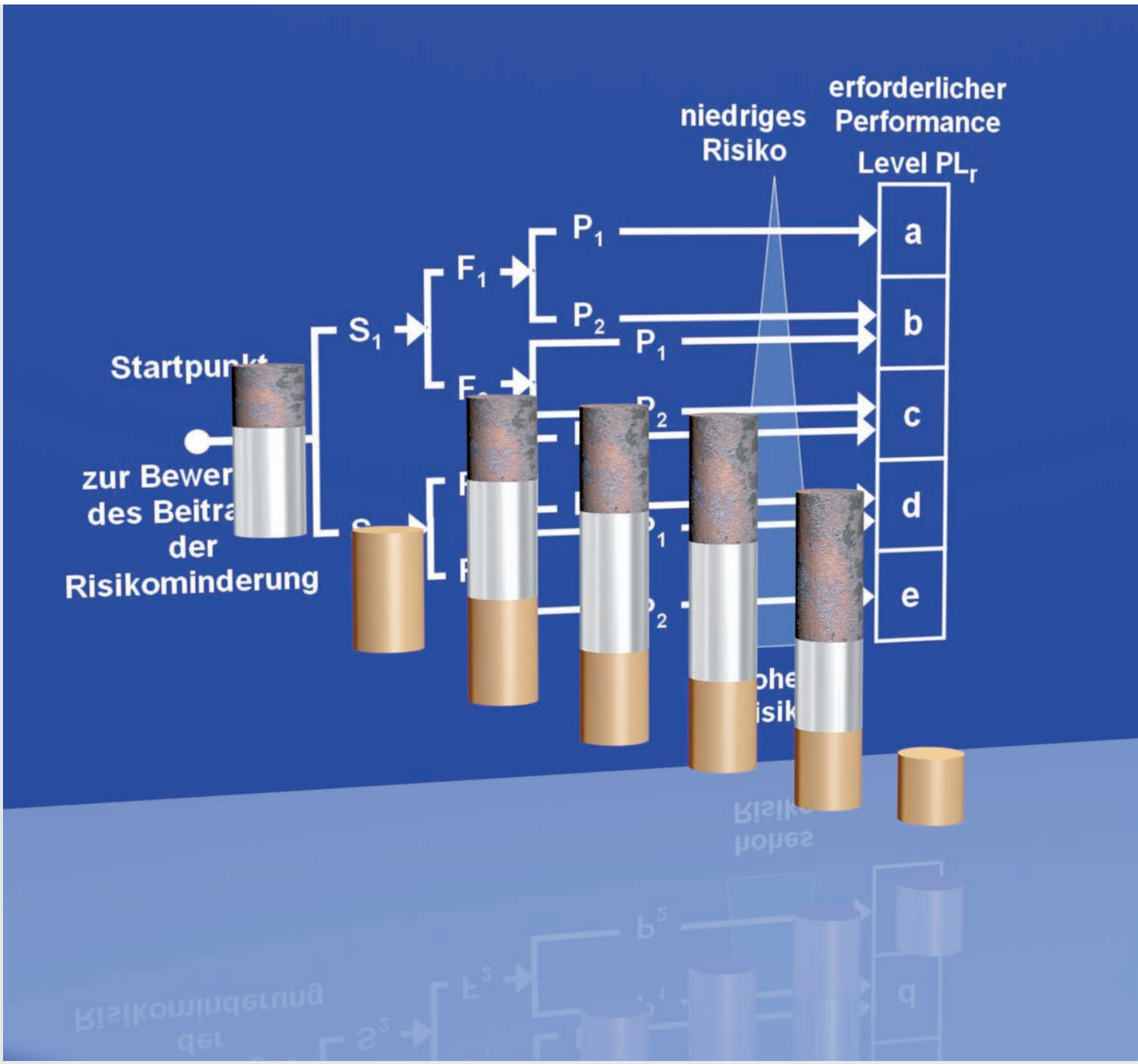
Deutsche Gesetzliche
Unfallversicherung

BGIA-Report 2/2008

Funktionale Sicherheit von Maschinensteuerungen

– Anwendung der DIN EN ISO 13849 –



BGIA-Report 2/2008

Funktionale Sicherheit von Maschinensteuerungen

– Anwendung der DIN EN ISO 13849 –

Autoren: Michael Hauke, Michael Schaefer, Ralf Apfeld, Thomas Bömer, Michael Huelke, Torsten Borowski, Karl-Heinz Büllesbach, Michael Dorra, Hans-Georg Foermer-Schaefer, Wolfgang Grigulewitsch, Klaus-Dieter Heimann, Burkhard Köhler, Michael Krauß, Werner Kühlem, Oliver Lohmaier, Karlheinz Meffert, Jan Pilger, Günter Reuß, Udo Schuster, Helmut Zilligen
Fachbereich 5, Unfallverhütung – Produktsicherheit
BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (DGUV), Sankt Augustin

