auf die Baueinheit, z. B. bestehend aus Hauptventil und Vorsteuerventil.

D.2.4.2 Umrechnung von B_{10D} in $MTTF_D$

Die Norm erwartet für das vereinfachte Verfahren zur Abschätzung eines PL die Angabe eines $MTTF_D$-Wertes zur Berücksichtigung zufälliger Bauteilausfälle. Für elektromechanische und pneumatische Bauteile liegen aber typischerweise B_{10D}-Werte vor, die noch in $MTTF_D$-Werte umgerechnet werden müssen. Die Norm bietet dazu eine Näherungsformel an, die an bestimmte Voraussetzungen geknüpft ist:

$$MTTF_D = \frac{T_{10D}}{0{,}1} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} \qquad \text{(D.3)}$$

Diese Näherung basiert auf einer Umformung in zwei Schritten. Zunächst wird der in der Pseudo-Einheit „Zyklen“ angegebene B_{10D}-Wert in einen T_{10D}-Wert umgerechnet. Dabei handelt es sich um die Zeit, bei der 10 % der betrachteten Bauteile gefährlich ausgefallen sind:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \qquad \text{(D.4)}$$

Als Umrechnungsfaktor dient dabei die mittlere Anzahl jährlicher Betätigungen n_{op} (in Zyklen pro Jahr) auf der Grundlage folgender Parameter, die für die zu erwartende Anwendung (ggf. als Worst-case-Ansatz) zu schätzen sind:

- h_{op} ⇢ mittlere Betriebszeit in Stunden (h) je Tag
- d_{op} ⇢ mittlere Betriebszeit in Tagen je Jahr
- t_{Zyklus} ⇢ mittlere Betriebszeit zwischen dem Beginn zweier aufeinander folgender Zyklen des Bauteils (z. B. Schalten eines Ventils) in Sekunden (s) je Zyklus

Aus diesen Parametern kann n_{op} (in Zyklen pro Jahr) folgendermaßen ermittelt werden:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{Zyklus}} \cdot 3\,600\ \frac{s}{h} \qquad \text{(D.5)}$$

Der zweite Schritt der in Gleichung (D.3) verborgenen Näherung besteht in der Annahme einer zeitkonstanten „Ersatz-Ausfallrate“ für das eigentliche, von Verschleiß dominierte Ausfallverhalten. Diese Näherung funktioniert allerdings in ausreichender Güte nur bis zum Erreichen des T_{10D}-Wertes (der in „Zyklen“ dem B_{10D}-Wert entspricht).

Dieser Teil der Näherung wird in Abbildung D.3 illustriert. Die durchgezogene Kurve stellt die ursprüngliche Weibull-Verteilung mit einem angenommenen Formfaktor b = 3 dar. Im Spezialfall b = 1 geht die Weibull-Verteilung in eine Exponentialverteilung über, die durch eine zeitkonstante Ausfallrate gekennzeichnet ist. Die gestrichelte Linie gehört nun zu jener Exponentialverteilung, die der zeitkonstanten „Ersatz-Ausfallrate“ entspricht, die gleich dem Kehrwert der mit Gleichung (D.3) ermittelten $MTTF_D$ ist. Die so ermittelte $MTTF_D$ stellt sicher, dass die gestrichelt dargestellte Exponentialverteilung die ursprüngliche Weibull-Verteilung im Punkt ($t = T_{10D}$; $F_D = 10\,\%$) schneidet. Beide Verteilungen erreichen also nach Ablauf von T_{10D} den Punkt, an dem 10 % der betrachteten Bauteile gefährlich ausgefallen sind. In Abbildung D.3 lässt sich erkennen, dass die eigentliche Ausfallrate vor Erreichen der Verschleißphase sehr gering ist und bis T_{10D} unterhalb der genäherten Exponentialverteilung verläuft – es handelt sich hier also um eine Näherung zur sicheren Seite. Es ist auch zu erkennen, dass die Begrenzung der Einsatzdauer auf T_{10D} sehr wichtig ist: Oberhalb steigt der real zu erwartende Anteil gefährlicher Ausfälle mit der Zeit gegenüber der exponentiellen Ersatzfunktion deutlich an. Die Gültigkeit der Näherung auf der Basis der zeitkonstanten Ersatz-Ausfallrate kann verlängert werden, indem das betroffene Bauteil bei Erreichen des T_{10D}-Wertes vorsorglich erneuert wird.

Im unteren Teil von Abbildung D.3 wird deutlich, dass auch die gewählte „Ersatz-Ausfallrate“ $\lambda_D = 1/MTTF_D$ der exponentiellen Näherung ungefähr dem arithmetischen Mittelwert der real zu erwartenden Ausfallrate bis zum Zeitpunkt T_{10D} entspricht.

Jenseits von T_{10D} ergeben sich jedoch durch das Eintreten in die Verschleißphase starke Abweichungen.

Gleichung (D.3) ergibt sich aus der Bedingung

$$F(T_{10D}) = 1 - \exp(-\lambda_D \cdot T_{10D}) = 10\ \%$$

für die die Näherung bildende Exponentialverteilung, wobei λ_D die erwähnte „Ersatz-Ausfallrate“ darstellt. Umformung führt auf $\lambda_D = -\ln(0{,}9)/T_{10D}$. Da $\ln(0{,}9)$ in guter Näherung 0,1 entspricht und $MTTF_D = 1/\lambda_D$ gilt, folgt schließlich $MTTF_D \approx T_{10D}/0{,}1$.

D.2.5 Verfahren guter ingenieurmäßiger Praxis

Sind keine Herstellerangaben für die Zuverlässigkeit von Bauteilen verfügbar, schlägt die Norm als erste Alternative vor, dort gelistete typische Werte zu verwenden. Als Unterstützung liefert sie für mechanische, hydraulische und pneumatische Komponenten sowie für häufig in der Praxis eingesetzte elektromechanische Sicherheitsbauteile „typische Werte“ mit. Diese Werte sind als $MTTF_D$-Werte oder B_{10D}-Werte in Tabelle D.2 aufgeführt. Der B_{10D}-Wert, den der Bauteilhersteller durch Prüfung ermittelt, gibt die mittlere Anzahl von Zyklen an, bei der 10 % der Bauteile gefahrbringend ausgefallen sind. Mithilfe dieses Wertes ist es möglich, den $MTTF_D$-Wert abzuschätzen. Die Verwendung der Werte aus Tabelle D.2 ist allerdings an verschiedene Voraussetzungen gebunden:

- Der Hersteller des Bauteils bestätigt die Verwendung von grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013 oder der entsprechenden Norm (siehe Tabelle D.2) für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).

- Der Hersteller eines Bauteils, das in einer Steuerung der Kategorie 1, 2, 3 oder 4 verwendet werden soll, bestätigt die Verwendung bewährter Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013 oder der entsprechenden Norm (siehe Tabelle D.2) für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).

- Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den SRP/CS-Konstrukteur und den Anwender fest und informiert diese über ihre Verantwortung, die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 für die Implementierung und den Betrieb des Bauteils zu erfüllen.

- Der SPR/CS-Konstrukteur und der Anwender erfüllen die grundlegenden und/oder bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 für die Implementierung und den Betrieb des Bauteils.

Mit der Umsetzung dieser Anforderungen soll sichergestellt werden, dass die Anwendung grundlegender und/oder bewährter Sicherheitsprinzipien von der Herstellung über die Implementierung bis zum laufenden Betrieb des Bauteils gewährleistet ist. Auch die Schnittstelle zwischen Hersteller, SRP/CS-Konstrukteur und Anwender bzw. Betreiber der Maschine ist klar definiert: Der Hersteller muss die Berücksichtigung der Sicherheitsprinzipien bei der Konstruktion verbindlich bestätigen und alle relevanten Informationen zu Einsatz- und Betriebsbedingungen zur Verfügung stellen. Der SRP/CS-Konstrukteur und der Anwender bzw. Betreiber der Maschine ihrerseits sind für die Einhaltung aller Sicherheitsprinzipien verantwortlich, die Implementierung und Betrieb des Bauteils betreffen. Unter diesen Voraussetzungen kann bei der Berechnung der $MTTF_D$, ggf. über B_{10D}, auf die in Tabelle D.2 zitierten typischen Werte zugegriffen werden. Der oben begründete $MTTF_D$-Wert von 150 Jahren für hydraulische Steuerungskomponenten wird hier auch auf mechanische Komponenten ausgedehnt. Dieser Hilfswert kann verwendet werden, wenn zwar kein Fehlerausschluss begründet werden kann, aber der Einsatz grundlegender bzw. bewährter Sicherheitsprinzipien gewährleistet ist. Außerdem werden B_{10D}-Werte für elektromechanische Bauteile genannt, die nach dem ebenfalls oben vorgestellten Verfahren mit der durchschnittlichen Anzahl jährlicher Betätigungen n_{op} in einen $MTTF_D$-Wert umgerechnet werden können.

Alle Werte in der Tabelle beziehen sich nur auf gefahrbringende Ausfälle, was durch den Index „D“ ausgedrückt ist. Hier wurde in der Regel unterstellt, dass nur die Hälfte aller Ausfälle gefahrbringend ist. In der dritten Ausgabe der Norm wurde für „Schütze mit nominaler Last“ allerdings von dieser Regel abgewichen und der in der Produktnorm DIN EN 60947-4-1 [5], Tabelle K.2, angegebene Anteil gefahrbringender Ausfälle (75 % Öffnungsfehler oder Kurzschluss) für die Umrechnung genutzt. Dies führt auf einen gegenüber der zweiten Ausgabe der Norm reduzierten B_{10D}-Wert von 1 300 000 Zyklen (vorher 2 000 000 Zyklen). Die hier angegebenen Werte können also durchaus optimistischer aussehen als Datenblattangaben von Herstellern, die sich im Sinne der Verfügbarkeit auf alle Fehlerarten beziehen, die den Funktionsablauf beeinträchtigen können. Bei einigen elektromechanischen Bauteilen, beispielsweise Relais, Hilfsschützen und Schützen, geht die elektrische Belastung der Kontakte stark in den B_{10D}-Wert ein, was durch vielfältige Beobachtungen aus der Praxis bestätigt wird. Bei geringer elektrischer Last (typischerweise ohmscher Last) – DIN EN ISO 13849-1 spricht hier von bis zu 20 % des Bemessungswertes – ergeben sich deutlich bessere Werte. Hier wurde dann die mechanische statt der elektrischen Lebensdauer unterstellt (siehe Abschnitt D.2.4). Je nach Art (ohmsch oder induktiv) und Größe der Last können auch B_{10D}-Zwischenwerte der hier genannten Extreme abgeleitet werden. Bei den in der Tabelle aufgeführten Positionsschaltern, Zuhaltungen, Not-Halt-Geräten und Tastern, beispielsweise Zustimmungsschaltern, wird für den elektrischen Teil meist das Sicherheitsprinzip der Zwangsöffnung vorausgesetzt. Zwischen der zweiten und dritten Ausgabe der Norm haben sich für diese Bauteile im Rahmen des Verfahrens der guten ingenieurmäßigen Praxis einige Änderungen ergeben, die sich aus der Erfahrung mit der praktischen Anwendung ergaben. Daher wird dieses Thema in den folgenden Abschnitten D.2.5.1 bis D.2.5.6 separat ausführlich erläutert.

Naturgemäß handelt es sich bei diesen Ansätzen um starke Vereinfachungen der komplexen realen Zusammenhänge. So kann zum Beispiel insbesondere ein sehr geringer Laststrom bei seltener Betätigung zu einem Kaltverschweißen elektrischer Kontakte führen. Diese Effekte sollen aber durch die geforderte Anwendung grundlegender bzw. bewährter Sicherheitsprinzipien vermieden werden, zu denen auch die Eignung und Angepasst-

heit der mechanischen wie der elektrischen Bauteileigenschaften an die zu erwartende Belastung gehören.

D.2.5.1 Modellierung von elektromechanischen Bauteilen (Positionsschalter, Zuhaltungen, Not-Halt-Geräte, Zustimmungsschalter und Drucktaster)

In der bisherigen praktischen Anwendung der Norm hat sich gezeigt, dass große Unsicherheit bei der Modellierung elektromechanischer Bauteile besteht. Dies zeigt sich auch darin, dass beide Teile der Norm hier teilweise eine unterschiedliche Sprache sprechen: Während im ersten Teil im Rahmen des Verfahrens guter ingenieurmäßiger Praxis (siehe Tabelle D.2) ein Ansatz über B_{10D}-Werte gewählt wird, kümmert sich der zweite Teil um mögliche Fehlerausschlüsse. Hier kommt erschwerend hinzu, dass eine eindeutige Trennung zwischen mechanischem und elektrischem Teil für viele dieser Bauteile kaum möglich ist. Daher werden im Folgenden zunächst allgemein die Anforderungen und Hinweise aus beiden Normteilen vorgestellt, um dann für die verschiedenen elektromechanischen Bauteile eine pragmatische Modellierung vorzuschlagen, die sich hauptsächlich am Teil 1 der Norm orientiert. Teil 2 ist alternativ ebenfalls anwendbar, die praktische Umsetzung scheitert aber oft daran, dass ein kompletter Fehlerausschluss für den mechanischen und elektrischen Teil eine Bestätigung des Herstellers, z. B. im Datenblatt, erfordert oder die genaue Kenntnis der Einsatzbedingungen voraussetzt. Beide Voraussetzungen sind in der Praxis oft nicht gegeben.

Was sagt die Norm? – Elektromechanische Bauteile nach Teil 1 der Norm

DIN EN ISO 13849-1:2016 schlägt mit dem oben eingeführten Verfahren guter ingenieurmäßiger Praxis vor, dass unter den nachfolgenden Voraussetzungen die in Tabelle D.2 genannten typischen B_{10D}-Werte [N] für Positionsschalter, Zuhaltungen, Not-Halt-Geräte, Zustimmungsschalter und Drucktaster angenommen werden dürfen:

- Verwendung von grundlegenden und bewährten Sicherheitsprinzipien bei Konstruktion, Anwendung und Betrieb des Bauteils (siehe Tabellen D.1 und D.2 nach DIN EN ISO 13849-2) und

- Möglichkeit des Fehlerausschlusses für Zwangsöffnung (Kontakte nach DIN EN 60947-5-1, Anhang K, in den Prinzipschaltbildern gekennzeichnet durch ⊖)

Herstellerangaben [H] sind gegenüber den typischen Werten nach Norm natürlich immer zu bevorzugen. Zur Modellierung wird in der Norm darauf hingewiesen, dass die Bauteile *„als Teilsystem der Kategorie 1 oder Kategorie 3/4 abgeschätzt werden [können], je nach Anzahl der elektrischen Ausgangskontakte und der Fehlererkennung im nachgeordneten SRP/CS. Jedes Kontaktelement (einschließlich der mechanischen Betätigung) kann als ein Kanal mit entsprechendem B_{10D}-Wert betrachtet werden."*

Obwohl dieser Hinweis sich direkt nur auf Not-Halt-Geräte und Zustimmungsschalter bezieht, kann das dort genannte Prinzip auch auf andere elektromechanische Bauteile übertragen werden.

Dass die ein- oder zweikanalige Modellierung von der Anzahl der elektrischen Ausgangskontakte bestimmt wird, obwohl für zwangsöffnende Kontaktelemente ja ein Fehlerausschluss für Zwangsöffnung angenommen werden kann, erscheint zunächst unstimmig. Durch den Hinweis, dass der B_{10D}-Wert jedes Kanals für das Kontaktelement einschließlich der mechanischen Betätigung gelten soll, wird jedoch klar, dass es sich hier um einen Kunstgriff handelt, der das komplexe Zusammenspiel von mechanischen und elektrischen Elementen in den genannten elektromechanischen Bauteilen auf möglichst einfache Weise darstellen soll. Hier standen nicht die Details der elektromechanischen Konstruktion im Vordergrund, sondern ein möglichst simples Kochrezept:

- Ein elektromechanisches Bauteil mit **einem** zwangsöffnenden Kontaktelement, das die o. g. Voraussetzungen erfüllt, kann als Teil eines Kategorie-1-Subsystems modelliert werden. Im Funktionskanal enthält das Subsystem einen Block mit dem entsprechenden B_{10D}-Wert.

- Ein elektromechanisches Bauteil mit (mindestens) **zwei** zwangsöffnenden Kontaktelementen, das die o. g. Voraussetzungen erfüllt, kann je nach der Fehlererkennung im nachgeordneten SRP/CS als Bestandteil eines Kategorie-3- oder -4-Subsystems modelliert werden. In den beiden Funktionskanälen enthält das Subsystem je einen Block mit dem entsprechenden B_{10D}-Wert.

DIN EN ISO 13849-1 ergänzt über den allgemeinen Fall hinausgehend, dass es *„in einigen Fällen […] möglich sein [kann], dass der Maschinenhersteller einen Fehlerausschluss nach DIN EN ISO 13849-2, Tabelle D.8, unter Berücksichtigung der jeweiligen Anwendungs- und Umgebungsbedingungen des Gerätes anwenden kann."* Die Formulierung des Fehlerausschlusses für ein elektromechanisches Bauteil ist dabei einerseits Sache des Bauteilherstellers, nur er kennt die Details der mechanischen Konstruktion. Andererseits muss man bei der Anwendung prüfen, ob ein Fehlerausschluss unter Berücksichtigung von Umgebungs-, Betriebs- und Anwendungsaspekten zulässig ist. Dies sind Sonderfälle, in denen der Maschinenhersteller in Rücksprache mit dem Bauteilhersteller individuell für spezifische Applikationen bestimmte Fehler ausschließt.

Was sagt die Norm? – Elektromechanische Bauteile nach Teil 2 der Norm

Tabelle D.8 aus DIN EN ISO 13849-2 gilt für Schalter, z. B. elektromechanische Positionsschalter und Handschalter, und ist daher für alle o. g. elektromechanischen Bauteile anwendbar. Für einen Ausschluss des Fehlers „Nichtöffnen von Kontakten" werden dort folgende Bedingungen genannt:

- Die Schalter müssen DIN EN 60947-5-1:2018, Anhang K, erfüllen, also zwangsöffnende Kontaktelemente besitzen.

- Der Fehlerausschluss gilt nur bis maximal PL d. Für PL e sind redundante Bauteile erforderlich, also ein zweiter (Positions-) Schalter (Ausnahme: Not-Halt-Geräte).

Damit ergibt sich für Positionsschalter (mit und ohne separatem Betätiger), Zuhaltungen, Zustimmungsschalter und Drucktaster

unabhängig von der Zahl der elektrischen Kontaktelemente folgende Bewertung:

- bis PL d: Fehlerausschluss ist zulässig, der auch für die Mechanik erfolgen kann, was auch eine Bestätigung des Herstellers voraussetzt. Modellierung als gekapseltes Subsystem der Kategorie 3 (einfehlersicher) und direkte Angabe von PL d und PFH_D Null. In SISTEMA (unter Subsystem, Registerkarte „PL“) muss dazu die Kopplung zwischen PL und PFH_D aufgehoben werden.

- PL e: kein Fehlerausschluss (für mechanische und elektrische Aspekte) zulässig

Für Not-Halt-Geräte nach DIN EN 60947-5-5 ist ein Fehlerausschluss hinsichtlich des „Nichtöffnens von Kontakten“ für mechanische Aspekte bis PL e zulässig, wenn eine Höchstzahl von Betätigungen berücksichtigt wird. In der Vergangenheit wurde hier die Lebensdauerschaltspielzahl von 6 050 Betätigungen nach DIN EN 60947-5-5 herangezogen.

Wie im vorherigen Abschnitt erwähnt, ist die prinzipielle Zulässigkeit von Fehlerausschlüssen nur von begrenzter praktischer Relevanz.

Im Folgenden werden die in der Norm genannten Anforderungen auf häufig verwendete elektromechanische Bauteile angewendet.

D.2.5.2 Positionsschalter

Nach DIN EN 60947-5-1 hergestellte elektromechanische Positionsschalter mit einem oder zwei zwangsöffnenden elektrischen Kontaktelementen nach DIN EN 60947-5-1, Anhang K, können wie in Tabelle D.3 beschrieben betrachtet werden. Der (ein- oder zweikanalig) ansetzbare B_{10D}-Wert nach dem Verfahren guter ingenieurmäßiger Praxis beträgt für Positionsschalter mit separatem Betätiger 2 000 000 Zyklen und für alle anderen Positionsschalter 20 000 000 Zyklen.

Neben dem Schalter selbst ist auch seine formschlüssige Betätigung (z. B. die Anfahrmechanik, die Betätigerbefestigung) relevant. Für die dazu erforderliche Fehlerbetrachtung inkl. möglicher Fehlerausschlüsse sind zusätzlich die relevanten Anforderungen aus DIN EN ISO 13849-2, Anhang A, zu erfüllen. Nach DIN EN ISO 13849-2, Tabelle D.8, ist mit einem einzelnen Positionsschalter (auch bei zwei Kontaktelementen) maximal PL d erreichbar. In den relevanten C-Normen für Maschinen können gegebenenfalls abweichende Vorgaben aufgeführt sein, z. B. die Verwendung von zwei Positionsschaltern für Kategorie 3.

Hinweise über die Auswahl und Anbringung von Positionsschaltern sind in der DGUV Information 203-079 [6] aufgeführt.

D.2.5.3 Zuhaltungen

Mit Zuhaltungen sind an dieser Stelle Einrichtungen zum mechanischen Blockieren geschlossener Schutzeinrichtungen mit integriertem oder integrierten Positionsschalter(n) als Baueinheit gemeint, mit denen die Sicherheitsfunktionen „Zuhaltung“ und „Verriegelung“ (Stellungsüberwachung der Schutzeinrichtung) realisiert werden können. Von der Sicherheitsfunktion „Zuhaltung“ wird im Folgenden nur die Stellungsüberwachung des Sperrmittels betrachtet. Zur vollständigen Betrachtung der Sicherheitsfunktion Zuhaltung siehe Abschnitt 8.2.19 (Beispiel 19). Neben den Mitteln zur Überwachung der Stellung einer Schutzeinrichtung besitzt eine Verriegelungseinrichtung mit Zuhaltung zusätzlich eine Vorrichtung zum Blockieren der beweglichen Schutzeinrichtung in der geschlossenen Position. Solange diese Vorrichtung aktiv ist, kann die Schutzeinrichtung nicht geöffnet werden.