Redaktion: Zentralbereich des BGIA, Referat Informationsmanagement

Broschürenversand: info@dguv.de

Herausgeber: Deutsche Gesetzliche Unfallversicherung (DGUV)
Mittelstraße 51, D – 10117 Berlin
Telefon: 030 288763-800
Telefax: 030 288763-808
Internet: www.dguv.de
2., geänderte Auflage
– Dezember 2008 –

Satz und Layout: Deutsche Gesetzliche Unfallversicherung (DGUV)

Druck: Plump OHG, Rheinbreitbach

ISBN: 978-3-88383-771-0
ISSN: 0173-0387

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

Die Norm DIN EN ISO 13849 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ macht Vorgaben für die Gestaltung von sicherheitsbezogenen Teilen von Steuerungen. Dieser Report stellt die wesentlichen Inhalte der Norm in ihrer stark überarbeiteten Fassung von 2007 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, dass die Anforderungen der DIN EN ISO 13849 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 DIN EN ISO 13849 -

The DIN EN ISO 13849 standard, “Safety of machinery – Safety-related parts of control systems”, contains provisions governing the design of such parts. This report describes the essential subject-matter of the standard in its heavily revised 2007 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, 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 also 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 that the requirements of DIN EN ISO 13849 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
Sécurité fonctionnelle des commandes de machines – Application de la norme DIN EN ISO 13849 –

La norme DIN EN ISO 13849 « Sécurité des machines – Parties des systèmes de commande relatives à la sécurité » émet des prescriptions pour la conception de parties de systèmes de commande relatives à la sécurité. Ce rapport présente les éléments essentiels de la norme dans sa version, largement révisée, de 2007 et explique son application à l'aide de nombreux exemples issus des secteurs de l'électromécanique, la fluidique, l'électronique et l'électronique programmable, mais aussi des commandes de technologies diverses. On y montre le lien existant entre la norme et les exigences de sécurité de base contenues dans la directive Machines et certaines procédures d'évaluation des risques y sont présentées. A partir de ces informations, le rapport permet de sélectionner le niveau de performance (required Performance Level PL_r) nécessaire pour les fonctions de sécurité de technique de commande. On y explique en détails comment déterminer le niveau de performance PL vraiment atteint. On y aborde dans les détails les exigences en matière d'obtention du niveau de performance et ses catégories respectives, la fiabilité des composants, la couverture du diagnostic, la sécurité des logiciels et les mesures contre les défaillances systématiques ainsi que les défaillances de cause commune. S'y ajoutent des informations générales concernant l'application des exigences dans la pratique de la technique des commandes. De nombreux exemples de montages montrent, en allant jusqu'au niveau des composants, comment appliquer techniquement le niveau de performance a à e avec les catégories B à 4 dans les technologies respectives. Ils donnent ainsi des indications concernant les principes de sécurité utilisés et concernant les composants éprouvé en matière de technique de sécurité. Un grand nombre de documents complémentaires mentionnés permettent une meilleure compréhension des exemples donnés. Ce rapport montre que les exigences de la norme DIN EN ISO 13849 peuvent être techniquement mises en pratique et apporte ainsi une aide pour une application et une interprétation cohérente de la norme au niveau national et international.

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

La norma DIN EN ISO 13849 «Seguridad de las máquinas – partes de 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 presenta los contenidos esenciales de la norma en su versión sustancialmente revisada de 2007 y explica su aplicación a través de numerosos ejemplos de los ramos de la electromecánica, ingeniería de fluidos, electrotécnica y tecnología informática, entre ellos también sistemas de mando de tecnología mixta. Se demuestra la relación de la norma con los requisitos fundamentales de seguridad de la directiva Máquinas, presentando posibles procedimientos para la evaluación de los riesgos. Sobre la base de estas informaciones, el informe permite seleccionar el nivel de prestaciones necesario (required Performance Level PL_r) para funciones de seguridad en la técnica de control. Se explica detalladamente la determinación del Performance Level PL realmente alcanzado. Se exponen en detalle los requisitos para alcanzar el respectivo Performance Level y sus respectivas categorías, la fiabilidad de los componentes, los grados de cobertura del diagnóstico, la seguridad del software y las medidas contra fallos sistemáticos, así como errores originados por una causa común. Informaciones de trasfondo sobre la implementación de los requisitos en la práctica de la ingeniería de control completan la oferta. Numerosos ejemplos de circuitos que abarcan hasta el nivel de los componentes muestran cómo se puede implementar técnicamente el Performance Level «a» a «e» con las categorías B a 4 en las diversas tecnologías. Estos ejemplos dan indicaciones sobre los principios de seguridad aplicados y los componentes comprobados desde el punto de vista de la técnica de seguridad. Numerosas referencias bibliográficas ayudan a comprender mejor los diversos ejemplos. El informe demuestra que los requisitos de la norma DIN EN ISO 13849 pueden implementarse en la práctica técnica y contribuye, de esta forma, a la aplicación e interpretación unitaria de la norma a nivel nacional e internacional.

Inhaltsverzeichnis

Seite

Seite

Seite

Anhang

Vorwort

Vor zehn Jahren erschien der BIA-Report 6/97 „Kategorien für sicherheitsbezogene Steuerungen nach EN 954-1“, der sich im Laufe der Zeit als Bestseller herausstellte. Mehr als 12 000 deutsch- und 6 000 englischsprachige gedruckte Exemplare wurden seitdem versendet, noch höher sind die Zahlen der Downloads auf den Internetseiten des BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung[1]. Selbst ins Japanische ist der Report übersetzt worden.

In diesen zehn Jahren werden nun schon sicherheitsrelevante Steuerungen von Maschinen, ob mechanisch, pneumatisch, hydraulisch oder elektrisch, nach DIN EN 954-1 erfolgreich in fünf Kategorien eingeteilt. Mit dem Vormarsch programmierbar elektronischer Systeme ergab sich aber die Notwendigkeit einer grundlegenden Revision dieser Norm. Diese schwierige Aufgabe hat nun mit der Publikation der Norm DIN EN ISO 13849-1:2007-07 ihren Abschluss gefunden. Wesentliche Neuerung ist die Einbeziehung wahrscheinlichkeitstheoretischer Ansätze zur sicherheitstechnischen Beurteilung und Auslegung von Steuerungen. Dieser Ansatz mit der Betrachtung von Ausfallwahrscheinlichkeiten von Bauteilen ist in der elektrischen Sicherheits-Grundnormen-Reihe DIN EN/IEC 61508 verankert. Mit dem Anspruch, weiterhin alle Technologien angemessen und vor allem praktikabel zu klassifizieren, wurden die Kategorien erfolgreich in das umfassendere Konzept des Performance Level eingebettet.

Dem Normensetzer ist es nicht zuletzt durch die intensive Mitwirkung erfahrener Experten des BGIA gelungen, die Nachfolgenorm DIN EN ISO 13849-1 so zu gestalten, dass sie bei aller Komplexität der Materie praktisch anwendbar bleibt. Sie liegt seit Mai 2007 harmonisiert vor. Ein Positionspapier (siehe Anhang I, Seite 249) des Verbandes Deutscher Maschinen- und Anlagenbau e.V. (VDMA) unterstützt ausdrücklich ihre Anwendbarkeit im deutschen Anlagen- und Maschinenbau. Deshalb ist nun der richtige Zeitpunkt für einen neuen, vollständig überarbeiteten BGIA-Report zu sicherheitsrelevanten Steuerungen von Maschinen gekommen. Mit den zunehmend komplexeren Technologien in der Sicherheitstechnik ändern sich auch die Anforderungen und Erwartungshaltungen an Anwendungshilfen. Der vorliegende Report und auch die im BGIA entwickelte Software „SISTEMA – Sicherheit von Steuerungen an Maschinen“ versuchen, die Brücke zwischen „alter“ und „neuer“ Norm zu schlagen. Sie bieten dem Leser bzw. Anwender einen einfachen Einstieg in die neuen Methodiken. Ein Team von 20 Autoren hat die Texte und vor allem die so wichtigen Schaltungsbeispiele erarbeitet, diskutiert und validiert und führt den Leser so Schritt für Schritt in die „Geheimnisse“ der Norm DIN EN ISO 13849-1:2007 und ihre praktische Anwendung ein. Hierbei ist der Report selbstverständlich kein Ersatz für die Norm, er enthält jedoch wertvolle Tipps und vor allem schon in der Praxis erarbeitete Erweiterungen und Hilfen. Der Report ist als Lehrbuch und Nachschlagewerk gedacht; beiden Ansprüchen soll und kann er gerecht werden.