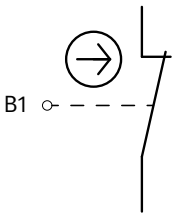
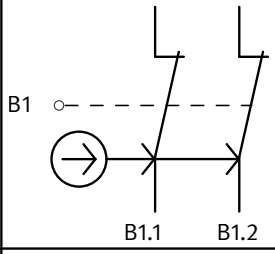
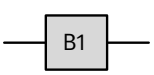
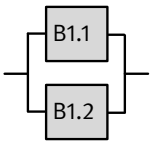
Prinzip-schaltbild		
Sicherheits-bezogenes Block-diagramm		
Modellierung	Block B1 B_{10D} = 2 000 000 bzw. 20 000 000 Zyklen [N] oder Herstellerangabe [H]	Blöcke B1.1 und B1.2 jeweils B_{10D} = 2 000 000 bzw. 20 000 000 Zyklen [N] oder Herstellerangabe [H]
Kategorie und PL	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

Tabelle D.3:
Modellierung von Positionsschaltern im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Für Zuhaltungen gibt es keine Produktnorm. Grundlegende sicherheitstechnische Anforderungen sind jedoch in DIN EN ISO 14119 aufgeführt. Zusätzlich gibt es für Zuhaltungen als „Baueinheit“ den Prüfgrundsatz GS-ET-19 [7]. Danach enthalten elektromechanische Zuhaltungen einen Positionsschalter für die Stellungsüberwachung der Schutzeinrichtung („Schutztür“) **und** einen Positionsschalter für die Stellungsüberwachung des Sperrmittels (siehe Abbildung D.4).

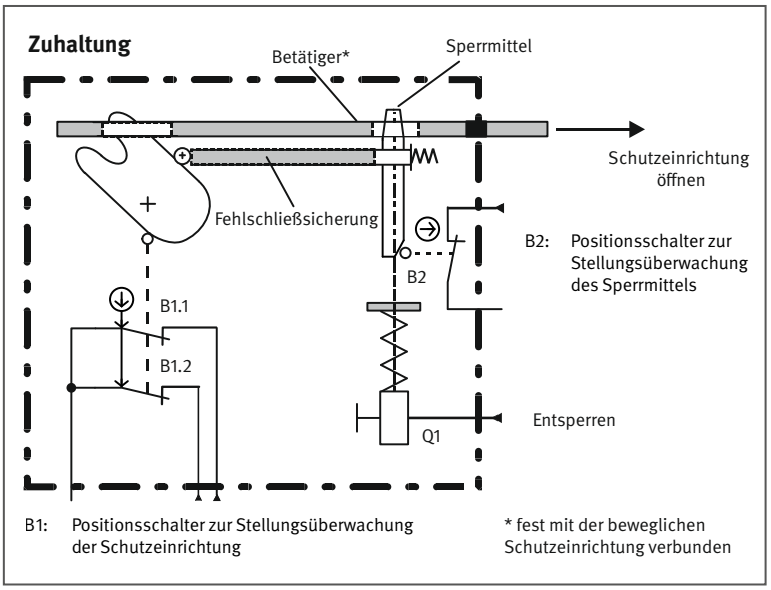
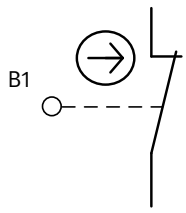
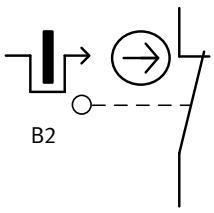
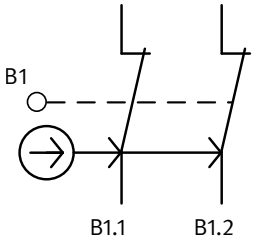
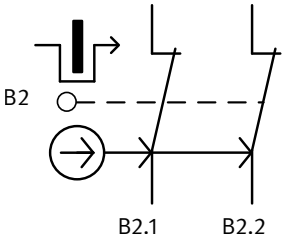
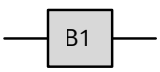
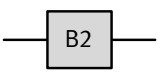
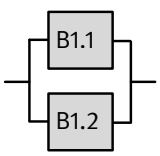
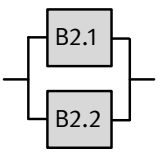


Abbildung D.4:
Prinzipielle Darstellung einer Zuhaltung mit Fehlschließsicherung und zusätzlicher Stellungsüberwachung der Schutzeinrichtung („Verriegelung“)

Ist die Zuhaltung konstruktiv mit einer „Fehlschließsicherung“ ausgeführt, kann auf den Positionsschalter für die Stellungsüberwachung der Schutzeinrichtung verzichtet werden: Wenn sich das Sperrmittel in zuhaltender Stellung befindet, kann von einer geschlossenen Schutzeinrichtung ausgegangen werden. Befindet sich das Sperrmittel in nicht zuhaltender Stellung, kann keine Aussage über die Stellung der Schutzeinrichtung gemacht werden.

Zuhaltungen können, unter Berücksichtigung der Anforderungen aus DIN EN ISO 14119 und dem Prüfgrundsatz GS-ET-19, wie in den Tabellen D.4 und D.5 beschrieben betrachtet werden.

Tabelle D.4:
Modellierung von Zuhaltungen **ohne** Fehlschließsicherung im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Zuhaltung **ohne** Fehlschließsicherung				
Prinzip-schaltbild	**Stellungsüberwachung Schutzeinrichtung** 	**Stellungsüberwachung Sperrmittel** 	**Stellungsüberwachung Schutzeinrichtung** 	**Stellungsüberwachung Sperrmittel** 
Sicherheits-bezogenes Block-diagramm				
Modellierung	Blöcke B1 und B2 jeweils B_{10D} = 2 000 000 Zyklen [N] oder Herstellerangabe [H]		Blöcke B1.1, B1.2, B2.1 und B2.2 jeweils B_{10D} = 2 000 000 Zyklen [N] oder Herstellerangabe [H]	
Kategorie und PL	Kategorie 1 maximal PL c		Kategorie 3 maximal PL d	

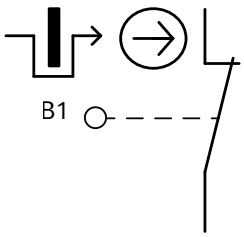
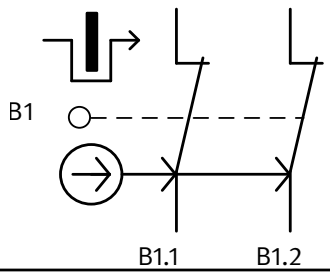
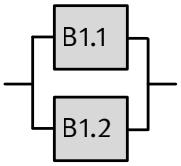
Zuhaltung **mit** Fehlschließsicherung		
Prinzip-schaltbild	Stellungsüberwachung Sperrmittel 	Stellungsüberwachung Sperrmittel 
Sicherheits-bezogenes Block-diagramm		
Modellierung	Block B1 B_{10D} = 2 000 000 Zyklen [N] oder Herstellerangabe [H]	Blöcke B1.1 und 1.2 jeweils B_{10D} = 2 000 000 Zyklen [N] oder Herstellerangabe [H]
Kategorie und PL	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

Tabelle D.5:
Modellierung von Zuhaltungen **mit** Fehlschließsicherung im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Zusammengefasst gilt für Zuhaltungen:

- Der (ein- oder zweikanalig) ansetzbare B_{10D}-Wert nach dem Verfahren guter ingenieurmäßiger Praxis beträgt für Zuhaltungen 2 000 000 Zyklen.
- Das Vorhandensein der „Fehlschließsicherung“ sowie den zugehörigen Fehlerausschluss für die Mechanik muss der Hersteller bestätigen.
- Mit einer einzelnen Zuhaltung als „Baueinheit“ ist für die „Verriegelungsfunktion“ (auch bei zwei Kontaktelementen je Positionsschalter) nach DIN EN ISO 13849-2, Tabelle D.8, maximal PL d erreichbar. Möchte man einen PL e erreichen, ist dies nur mit einem externen zusätzlichen Positionsschalter zur Stellungsüberwachung der Schutzeinrichtung möglich.
- Bei Zuhaltungen als „Baueinheit“ ist die „Zuhaltefunktion“ auf PL d beschränkt, da der Positionsschalter für die Sperrmittelüberwachung und die zugehörige Anfahrmechanik nur einmal vorhanden ist.
- In den relevanten C-Normen für Maschinen gegebene Einschränkungen sind zu beachten.

Hinweise über die Auswahl und Anbringung von Zuhaltungen sind in der DGUV Information 203-079 [6] aufgeführt.

D.2.5.4 Not-Halt-Gerät

Nach der Produktnorm DIN EN 60947-5-5 gebaute Not-Halt-Geräte können wie in Tabelle D.6 (siehe Seite 262) beschrieben betrachtet werden.

D.2.5.5 Zustimmungsschalter

Nach der Produktnorm DIN EN 60947-5-8 oder dem Prüfgrundsatz GS-ET-22 [8] gebaute Drei-Stellungs-Zustimmungsschalter können wie in Tabelle D.7 (siehe Seite 262) beschrieben betrachtet werden. In der Praxis existieren Zustimmungsschalter mit unterschiedlichen Kontaktsätzen (unterschiedliche Anzahl Öffner/Schließer).

Die sicherheitsrelevante Aufhebung der Zustimmungsfunktion wird bei Drei-Stellungs-Zustimmungsschaltern durch das Loslassen oder Durchdrücken erreicht. Beide Funktionen können in gleicher Weise bewertet werden, zusätzlich muss beim Loslassen aber besonders auf die Überdimensionierung der elektrischen (hier: Schließer-)Kontakte bezogen auf die Last geachtet werden. Nachfolgend werden die Funktionen „Loslassen“ und „Durchdrücken“ in einer Sicherheitsfunktion zusammengefasst, da die Betätigungsrichtung nicht vorhersehbar ist.

Die Produktnorm DIN EN 60947-5-8 stellt keine konstruktiven Anforderungen an die Öffnungsfunktion. Dies gilt sowohl für die Schließer- als auch für die Öffnerkontakte (Loslassen oder Durchdrücken). Im Besonderen werden keine zwangsöffnenden elektrischen Kontaktelemente nach DIN EN 60947-5-1, Anhang K, gefordert. In diesem Fall handelt es sich daher nicht um bewährte Bauteile und dadurch ist Kategorie 1 nicht möglich.

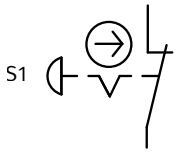
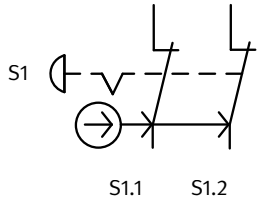
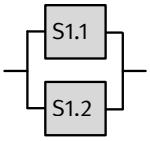
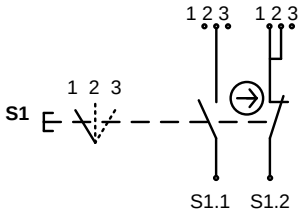
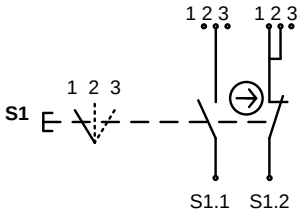
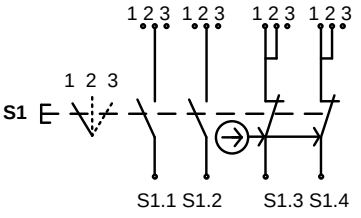
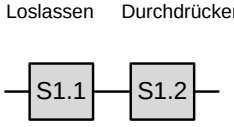
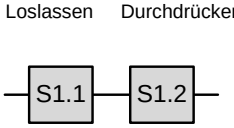
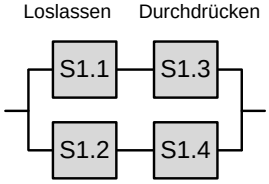
Prinzip-schaltbild		
Sicherheits-bezogenes Block-diagramm		
Modellierung	Block S1 B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H]	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H]
Kategorie und PL	Kategorie 1 maximal PL c	Kategorie 3 oder 4 maximal PL e

Tabelle D.6:
Modellierung von Not-Halt-Geräten im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie- und PL-Zuordnung

Tabelle D.7:
Modellierung von Drei-Stellungs-Zustimmungsschaltern im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Prinzip-schaltbild			
Bedingung	Öffnerkontakt entsprechend DIN EN 60947-5-1 Anh. K	Zustimmungsschalter nach GS-ET-22	Zustimmungsschalter nach GS-ET-22
Sicherheits-bezogenes Block-diagramm			
Modellierung	Block S1.1 B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H] Block S1.2 Fehlerausschluss, λ_D=0	Block S1.1 B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H] Block S1.2 Fehlerausschluss, λ_D=0	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H] Blöcke S1.3 und S1.4 jeweils Fehlerausschluss, λ_D=0
Kategorie und PL	Kategorie B maximal PL b a)	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

a) Schließerkontakt S1.1 limitiert den erreichbaren PL auf b.
b) Im nachfolgenden SRP/CS ist eine ausreichende Fehlererkennung für die elektrischen Kontakte vorhanden.

Der Prüfgrundsatz GS-ET-22 stellt besondere konstruktive Anforderungen, z. B.:

- für die Funktion „Loslassen“ die Verwendung bewährter Federn oder einen zweikanaligen Aufbau mit Kontaktüberwachung
- für die Funktion „Durchdrücken“ zwangsöffnende elektrische Kontaktelemente nach DIN EN 60947-5-1, Anhang K, oder zweikanalige Signalgabe mit entsprechender steuerungstechnischer Überwachung

Durch die konstruktive Ausführung nach GS-ET-22 ist eine vergleichbare Sicherheit zu einem bewährten Bauteil gegeben.

Zwei-Stellungs-Zustimmungsschalter realisieren nur die Sicherheitsfunktion „Loslassen“ und sind in der Produktnorm DIN EN 60947-5-8 nicht enthalten. Wenn sie dem Prüfgrundsatz GS-ET-22 entsprechen, gilt die gleiche Bewertung wie in Tabelle D.7 für Schließerkontakte der Drei-Stellungs-Zustimmungsschalter angegeben: einkanalig in Kategorie 1 mit maximal PL c oder zweikanalig in Kategorie 3 mit maximal PL d.

D.2.5.6 Drucktaster

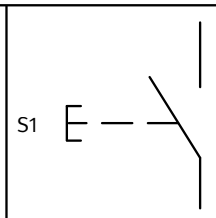
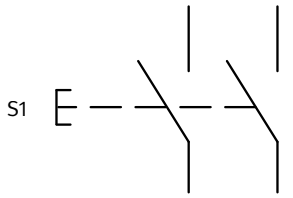
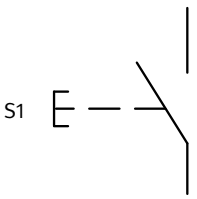
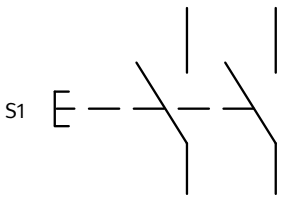
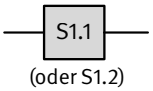
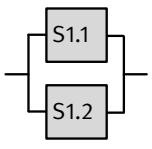
Drucktaster nach DIN EN ISO 13849-2, Tabelle D.8, kommen beispielsweise zum Auslösen einer zeitlich und/oder örtlich begrenzten Bewegung im Rahmen des Tippbetriebes zur Anwendung. Sie sind in diesem Anwendungsfall immer als „Schließer“ ausgeführt, wobei für die Sicherheitsfunktion das zuverlässige **Öffnen** des Schließers nach vorhergehender Betätigung entscheidend ist (vergleichbar mit dem grundlegenden Sicherheitsprinzip der Energietrennung – „Ruhestromprinzip“ – nach DIN EN ISO 13849-2, Tabelle D.1). Hierbei gilt dieselbe Betrachtung wie für die Funktion „Loslassen“ des Zwei-Stellungs-Zustimmungsschalters. Auch hier muss besonders auf Überdimensionierung der elektrischen Kontakte bezogen auf die Last geachtet werden.

C-Normen für Maschinen fordern oft für den Tippbetrieb ein Not-Halt-Gerät in der Nähe des Drucktasters. Kommt es nach Loslassen des Druck- bzw. Tipptasters zu einem Nichtöffnen des Schließers, lässt sich die gefahrbringende Bewegung durch Betätigen des Not-Halt-Gerätes stoppen. Weiterhin ist der Tippbetrieb oft auch nur weg- oder zeitbegrenzt und/oder bei aktivierter Sicherheitsfunktion SLS (Sicher begrenzte Geschwindigkeit) erlaubt. Diese Maßnahmen lassen sich bei der Bestimmung des PL (z. B. mit SISTEMA) nicht quantifizieren, da sie dem willensabhängigen Handeln unterliegen. Es ist daher ratsam, die spezifischen ergänzenden Anforderungen in einer C-Norm für den Tippbetrieb bei der Festlegung des PL_r zu berücksichtigen.

Weiterhin muss die Verhinderung eines unerwarteten Anlaufs beachtet werden, was dazu führt, dass schon für die beiden PL-b-Varianten in Tabelle D.8 Befehlsgeräte nach DIN EN 60947-5-1 verwendet werden müssen, um beispielsweise nach Tabelle D.8 in DIN EN ISO 13849-2 den Kurzschluss von benachbarten Kontakten, die voneinander isoliert sind, ausschließen zu können.

Für höhere Risiken (PL c oder d) sind Befehlsgeräte nur nach DIN EN 60947-5-1 nicht ausreichend, da diese wegen des möglichen Öffnungsversagens nur Kategorie B entsprechen. Hier können alternativ „sichere“ Drucktaster, beispielsweise zweistufige Zustimmungstaster nach GS-ET-22, verwendet werden. Diese eignen sich bei Ausführungen mit einem Schließer bis maximal PL c oder als zweikanalige Ausführung bis maximal PL d.

Tabelle D.8:
Modellierung von Drucktastern im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Prinzip-schaltbild				
Bedingung	Drucktaster nach DIN EN 60947-5-1	Drucktaster nach DIN EN 60947-5-1	zweistufiger Zustimmungstaster nach GS-ET-22	zweistufiger Zustimmungstaster nach GS-ET-22
Sicherheits-bezogenes Block-diagramm		 (oder S1.2)		
Modellierung	Block S1 B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H]	Block S1.1 oder S1.2 jeweils B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H]	Block S1 B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H]	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen [N] oder Herstellerangabe [H]
Kategorie und PL	Kategorie B maximal PL b	Kategorie B maximal PL b	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

D.2.6 $MTTF_D$ elektronischer Steuerungskomponenten

Wie bereits erwähnt, ist die Angabe der Ausfallraten λ bzw. λ_D, z. B. als FIT-Werte (Failures In Time, d. h. Ausfälle in 10^9 Bauteilstunden), für elektronische Bauteile schon seit Längerem üblich. Daher ist die Chance recht hoch, über den Hersteller an Zuverlässigkeitsinformationen zu kommen. Unter Umständen müssen diese Angaben in $MTTF_D$-Werte umgerechnet werden, z. B. mithilfe der vereinfachenden Annahme, dass nur 50 % aller Ausfälle gefahrbringend sind. Sind keine Herstellerangaben erhältlich, so kann eine Reihe von bekannten Datensammlungen herangezogen werden, von denen Folgende in DIN EN ISO 13849-1 beispielhaft zitiert werden:

- Siemens Standard SN 29500, Ausfallraten Bauelemente, Erwartungswerte, Hrsg.: Siemens AG, Corporate Technology, Technology & Innovation Management, München 2004-2014 (wird unregelmäßig aktualisiert, Bestellanfragen an:)
  ▸ michaela.pabst@siemens.com oder
  ▸ thomas.haizmann@siemens.com

- IEC/TR 62380, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment, Hrsg.: International Electrotechnical Commission (IEC), Genf 2004

- Handbook of 217Plus Reliability Prediction Models, Quanterion Solutions Incorporated, Utica, New York, 2015
  ▸ www.quanterion.com
  (Fortführung des MIL-HDBK-217F)

- Telcordia SR-332, Reliability Prediction Procedure for Electronic Equipment, Issue 4, Mar 2016
  ▸ telecom-info.telcordia.com

- EPRD-2014, Electronic Parts Reliability Data (RAC-STD-6100), Quanterion Solutions Incorporated, Utica, New York, 2015
  ▸ www.quanterion.com

- NPRD-2016, Nonelectronic Parts Reliability Data (RAC-STD-6200), Quanterion Solutions Incorporated, Utica, New York, 2015
  ▸ www.quanterion.com

- British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)

- Chinese Military Standard, GJB/z 299B & 299C

Neben diesen Datensammlungen gibt es auf dem Markt eine Reihe von Hilfsprogrammen, die diese oder andere Datenbanken per Software zugänglich macht. In den meisten Datenbanken sind elektronische Komponenten nach Bauteilart und weiteren Kriterien (z. B. Bauform, Material, Gehäuse) katalogisiert. Meist werden zunächst Basis-Ausfallraten für Referenzbedingungen genannt (z. B. für 40 °C Bauteil-Umgebungstemperatur und nominale Last), die für davon abweichende Beanspruchungen durch Anpassungsfaktoren auf die realen Einsatzbedingungen korrigiert werden können. In der Norm sind in den Tabellen C.2 bis C.7 sogar für einige typische elektronische Komponenten Werte aufgelistet, die der Datensammlung SN 29500 entnommen sind. In der dritten Ausgabe der Norm wurden allerdings die vorher vorhandenen Spalten mit eingerechnetem Sicherheitsfaktor von 10 („ungünstigster Fall“) gelöscht. Bei korrekter Verwendung der Datenquellen ist ein zusätzlicher Sicherheitsfaktor in der Regel nicht erforderlich. Die Anpassung an Beanspruchungen außerhalb der Referenzbedingungen wird in der Norm nicht explizit gefordert und sollte im Sinne der Einfachheit mit Augenmaß angewendet werden.