Dr. Karlheinz Meffert
Direktor des BGIA

[1] *Früher: Berufsgenossenschaftliches Institut für Arbeitssicherheit – BIA*

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 1 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 kodifizierten Fassung 98/37/EG [1] der Maschinenrichtlinie fallen neben Maschinen auch Sicherheitsbauteile, die vom Hersteller mit dem Verwendungszweck der Gewährleistung einer Sicherheitsfunktion in Verkehr gebracht werden und deren Ausfall oder Fehlfunktion die Sicherheit oder die Gesundheit von Personen im Wirkbereich der Maschine gefährden können, unter den Anwendungsbereich dieser Richtlinie.

Die grundlegenden Anforderungen der Maschinenrichtlinie an Maschinen und Sicherheitsbauteile 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 den Hersteller, eine Gefahrenanalyse vorzunehmen, um alle mit der Maschine verbundenen Gefahren zu ermitteln. Drei Grundsätze werden genannt, um die mit den einzelnen Gefährdungen verbundenen Unfallrisiken auf ein akzeptables Maß zu reduzieren:

- Beseitigung oder Minimierung der Gefahren durch die Konstruktion selbst
- Ergreifen der notwendigen Schutzmaßnahmen gegen nicht zu beseitigende Gefahren und
- Unterrichtung der Benutzer über Restgefahren

Nach Artikel 5 lässt die Einhaltung harmonisierter europäischer Normen, deren Fundstelle im Amtsblatt der EU veröffentlicht worden ist („Listung"), die Übereinstimmung mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie vermuten. Mehrere europäische Normentwürfe und inzwischen harmonisierte europäische Normen vertiefen bzw. konkretisieren die im Anhang I der Maschinenrichtlinie zugrunde gelegte Philosophie zur Erreichung der Arbeitssicherheit an Maschinen. Die Normenreihe DIN EN ISO 12100 [2; 3] behandelt z.B. Grundbegriffe und allgemeine Gestaltungsleitsätze für die Sicherheit von Maschinen. Das gesamte Verfahren zur Identifizierung von Gefährdungen sowie zur Risikoeinschätzung und Risikobewertung der einzelnen Gefährdungen wird im neuen Entwurf der DIN EN ISO 14121-1 [4] und ihrem technischen Report ISO/DTR 14121-2 [5] beschrieben. Auf der Basis dieser beiden grundlegenden Normen beschreibt die Normenreihe DIN EN ISO 13849-1:2007 [6] und DIN EN ISO 13849-2:2003 [7] 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 Norm DIN EN 954-1 ist die oben bereits skizzierte technologieunabhängige Behandlung von sicherheitsbezogenen Teilen von Steuerungen. Diese Vorgehensweise wurde in DIN EN ISO 13849-1:2007 beibehalten und wesentlich erweitert. Nun sind über die Einführung des Performance Levels Kombinationen verschiedener Steuerungsstrukturen mit verschiedenen Technologien einfach realisierbar. Damit bietet die neue Norm auf weniger als 100 Seiten alles Notwendige in einem Guss. Die Methoden sind von der konkreten Anwendung oder Technologie unabhängig formuliert und können deshalb von nahezu allen Produktnormen (C-Normen) in Bezug genommen sowie in den maschinenspezifischen Normen erwähnt werden.

Die Norm erhält als harmonisierte Norm nach Inkrafttreten der neuen Maschinenrichtlinie [8] am 29. Dezember 2009 ein stärkeres Gewicht. Wesentliche Neuerung ist beispielsweise die Aufnahme von sicherheitsrelevanten Logiken – auch sicherheitsbezogene Teile von Steuerungen genannt – in den Anhang IV der neuen Richtlinie. 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 dann zwar nicht mehr EG-baumusterprüfpflichtig[1] – sie können u.a. auch durch

---

[1] *Neben der EG-Baumusterprüfung kann der Hersteller nach heute gültiger Maschinenrichtlinie bei Vorliegen einer harmonisierten und gelisteten Norm auch erklären, dass er nach dieser harmonisierten und gelisteten C-Norm gebaut hat und er muss die Unterlagen entweder bei einer notifizierten Prüfstelle hinterlegen oder dort prüfen lassen und hinterlegen.*

ein erweitertes, von einer notifizierten Prüfstelle geprüftes Qualitätsmanagement(QM)-System des Herstellers in den Markt eingeführt werden –, jedoch rücken Steuerungen mit der neuen Richtlinie verstärkt in den Mittelpunkt der Sicherheitsbetrachtung [9; 10].

DIN EN ISO 13849-1:2007 [6] tritt mit dem bereits vorher harmonisierten zweiten Teil DIN EN ISO 13849-2:2003 [7] die Nachfolge der DIN EN 954-1:1997 [11] an. Nach erstmaligem Erscheinen im Februar 2007 ist nun eine leicht korrigierte DIN-Fassung vom Juli 2007 gültig.[1] Erstmals gibt es beim DIN eine dreijährige Übergangsfrist bis zum November 2009, in der die DIN EN 954-1:1997 parallel gültig bleibt – der Anwender kann bis zu deren Rückzugsdatum also beide Normen alternativ anwenden. Um den Übergang von den altbekannten geforderten Kategorien hin zum erforderlichen Performance Level PL_r nach der neuen Norm zu erleichtern, wird in Kapitel 5 dieses Reports eine mögliche Vorgehensweise beschrieben.

Der vorliegende BGIA-Report hat zum Ziel, die Anwendung der DIN EN ISO 13849 zu erläutern und insbesondere anhand zahlreicher Lösungen die praktische Realisierung beispielhaft aufzuzeigen. 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 BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung aus fast dreißigjähriger 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 Konstrukteuren, Betreibern sowie Arbeitsschutzexperten 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 Beispiele sind in zahlreichen konkreten Anwendungen technisch umgesetzt worden.

Die Internet-Adresse „www.dguv.de/bgia/13849“ bietet einen zentralen Zugang zu allen BGIA-Informationen und Hilfen zur funktionalen Sicherheit von Maschinensteuerungen (siehe Abbildung 2.1). Neben der freien BGIA-Software „SISTEMA“ (Sicherheit von Steuerungen an Maschinen) können dort auch die SISTEMA-Projektdateien zu den Schaltungsbeispielen aus Kapitel 8 heruntergeladen werden. Zukünftige Erweiterungen sollen dem Anwender stets aktuelle Hilfen zur Verfügung stellen.