D.3 Integration bereits zertifizierter Komponenten und Geräte

In zunehmendem Maß versehen Hersteller ihre Komponenten bereits mit der Angabe einer $MTTF_D$ im Datenblatt. Bei Komponenten, die als Subsysteme in einem SRP/CS eingesetzt werden sollen, nennt der Hersteller einen PL nach DIN EN ISO 13849-1 oder einen SIL nach DIN EN 61508, DIN EN 62061 oder DIN EN 61800-5-2, verbunden mit der Angabe einer „durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde“ PFH_D (bzw. PFH-Wert nach DIN EN 61508). Falls solche Komponenten nur in einem Kanal des SRP/CS verwendet werden, kann die angegebene Ausfallwahrscheinlichkeit pro Stunde (PFH_D) als Ersatzwert für die Ausfallrate in die gefährliche Richtung betrachtet werden (siehe Gl. [D.6], wobei komponenteninterne Merkmale wie Redundanz und Eigendiagnose bereits berücksichtigt sind. Ausführlichere Hinweise dazu gibt das SISTEMA-Kochbuch 4 [9] in Kapitel 2.

$$MTTF_D = \frac{1}{\lambda_D} \approx \frac{1}{PFH_D} \quad \begin{matrix}(\text{„Black-Box“-Komponenten mit } PFH_D \\ \text{innerhalb eines Kanals})\end{matrix} \qquad (D.6)$$

D.4 „Parts Count“-Verfahren

Sind die $MTTF_D$-Werte aller sicherheitsrelevanten Komponenten bekannt, so muss hieraus zunächst die $MTTF_D$ jedes Blocks berechnet werden. Dieser Schritt lässt sich zwar per FMEA (Ausfalleffektanalyse) sehr detailliert durchführen (siehe Anhang B), allerdings müssen dazu im Idealfall die unterschiedlichen Ausfallarten jeder sicherheitsrelevanten Komponente und ihre Wirkung für den Block analysiert werden. Dieser Ansatz lohnt sich – gemessen am Aufwand – daher meist nur für Komponenten mit einer hohen Ausfallrate, d. h. einem kleinen $MTTF_D$-Wert. Als schnelle Alternative, die im Mittel auch nicht zu viel schlechteren Werten führt, bietet DIN EN ISO 13849-1 das sogenannte „Parts Count“-Verfahren an. Im Wesentlichen handelt es sich dabei um eine Summation mit zwei Hauptannahmen:

- Für alle Ausfallarten einer Komponente und deren Auswirkungen auf den Block wird pauschal eine Aufteilung je zur Hälfte in ungefährliche und gefahrbringende Ausfälle angesetzt. Dies bedeutet, dass die Hälfte der Ausfallrate λ einer Komponente zur gefahrbringenden Ausfallrate λ_D des zugehörigen Blocks beiträgt. Wurde für die Komponente bereits der gefahrbringende Anteil der Ausfallrate λ_D bestimmt, so wird der gleiche Wert λ_D auch dem Block angerechnet.

- Die gefahrbringende Ausfallrate λ_D des Blocks wird dann durch Summation der λ_D-Beiträge aller N im jeweiligen Block

vorhandenen sicherheitsrelevanten Komponenten gebildet (wobei sich die Beiträge identischer Komponenten einfach zusammenfassen lassen):

$$\lambda_D = \frac{1}{2}\sum_{i=1}^{N}\lambda_i \text{ bzw. } \lambda_D = \sum_{i=1}^{N}\lambda_{Di} \qquad (D.7)$$

Da die Norm wie oben erläutert von konstanten Ausfallraten ausgeht, lassen sich Ausfallraten λ_D einfach durch Kehrwertbildung in $MTTF_D$-Werte umrechnen. Wird dieser Zusammenhang zugrunde gelegt, so ergibt sich der $MTTF_D$-Wert eines Blocks leicht aus den $MTTF_D$-Werten der zugehörigen Komponenten. Ein Beispiel für die Anwendung des „Parts Count"-Verfahrens findet sich in Kapitel 6.

D.5 Reihenschaltung von Blöcken in einem Kanal und $MTTF_D$-Begrenzung

Liegen $MTTF_D$-Werte bzw. Ausfallraten λ_D für jeden Block vor, lässt sich durch Summation der Ausfallraten aller an einem Kanal beteiligten Blöcke ebenfalls gemäß Gl. (D.7) die $MTTF_D$ für jeden Kanal berechnen. Dabei wird unterstellt, dass der gefährliche Ausfall eines beliebigen Blocks in der Kette der Blöcke, die einen Kanal darstellt, auch als gefährlicher Ausfall des Kanals zu werten ist. Da unter Umständen aber durch nachgeordnete Blöcke ein gefährlicher Ausfall von davor angeordneten Blöcken bemerkt werden kann, bildet diese Annahme eine Abschätzung zur sicheren Seite. In dieser Phase der $MTTF_D$-Bestimmung greift die Kappungsregel der Norm: Mit Ausnahme von Kategorie 4 wird jeder $MTTF_D$-Wert eines Kanals, der rechnerisch > 100 Jahre ist, regelgemäß auf den Höchstwert von 100 Jahren reduziert. Bei Kategorie 4 betragt die Kappungsgrenze 2500 Jahre. Durch diese Regel wird die Überbewertung der Bauteilzuverlässigkeiten gegenüber den anderen für den PL relevanten Größen wie Architektur, Tests und Ausfälle infolge gemeinsamer Ursache vermieden.

D.6 Symmetrisierung bei mehreren Kanälen

Sobald zwei Kanäle in einer Steuerung vorhanden sind (dies ist in der Regel bei Kategorie 3 und 4 der Fall), die unterschiedliche $MTTF_D$-Werte aufweisen, stellt sich die Frage, welcher der $MTTF_D$-Werte für jeden Kanal bei der Bestimmung des PL mithilfe des Säulendiagramms verwendet werden soll. Auch für diese Frage hält DIN EN ISO 13849-1 eine einfache Formel als Antwort bereit:

$$MTTF_D = \frac{2}{3}\left(MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right) \qquad (D.8)$$

Die mittlere $MTTF_D$ pro Kanal ergibt sich also durch eine Mittelungsformel aus den $MTTF_D$-Werten beider redundanter Kanäle C1 und C2 (diese Formel lässt sich mathematisch herleiten, indem der $MTTF_D$-Wert für ein zweikanaliges System ohne Diagnose, aber mit bekannten $MTTF_D$-Werten beider Kanäle – $MTTF_{DC1}$ und $MTTF_{DC2}$ – gesucht wird [10]). Damit ist die sukzessive Zusammenfassung der $MTTF_D$-Werte aller an der Steuerung beteiligten Komponenten abgeschlossen. Das Ergebnis ist ein Kennwert für die typische Zuverlässigkeit der in der Steuerung vorhandenen Komponenten ohne Berücksichtigung von Redundanz, Diagnose oder CCF (Ausfälle infolge gemeinsamer Ursache, vgl. Anhang F). Während $MTTF_D$ bereits für jeden beteiligten Kanal auf 100 Jahre (Kategorie 4: 2500 Jahre) begrenzt wird, ist die Einteilung der $MTTF_D$-Werte in eine der drei Klassen „niedrig", „mittel" oder „hoch" erst nach der Symmetrisierung sinnvoll. Der symmetrisierte Wert geht als ein Parameter neben der Kategorie, dem durchschnittlichen Diagnosedeckungsgrad und den Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in die numerische Bestimmung des PL ein. Daneben wird je nach zu erreichender Kategorie ein minimaler $MTTF_D$-Wert von drei Jahren (für Kategorie B, 2 und 3) oder 30 Jahren (für Kategorie 1 und 4) benötigt.

Literatur

[1] *Birolini, A.:* Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management. 3. Aufl. Springer, Berlin 1991

[2] *Bork, T.; Schaefer, M.:* Aus Aktivität wird Vorsicht – Sinn und Unsinn der Quantifizierung. O + P Ölhydraulik und Pneumatik 51 (2007) Nr. 3, S. 78-85
▸ www.dguv.de/medien/ifa/de/pub/grl/pdf/2007_016.pdf

[3] *Schuster, U.:* Untersuchung des Alterungsprozesses von hydraulischen Ventilen. BGIA-Report 6/2004. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2004
▸ www.dguv.de/ifa, Webcode: d6362

[4] *Weibull, W.:* A statistical distribution function of wide applicability. J. Appl. Mech. 18 (1951), S. 292-297

[5] DIN EN 60947-4-1: Niederspannungsschaltgeräte – Teil 4-1: Schütze und Motorstarter – Elektromechanische Schütze und Motorstarter (01.11). Beuth, Berlin 2011

[6] DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. August 2014 – aktualisierte Fassung Dezember 2015
▸ http://publikationen.dguv.de/dguv/udt_dguv_main.aspx?FDOCUID=26231

[7] Grundsätze für die Prüfung und Zertifizierung von Verriegelungseinrichtungen mit Zuhaltung, Prüfgrundsatz GS-ET-19. Hrsg.: DGUV Test, Prüf- und Zertifizierungsstelle Elektrotechnik, Mai 2015
▸ www.bgetem.de, Webcode: 12700341

[8] Grundsätze für die Prüfung und Zertifizierung von elektromechanischen Zustimmungsschaltern und Zustimmungseinrichtungen, Prüfgrundsatz GS-ET-22. Hrsg.: DGUV Test, Prüf- und Zertifizierungsstelle Elektrotechnik, November 2009
► www.bgetem.de, Webcode: 12700341

[9] Das SISTEMA-Kochbuch 6: Wenn die vorgesehenen Architekturen nicht passen
► www.dguv.de/ifa, Webcode: d109240

[10] *Goble, W. M.:* Control systems safety evaluation and reliability. 3rd ed. Hrsg.: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010
► www.isa.org

Anhang E:
Bestimmung des Diagnosedeckungsgrades (DC)

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Hinweis zur möglichen Reduzierung des DC bei Kaskadierung, z. B. von elektromechanischen Positionsschaltern, eingefügt
- zwei DC-Maßnahmen „Redundanter Abschaltpfad ohne Überwachung des Aktors“ und „Redundanter Abschaltpfad mit Überwachung eines der Aktoren entweder durch die Logik oder durch die Testeinrichtung“ aus Tabelle E.2 gelöscht
- Abbildung E.3 geändert
- die Bedingungen für das vereinfachte Verfahren in Kategorie 2 geändert (Testung bei Anforderung als Alternative zu 100-mal häufiger Testen als Anfordern, Testkanal mindestens halb so zuverlässig wie der Funktionskanal statt $MTTF_{D\,L} \geq 0{,}5 * MTTF_{D\,TE}$)
- Beispiele aus der Norm zu „Fehlererkennung im Prozess“ eingefügt

Der Diagnosedeckungsgrad *DC* (Diagnostic Coverage) ist ein Maß für die Wirksamkeit der Selbsttest- und Überwachungsmaßnahmen in einer Steuerung. Er kann sich auf Bauelemente, Blöcke oder ganze Subsysteme (DC_{avg}) beziehen. Die genaue Definition des DC beruht auf einer Einteilung von Ausfällen in drei Gruppen (siehe Abbildung E.1):

- Ungefährliche Ausfälle S (safe): Diese führen automatisch dazu, dass ein sicherer Zustand eingenommen wird, aus dem heraus keine Gefährdungen entstehen (Beispiel: Offenbleiben eines Schützes oder Geschlossenbleiben eines Ventils mit der Folge der Energieunterbrechung und damit eines Stillstands potenziell gefahrbringender Bewegungen).

- Erkennbare gefahrbringende Ausfälle DD (dangerous detectable): Diese potenziell gefahrbringenden Ausfälle werden durch Test- oder Überwachungsmaßnahmen erkannt und in einen sicheren Zustand überführt (Beispiel: Geschlossenbleiben eines Schützes oder Offenbleiben eines Ventils, das durch einen Rücklesekontakt oder eine Stellungsüberwachung erkannt und sicher abgefangen wird).

- Unerkennbar gefahrbringende Ausfälle DU (dangerous undetectable): Diese potenziell gefahrbringenden Ausfälle werden nicht erkannt (Beispiel: unbemerktes Geschlossenbleiben eines Schützes oder Offenbleiben eines Ventils, wodurch bei einer Anforderung eines sicher abgeschalteten Moments kein Stillsetzen einer gefahrbringenden Bewegung erfolgt).

Bei mehrkanaligen Systemen wird die Bezeichnung „gefahrbringender Ausfall“ im Hinblick auf einen einzelnen Kanal verwendet, obwohl damit noch kein gefahrbringender Systemausfall gegeben sein muss. „DD“ und „DU“ lassen sich zur Gruppe der gefahrbringenden Ausfälle D (dangerous) zusammenfassen. Auch die ungefährlichen Ausfälle können erkennbar oder unerkennbar sein, was aber unerheblich ist, da in beiden Fällen der sichere Zustand eingenommen wird.

Der Diagnosedeckungsgrad bestimmt sich durch den Anteil der erkennbaren gefahrbringenden Ausfälle (DD) an allen gefahrbringenden Ausfällen (D) und wird meist als Prozentzahl notiert. Zu seiner Berechnung, z. B. im Zusammenhang mit einer FMEA (Ausfalleffektanalyse, siehe Anhang B), werden die aufsummierten Ausfallraten λ_{DD} und λ_{D} der Betrachtungseinheit zueinander ins Verhältnis gesetzt. Hier zeigt sich, dass der *DC* eine Kenngröße ist, die der getesteten Einheit (z. B. Block) zugeordnet wird und nicht der Testeinrichtung, welche die Tests durchführt. Um die DC-Bestimmung zu vereinfachen, bietet DIN EN ISO 13849-1 neben der FMEA einen anderen Weg an: Sie schlägt für typische Diagnosemaßnahmen DC-Eckwerte vor, von deren Erreichung ausgegangen werden kann, wenn die entsprechende Maßnahme korrekt umgesetzt wird. Auf diese Weise reicht eine tabellarische Bewertung der pro Einheit umgesetzten Diagnosemaßnahmen aus. Dies ist in ähnlicher Weise oft gängige und ökonomisch sinnvolle Praxis von Prüfstellen.

$$DC = \frac{\sum \lambda_{DD}}{\sum (\lambda_{DD} + \lambda_{DU})}$$

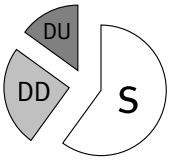


Abbildung E.1:
Illustration des Diagnosedeckungsgrades

Da der Anteil der unerkennbar gefahrbringenden Ausfälle (also 1 – DC) die für die Ausfallwahrscheinlichkeit relevante Größe zur Bewertung der realisierten Test- und Überwachungsmaßnahmen ist, erklärt sich die Wahl der Eckwerte (60, 90 und 99 %), mit deren Hilfe vier DC-Qualitätsstufen gebildet werden (Tabelle E.1).

Tabelle E.1:
Die vier Stufen des Diagnosedeckungsgrades im vereinfachten Ansatz der DIN EN ISO 13849-1

DC (Diagnosedeckungsgrad)	
Bezeichnung	**Bereich**
kein	$DC < 60\,\%$
niedrig	$60\,\% \leq DC < 90\,\%$
mittel	$90\,\% \leq DC < 99\,\%$
hoch	$99\,\% \leq DC$

Grundsätzlich muss unterschieden werden zwischen dem *DC* eines einzelnen Tests für eine bestimmte Komponente bzw. einen Block und dem durchschnittlichen Diagnosedeckungsgrad DC_{avg} (average) für das gesamte betrachtete Subsystem einer sicherheitsbezogenen Steuerung (SRP/CS). Die Gruppenbildung mithilfe der Eckwerte wird dabei sowohl zur Qualifizierung der einzelnen Tests herangezogen als auch bei der Benennung von DC_{avg}. Da DC_{avg} eine der Eingangsgrößen für die vereinfachte Quantifizierung der Ausfallwahrscheinlichkeit mithilfe des Säulendiagramms ist, wird der berechnete DC_{avg}-Wert auf den nächst niedrigeren der vier Eckwerte (0 %, 60 %, 90 % und 99 %) aus Tabelle E.1 abgerundet und dadurch in eine der vier DC-Klassen (kein, niedrig, mittel, hoch) eingeordnet. Beispielsweise wird ein DC_{avg}-Wert von 80 % im vereinfachten Ansatz auf einen Wert von 60 % herabgestuft (anders als im IFA-Software-Assistenten SISTEMA, der in der Grundeinstellung mit DC_{avg}-Zwischenwerten rechnet, siehe Anhang H). Im Folgenden wird zunächst auf den *DC* einzelner Tests und danach auf die Berechnung von DC_{avg} eingegangen.

In Tabelle E.2 sind typische Test- und Überwachungsmaßnahmen bezogen auf Komponenten (in der Regel Elemente oder Blöcke) und ihre DC-Bewertung nach DIN EN ISO 13849-1 dar-

Tabelle E.2:
DC-Eckwerte für typische Test- und Ü erwachungsmaßnahmen auf Komponenten- bzw. Blockebene nach DIN EN ISO 13849-1

Maßnahme	hauptsächlich relevant für			*DC* [%]	Maßnahmen-Beschreibung
	I	L	O		
Zyklische Testung/Dynamisierung	X			90	Periodische Generierung eines Signalwechsels mit Überwachung des Ergebnisses
Plausibilität/Rücklesung/(Kreuz-)Vergleich					
• ohne Dynamisierung	X		X	0-99	Der erreichte DC-Wert ist abhängig von der Häufigkeit eines Signalwechsels in der Anwendung (zur minimalen Testhäufigkeit siehe Abschnitt 6.2.14).
• mit Dynamisierung, ohne hochwertige Fehlererkennung	X		X	90	
• mit Dynamisierung, mit hochwertiger Fehlererkennung	X		X	99	
Indirekte Überwachung	X	X	X	90-99	Der erreichte DC-Wert ist abhängig von der Anwendung.
Direkte Überwachung	X	X	X	99	
Fehlererkennung durch den Prozess	X	X	X	0-99 (1)	Der erreichte DC-Wert ist abhängig von der Anwendung, diese Maßnahme alleine ist nicht ausreichend um PL e zu erreichen. (2)

gestellt. Für jede Funktion (I, L, O bzw. Eingabe, Logik, Ausgabe), Kategorie und Technologie sind unterschiedliche Maßnahmen üblich. Ihre Bewertung kann abhängig von der Ausführung oder äußeren Umständen schwanken, z. B. je nach Anwendung, in der die Steuerung betrieben wird. Die indirekte Überwachung durch Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen lässt in manchen Anwendungen z. B. keinen Rückschluss zu, ob jeder von zwei redundanten Steuerungskanälen die Sicherheitsfunktion noch unabhängig ausführen kann. Generell wird bei der Bewertung als DC-Zahlenwert nicht unterschieden zwischen automatischen (z. B. regelmäßig ablaufenden Programmroutinen) oder willensabhängigen Tests (z. B. manuell durch den Bediener in regelmäßigen Abständen eingeleitete Tests), siehe dazu auch Abschnitt 6.2.14. Prinzipiell ist ebenfalls unerheblich, welche Einheit einen Test durchführt, z. B. bei Selbsttests. Allerdings ist nur bei entsprechender Unabhängigkeit (Einfehlersicherheit, Widerstandsfähigkeit gegen Ausfälle infolge gemeinsamer Ursache) von testender und getesteter Einheit ein Test überhaupt wirksam. Wichtig ist weiterhin, dass nach Erkennung eines gefahrbringenden Ausfalls auch der sichere Zustand eingenommen wird. Wird z. B. das Verschweißen eines Hauptschützes erkannt, aber ohne eine Möglichkeit zur rechtzeitigen Stillsetzung einer gefahrbringenden Bewegung, so ist die Erkennung nutzlos und mit einem *DC* von 0 % zu bewerten.

Zur DC-Maßnahme „Fehlererkennung durch den Prozess“ gibt die Norm in ihrer dritten Ausgabe Hinweise in Form von Beispielen: *„Die DC Maßnahme ‚Fehlererkennung durch den Prozess‘ darf nur angewendet werden, wenn das sicherheitsbezogene Bauteil am Fertigungsprozess beteiligt ist, z. B. wenn eine normale PLC oder normale Sensoren für die Fertigung eines Werkstücks benutzt werden, und als Teil von einem von zwei redundanten Funktionskanälen, die die Sicherheitsfunktion ausführen, fungieren. Das geeignete DC-Level hängt von der Überschneidung der gewöhnlich verwendeten Ressourcen (Logik, Eingänge/Ausgänge, usw.) ab. Wenn z. B. alle Fehler eines Drehreglers in einer Druckmaschine zu stark sichtbaren Fehlern im Druckvorgang führen, wird der DC für den Sensor, der eine sicher begrenzte Geschwindigkeit überwacht, zwischen 90 % und 99 % angenommen.“* Für PL_r = e ist diese Maßnahme alleine nicht ausreichend (siehe Tabelle E.2) und führt bei der Verwendung von SISTEMA zu einer roten Warnmeldung. Bei ausreichender Rechtfertigung, z. B. durch weitere DC-Maßnahmen, die auf denselben Block wirken, oder wenn der komplementäre Block des redundanten Kanals eine andere DC-Maßnahme umsetzt, deren DC mindestens so groß ist wie die angenommene *DC* durch den Prozess, kann diese Maßnahme trotzdem in Rechnung gestellt werden. In SISTEMA kann dies durch eine direkte DC-Eingabe mit manueller Wahl der Prozentstufe erfolgen bei gleichzeitiger Dokumentation der Rechtfertigung.