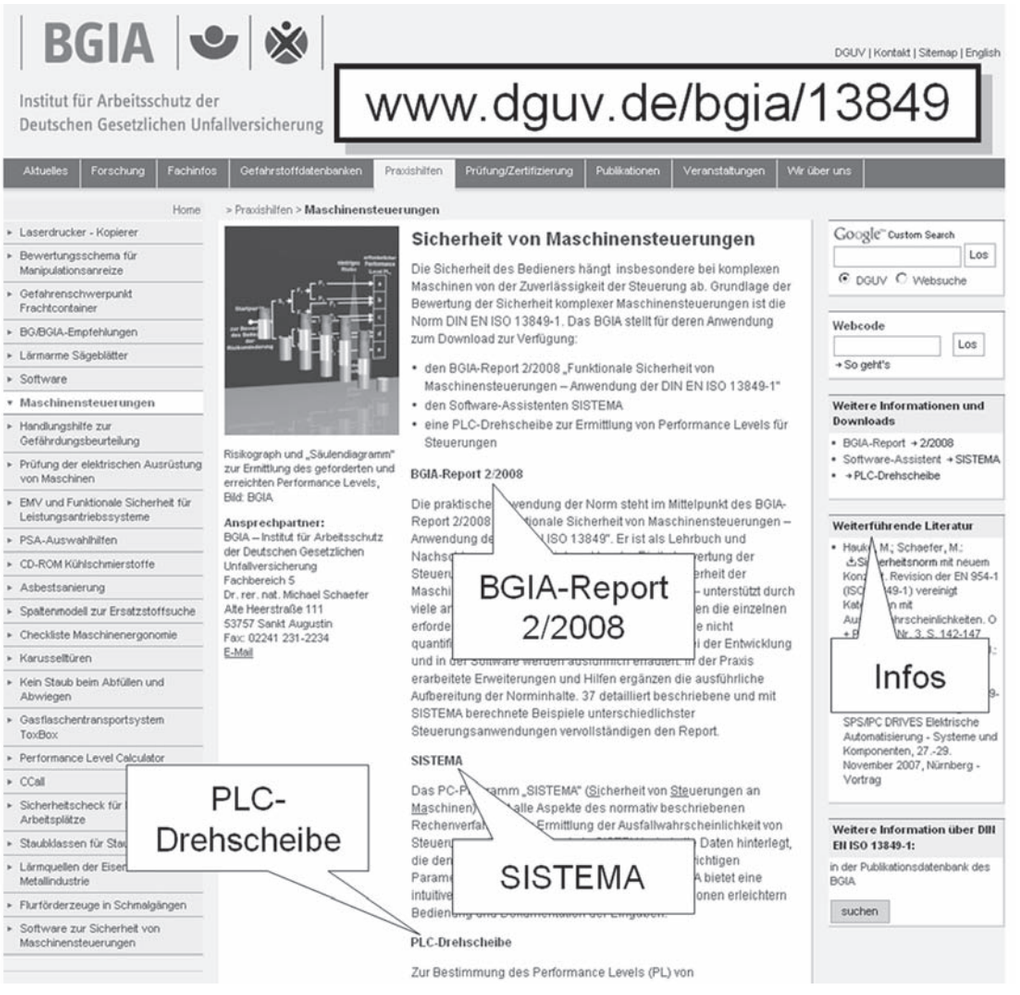


Abbildung 2.1: Die Internetseite „www.dguv.de/bgia/13849“ bietet Links zu allen Praxishilfen zur Sicherheit von Maschinensteuerungen

[1] *Beide Normteile wurden in den Fassungen DIN EN ISO 13849-1:2008-12 und DIN EN ISO 13849-2:2008-09 neu herausgegeben. Die Änderungen zu den Vorgängerfassungen betreffen die Anhänge ZA und ZB, um den Bezug auf die neue Maschinenrichtlinie umzusetzen.*

3 Basisnormen zur funktionalen Sicherheit von Maschinensteuerungen

Neben der in diesem Report behandelten Norm DIN EN ISO 13849 gibt es alternative, aber relevante Normen im Bereich der funktionalen Sicherheit[1]. Dies sind, wie in Abbildung 3.1 dargestellt, die Normen der Reihe DIN EN 61508 [12] und ihre Sektornorm DIN EN 62061 [13] 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]. In der Betriebsart mit niedriger Anforderungsrate ist die Maßzahl die mittlere Ausfallwahrscheinlichkeit der entworfenen Funktion bei Anforderung *PFD* (Average **P**robability of **F**ailure to Perform its Design Function on **D**emand), während die Definition für die Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung als Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde *PFH* (**P**robability of a Dangerous **F**ailure per **H**our) erfolgt (weitere Informationen siehe auch [14]). Im Maschinenbereich und damit in DIN EN 62061 ist nur die zweite Definition relevant. Auch sind SIL-4-Systeme mit höheren Risiken im Maschinenbereich nicht bekannt und werden daher in DIN EN 62061 nicht betrachtet (Abbildung 3.2, siehe Seite 16). Der grundlegende Ansatz dieser Normen, Ausfallwahrscheinlichkeiten und nicht speziell auch Strukturen als charakteristische Kenngröße zu definieren, erscheint zunächst universeller. Der Ansatz der DIN EN ISO 13849-1 bietet 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 seit 2003 auch ein Teil 2 mit dem Titel „Validierung“, der mit dem Erscheinen des revidierten Teils 1 jedoch überarbeitet und angepasst werden muss. Trotzdem passen die dort genannten Anforderungen bereits erstaunlich gut zum überarbeiteten Teil 1. Die Anhänge A bis D des Teils 2 enthalten umfangreiches Material zu den Themen „grundlegende Sicherheitsprinzipien“, „bewährte Sicherheitsprinzipien“, „bewährte Bauteile“ und „Fehlerlisten“, das auch unter dem neuen Teil 1 gültig ist; Details hierzu sind im Anhang C dieses Reports dargestellt.

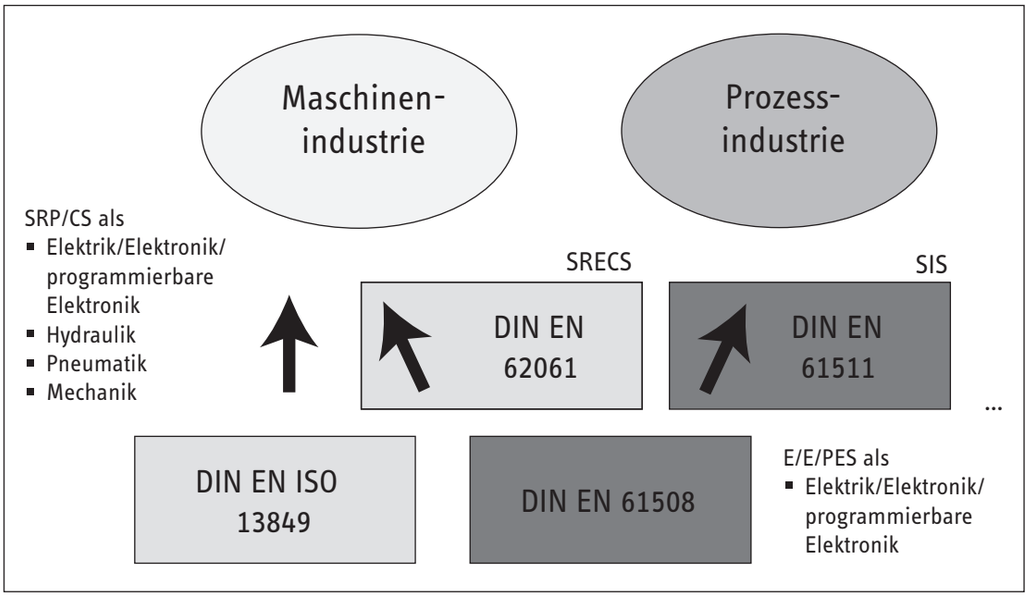


Abbildung 3.1: Anwendungsbereiche verschiedener Basisnormen zur funktionalen Sicherheit; SRP/CS: sicherheitsbezogene Teile einer Steuerung; SRECS: sicherheitsbezogenes elektrisches Steuerungssystem; SIS: sicherheitstechnisches System; E/E/PES: elektrisch/elektronisch/programmierbar elektronisches System

---

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 noch sogenannte deterministische Anforderungen, die im jeweiligen Level erfüllt werden müssen.*

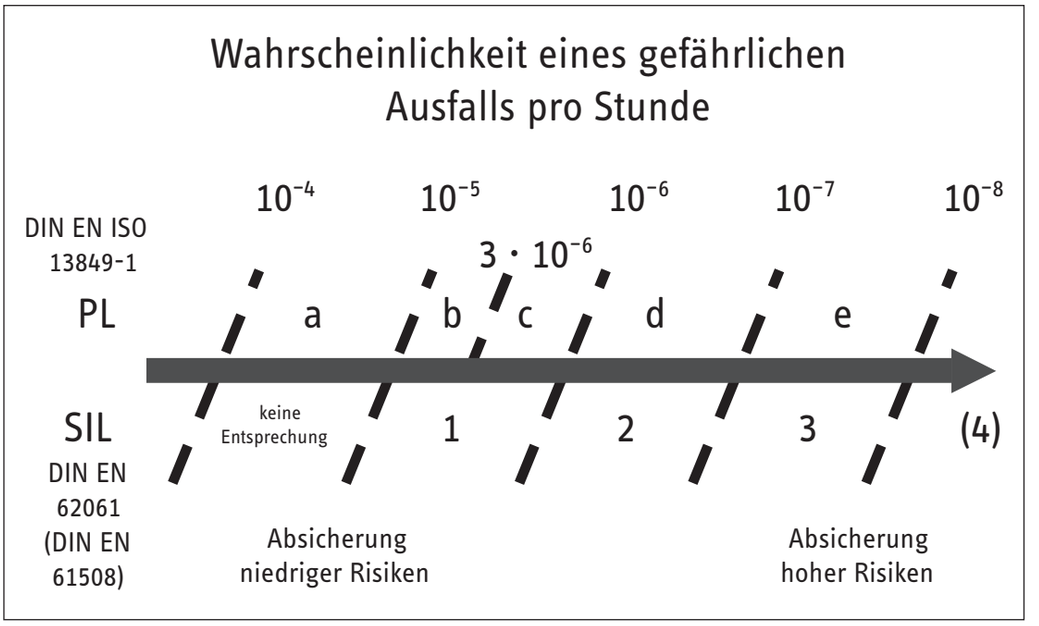


Abbildung 3.2: Performance Level (PL) und Sicherheits-Integritätslevel (SIL) als Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde

Die augenscheinliche Überlappung des Regelungsanspruchs beider Normenwelten kann für Steuerungshersteller und andere Normennutzer 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[1] 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 die Revision der DIN EN ISO 13849-1 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 [15]). Zahlenmäßig gibt es dabei korrespondierende Klassen (siehe Abbildung 3.2), die im praktischen Alltag schnell erste Abschätzungen erlauben. Schon im Entwurfsstadium der beiden Normen DIN EN ISO 13849-1 und DIN EN 62061 wurde von Mitgliedern der Normenkomitees eine Information zur empfohlenen Anwendung erarbeitet und nahezu wortgleich in den Einleitungen der Normen veröffentlicht. Zentrales Element ist dabei eine Tabelle, die dem Leser eine Hilfestellung zur Auswahl der passenden Norm für seinen Anwendungsfall geben soll. Diese Übersicht muss jedoch als veraltet gelten, da sie in Bezug auf DIN EN ISO 13849-1 den Stand des Entwurfs wiedergibt. Die genannten Einschränkungen sind für die aktuelle Fassung der Norm nicht mehr gültig. Faktisch gibt es keine Beschränkungen mehr, lediglich muss sicherheitsbezogene Embedded-Software (SRESW) bei Nichtvorliegen vollständiger Diversität dem Abschnitt 7 der DIN EN 61508-3:2002 entsprechen (siehe auch Abschnitt 6.3 dieses Reports). Auch sind die vorgesehenen Architekturen im Sinne der Norm eher ein Angebot (vereinfachter Ansatz) als eine Verpflichtung. Sie sind jedoch als zentrales Element der Vereinfachung des nun 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 die Tabelle nahe, dass auch komplexe, z.B. programmierbare Elektronik in den Anwendungsbereich der Norm fällt. 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. Abbildung 3.3 zeigt eine „angepasste Empfehlung“, die sich an den aktuellen Ständen der Norm und deren Anwendungsbereichen orientiert.