<table>
<tr><th>typische Realisierung in verschiedenen Technologien</th><th rowspan="2">Pneumatik</th><th rowspan="2">Hydraulik</th><th rowspan="2">Elektrik</th><th rowspan="2">(Programmierbare) Elektronik</th></tr>
<tr><th>Mechanik</th></tr>
<tr><td colspan="5">siehe Maßnahmenbeschreibung</td></tr>
<tr><td></td><td colspan="4">manuelle Initiierung der Prüffunktion</td></tr>
<tr><td></td><td colspan="3">Vergleich von Eingängen oder Ausgängen ohne Kurzschlusserkennung</td><td></td></tr>
<tr><td></td><td>Positionserfassung des Ventilschiebers, Höhe des DC abhängig von der konkreten Ausführung</td><td colspan="2">Kreuzvergleich von Eingängen oder Ausgängen mit Kurzschlusserkennung und Erkennung statischer Fehler, z. B. mithilfe von Sicherheitsbausteinen</td><td>Kreuzvergleich von Signalen und Zwischenwerten mit Kurzschlusserkennung, Erkennung statischer Fehler und zeitliche und logische Programmlaufüberwachung; dynamischer Kreuzvergleich unabhängig gewonnener Stellungs- oder Geschwindigkeitsinformationen</td></tr>
<tr><td>Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen</td><td>Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen; Ventilüberwachung durch Druckschalter</td><td colspan="3">Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen</td></tr>
<tr><td>Stellungsüberwachung direkt am überwachten Steuerungselement</td><td>Stellungsüberwachung direkt am Ventilschieber über den gesamten Hub</td><td colspan="2">Stellungsüberwachung durch zwangsgeführte Rücklesekontakte (antivalente Öffnerkontakte)</td><td>Signalüberwachung durch Rücklesung z.B. mittels Optokopplern</td></tr>
<tr><td colspan="5">Versagen der Prozessregelung, die sich durch Fehlfunktion, Beschädigung von Werkstück oder Maschinenteilen, Prozessunterbrechung oder -verzögerung funktional bemerkbar macht, ohne sofort eine Gefährdung darzustellen</td></tr>
</table>

Tabelle E.2 (Fortsetzung)

Maßnahme	hauptsächlich relevant für			*DC* [%]	Maßnahmen-Beschreibung
	I	L	O		
Überwachung von Eigenschaften	X			60	
Programmlaufüberwachung					
• einfache zeitliche		X		60	zeitliche Überwachung
• zeitlich und logisch		X		90	
Selbsttests bei Anlauf		X	(X)	90	zur Erkennung verborgener Fehler, *DC* abhängig von der Testausführung
Testung der Überwachungseinrichtung		X		90	Testung der Reaktionsmöglichkeit der Überwachungseinrichtung durch den Hauptkanal nach Anlauf, oder wann immer die Sicherheitsfunktion angefordert wird, oder wann immer ein externes Signal dies durch eine Eingangseinrichtung anfordert
Dynamische Prinzipien		X		*99*	alle Bauteile der Logik erfordern eine Zustandsänderung EIN-AUS-EIN, wenn die Sicherheitsfunktion angefordert wird
Speicher- und CPU-Tests					
• Invarianter Speicher: Signatur einfacher Wortbreite (8 Bit)		X		90	
• Invarianter Speicher: Signatur doppelter Wortbreite (16 Bit)		X		*99*	
• Varianter Speicher: RAM-Test durch Verwendung redundanter Daten, z. B. Flags, Merker, Konstanten, Timer, und Kreuzvergleich dieser Daten		X		60	
• Varianter Speicher: Test der Lesbarkeit und der Beschreibbarkeit der verwendeten Speicherzellen		X		60	
• Varianter Speicher: RAM Überwachung mit modifiziertem Hammingcode oder RAM Selbsttest (z. B.„Galpat“ oder „Abraham”)		X		*99*	
• Verarbeitungseinheit: Selbsttest durch Software		X		60-90	
• Verarbeitungseinheit: Kodierte Verarbeitung		X		90-99	
Redundanter Abschaltpfad mit Überwachung der Betätigungselemente durch die Logik und Testeinrichtung			X	*99*	

(1) Zum Beispiel zu ermitteln über eine FMEA durch Bildung des Quotienten der erkannten gefahrbringenden Ausfälle zu allen gefahrbringenden Ausfällen (weitere Hinweise im Text)

(2) PL e erfordert in der Regel zwei Kanäle. Daher sollte mindestens der komplementäre Block des redundanten Kanals eine andere DC-Maßnahme umsetzen, deren *DC* mindestens so groß sein sollte wie der angenommene *DC* durch den Prozess (weitere Hinweise im Text).

typische Realisierung in verschiedenen Technologien Mechanik	Pneumatik	Hydraulik	Elektrik	(Programmierbare) Elektronik
Überwachung von Antwortzeiten, Signalstärke analoger Signale			Überwachung von Antwortzeiten, Signalstärke analoger Signale (z.B. Widerstand, Kapazität)	
	nicht relevant			Zeitglied als Watchdog, mit Triggersignalen im Programm der Logik
	nicht relevant			durch einen Watchdog, wobei die Testeinrichtung Plausibilitätstests des Verhaltens der Logik durchführt
			Erkennung z.B. verschweißter Kontakte durch Ansteuerung und Rücklesung	Erkennung verborgener Fehler in Programm- und Datenspeicher, Eingangs-/ Ausgangsanschlüssen, Schnittstellen
				Testung der Reaktionsmöglichkeit des Watchdogs
	Verriegelungsschaltungen in Pneumatik		Verriegelungsschaltungen in Relaistechnik	
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung

Zu den in Tabelle E.2 genannten Test- und Überwachungsmaßnahmen gilt als zusätzliche Anforderung: Wird „mittel“ oder „hoch“ als DC für die Logik gefordert, muss mindestens je eine Maßnahme für varianten Speicher, invarianten Speicher und Verarbeitungseinheit mit mindestens je 60 % gewählt werden. Es können auch andere Maßnahmen als die in Tabelle E.2 genannten verwendet werden.

Weitere Informationen zur DC-Bestimmung für typische Testmaßnahmen finden sich z. B. in den Tabellen A.2 bis A.14 der DIN EN 61508-2 [1]. Dort sind die Eckwerte von 60, 90 und 99 % als maximaler durch die jeweilige Maßnahme zu erreichender DC notiert. Bei geeigneter uneingeschränkter Umsetzung der genannten Maßnahmen kann dieser Höchstwert aber in der Regel zur Abschätzung herangezogen werden. Anhang E der DIN EN ISO 13849-2 [2] zeigt ein ausführliches Beispiel für die Validierung des Ausfallverhaltens und der Diagnosemaßnahmen an einer automatischen Montagemaschine.

Nach der Bestimmung des *DC* für einzelne Testmaßnahmen und vor der Berechnung des DC_{avg} muss der DC-Wert pro Block ermittelt werden. Meist wirkt eine einzelne Testmaßnahme auf einen gesamten Block (z. B. Kreuzvergleich): Dann kann der Einzelwert einfach für den Block übernommen werden. Es sind aber weitere Konstellationen möglich:

- Wird ein Block durch mehrere Einzelmaßnahmen überwacht (siehe Abbildung E.2), so ist der Block-DC mindestens so gut wie der beste Einzel-DC. Bei gegenseitiger Ergänzung ist sogar ein höherer Block-DC möglich. Dessen Bestimmung erfordert aber dann eine Analyse der durch jeden Test abgedeckten Ausfälle, ähnlich einer FMEA.

- Ein Block besteht aus mehreren Einheiten, von denen jede durch andere Maßnahmen getestet wird, z. B. programmierbare Elektronik mit separaten Tests für Speicher und Verarbeitungseinheit (siehe Abbildung E.3). Dann ist der Block-DC mindestens so gut wie der schlechteste Einzel-DC. (Ob es zulässig ist, dass hier Einheiten ohne Testung vorkommen, muss mit der entsprechenden Kategorie-Definition, siehe Abschnitte 6.2.5 bis 6.2.7, abgestimmt werden; bei dem *DC* der Logik gelten weitere Anforderungen, s. o.) Ein besserer und genauerer Wert für den Block-DC lässt sich durch Gewichtung des Einzel-DC-Wertes mit der zugehörigen Ausfallrate λ_D (= $1/MTTF_D$) erreichen. Auch auf Block-Ebene kann hierzu Gl. (E.1) als Mittelungsformel verwendet werden. Je nach Genauigkeit gipfelt eine solche Analyse allerdings ebenfalls in einer FMEA.

- Bei einer Kaskadierung, z. B. von elektromechanischen Positionsschaltern, die über gemeinsame Anschlussleitungen mit einem Sicherheitsbaustein verbunden sind, kann es zu einer Reduzierung des *DC* kommen. Durch eine elektrisch zweikanalige Ausführung können bestimmte Fehler eines Positionsschalters durch logisch nicht plausible Signale beider elektrischen Kontakte vom Sicherheitsbaustein aufgedeckt werden. So wird nach Schließen der Tür mit dem defekten Schalter der Start der Maschine verhindert. Wird außer der Tür mit dem gefährlich ausgefallenen Positionsschalter noch eine weitere geöffnet, kann – je nach Reihenfolge – die Fehlererkennung nicht erfolgen. Die Kaskadierung führt damit zu einer Reduzierung des *DC*, die u. a. abhängig ist von der Anzahl der Schutztüren und der Häufigkeit ihres Öffnens. Details dazu und zur Abschätzung des *DC* für solche Konstellationen sind in ISO/TR 24119 [3] dargestellt. Dort wird in Abschnitt 6.1 bei Kaskadierung PL e ausgeschlossen. Wird wie in Beispiel 28 (siehe Abschnitt 8.2.28) für jeden Positionsschalter ein zusätzlicher Kontakt zur Fehlererkennung eingesetzt, dann ist die Fehlererkennung auch bei Kaskadierung nicht eingeschränkt und PL e erreichbar.

Der durchschnittliche *DC* für ein SRP/CS (auf Subsystem-Ebene) wird mit DC_{avg} bezeichnet und errechnet sich aus den DC-Werten aller Blöcke in Funktionskanälen. Im Gegensatz zur $MTTF_D$ pro Kanal wird nicht zwischen den Steuerungskanälen unterschieden, sondern direkt ein Gesamtwert ermittelt. Die Mittelungsformel gewichtet die Einzel-DC-Werte mit der zugehörigen Ausfallrate λ_D (= $1/MTTF_D$) jedes Blocks. Dies gewährleistet, dass Blöcke mit einer hohen Ausfallrate, d. h. geringen $MTTF_D$, stärker berücksichtigt werden als Blöcke, deren gefahrbringender Ausfall vergleichsweise unwahrscheinlich ist. Die Mittelungsformel lautet:

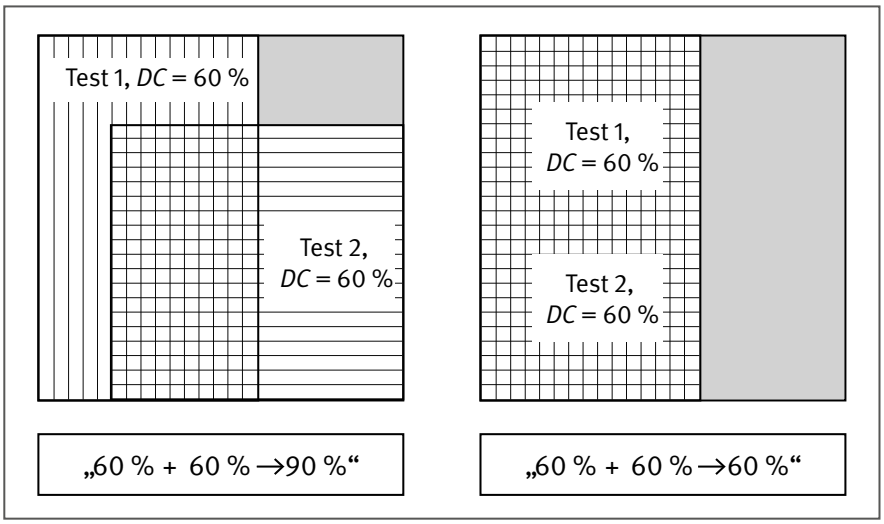


Abbildung E.2:
Wirken auf einen Block mehrere Tests, so kann deren Überlappung zu einem höheren Gesamt-DC führen (links) oder auch nicht (rechts); die schraffierten Flächen repräsentieren den Anteil der erkannten gefahrbringenden Ausfälle; die quadratische Gesamtfläche repräsentiert alle gefahrbringenden Ausfälle (100 %)

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}} \quad \text{(E.1)}$$

Die Summation läuft über alle relevanten Blöcke mit folgender Festlegung:

- Für Blöcke ohne *DC* wird ein *DC* = 0 % eingesetzt. Diese tragen damit nur zum Nenner des Bruchs bei. Ob fehlende Diagnose für Blöcke im Einklang mit den Anforderungen der jeweiligen Kategorie steht, muss im Einzelfall entschieden werden. Kategorie 2 fordert pauschal den „Test der Sicherheitsfunktion", Kategorie 3 die Fehlererkennung, „wenn immer in angemessener Weise durchführbar", Kategorie 4 fordert ebenfalls die Erkennung des einzelnen Fehlers und nur „wenn diese Erkennung nicht möglich ist", die Ausführung der Sicherheitsfunktion auch bei Anhäufung unerkannter Fehler.

- Für Blöcke mit Fehlerausschluss bezüglich der gefahrbringenden Ausfallrichtung (verschwindende Ausfallrate λ_D bzw. unendlich hoher $MTTF_D$) wird der entsprechende Summand im Zähler und im Nenner weggelassen.

- Alle Blöcke, die Sicherheitsfunktionen in den verschiedenen Funktionskanälen ausführen, werden berücksichtigt. Blöcke, die nur allein der Testung dienen, werden nicht berücksichtigt. Für Kategorie-2-Strukturen bedeutet dies, dass Blöcke des Testkanals („TE" und „OTE") nicht mitgezählt werden. In Kategorie 3 und 4 wird der Mittelwert direkt über beide Kanäle hinweg gebildet, eine gesonderte Symmetrisierung wie bei der $MTTF_D$ pro Kanal entfällt.

Für eine detaillierte Analyse des Einflusses der Tests auf die Ausfallwahrscheinlichkeit des Gesamtsystems sind neben dem *DC* weitere Größen zu berücksichtigen. Dazu zählt neben der Testrate z. B. die Ausfallrate der Testeinrichtung selbst. In mehrkanaligen Systemen hat allerdings die Häufigkeit eines Tests geringere Auswirkungen, da die dabei relevanten Zeiten in aller Regel sehr viel kleiner sind als die $MTTF_D$-Werte der Kanäle. Bevor also die Beeinträchtigung eines Tests für das System relevant wird, müssen erst mehrere Kanäle ausfallen, was sehr unwahrscheinlich ist, solange die Testzyklen sehr viel kleiner bleiben als die $MTTF_D$ eines Kanals. Abschnitt 6.2.14 gibt ausführlichere Erläuterungen zur notwendigen Testhäufigkeit. In Kategorie-2-Strukturen macht jedoch der Ausfall der Testeinrichtung aus einem einkanalig getesteten System ein einkanalig ungetestetes System. Der nächst gefährliche Ausfall im Funktionskanal kann dann nicht mehr erkannt werden und führt direkt dazu, dass die Sicherheitsfunktion nicht mehr ausgeführt werden kann. Daher gelten für die vereinfachte Beurteilung der Ausfallwahrscheinlichkeit von Kategorie-2-Systemen neben Anforderungen zum *DC* weitere Voraussetzungen:

- Alle Testraten sollten mindestens 100-mal (ausnahmsweise mindestens 25-mal) größer sein als die Anforderungsrate der Sicherheitsfunktion oder die Testung sollte bei Anforderung der Sicherheitsfunktion so schnell ausgeführt werden, dass der sichere Zustand erreicht wird, bevor es zu einer Gefährdung kommt. Damit soll gewährleistet werden, dass ein Ausfall durch einen Test bemerkt werden kann, bevor eine Anforderung der Sicherheitsfunktion nicht bedient werden kann (siehe auch Anhang G).

- Die $MTTF_D$ des Testkanals (TE und OTE) sollte mindestens halb so groß sein wie die $MTTF_D$ des Funktionskanals (I, L und O). Durch diese Annahme wird sichergestellt, dass die Ausfallwahrscheinlichkeit des Testkanals nicht unangemessen hoch

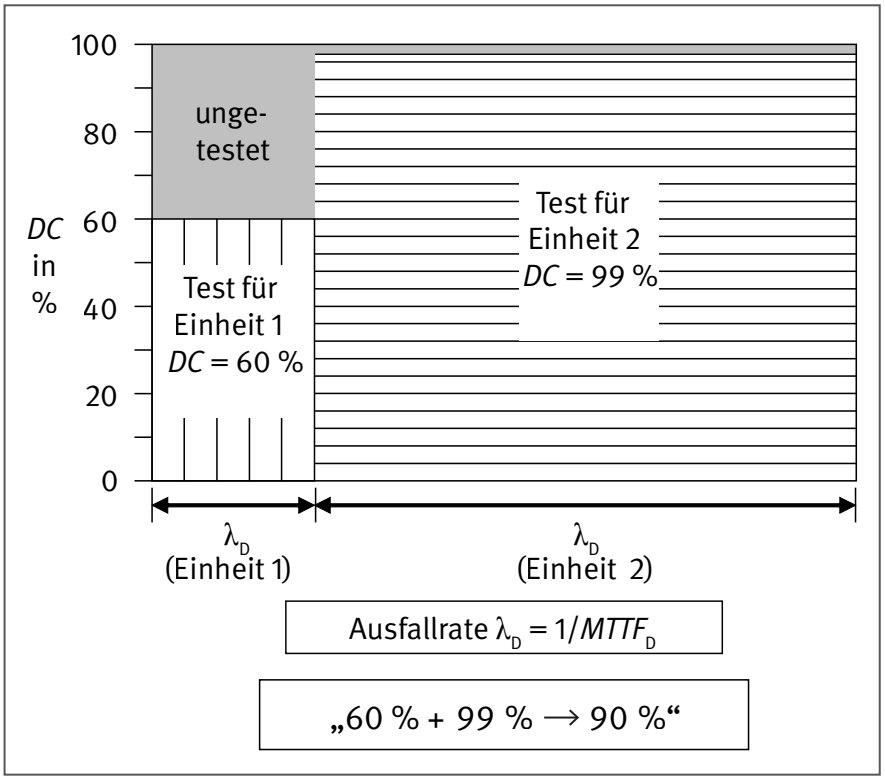


Abbildung E.3:
Bei der DC-Mittelung für mehrere Einheiten eines Blocks führt die Gewichtung der Einzel-DC von 60 % und 99 % mit λ_D auf einen anderen Wert (90 %) als z. B. das ungewichtete arithmetische Mittel (79,5 %)

ist. Ist diese Bedingung verletzt (auch nach Begrenzung der $MTTF_D$ des Funktionskanals auf 100 Jahre), so ist es natürlich zulässig, die Ausfallwahrscheinlichkeit mit einer $MTTF_D$ des Funktionskanals zu berechnen, die rechnerisch auf die doppelte $MTTF_D$ des realisierten Testkanals reduziert wird.

Literatur

[1] DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (12.02). Beuth, Berlin 2002

[2] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (02/2013). Beuth, Berlin 2013

[3] ISO/TR 24119: Safety of machinery – Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts (11/15). Beuth, Berlin 2015

Anhang F:
Ausfälle infolge gemeinsamer Ursache (CCF)

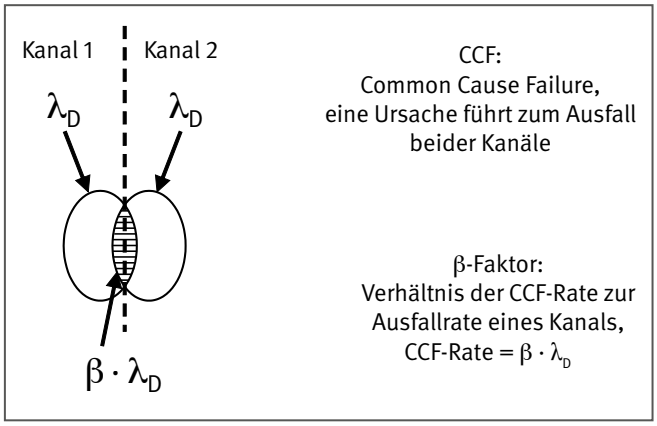
Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

Text der Maßnahmenbeschreibungen an die dritte Ausgabe der Norm angepasst

Der Begriff des Ausfalls infolge gemeinsamer Ursache – Common Cause Failure (CCF) – beschreibt die Tatsache, dass in einem redundanten System oder einem einkanaligen System mit separatem Testkanal durch eine Ursache mehrere Kanäle außer Kraft gesetzt werden können. Die gewünschte Einfehlersicherheit einer redundanten Struktur wird damit unterlaufen. Deshalb ist es sehr wichtig, diese Fehlerquelle möglichst auszuschalten. Die CCF-Auslöser können physikalischer Natur sein, z. B. Übertemperatur oder starke elektromagnetische Störungen, oder systematischer Art, z. B. fehlerhaftes Schaltungsdesign oder Programmierfehler bei identischer Software in beiden Kanälen.

Ein üblicher Ansatz zur Quantifizierung der „CCF-Anfälligkeit" einer Steuerung ist das sogenannte Beta-Faktor-Modell. Dabei wird davon ausgegangen, dass mit einem bestimmten Anteil der gefährlichen Ausfälle in einem Kanal infolge derselben Ursache auch gefährliche Ausfälle im zweiten Kanal einhergehen. Dieser Sachverhalt ist in Abbildung F.1 dargestellt: Die gefährlichen Ausfallraten beider Kanäle (symbolisch dargestellt als Ellipsenflächen) besitzen eine schraffiert dargestellte CCF-Überlappung. Der Proportionalitätsfaktor zwischen der CCF-Rate und der gefährlichen Ausfallrate des einzelnen Kanals λ_D wird üblicherweise mit β bezeichnet (Common Cause Faktor oder auch Beta-Faktor).

Abbildung F.1:
Illustration des Ausfalls infolge gemeinsamer Ursache (CCF) anhand des Beta-Faktor-Modells



Die exakte Berechnung des Beta-Faktors für eine konkrete Steuerung ist nahezu unmöglich, besonders da dies im Vorfeld vor der eigentlichen Konstruktion geschehen soll. DIN EN 61508-6 [1], Anhang D, bedient sich dazu eines Punkteschemas, um β-Werte zwischen 0,5 und 10 % zu ermitteln. In einer langen Liste aus nach verschiedenen Ursachen sortierten Maßnahmen werden Punkte vergeben, die in der Summe nach Anwendung einiger Regeln zu einem β-Schätzwert führen. DIN EN ISO 13849-1 greift diese Methode auf – sowohl vereinfacht als auch für den Maschinenschutz angepasst. Die Vereinfachung wurde auf der Basis von technischen Maßnahmen vorgenommen, die von Fachleuten als besonders hilfreich zur CCF-Vermeidung angesehen wurden. Es handelt sich allerdings um einen Kompromiss, der nicht wissenschaftlich, aber empirisch begründet werden kann:

- Die Liste der CCF-Gegenmaßnahmen wurde auf die im Maschinenschutz relevanten und hauptsächlich technischen Lösungen konzentriert.
- Statt mehrerer möglicher β-Werte wurde ein einziger Zielwert von höchstens 2 % ausgewählt, der nur entweder erreicht oder verfehlt werden kann. Die vereinfachte Methode zur Bestimmung des Performance Levels nach DIN EN ISO 13849-1 basiert auf der Annahme eines Beta-Faktors von 2 %.
- Die Rechenregeln für das Punkteschema wurden auf zwei Schritte zusammengefasst: Jede Maßnahme kann nur voll erfüllt (volle Punktzahl) oder nicht erfüllt sein (Punktzahl Null), anteilige Punktzahlen für unvollständig erfüllte Maßnahmen werden nicht angerechnet. Wenn Maßnahmen (z. B. Diversität, Verwendung bewährter Bauteile) nur in einzelnen SRP/CS als Subsysteme komplett erfüllt werden, können subsystemweise unterschiedliche Maßnahmenbündel gegen CCF wirken. Die Mindestpunktzahl von 65 Punkten muss für die Kategorien 2, 3 und 4 erfüllt werden, um die vereinfachte Methode zur Bestimmung des Performance Levels anwenden zu können. Maximal können 100 Punkte erreicht werden.

Bei der Bewertung der Maßnahmen ist Folgendes zu beachten:

- Die Maßnahmen sind mit besonderem Schwerpunkt auf ihre Wirksamkeit gegen CCF zu bewerten. Beispielsweise fordern die Produktnormen ohnehin Unempfindlichkeit gegenüber Umwelteinflüssen und elektromagnetischen Störungen. Darüber hinaus ist zu beurteilen, ob diese Einwirkungen als Ursachen für gemeinsame Fehler wirksam minimiert wurden.

- Je nach Steuerungstechnologie unterscheiden sich die physikalischen Gegenmaßnahmen, z. B. sind unter Umwelteinflüssen bei elektrischen Steuerungen elektromagnetische Störungen eher relevant, während es bei fluidischen Steuerungen eher Verunreinigungen des Mediums sind. Gegenmaßnahmen sind daher angepasst auf die verwendete Technologie zu bewerten.

- Einen Sonderfall stellt die getestete Struktur von Kategorie-2-Systemen dar. Hier betrifft CCF den gemeinsamen Ausfall des Funktions- und des Testkanals. Ein gemeinsamer Ausfall führt dazu, dass der Strukturvorteil durch CCF zunichte gemacht wird. Die Bewertung der Maßnahmen ist dazu sinngemäß auf die Besonderheiten der Kategorie-2-Struktur anzupassen.

- Für eine Maßnahme gegen Ausfälle infolge gemeinsamer Ursache, die aufgrund der inhärenten Eigenschaften der Steuerung nicht auftreten können, darf die volle Punktzahl angerechnet werden.

Die Maßnahmen gegen gemeinsame Ausfälle und die assoziierten Punktzahlen aus DIN EN ISO 13849-1 im Einzelnen sind Folgende:

- Trennung (15 Punkte):
  Physikalische Trennung zwischen den Signalpfaden, z. B.
  – getrennte Verdrahtung/Verrohrung
  – Erkennung von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Testung
  – separate Schirmung der Signalpfade beider Kanäle
  – ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen

- Diversität (20 Punkte):
  In beiden Steuerungskanälen werden unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien verwendet. Beispiele dafür sind:
  – ein Kanal aus programmierbarer Elektronik aufgebaut, der andere fest verdrahtet
  – Initiierung auf unterschiedliche Art, z. B. mittels Position, Druck oder Temperatur
  – digitale und analoge Messung von Variablen (z. B. Abstand, Druck oder Temperatur)
  – Bauteile von unterschiedlichen Herstellern

- Entwurf/Anwendung/Erfahrung:
  Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur usw. (15 Punkte) und Verwendung bewährter Bauteile (5 Punkte)

- Beurteilung/Analyse (5 Punkte):
  Für jedes Teil des SRP/CS wurde eine Ausfalleffektanalyse durchgeführt und ihre Ergebnisse wurden im Entwicklungsprozess berücksichtigt, um Ausfälle infolge gemeinsamer Ursache zu vermeiden.

- Kompetenz/Ausbildung (5 Punkte):
  Schulung des Konstruktionspersonals darin, die Ursachen und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen

- Umgebungsbedingungen hinsichtlich Schutz vor schädlichen Einflüssen auf elektrische/elektronische und fluidtechnische Systeme (25 Punkte):
  – Elektrische Systeme: Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMV) im Einklang mit den zutreffenden Normen.
  – Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums

  Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.

- Umgebungsbedingungen hinsichtlich anderer Einflüsse (10 Punkte):
  Berücksichtigung der Anforderungen hinsichtlich der Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den relevanten Normen festgelegt)

Literatur

[1] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (02.11). Beuth, Berlin 2011

Anhang G:
Was steckt hinter dem Säulendiagramm in Bild 5 der DIN EN ISO 13849-1?

Änderung gegenüber der 2. Auflage (BGIA-Report 2/2008):

- Neue Norm-Anmerkung 1 aus Anhang K wird erwähnt
- Erläuterungen zu den Zeitverhältnissen bei der Testung aus Normabschnitt 4.5.4 an die neue Normversion angepasst
- Erläuterungen zur Verlängerung der Gebrauchsdauer über 20 Jahre hinaus eingefügt
- Abschnitt „Literatur“ aktualisiert
- Reihenfolge der Abbildungen an den Textverlauf angepasst

Anders als die Vorgänger-Norm DIN EN 954-1 [1] sieht DIN EN ISO 13849-1 zusätzlich zur Kategorieprüfung den Nachweis eines Performance Levels (PL) vor. Numerisch leitet sich der Performance Level gemäß Tabelle 6.1 dieses Reports aus der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls des Systems je Stunde ab, die auch als PFH_D (Probability of a Dangerous Failure per Hour, vgl. Fußnote 4 in Kapitel 3, Seite 17) bezeichnet wird. Diese Größe muss aus der Systemstruktur, den Bauelementausfallraten, dem Diagnosedeckungsgrad der automatischen Tests, der Gebrauchsdauer des Systems und, bei entsprechender Systemstruktur, der Empfindlichkeit des Systems gegenüber Ausfällen infolge gemeinsamer Ursache CCF (Common Cause Failures) ermittelt werden.

Zu diesem Zweck dienen Rechenmodelle, die das Zusammenwirken der genannten Faktoren berücksichtigen und als Ergebnis die PFH_D liefern (als Mittelwert während der Gebrauchsdauer). Eigentlich müsste bei der Anwendung der Norm für jedes zu untersuchende System ein maßgeschneidertes Modell erstellt werden. Für einige gebräuchliche Strukturvarianten, die „vorgesehenen Architekturen“ aus DIN EN ISO 13849-1, Abschnitt 6.2 (vgl. Abschnitte 6.2.1 bis 6.2.7 dieses Reports), wurden im IFA Markov-Modelle entwickelt, deren numerische Ergebnisse als „Säulendiagramm“ in der Norm in Abschnitt 4.5.4, Bild 5 (Abbildung 6.10 bzw. G.1 [Seite 278] dieses Reports), zusammengetragen sind. Dadurch kann auf die Entwicklung eines eigenen Rechenmodells und eine komplexe Berechnung verzichtet werden, falls das System im Wesentlichen die Gestalt einer der vorgesehenen Architekturen hat oder es sich in Subsysteme von solcher Gestalt zerlegen lässt (vgl. hierzu Abschnitt 6.3 und Anhang H der DIN EN ISO 13849-1 oder Abschnitt 6.4 dieses Reports). Eine grundlegende Einführung in die Technik der Markov-Modellierung findet man z. B. in [2].

Um ein übersichtliches Diagramm zu erhalten, mussten einige Einschränkungen und Vereinfachungen vorgenommen werden. Zum einen begrenzt die Norm die Anzahl der vorgesehenen Architekturen und damit die Anzahl der notwendigen Modelle. Zum anderen wurde die Vielzahl der Eingangsparameter durch sinnvolle Bündelung verringert. Hierzu wurden die Größen $MTTF_D$ und DC_{avg} eingeführt, die jeweils mehrere Eingangsparameter zusammenfassen.

Die im Diagramm verwendete $MTTF_D$ hat die Bedeutung einer mittleren Zeit bis zum Ausfall jedes Kanals in dessen gefahrbringende Ausfallrichtung (Mean Time to Dangerous Failure). Die $MTTF_D$-Werte mehrerer Funktionsblöcke werden dabei zu einer einzigen Kanal-$MTTF_D$ zusammengefasst (Kapitel 6 und Anhang D). Allen $MTTF_D$-Werten liegt die Annahme konstanter Bauelement-Ausfallraten λ_D zugrunde, wodurch die Beziehung $MTTF_D = 1/\lambda_D$ gilt. Bei Zweikanaligkeit mit unterschiedlicher Kanal-$MTTF_D$ wird mit einer gemittelten Ersatz-$MTTF_D$ gearbeitet. Hingegen gibt der Wert DC_{avg} den gewichteten Mittelwert des Diagnosedeckungsgrades für das gesamte System an, der für die Zuordnung zu einer der vier DC_{avg}-Stufen (vgl. Tabelle 6.4) benutzt wird.

Die Sinnhaftigkeit und Zulässigkeit dieser Zusammenfassungen innerhalb der geforderten Quantifizierungsgenauigkeit wurden durch umfangreiche Testrechnungen nachgewiesen. Das gilt auch für das in Abschnitt 4.5.4 der Norm zugelassene Verhältnis der $MTTF_D$-Werte von Test- und Funktionskanal bei der Kategorie-2-Architektur: Die $MTTF_D$ des Testkanals muss mindestens den halben Wert der $MTTF_D$ für den Funktionskanal aufweisen. Bei redundanzbehafteten Strukturen wurde schließlich vorausgesetzt, dass Ausfälle gemeinsamer Ursache auf ein angemessenes Niveau reduziert sind: Nur maximal 2 % der gefährlichen Ausfälle dürfen eine gemeinsame Ursache haben. Dies ist bei der Anwendung der Norm mit einem einfachen Schätzverfahren (Anhang F) jeweils zu belegen.

Die Markov-Modelle, die dem Säulendiagramm aus DIN EN ISO 13849-1 (bzw. Abbildung G.1 dieses Reports) zugrunde liegen, berücksichtigen den Betrieb der Systeme unter Randbedingungen, die für den Maschinenbereich realistisch sind. Sie gehen davon aus, dass die Systeme

- mindestens einer Anforderung der Sicherheitsfunktion pro Jahr ausgesetzt sind,
- sich bei selbsttätiger Erkennung eines internen Fehlers in den sicheren Zustand „Betriebshemmung“ versetzen und dann in der Regel kurz darauf (spätestens nach einigen Stunden) manuell abgeschaltet werden,

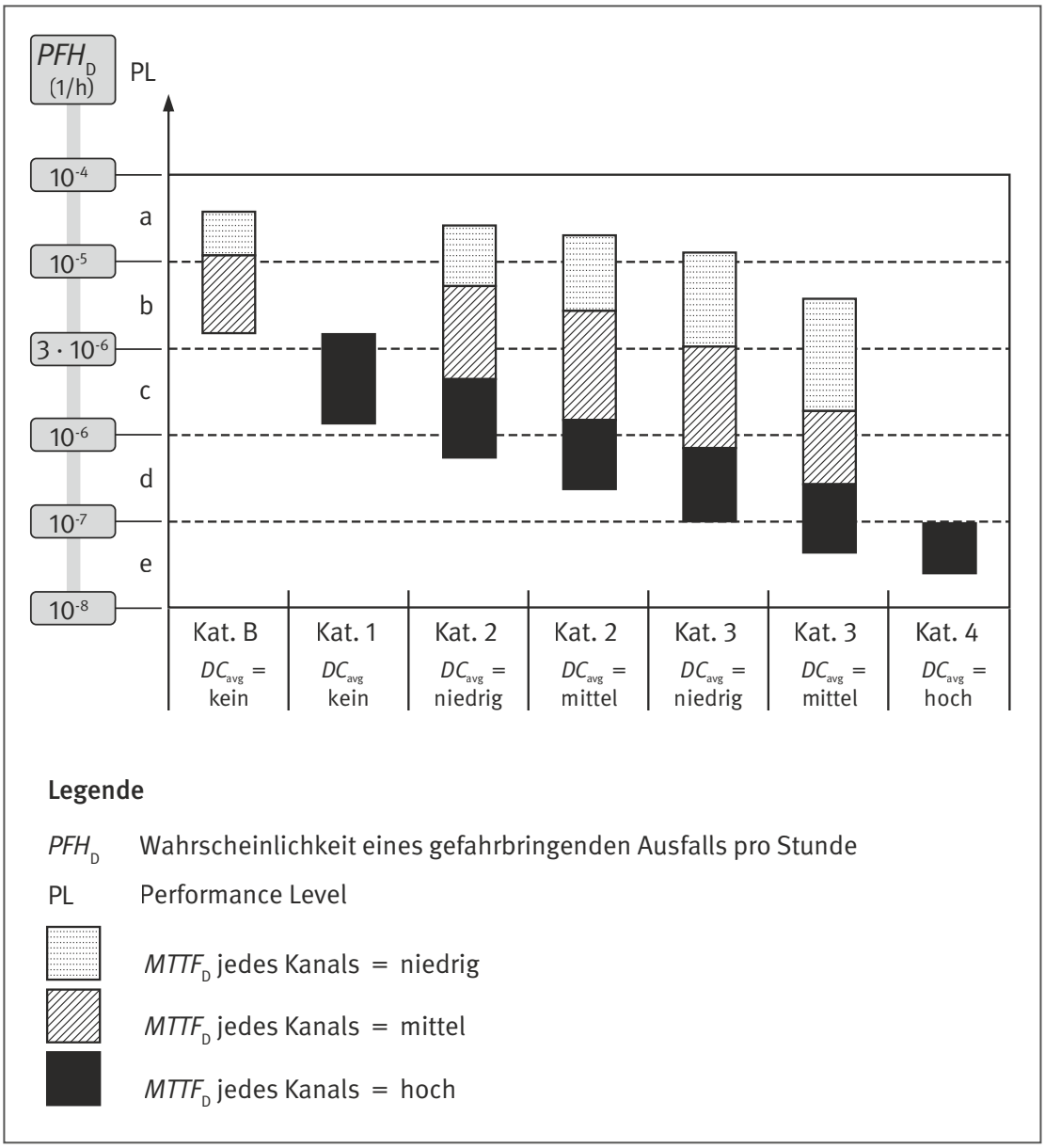


Abbildung G.1: PFH_D und Performance Level in Abhängigkeit von Kategorie, DC_{avg} und $MTTF_D$

- nach Eintritt der Betriebshemmung oder nach einem Unfall bzw. erkanntem gefährlichen Versagen repariert oder ersetzt und wieder in Betrieb genommen werden.

Unter diesen Randbedingungen stellt die quantitative Zielgröße der Modellierung, die PFH_D, die durchschnittliche Anzahl der ausfallbedingt nicht bedienten Anforderungen der Sicherheitsfunktion pro Stunde dar. Bei kontinuierlich vorliegender Anforderung (Continuous Mode of Operation) gibt sie die Anzahl der gefährlichen Systemausfälle pro Stunde an. Bei Kategorie 2 wird vorausgesetzt, dass die Testung vollständig wirksam ist. Dies kann durch ein adäquates Verhältnis von Test- und Anforderungsrate oder durch ausreichend schnelle Fehlerreaktion erreicht werden (vgl. Abschnitt 6.2.14). Da die so ermittelte PFH_D allein Zufallsausfälle berücksichtigt, nicht jedoch systematische Ausfälle und andere negative Effekte, ist sie als theoretische Leistungskenngröße anzusehen, welche die sicherheitstechnische Güte eines Designs bewertet, aber keine Aussagen etwa zur Unfallhäufigkeit gestattet. Diese PFH_D ist die mathematische Größe, die auf der vertikalen Achse des Säulendiagramms aufgetragen ist (vgl. Abbildung G.1).

Trotz der prinzipiellen Berücksichtigung von Anforderungen der Sicherheitsfunktion und der Reparatur wirken sich die absoluten Größen von Anforderungsrate und Reparaturrate (Kehrwert der mittleren Reparaturzeit) nur in vernachlässigbar kleinem Maß auf die so verstandene PFH_D aus. Lediglich bei der für Kategorie 2 vorgesehenen Architektur muss gefordert werden, dass die Testung sehr viel häufiger erfolgt als die Anforderung der Sicherheitsfunktion (Alternative: Die Testung erfolgt unmittelbar bei der Anforderung und die Zeiten für die Fehlererkennung und die sicherheitsgerichtete Reaktion sind zusammen kürzer als die spezifizierte Systemreaktionszeit, vgl. DIN EN ISO 13849-1, Abschnitt 4.5.4). Die Norm schlägt eine mindestens 100-mal größere Testrate im Vergleich zur Anforderungsrate vor. Aber selbst bis hinunter zu einem Verhältnis von 25 : 1 erhöht sich die PFH_D lediglich um ca. 10 %, was durch einen Korrekturfaktor von 1,1 berücksichtigt werden kann (vgl. Anmerkung 1 der Norm in Anhang K). Durch diese Ratenverhältnisse wird eine inakzeptabel große Wirkungseinbuße der Diagnose durch zu seltene Testausführung vermieden. Bei den Kategorien B, 1, 3 und 4 ist der Einfluss der Anforderungsrate auf die PFH_D vernachlässigbar gering. Die per Diagramm ermittelten PFH_D-Werte für diese

Kategorien B, 1, 3 und 4 gelten daher für beliebige Anforderungsraten und beliebige (mittlere) Reparaturzeiten. Bei weniger als einer Anforderung pro Jahr liefert das Säulendiagramm eine Abschätzung zur sicheren Seite. Bei den Kategorien 3 und 4 gelten die PFH_D-Werte für ausreichend große Testhäufigkeiten (siehe Erläuterungen in Abschnitt 6.2.14).

Soll die Gebrauchsdauer eines SRP/CS 20 Jahre überschreiten, so verlieren die nach dem vereinfachten Verfahren (Anhang K der Norm) ermittelten PFH_D-Werte in den meisten Fällen ihre Grundlage. Unter Umständen kann diese Situation mit wenigen Nachbesserungen trotzdem im Rahmen des vereinfachten Verfahrens behandelt werden. Dabei sind zwei Fälle zu unterscheiden:

- Im ersten Fall ist das SRP/CS von vornherein für eine Gebrauchsdauer größer als 20 Jahre spezifiziert. Dann kann der Einfluss der höheren Gebrauchsdauer aus den Markov-Modellen, die Anhang K der Norm zugrunde liegen, zur sicheren Seite hin folgendermaßen abgeschätzt werden: Pro fünf Jahre längere Gebrauchsdauer als 20 Jahre wird bei den Kategorien 2, 3 und 4 ein prozentualer PFH_D-Zuschlag von 15 % eingerechnet (Kategorie B oder 1 erfordern keine PFH_D-Anpassung). Es ist nicht sinnvoll, die Gebrauchsdauer über 30 Jahre hinaus zu vergrößern. Das vereinfachte Verfahren und SISTEMA sind also trotzdem nutzbar. Voraussetzung sind konstante Ausfallraten unabhängig von der Gebrauchsdauer. Für Verschleißbauteile bedeutet dies, dass diese für die spezifizierte höhere Gebrauchsdauer T_M ausgelegt werden müssen ($T_{10D} \geq T_M$) oder nach Ablauf von T_{10D} jeweils vorsorglich ausgetauscht werden müssen.

- Im zweiten Fall war das SRP/CS ausgelegt für 20 Jahre Gebrauchsdauer, soll aber nun darüber hinaus weiterverwendet werden. Dann kann die aus der Markov-Modellierung zu erwartende PFH_D-Verschlechterung mit einem wie im ersten Fall beschriebenen Zuschlag abgeschätzt werden. Kritisch wird es bei enthaltenen Verschleißbauteilen oder sich durch Alterung verschlechternden Bauteilen, zu denen typischerweise „chemische“ Bauteile (z. B. „nasse“ Elektrolytkondensatoren, Batterien, elektrochemische Sensoren), mechanische Bauteile (z. B. Bremse, Kupplung), elektromechanische Bauteile (z. B. Schalter, Relais, Schütze), fluidtechnische Bauteile (z. B. Ventile) und manche optische Bauteile (z. B. Optokoppler) gehören. Hier kann der Betreiber der Maschine in der Regel nicht selbst beurteilen, ob alle enthaltenen Bauteile auch für eine verlängerte Gebrauchsdauer ausgelegt sind oder welche Maßnahmen, z. B. vorsorglicher Austausch einzelner Bauteile, Proof-Test usw., in diesem Fall durchzuführen sind. Eine Verlängerung der Gebrauchsdauer – bei o. g. PFH_D-Zuschlag – kann dann nur erfolgen, wenn Herstellerangaben darüber vorliegen, was bei einer Verlängerung der Gebrauchsdauer zu tun ist, und wenn diese Maßnahmen vom Betreiber umgesetzt werden.

Die Säulen für Kategorie B und 1 in Abbildung G.1 wurden mithilfe eines Modells berechnet, das die Anforderung der Sicherheitsfunktion und die Reparatur berücksichtigt. Die PFH_D-Werte bei diesen Kategorien lassen sich aber auch sehr gut durch die einfache Beziehung $PFH_D \approx \lambda_D = 1/MTTF_D$ annähern. Dies bedeutet nichts anderes, als dass die PFH_D des einkanaligen ungetesteten Systems ($DC_{avg} = 0$) praktisch dessen Ausfallrate in die gefährliche Richtung entspricht.

Für die anderen Kategorien ist jedoch eine aufwendigere Rechenmethode erforderlich. Die prinzipielle Modellierungsweise wird im Folgenden beispielhaft an der „vorgesehenen Architektur“ für Kategorie 2 erläutert. Diese Struktur ist in Abbildung G.2 nochmals dargestellt. Es gibt fünf Funktionsblöcke, von denen die Blöcke I (Input), L (Logic) und O (Output) die eigentliche Sicherheitsfunktion in logischer Reihenschaltung ausführen. Der Block L testet die Blöcke I, O und sich selbst im Zusammenspiel mit dem Funktionsblock TE (Test Equipment). Der Funktionsblock OTE (Output of TE) kann bei Ausfall des

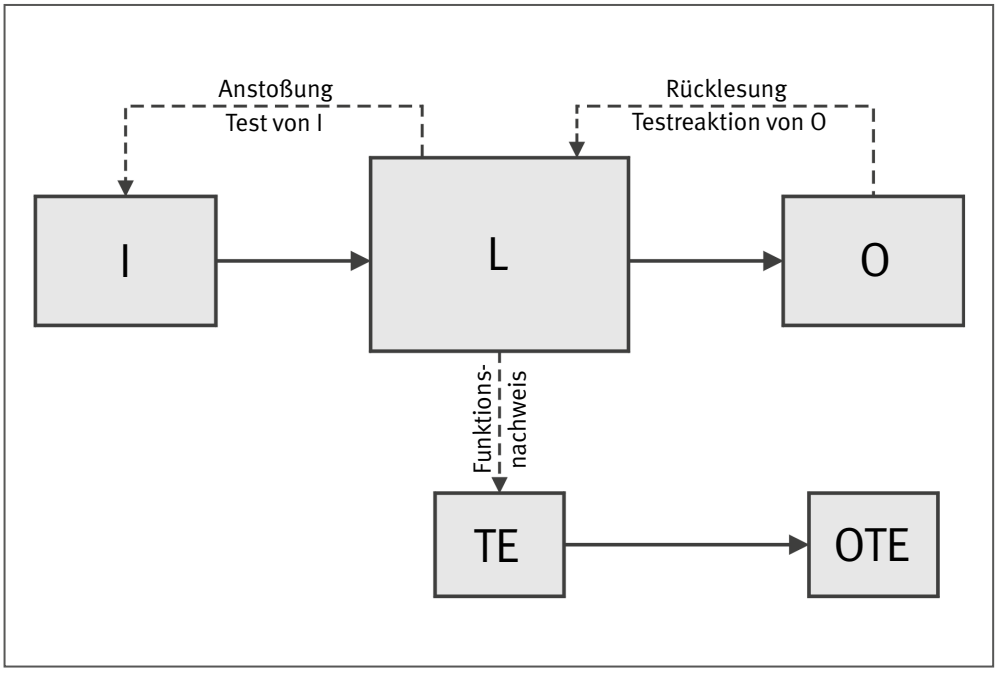


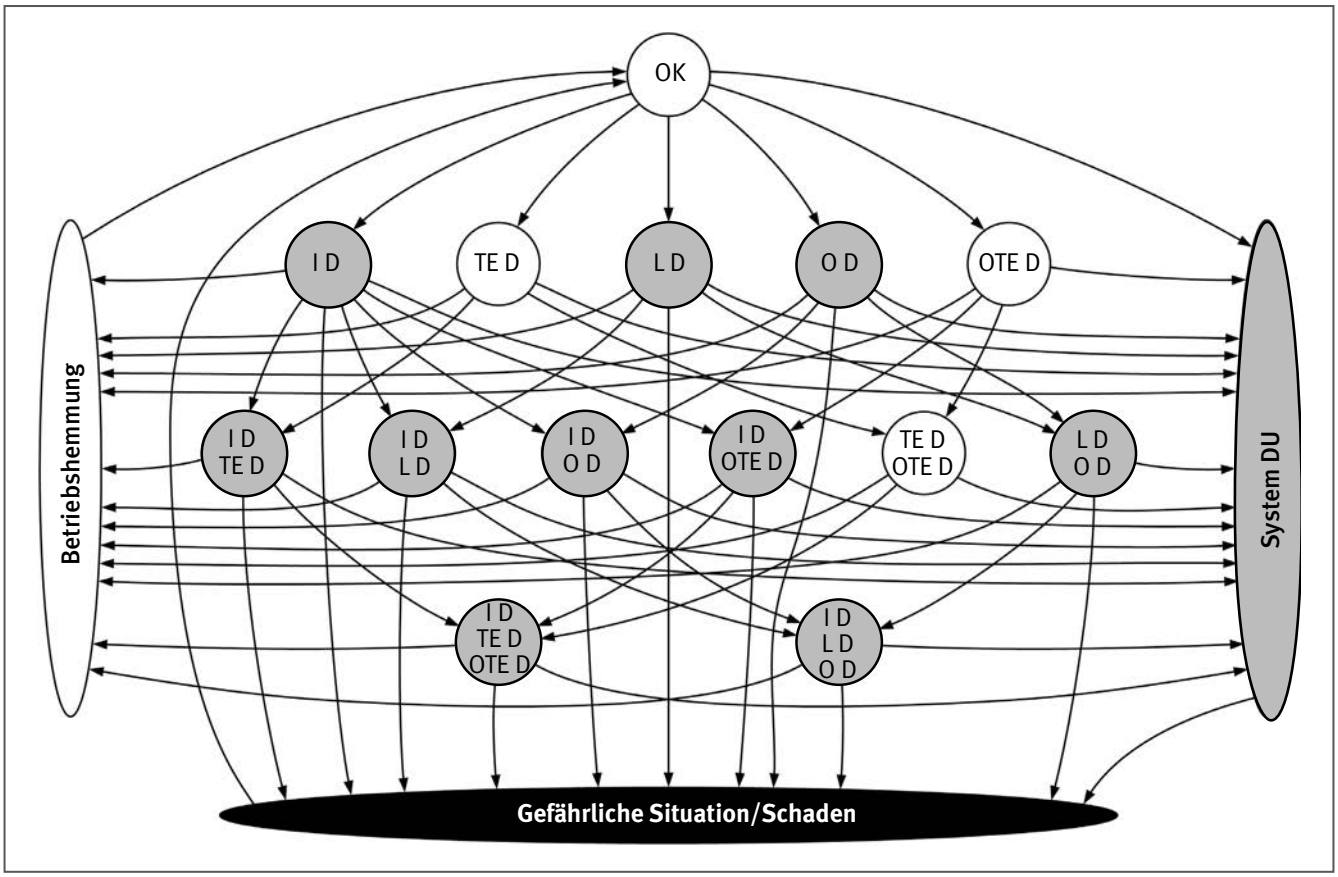
Abbildung G.2:
Vorgesehene Architektur für Kategorie 2 nach DIN EN ISO 13849-1, Abschnitt 6.2.5

Hauptkanals I-L-O einen sicheren Zustand herbeiführen. Die nicht direkt funktionsnotwendigen zusätzlichen Funktionsblöcke TE und OTE stellen somit eine Art Ersatzkanal für den Fehlerfall zur Verfügung, der jedoch – anders als ein „echter" zweiter Kanal – nur bei erkannten Ausfällen im Hauptkanal wirkt.

Aus dem sicherheitsbezogenen Blockdiagramm in Abbildung G.2 kann der Zustandsgraph in Abbildung G.3 abgeleitet werden. Dazu werden zunächst alle $2^5 = 32$ Ausfallkombinationen der fünf Funktionsblöcke gebildet. Der Zustand ohne Ausfall ist der oben abgebildete OK-Zustand. Darunter folgt eine Reihe von Zuständen mit nur einem ausgefallenen Funktionsblock, dann eine Reihe mit zwei ausgefallenen Blöcken usw. Die Zustandsbezeichnung benennt jeweils die ausgefallenen Funktionsblöcke mit einem nachgestellten „D" für „Dangerous", das den Ausfall des Blocks in dessen „gefährliche" (= sicherheitstechnisch ungünstige) Ausfallrichtung symbolisiert. Durch Ausfälle von Funktionsblöcken, abgebildet durch Pfeile, werden Folgezustände erreicht. Zustände, in denen das System die Sicherheitsfunktion nicht mehr ausführen kann, sind **grau** dargestellt. Wo immer eine Erkennung des Ausfalls möglich ist und als Folge sicherheitsgerichtet reagiert werden kann, gibt es einen Übergang in den links dargestellten Zustand „Betriebshemmung". Von den 32 Ausfallkombinationen sind zur Modellvereinfachung diejenigen zusammengefasst, in denen das System in gefährlicher Richtung und (für sich selbst) unerkennbar ausgefallen ist. Dieser Sammelzustand mit der Bezeichnung „System DU" (Dangerous Undetectable) ist rechts dargestellt. Er kann aus verschiedenen Zuständen durch den Ausfall von Funktionsblöcken erreicht werden. In Abbildung G.3 ist unten der Zustand „Gefährliche Situation/Schaden" zu sehen. In ihn gelangt das System nur aus gefährlichen (grau dargestellten) Vorzuständen, und zwar immer dann, wenn die Sicherheitsfunktion angefordert wird. Wie der Zustand „Betriebshemmung" so wird auch dieser Zustand durch Reparatur in Richtung OK-Zustand verlassen. Zusätzliche Übergangspfeile, z. B. von „OK" nach „System DU", ergeben sich durch gleichzeitige Ausfälle mehrerer Funktionsblöcke infolge einer gemeinsamen Ursache (Common Cause Failures, CCF). Es wird angenommen, dass bei 2 % der Ausfälle eines der Funktionsblöcke L und TE in gefährliche Richtung aufgrund derselben Ursache auch der jeweils andere Block gefährlich ausfällt. Dasselbe wird auch von den Funktionsblöcken O und OTE angenommen.

Allen Pfeilen sind Übergangsraten zugeordnet, deren Größe sich aus den jeweiligen Übergangsprozessen (Ausfällen, Tests, Anforderungen, Reparaturen) ergibt. Auch bewirkt die Berücksichtigung von Common Cause Failures (CCF) an verschiedenen Stellen eine Änderung der ursprünglichen Übergangsrate. Bei der Berechnung des Säulendiagramms wird der ungünstige Fall angenommen, dass die im System eingesetzte Testeinrichtung selbst nicht getestet wird. Darum wird einigen Übergängen in Abbildung G.3 die Rate Null zugewiesen. Systeme, die ihre Testeinrichtung testen, sind dadurch zur sicheren Seite abgeschätzt. Zur vereinfachten Berechnung nach der Markov-Methode wird angenommen, dass alle Übergangsprozesse durch exponentialverteilte Zustandsverweildauern gekenn-

Abbildung G.3:
Zustandsgraph des Markov-Modells zur vorgesehenen Architektur für Kategorie 2 für die Ermittlung der PFH_D



zeichnet sind, obwohl dies streng genommen nur für die Zufallsausfälle mit konstanter Rate gilt. Separate Betrachtungen rechtfertigen diese Vereinfachung.

Man geht davon aus, dass sich das System zu Beginn der Gebrauchszeit mit der Wahrscheinlichkeit 1 im OK-Zustand befindet und die Wahrscheinlichkeit aller anderen möglichen Systemzustände 0 beträgt. Während der angenommenen Gebrauchsdauer von 20 Jahren ändern sich alle Zustandswahrscheinlichkeiten allmählich: Ausgehend vom OK-Zustand verteilen sie sich entlang der Übergangspfeile um. Die Summe der Zustandswahrscheinlichkeiten bleibt konstant 1. Dabei ergibt sich auch ein zeitabhängiger Zufluss in den Zustand „Gefährliche Situation/Schaden“, dessen zeitlicher Mittelwert während der 20-jährigen Gebrauchsdauer die PFH_D darstellt, d. h. die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Systems je Stunde.

Diese PFH_D ist auf der vertikalen Achse des Säulendiagramms für die verschiedenen „vorgesehenen Architekturen“ nach Abschnitt 6.2 der Norm (vgl. Abschnitte 6.2.3 bis 6.2.7 dieses Reports) aufgetragen, wobei die Kategorien 2 und 3 noch nach dem durchschnittlichen Diagnosedeckungsgrad (DC_{avg}) unterteilt wurden. Die Säulen entstehen, indem für eine Kombination aus Architektur (bzw. dem zugeordneten Markov-Modell) und DC_{avg} die $MTTF_D$, d. h. die mittlere Zeit bis zum Ausfall des (bzw. eines) Funktionskanals in dessen gefährliche Richtung, variiert wird. So können beispielsweise mit dem Markov-Modell in Abbildung G.3 die beiden Säulen für die vorgesehene Kategorie-2-Architektur berechnet werden. (Tatsächlich wurde aus rechentechnischen Gründen ein hiervon abweichendes äquivalentes Ersatzmodell benutzt, das hier nicht dargestellt wird, weil sein Zusammenhang mit dem Blockbild von Abbildung G.2 weniger leicht einsichtig ist. Das Ersatzmodell liefert praktisch identische Ergebnisse.) Die übrigen Säulen basieren auf weiteren Markov-Modellen, die für die entsprechenden vorgesehenen Architekturen ebenfalls nach den oben beschriebenen Prinzipien entwickelt wurden.

Gemäß Tabelle 6.1 wurden den PFH_D-Intervallen auf der logarithmisch geteilten PFH_D-Skala die Performance Levels a bis e zugewiesen. Dies ist in Abbildung G.1 gezeigt, in der Bild 5 der Norm DIN EN ISO 13849-1 um eine zusätzliche PFH_D-Skala ergänzt wurde.

Eine Besonderheit gibt es beim PFH_D-Intervall von 10^{-6}/h bis 10^{-5}/h. Es ist auf die beiden benachbarten Performance Levels b und c abgebildet. Durch die mittige Teilung der logarithmischen Skala liegt die Grenze zwischen Performance Level b und Performance Level c beim geometrischen Mittelwert von 10^{-6}/h und 10^{-5}/h, d. h. bei $\sqrt{10} \cdot 10^{-6}/h \approx 3 \cdot 10^{-6}/h$. Die Zuordnung von PFH_D-Intervallen und Performance Level deckt sich im Wesentlichen mit DIN EN 61508-1, Tabelle 3, und DIN EN 61508-5, Bild E.2 (siehe [3; 4]).

In Anhang K der Norm ist der Inhalt von Abbildung G.1 in Form von Tabelle K.1 numerisch wiedergegeben. Mithilfe von Tabelle K.1 kann der Performance Level präziser ermittelt werden als mit der Abbildung, was insbesondere dann nützlich ist, wenn PFH_D-Beiträge von mehreren kaskadierten Teilsystemen aufsummiert werden müssen. Hingegen bietet das Säulendiagramm vor allem eine schnelle Übersicht über die PL-Tauglichkeit verschiedener technischer Lösungswege und kann somit bei deren Vorauswahl helfen. Die Informationen aus Tabelle K.1 der Norm sind auch in dem „Performance Level Calculator“ (PLC) enthalten, einer handlichen Drehscheibe aus Karton zur PL-Bestimmung, die beim IFA erhältlich ist [5].

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. Wird dann das vereinfachte Quantifizierungsverfahren aus DIN EN ISO 13849-1 angewendet, muss rein formal jeweils mit der nächstkleineren 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 deutlich schlechteren Bewertung 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 (vgl. DC_{avg}-Formel z. B. in Abschnitt 6.2.14). Die kleine Verbesserung der Kanal-$MTTF_D$ wird dann durch die formal vollzogene Herabstufung von DC_{avg} auf die nächstkleinere Stufe überkompensiert, wodurch die ermittelte PFH_D 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 Norm (vgl. Abbildung G.1 dieses Reports).

Der beschriebene Effekt kann verhindert oder gemildert werden, indem anstelle von Abbildung G.1 eine Grafik mit feinerer Abstufung der DC_{avg}-Werte benutzt wird (Abbildung G.4, siehe Seite 282). Mit Rücksicht auf die begrenzte Genauigkeit von DC_{avg}-Werten (vgl. DIN EN ISO 13849-1, Tabelle 5, Anmerkung 2) wurden für alle Kategorien auch die minimal möglichen DC_{avg}-Werte berücksichtigt. Zur PFH_D-Bestimmung bietet sich der IFA-Softwareassistent „SISTEMA“ an (siehe Anhang H). Er interpoliert sogar zwischen den in Abbildung G.4 gezeigten Säulen. Generell kann dadurch eine starke Herabstufung von DC_{avg} vermieden und oft ein genauerer und zugleich besserer PFH_D-Wert ermittelt werden.

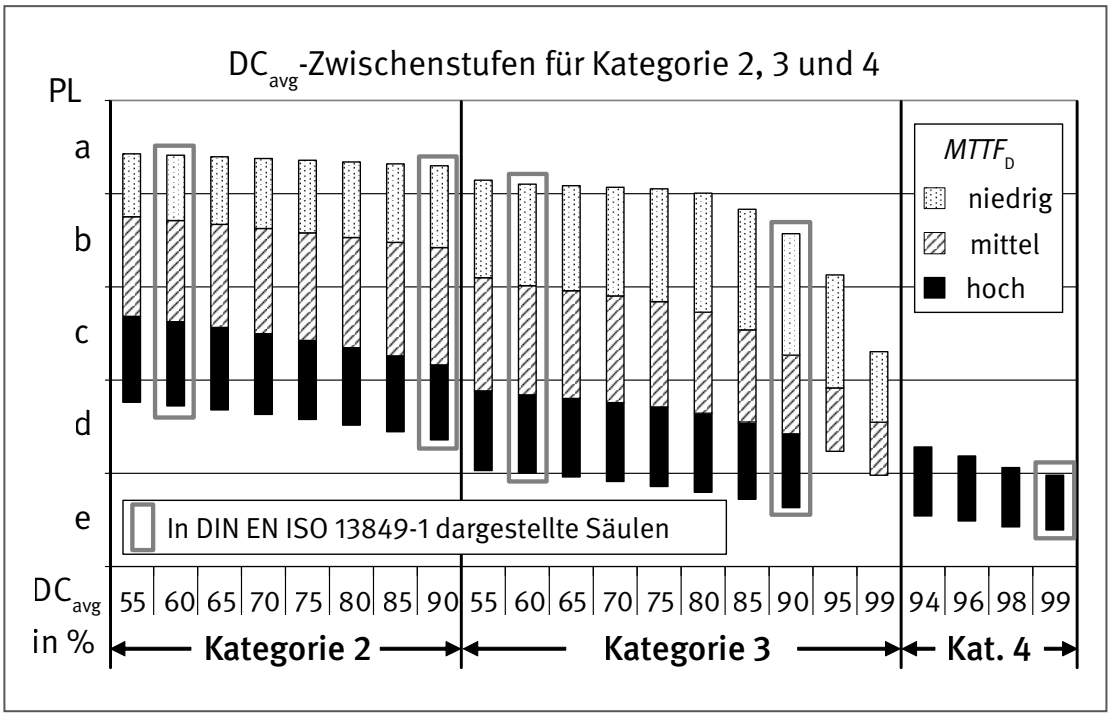


Abbildung G.4: Performance Level bei feinstufigerer Auflösung der DC_{avg}-Skala (Erweiterung von Bild 5 aus DIN EN ISO 13849-1)

Literatur

[1] DIN EN 954-1: Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (03.97). Beuth, Berlin 1997

[2] *Goble, W. M.:* Control systems safety evaluation and reliability. 3rd ed. Hrsg.: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010

[3] DIN EN 61508-1: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010) (02.11). Beuth, Berlin 2011

[4] DIN EN 61508-5: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010) (02.11). Beuth, Berlin 2011

[5] *Schaefer, M.; Hauke, M.:* Performance Level Calculator – PLC. 5. Aufl. Hrsg.: Institut für Arbeitsschutz (IFA) der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V. – Fachverband Automation, Frankfurt am Main, und Verband Deutscher Maschinen- und Anlagenbau e. V. – VDMA, Frankfurt am Main 2015
▸ www.dguv.de/webcode/d3508

Anhang H:
SISTEMA – Der Softwareassistent zur Bewertung von SRP/CS

H.1 Was kann SISTEMA?

Mit dem Software-Assistenten SISTEMA (Sicherheit von Steuerungen an Maschinen) steht zur Entwicklung und Prüfung 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 die Möglichkeit, die Struktur der sicherheitsbezogenen Steuerungsteile auf der Basis der sogenannten vorgesehenen Architekturen nachzubilden und erlaubt schließlich eine automatisierte Berechnung der Zuverlässigkeitswerte auf verschiedenen Detailebenen einschließlich des erreichten Performance Levels (PL) und der Ausfallwahrscheinlichkeit PFH_D.

Über Eingabemasken werden relevante Parameter wie Risikoparameter zur Bestimmung des erforderlichen Performance Levels (PL_r), die Kategorie des SRP/CS, die Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) bei mehrkanaligen Systemen, die mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$) und der Diagnosedeckungsgrad (DC) von Bauelementen bzw. Blöcken Schritt für Schritt erfasst. Nachdem die geforderten Daten in SISTEMA eingetragen wurden, sind die berechneten Ergebnisse praktischerweise sogleich sichtbar: Jede Parameteränderung wird in ihrer Auswirkung auf das Gesamtsystem über die Programmoberfläche direkt angezeigt. Das umständliche Nachschlagen in Tabellen und Berechnen nach Formeln (Bestimmung der $MTTF_D$ nach dem „Parts Count"-Verfahren, Symmetrisierung der $MTTF_D$ für jeden Kanal, Abschätzung des DC_{avg}, Ermittlung von PFH_D und PL etc.) wird durch die Software übernommen und entfällt daher weitestgehend. Dies ermöglicht es, ohne großen Aufwand probeweise Parameterwerte zu variieren, um so die Auswirkungen von Änderungen zu beurteilen. Die Resultate werden schließlich in einem druckbaren Report zusammengefasst.

H.2 Wie wird SISTEMA verwendet?

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

Man eröffnet zunächst ein Projekt und kann darin die Maschine bzw. die Gefahrenstelle, die weiter betrachtet werden soll, definieren. Dem Projekt werden danach Sicherheitsfunktionen zugewiesen. Diese können festgelegt und dokumentiert sowie mit einem PL_r belegt werden. Der tatsächlich erreichte PL des parametrierten SRP/CS wird automatisch aus den Subsystemen ermittelt, die – in Serie geschaltet – die Sicherheitsfunktion ausführen. Den Subsystemen liegt jeweils – in Abhängigkeit von der gewählten Kategorie – eine sogenannte 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 entweder direkt ein $MTTF_D$-Wert und ein DC-Wert eingetragen wird, oder aber auf der niedrigsten Hierarchieebene die Werte für die einzelnen Elemente eingetragen werden, aus denen sich der Block zusammensetzt.

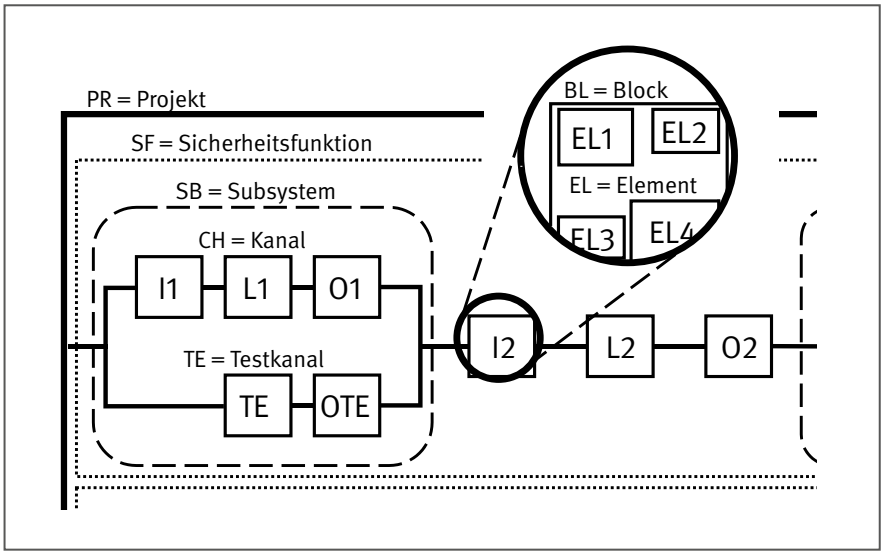


Abbildung H.1:
In SISTEMA betrachtete Hierarchieebenen

Weiterhin runden komfortable Bibliotheksfunktionen den Leistungsumfang von SISTEMA ab. Viele Hersteller von Komponenten und Bauteilen bieten Bibliotheken mit Daten ihrer Produkte an. Auf den Internetseiten des IFA sind Links zu diesen Bibliotheken gelistet (www.dguv.de/ifa, Webcode: d92599). Man kann aber auch eigene Bibliotheken erstellen, in denen selbst entwickelte Subsysteme oder häufig verwendete Bauteile abspeichert werden können. Bibliotheken können lokal, aber auch zentral auf Servern abgelegt sein.

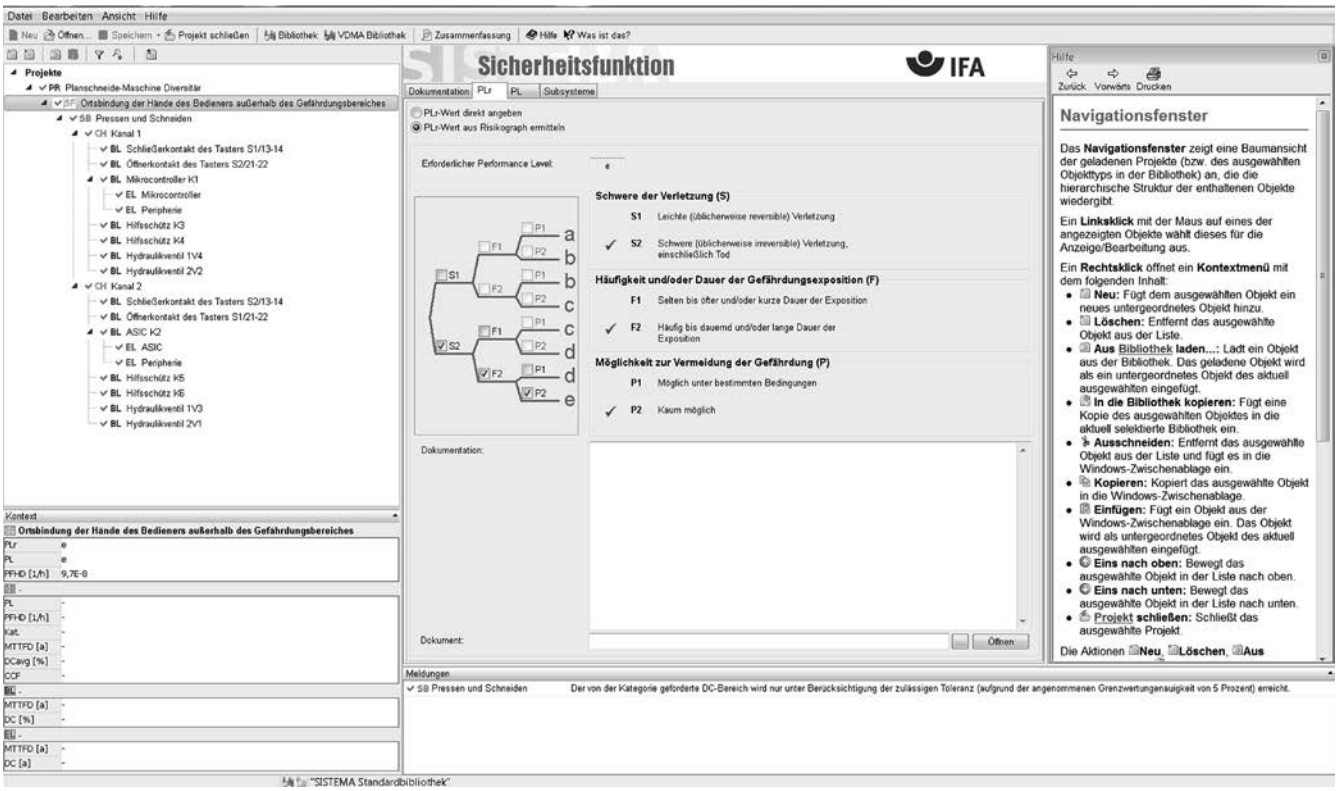
H.3 Die Benutzerschnittstelle von SISTEMA

Die Programmoberfläche von SISTEMA gliedert sich in vier Bereiche (siehe Abbildung H.2). Den größten Anteil der Fläche nimmt der Arbeitsbereich in der Mitte ein. Er enthält je nach aktiver Sicht eine editierbare Eingabemaske oder einen Abschnitt aus dem Übersichtsdokument. Der Inhalt der jeweiligen Sicht ist durch das ausgewählte Grundelement aus der weiter oben genannten Hierarchie 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. Wird beispielsweise ein 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 neben der Verzweigung. Ein rotes Kreuz 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. Ein gelber Punkt bedeutet, dass ein Hinweis vorliegt – z. B. wenn ein Grundelement noch unbenannt ist. Alle anderen Grundelemente werden mit grünem Häkchen 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_D, $MTTF_D$, DC_{avg} und CCF-Punktezahl des übergeordneten Subsystems sowie PL_r, PL und PFH_D der übergeordneten Sicherheitsfunktion (das gilt natürlich nur für Grundelemente, die in tieferen Hierarchieebenen liegen). So ist laufend sichtbar, wie sich Änderungen in den angezeigten Parametern bemerkbar machen.

Abbildung H.2:
Programmoberfläche von SISTEMA



Neben ihrer Flexibilität zeichnet sich die Programmoberfläche von SISTEMA durch eine komfortable und intuitive Bedienbarkeit aus. Kontextspezifische Hilfetexte auf der rechten Seite sollen den Einstieg erleichtern.

H.4 Wo ist SISTEMA zu erhalten?

Das Programm SISTEMA kann nach Registrierung kostenlos unter der Internetadresse www.dguv.de/ifa über den Webcode d11223 heruntergeladen werden. Die Weitergabe an Dritte ist erlaubt. Eine Veränderung von SISTEMA ist aber nicht gestattet. SISTEMA enthält folgende Sprachversionen: Deutsch, Englisch, Französisch, Italienisch, Spanisch und Finnisch. Weitere Sprachversionen (z. B. Japanisch) werden folgen. Anleitungen zur Benutzung von SISTEMA bieten die SISTEMA-Kochbücher (Webcode d109240) sowie die installierte Hilfedatei. Informationen und Hilfen zur DIN EN ISO 13849-1 finden Sie über den Webcode d18471 sowie über die Internetadresse www.dguv.de/ifa/13849.

Anhang I: Sicherheitsfunktion Betriebsartenwahl

I.1 Einleitung

In der Regel erfordert die Arbeit an einer Maschine neben dem automatisch ablaufenden Betrieb auch manuelle Eingriffe in den Gefahrenbereich. Da solche Eingriffe – wie sie etwa für das Einrichten, die Störungsbeseitigung oder die Reinigung notwendig werden können – meist mit einem erhöhten Risiko einhergehen, kommen je nach durchzuführender Tätigkeit unterschiedliche Betriebsarten zum Einsatz.

Mit der Anwahl einer Betriebsart werden an der Maschine Sicherheitsfunktionen aktiviert, die das jeweils vorherrschende Risiko auf ein akzeptables Maß mindern. Sicherheitstechnisch ist eine Betriebsart somit dadurch definiert, welche Sicherheitsfunktionen mit ihrer Anwahl aktiviert und welche deaktiviert werden. Fehler in der Betriebsartenwahl können dazu führen, dass erforderliche Sicherheitsfunktionen nicht aktiviert werden: Wird statt der angewählten Betriebsart eine andere aktiviert, so sind statt der für die geplante Tätigkeit erforderlichen Sicherheitsfunktionen andere Sicherheitsfunktionen aktiv. Im Extremfall kann ein Fehler in der Betriebsartenwahl sogar dazu führen, dass gar keine Sicherheitsfunktionen aktiv sind. Die mit beiden Fällen einhergehende Erhöhung des Risikos macht eine sicherheitstechnische Bewertung der Betriebsartenwahl notwendig.

Üblicherweise wird die Betriebsartenwahl durch elektromechanische Wahlschalter realisiert. Die Maschinenrichtlinie [1] macht hierzu eine Reihe von Vorgaben. So muss

- für die Betriebsartenwahl ein in jeder Stellung abschließbarer Wahlschalter vorhanden sein,
- die Aktivierung einer Betriebsart eindeutig sein (d. h. jede Stellung des Wahlschalters darf nur einer Betriebsart entsprechen) und
- die angewählte Betriebsart für die Bedienperson eindeutig erkennbar sein (z. B. anhand der Stellung des Wahlschalters).

Die Maschinenrichtlinie erlaubt, in der Anwendung den Wahlschalter durch eine andere Wahleinrichtung zu ersetzen, die die Nutzung bestimmter Maschinenfunktionen auf ausgewählte Personenkreise einschränken kann. Eine Verwendung elektronischer Betriebsmittel ist dabei nicht ausgeschlossen. Jedoch muss durch die eingesetzten sicherheitsrelevanten Stromkreise und Bauteile sowie die evtl. verwendete Software eine dem elektromechanischen Betriebsartenwahlschalter vergleichbare Sicherheit erreicht werden.

Da ein Fehler in der Betriebsartenwahl zu einer unmittelbaren Erhöhung des Risikos führen kann, ist die Betriebsartenwahl als sicherheitsrelevante Funktion zu betrachten. Als solche ist sie auch in Tabelle 8 der Norm aufgeführt. Es stellt sich die Frage, ob deren steuerungstechnischer Anteil zu jeder an der Maschine realisierten Sicherheitsfunktion gehört oder ob die Betriebsartenwahl als eine eigenständige Sicherheitsfunktion betrachtet werden kann. Analog zu der in Abschnitt 5.3.2 beschriebenen Vorgehensweise, bei der überlagerte Gefährdungen in einem Gefährdungsbereich in Gefährdungen durch einzelne Maschinenteile aufgeteilt werden können, bietet es sich an, auch die Betriebsartenwahl als eigene Sicherheitsfunktion zu behandeln. Damit wird auch vermieden, dass die zur Realisierung der Betriebsartenwahl verwendeten Bauteile in jeder einzelnen Sicherheitsfunktion zusätzlich die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH_D) erhöhen.

Wie zu Beginn erläutert, ist eine Betriebsart sicherheitstechnisch dadurch charakterisiert, welche Sicherheitsfunktionen durch ihre Anwahl aktiviert werden. Entsprechend lässt sich die Sicherheitsfunktion Betriebsartenwahl wie folgt definieren: Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen.

Es ist nun zu klären, wie der erforderliche Performance Level PL_r der Betriebsartenwahl anzusetzen ist. In manchen Fällen wird der PL_r der Betriebsartenwahl durch die verwendete Produktnorm bereits angegeben. Wo dies nicht der Fall ist, ist es folgerichtig, hier den höchsten PL_r aller an der Maschine aktivierbaren Sicherheitsfunktionen anzusetzen. Diese Regel ergibt sich aus der Tatsache, dass ein Versagen der Betriebsartenwahl dazu führen kann, dass erforderliche Sicherheitsfunktionen nicht aktiviert werden oder – im schlimmsten Fall, wenn die Betriebsartenwahl gänzlich versagt – die Maschine unbemerkt ohne jegliche Sicherheitsfunktion betrieben wird. Dies könnte z. B. an Werkzeugmaschinen beim Wechsel aus der Betriebsart „Einrichtbetrieb“ in die Betriebsart „Prozessbeobachtung“ zu einem inakzeptablen Anstieg des Risikos führen.

Mit Betrachtung der Betriebsartenwahl als Sicherheitsfunktion im Sinne der DIN EN ISO 13849-1 wird die Norm auch für die Bewertung der verwendeten Steuerungstechnik relevant. Hier können je nach den verwendeten Bauteilen unter Umständen Fehlerausschlüsse geltend gemacht werden. Dieses Vorgehen soll im Folgenden für übliche Bedienelemente zur Betriebsartenwahl gezeigt werden. Weitere Hinweise zur Betriebsartenwahl als Sicherheitsfunktion finden sich in Abschnitt 4.1 von [2].

I.2 Nockenbetätigte Wahlschalter

Für Schalter mit zwangsöffnenden Kontaktelementen nach DIN EN 60947-5-1 [3], Anhang K kann für das Nichtöffnen von Kontakten ein Fehlerausschluss gemäß Tabelle D.8 der DIN EN ISO 13849-2 [4] vorgenommen werden. Diese Schalter gelten auch als bewährte Bauteile, daher ist mit ihrem Einsatz eine Einstufung der Sicherheitsfunktion in Kategorie 1 nach der Norm möglich.

Sind bei Schaltern mit zwangsöffnenden Kontaktelementen zusätzlich die Fehlerausschlüsse für den Kurzschluss von benachbarten isolierten Kontakten und den gleichzeitigen Kurzschluss zwischen den drei Klemmen von Wechselkontakten gemäß Tabelle D.8 der DIN EN ISO 13849-2 möglich, müssen diese Bauteilfehler nicht angenommen werden. So ist bei einer elektrisch zweikanaligen Schaltung durch Fehlerausschluss in der einkanaligen Mechanik eine Modellierung als Kategorie-3-Subsystem und eine Realisierung bis Performance Level PL d möglich (siehe hierzu auch Beispiel 8 im IFA Report 7/2013 [2], Seite 70 ff.).

Für PL e können Fehlerausschlüsse nicht geltend gemacht werden. Hier sind zusätzliche Maßnahmen erforderlich. Zum Beispiel ist es möglich, die angewählte Betriebsart nach Anzeige über eine Benutzerschnittstelle durch die Bedienperson der Maschine bestätigen zu lassen. Gleichzeitig ist durch ein Aktivierungssystem (siehe Abschnitt I.3) in der sicherheitsgerichteten Steuerung in PL e sicherzustellen, dass auf der Maschine niemals mehr, aber auch nicht weniger als eine Betriebsart angewählt ist.

I.3 Elektronische Betriebsmittel

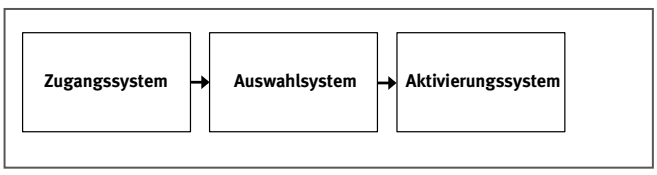
Bei elektronischen Betriebsmitteln ist ein Fehlerausschluss nicht möglich. Für die Fehlerbetrachtung der Betriebsartenwahl über elektronische Betriebsmittel ist daher eine weitere Analyse notwendig.

Hierfür ist zunächst herauszustellen, welche Funktionen der Betriebsartenwahl durch die Wahleinrichtung abgebildet werden müssen. Es ergeben sich folgende Teilfunktionen:

1. Zugang zur Betriebsartenwahl
2. Auswahl der Betriebsart
3. Aktivierung der Betriebsart

Bei einer mit elektronischen Betriebsmitteln realisierten Wahleinrichtung können die genannten Teilfunktionen in drei Teilsystemen (Abbildung I.1) realisiert werden [5]:

Abbildung I.1:
Struktur der Betriebsartenwahl



Zugangssystem

Das Zugangssystem ist der Teil der Wahleinrichtung, der die Möglichkeit zur Betriebsartenwahl auf bestimmte Personengruppen einschränkt und eine versehentliche oder missbräuchliche Betätigung des Auswahlsystems verhindert. Da die Anwahl jeder Betriebsart mit der Aktivierung anderer Sicherheitsfunktionen einhergeht, wird das Zugangssystem als sicherheitsrelevant betrachtet.

Bei elektromechanischen Wahleinrichtungen wird der Zugang durch den Schlüssel realisiert. Hier kann durch eine mechanische Codierung des Schlüssels die Anwahl nur bestimmter Betriebsarten freigegeben werden. Hinzu kommen organisatorische Maßnahmen, die den Zugriff auf den oder die Schlüssel auf bestimmte Personenkreise einschränken sollen.

Bei elektronischen Wahleinrichtungen kann der Zugang beispielsweise über RFID-Schlüssel (RFID: Radio-frequency identification) oder Passwörter und entsprechende organisatorische Maßnahmen realisiert werden. Für die sicherheitstechnische Betrachtung ist zu bewerten, ob im Hinblick auf die Zugangsbeschränkung eine vergleichbare Sicherheit wie durch einen Schlüssel bei elektromechanischen Wahleinrichtungen besteht (Integrität der Zugangsdaten, Codierung, Kopierschutz, organisatorische Maßnahmen usw.). Eine Berücksichtigung des Zugangssystems bei der Bestimmung der Ausfallwahrscheinlichkeit der Sicherheitsfunktion ist daher nicht erforderlich.

Auswahlsystem

Das Auswahlsystem legt die Betriebsart fest, die durch das Aktivierungssystem in der Steuerung aktiviert werden soll (siehe unten).

Bei elektromechanischen Wahleinrichtungen entspricht das Auswahlsystem dem handbetätigten Schaltknopf, dessen Stellung z. B. über eine Achse und Nockenscheiben mechanisch auf die elektrischen Kontaktelemente übertragen wird. Hier ist, wie oben beschrieben, durch Fehlerausschluss eine sicherheitstechnische Realisierung bis PL d unter Einbeziehung zusätzlicher Maßnahmen bis PL e möglich.

Bei elektronischen Wahleinrichtungen wird das Auswahlsystem in der Regel über eine Benutzerschnittstelle (Human Machine Interface, HMI) realisiert, beispielsweise über Touchpad oder Folientastatur. Über die Benutzerschnittstelle und eventuell weitere elektronische Komponenten legt die Bedienperson die in der Maschinensteuerung zu aktivierende Betriebsart fest. Da hier in der Regel Standardkomponenten zum Einsatz kommen, ist eine Einstufung eines in dieser Art realisierten Auswahlsystems in PL c oder höher nicht ohne Weiteres möglich. Eine Möglichkeit, hier dennoch die erforderliche Sicherheit zu erreichen, bietet Abschnitt 4.6.4 der Norm, in dem Vorgaben zur softwarebasierten Parametrisierung genannt werden. Da die Betriebsartenwahl über ein elektronisches Auswahlsystem einer softwarebasierten Parametrisierung gleichkommt, kann der genannte Abschnitt der Norm für die sicherheitstechnische Bewertung dieses Auswahlsystems herangezogen werden. Das dort beschriebene Verfahren umfasst die Auswahl der Betriebsart durch die Bedienperson, die Prüfung der ausgewählten

Betriebsart in der sicheren Steuerung sowie die Bestätigung der ausgewählten Betriebsart durch die Bedienperson. Dadurch wird sichergestellt, dass die Integrität der für die Parametrisierung verwendeten Daten entlang der gesamten Kommunikationskette aufrechterhalten bleibt und Verfälschungen erkannt werden. Insbesondere wird vermieden, dass ein Fehler in einer der Komponenten der Wahleinrichtung zur Anwahl oder Bestätigung einer falschen Betriebsart führen kann.

Aktivierungssystem

Auf dem Aktivierungssystem wird die eigentliche Sicherheitsfunktion Betriebsartenwahl, d. h. die Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen ausgeführt. Bei Verwendung elektronischer Wahleinrichtungen geht nur das Aktivierungssystem in die Quantifizierung der Betriebsartenwahl ein, wenn das Auswahlsystem – wie oben beschrieben – nach den Anforderungen der softwarebasierten Parametrisierung bewertet wird.

Für das Aktivierungssystem wird in Abhängigkeit von den hierfür verwendeten steuerungstechnischen Komponenten eine PFH_D ermittelt, die mindestens zu dem erforderlichen Performance Level PL_r der Sicherheitsfunktion Betriebsartenwahl führen muss.

Im Folgenden soll die Betriebsartenwahl über elektronische Wahleinrichtungen anhand eines Beispiels (Abbildung I.2) weiter erläutert werden.

I.4 Betriebsartenwahl mit einem elektronischen Schlüsselsystem als Zugangssystem – PL e

I.4.1 Sicherheitsfunktion

Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen.

I.4.2 Struktur

Im Beispiel wird das Zugangssystem durch ein elektronisches Schlüsselsystem gebildet. Auf dem elektronischen Schlüssel ist die jeweilige individuelle Berechtigungsstufe für den Zugang gespeichert.

Das Auswahlsystem besteht aus drei Komponenten: einem HMI mit Touchscreen zur Anzeige und Auswahl der je nach Berechtigungsstufe wählbaren Betriebsarten, einer Sicherheits-SPS zur Prüfung der Berechtigungsstufe und der angewählten Betriebsart sowie einer Standard-SPS zur Kommunikation zwischen den Komponenten.

Das Aktivierungssystem wird durch die Sicherheits-SPS gebildet. Diese setzt die Umschaltung der Betriebsart und so die Aktivierung der für die Betriebsart erforderlichen Sicherheitsfunktionen um. Zusätzlich stellt die Sicherheits-SPS sicher, dass immer eine Betriebsart und die dazugehörigen Sicherheitsfunktionen aktiv sind.

I.4.3 Funktionsbeschreibung

Schlüsselsystem/Standard-SPS

Bei Stecken eines Schlüssels in das Lesegerät wird die Berechtigungsstufe ausgelesen. Die Berechtigungsstufe legt in Abhängigkeit von der fachlichen Qualifikation der Bedienperson fest, zur Anwahl welcher Betriebsarten diese berechtigt sein soll. Das Lesegerät ist über eine Datenschnittstelle mit der Standard-SPS verbunden. Über die Datenschnittstelle wird nach dem Auslesen der Schlüsseldaten die Berechtigungsstufe an das HMI (a) und die Sicherheits-SPS (b) gesendet.

Zusätzlich zur Datenschnittstelle verfügt das Lesegerät über einen Relaisausgang, der abgeschaltet ist, solange sich kein Schlüssel in der Schlüsselaufnahme befindet oder die Schlüsseldaten nicht ausgelesen werden können. Der Relaisausgang

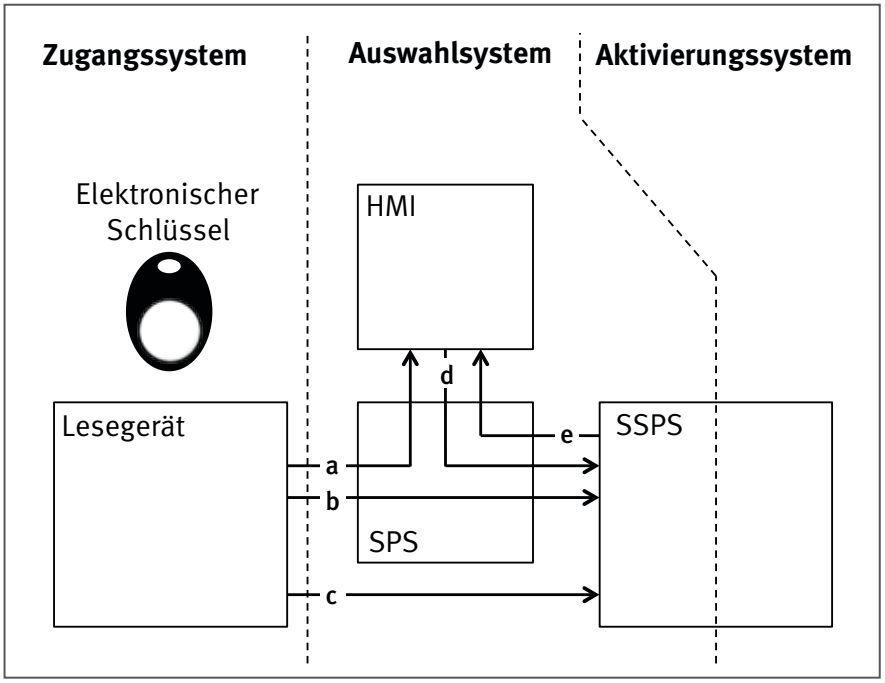


Abbildung I.2:
Beispiel Betriebsartenwahl mit einem elektronischen Schlüsselsystem als Zugangssystem; HMI: Human Machine Interface, SPS: Speicherprogrammierbare Steuerung (Standard), SSPS: Sicherheits-SPS, a bis e: Informationsfluss (siehe Funktionsbeschreibung)

ist mit einem sicheren Eingang der Sicherheits-SPS verbunden (c).

HMI

Auf dem HMI werden in Abhängigkeit von der Berechtigungsstufe die Betriebsarten angezeigt, zu deren Auswahl der Schlüssel berechtigt. Nach Auswahl einer Betriebsart wird diese über die Standard-SPS an die Sicherheits-SPS übermittelt (d). Die Sicherheits-SPS sendet auf gleichem Wege eine Rückmeldung über die gespeicherte Betriebsart an das HMI zurück, wo sie von der Bedienperson quittiert werden muss.

Sicherheits-SPS

Sobald nach Stecken des Schlüssels auf dem sicheren Eingang der Sicherheits-SPS ein Signalwechsel erfolgt, wird in der Sicherheits-SPS ein Verfahren gestartet, an dessen Ende die angewählte Betriebsart aktiviert wird. Das Verfahren umfasst folgende Einzelschritte:

1. Die auf dem Schlüssel gespeicherte Berechtigungsstufe wird auf Gültigkeit geprüft.

2. Die auf dem HMI angewählte Betriebsart wird daraufhin überprüft, ob sie einer gültigen Betriebsart entspricht und die Bedienperson auf der Basis der Berechtigungsstufe zu deren Anwahl berechtigt ist.

3. Die Betriebsart wird an das HMI zur Quittierung zurückgegeben (e).

4. Nach Quittierung der Betriebsart wird überprüft, ob die quittierte Betriebsart mit der zuvor angewählten übereinstimmt.

5. Die für die Betriebsart erforderlichen Sicherheitsfunktionen werden aktiviert.

I4.4 Sicherheitstechnische Bewertung

Das Lesegerät erfüllt in diesem Beispiel die strukturellen Anforderungen der Kategorie 3. Das bedeutet, dass es durch einen einzelnen Fehler nicht zu einer gleichzeitigen fehlerhaften Ausgabe auf der Datenschnittstelle und dem Relaisausgang kommen kann. Einzelne Fehler werden durch eine hochwertige Codierung der Berechtigungsstufe, den Kreuzvergleich im Lesegerät und die Erwartungshaltung in der Sicherheits-SPS erkannt. Damit erreicht das Lesegerät in Kombination mit dem elektronischen Schlüssel in seiner Funktion als Zugangssystem eine vergleichbare Sicherheit zum Schlüssel elektromechanischer Wahleinrichtungen.

Das beschriebene Verfahren zur Auswahl, Prüfung und Bestätigung der Betriebsart sowie die Programmierung dieses Verfahrens erfüllt die Anforderungen an eine softwarebasierte Parametrisierung nach Abschnitt 4.6.4 der Norm.

Die Programmierung der SRASW der Sicherheits-SPS erfolgt entsprechend den Anforderungen des PL e und den Hinweisen in Abschnitt 6.3.

Bei der Sicherheits-SPS handelt es sich um ein Sicherheitsbauteil für den Einsatz in PL e.

Die mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion Betriebsartenwahl wird aus der PFH_D für das Aktivierungssystem gebildet, im Beispiel die Sicherheits-SPS.

Weiterführende Literatur

[1] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). ABl. EU (2006) Nr. L 157, S. 24-86

[2] *Apfeld, R.; Zilligen, H.; Köhler, B.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA-Report 7/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2013
► www.dguv.de/ifa, webcode/d639540

[3] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (04.10). Beuth, Berlin 2010

[4] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (02.13). Beuth, Berlin 2013

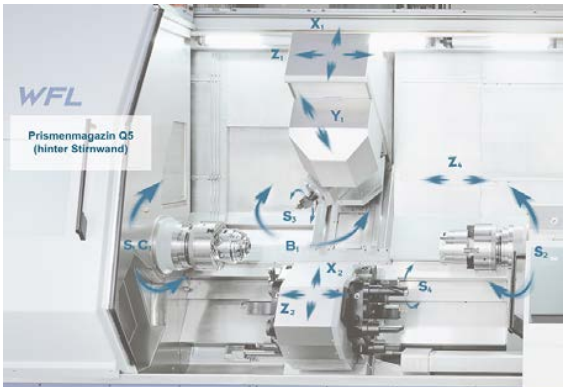
[5] DGUV Information: Sicherheitsbezogene Betriebsarten an spanenden Werkzeugmaschinen der Metallbearbeitung (FB HM-073). Ausg. 2/2016. Hrsg.: Fachbereich Holz und Metall der Deutschen Gesetzlichen Unfallversicherung e. V. (DGUV), Mainz 2016
► www.dguv.de/ifa, webcode/d545286

Anhang J:
Überlagerte Gefährdungen

Der folgende Inhalt ist aus dem Fachausschuss-Informationsblatt Nr. 47 übernommen. Dieses Informationsblatt wurde nach Veröffentlichung der dritten Normausgabe zurückgezogen, da seine regulatorischen Inhalte in die Norm übernommen wurden. Zur Illustration der Handhabung von überlagerten Gefährdungen wird es hier integriert.

Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen

In Arbeitsbereichen an komplexen Fertigungssystemen und Werkzeugmaschinen kann es zu Überlagerungen von Gefährdungen durch gefahrbringende Bewegungen kommen, hervorgerufen z. B. durch eine Vielzahl geregelter Achsantriebe. Dieses Informationsblatt beschreibt eine mit Arbeitsschutzexperten und dem Institut für Arbeitsschutz der DGUV abgestimmte Vorgehensweise, die es unter Anwendung der DIN EN ISO 13849-1 [1] oder DIN EN 62061 [2] erlaubt, Sicherheitsfunktionen bei überlagerten Gefährdungen abzubilden und zu berechnen.



Quelle: WFL Millturn Technologies GmbH & Co. KG

Bild 1: Achsschema einer Werkzeugmaschine

Überlagerte Gefährdungen sind charakterisiert durch das gleichzeitige Einwirken mehrerer Einzelgefährdungen auf eine oder mehrere zu schützende Personen, Körperteile oder Gliedmaßen, welche sich an einem Ort aufhalten oder gefahrbringende Bereiche erreichen können (siehe Bild 1).

Unter einer Einzelgefährdung wird sowohl die Bewegung einer einzelnen Achse, als z. B. auch eine Gefährdung durch die Bewegung eines gesamten Maschinenteils verstanden. Resultiert also die Bewegung eines Maschinenteils aus dem kinematischen Zusammenwirken einer oder mehrerer Achs- und Spindelantriebe (z. B. ein Fräswerkzeug am Support eines Bearbeitungszentrums), so kann dies als Einzelgefährdung betrachtet werden.

Inhaltsverzeichnis

1 Ausgangslage

Die Betrachtung von Einzelgefährdungen ist in der Sicherheitstechnik gängige Praxis und hat sich bewährt. Aus der probabilistischen Betrachtung nach DIN EN ISO 13849-1 oder DIN EN 61508 [3, 4] und DIN EN 62061 und der Risikobeurteilung für eine Gefährdungssituation ergibt sich jedoch, dass auch die Überlagerung von Gefährdungen betrachtet werden muss. Eine Diskussionsvorlage zu den Auswirkungen des probabilistischen Ansatzes auf die Betrachtung überlagerter Gefährdungen findet sich in [5], welcher durch dieses Informationsblatt präzisiert und erweitert wird.

Auf Grund der weitgefächerten Bandbreite von Gefährdungssituationen an den oben genannten Mensch-Maschine-Schnittstellen kann dieses Informationsblatt hinsichtlich deren Betrachtungsweise keine universelle bzw. allgemeingültige Festlegung geben. Es ist sowohl die Freiheit als auch die Aufgabe der Normung diesbezüglich maschinenspezifische Festlegungen in den jeweiligen Produkt- oder C-Normen zu beschreiben.

Problematisch ist, dass für Mensch-Maschine-Schnittstellen, auf die eine hohe Anzahl überlagerter Gefährdungen wirken, eine ausreichend kleine Ausfallwahrscheinlichkeit aller beteiligten sicherheitsbezogenen Steuerungsteile (Sensoren, Logik, mehrere Aktoren) kaum oder nur mit sehr hohem rechnerischen Aufwand (z.B. Markov-Modellierung) nachweisbar ist.

Ferner erhöhen überlagerte Gefährdungen mit unterschiedlichem Risiko (mit unterschiedlichem PL_r oder SIL) die Komplexität der Bestimmung der Ausfallwahrscheinlichkeit von Sicherheitsfunktionen, welches wiederum den Aufwand der Berechnung drastisch erhöht.

2 Praktische Behandlung überlagerter Gefährdungen

Eine genaue Überprüfung, welche Gefährdungen sich in einem konkreten Gefährdungsbereich tatsächlich überlagern, ist unerlässlich. Dabei sind die Maße der gefährdeten Körperteile und die bestimmungsgemäßen Handlungen des Maschinenpersonals genauso zu berücksichtigen

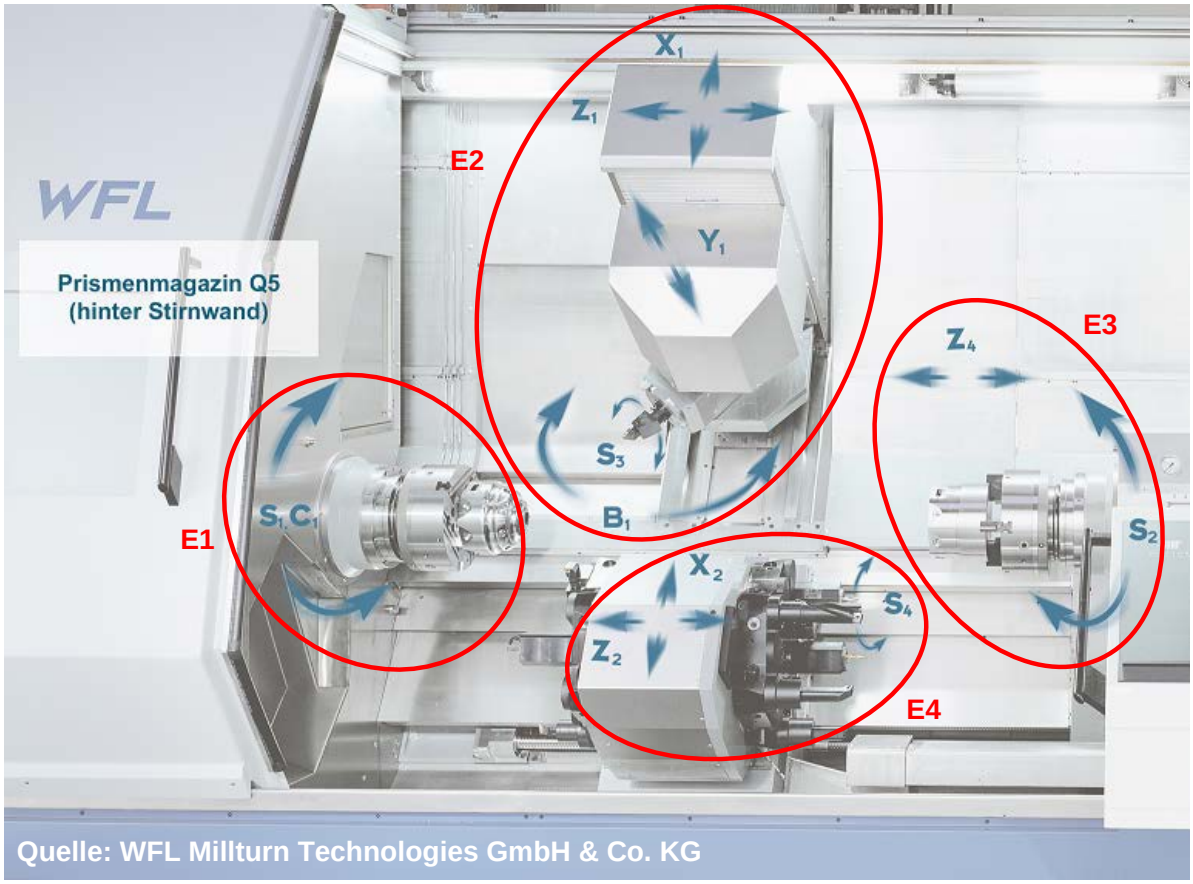


Bild 2: Unterschiedliche Einzelgefährdungen am Beispiel einer Werkzeugmaschine

wie die Bewegungsmöglichkeiten der gefährdenden Maschinenteile (z. B. durch Mehrachskinematik bewirkte vektorielle Bewegungen oder translatorische Einachsbewegungen).

Abhängig von der individuellen Risikobeurteilung ist es in der Praxis erlaubt, Sicherheitsfunktionen abzubilden, die, obwohl von überlagerten Gefährdungen gebildet, auf der Betrachtung deren Einzelgefährdungen basieren.

Leisten jedoch mehrere Aktoren (z. B. Schütze, Ventile, Antriebsregler) einen Beitrag zur Risikoreduzierung derselben Einzelgefährdung, müssen alle diese Aktoren in einer Sicherheitsfunktion zusammen betrachtet werden. Anders ausgedrückt: Alle Aktoren, die gefahrbringende Bewegungen ein und desselben Maschinenteils hervorrufen können, müssen in einer Sicherheitsfunktion zusammen betrachtet werden.

Wenn die individuelle Risikobeurteilung an der Maschine zur einer differenzierten Gefährdungsbeurteilung mit unterschiedlichen PL_r oder SIL führt, ist es in der Praxis erlaubt, Sicherheitsfunktionen abzubilden, die auf der Betrachtung von Einzelgefährdungen basieren.

Beispiele:

1. Resultiert die Bewegung eines Fräsers einer Werkzeugmaschine aus dem kinematischen Zusammenwirken von mehreren Einzelachsbewegungen, müssen alle diese Bewegung auslösenden Aktoren in einer Sicherheitsfunktion zusammengefasst werden. Die resultierende Bewegung setzt sich z.B. aus fünf Einzelbewegung zusammen, drei translatorischen Bewegungen in X_1, Y_1, Z_1-Richtung, einer Schwenkbewegung B_1 und einer rotatorischen Bewegung S_3 (siehe Bild 2, Einzelgefährdung E2).
2. Bewegungen eines einzigen Mehrachsroboters müssen in einer Sicherheitsfunktion zusammengefasst betrachtet werden (mehrere Roboter nebeneinander werden separat betrachtet).
3. Mehrere Spanneinrichtungen, die zusammen ein Teil festhalten (Ausfall einer der Spanneinrichtungen führt zum Lösen des Teils), müssen in einer Sicherheitsfunktion zusammengefasst werden.

Aus der Einzelbetrachtung kann nach Beispiel 1 die in Bild 2 gezeigte Berücksichtigung der von Antriebsachsen ausgehenden Gefährdungen beim Ableiten von Sicherheitsfunktionen ergeben. Das Bild zeigt beispielhaft vier rot umkreiste Einzelgefährdungen E1 bis E4 im Arbeitsraum einer Werkzeugmaschine:

E1: rotatorische (S_1) und translatorische (C_1, zur außermittigen Bearbeitung) Bewegung der linken Werkstückspindel

E2: rotatorische (S_3) und translatorische (X_1, Y_1, Z_1) Bewegung und Schwenkbewegung (B_1) der Frässpindel

E3: rotatorische (S_2) und translatorische (Z_4) Bewegung der rechten Werkstückspindel

E4: rotatorische (S_4) und translatorische Bewegung (X_2, Z_2) einer Werkzeugspindel (der Werkzeugrevolver ist indexiert, sodass dessen rotatorische Bewegung hier nicht betrachtet werden muss)

Aus diesen vier Einzelgefährdungen ergeben sich somit vier Sicherheitsfunktionen SF1 bis SF4. Die Sicherheitsfunktion SF1 zu E1 umfasst z. B. einen Achs- und einen Spindelantrieb (C_1, S_1). Die Sicherheitsfunktion SF2 zu E2 umfasst z. B. die Achsantriebe X_1, Y_1, Z_1, den Schwenkantrieb (B_1) und den Spindelantrieb (S_3).

Literatur:

[1] DIN EN ISO 13849-1 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze, 2016-06

[2] DIN EN IEC 62061 Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme, 2005-10

[3] IEC 61508-1 Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen, 2002-11 (vorgesehener Ersatz durch 65A/548/FDIS, 2009-12)

[4] IEC 61508-5 Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität, 1998-11 (vorgesehener Ersatz durch IEC 65A/552/FDIS, 2009-12)

[5] Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schäfer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) Nr. 6, S. 34-37

Anhang K:
EMV und funktionale Sicherheit im Maschinenbereich

DGUV Test
Prüf- und Zertifizierungssystem der Deutschen Gesetzlichen Unfallversicherung

EMV und funktionale Sicherheit im Maschinenbereich

Erhöhte Störfestigkeit im Kontext der DIN EN 13849-1 bei der Integration von SRP/CS

15
12/2016

DGUV Test Information

Ende 2015 erschien die DIN EN 61000-6-7 [1] als neue Fachgrundnorm zum Thema Störfestigkeitsanforderungen an Geräte und Einrichtungen zur Durchführung von Sicherheitsfunktionen im Einsatz an industriellen Standorten. Diese DGUV-Information soll für den Maschinenbau klarstellen, in wie weit im Rahmen der Systemintegration unter DIN EN 13849-1 [2] Anforderungen zu erhöhter Störfestigkeit zu berücksichtigen sind.

Anwendungsbereich der DIN EN ISO 13849-1 und der DIN EN 61000-6-7

DIN EN ISO 13849-1 beschreibt ihren Anwendungsbereich wie folgt:

> *„Dieser Teil der ISO 13849 stellt Sicherheitsanforderungen und einen Leitfaden für die Prinzipien der Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS) bereit, einschließlich der Entwicklung von Software.“*

Es gibt also zwei typische Anwendungsfelder dieser Norm: die Entwicklung von SRP/CS (= Gestaltung) und die sogenannte Systemintegration von bereits vorhandenen SRP/CS durch den Maschinenbau.

DIN EN 61000-6-7 gilt gemäß ihrem Anwendungsbereich für elektrische und elektronische Betriebsmittel, Geräte und Einrichtungen, die zur Verwendung in sicherheitsbezogenen Systemen an industriellen Standorten vorgesehen sind und mit der IEC 61508 und/oder anderen sektorspezifischen Normen zur funktionalen Sicherheit übereinstimmen sollen. Der Anwendungsbereich der Norm umfasst also nicht das endgültige sicherheitsbezogene System an der Maschine, wie das auch in Anmerkung 1 zum Anwendungsbereich weiter ausgeführt wird.

[1] DIN EN 61000-6-7: Elektromagnetische Verträglichkeit (EMV) – Teil 6-7: Fachgrundnormen – Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind (12.15), Beuth, Berlin 2015

[2] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (06.16), Beuth, Berlin 2016

Somit steht fest:

> Der Maschinenbau muss bei der Integration von SRP/CS die DIN EN 61000-6-7 keinesfalls direkt berücksichtigen, da diese Norm sich (nur) an die Entwicklung von SRP/CS richtet.

EMV-Anforderungen gemäß DIN EN ISO 13849-1

Die Norm DIN EN ISO 13849-1 fordert für SRP/CS der Kategorie B und somit auch für alle anderen Kategorien:

> *„Die SRP/CS müssen in Übereinstimmung mit den zutreffenden Normen mindestens so gestaltet, gebaut, ausgewählt … sein, um … elektro-magnetischen Störungen … standzuhalten. Wenn keine Produktnorm vorhanden ist, sollten zumindest die Anforderungen der IEC 61000-6-2 an die Störfestigkeit befolgt werden.“*

Diese Mindestanforderungen richten sich auch an den Maschinenbau. Sie müssen bei der Auswahl von SRP/CS für die Integration berücksichtigt werden.

Der Integrator muss jedoch feststellen, ob seine Maschine für den Einsatz in rauer elektromagnetischer Umgebung mit hoher Störbelastung vorgesehen ist. Dann muss er bei der Auswahl von SRP/CS berücksichtigen, ob diese eine erhöhte Störfestigkeit besitzen. Applikationen, für die die Auswahl von SRP/CS mit erhöhter Störfestigkeit notwendig sein kann, sind zum Beispiel:

- große Umrichterinstallationen,
- große Papierverarbeitungsmaschinen,
- große Holzbearbeitungsmaschinen,
- große Stanzanlagen,
- Maschinenanlagen mit großen Heizsystemen (z.B. für Klebevorgänge),
- industrielle GSM-Module im Schaltschrank oder in Maschinennähe,
- Elektroschweißen,
- Schiffsradar in Hafennähe,
- Flugradar in Flughafennähe,
- Militärbereiche.

Bei der Auswahl von SRP/CS sollte der Integrator weiterhin berücksichtigen, dass DIN EN 61000-6-7 nur die funktionale Sicherheit berücksichtigt. Die Erfüllung dieser Norm garantiert keine Funktion, d.h. Verfügbarkeit im Betrieb unter Störeinfluss. Kann der Integrator die Feststellung, ob eine erhöhte Störfestigkeit erforderlich ist, nicht treffen, so muss er dem Anwender mitteilen, dass seine Maschine nur für eine „normale“ Störfestigkeit ausgelegt ist.

Kontakt
Geschäftsstelle DGUV Test
Alte Heerstraße 111
53757 Sankt Augustin
Telefon: +49 2241 231-1467
Fax: +49 2241 231-841448
E-Mail: dguv-test@dguv.de

Anhang L: Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

K

L

M

Q

R

S

T

U

V

W

Z

Deutsche Gesetzliche
Unfallversicherung e.V. (DGUV)

Glinkastraße 40
10117 Berlin

Telefon: **+49 30 13001-0 (Zentrale)**
Fax: **+49 30 13001-9876**
E-Mail: **info@dguv.de**
Internet: **www.dguv.de**