[1] *IEC = International Electrotechnical Commission*

Auch wenn von vielen Experten die annähernde Gleichwertigkeit der Ergebnisse bei Anwendung der einen oder anderen Norm diskutiert wird, sind die Anforderungen im Detail durchaus unterschiedlich; so beschreibt DIN EN 62061 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. Die Darstellung orientiert sich (wohl bewusst) mit Verzicht auf Komplexität am „Normalfall“. Weitgehende Einigkeit besteht aber darin, dass keine Mischung der Anforderungen aus beiden Normen vorgenommen werden soll.

Entscheidende Argumente für die Wahl von DIN EN ISO 13849 als Basis zur Realisierung funktionaler Sicherheit im Maschinenbereich können also aus Sicht des Anwenders 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 Hersteller von in großer Anzahl hergestellten Sicherheitskomponenten, z.B. einer speicherprogrammierbaren Steuerung (SPS) für Sicherheitsanwendungen, 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.

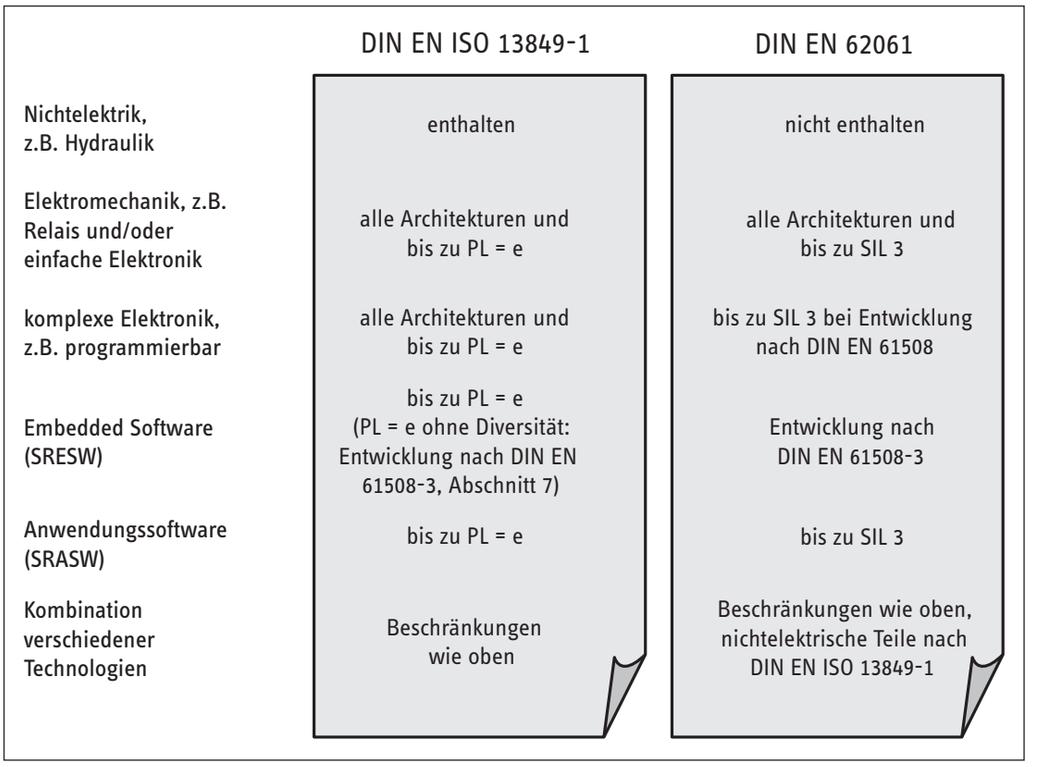


Abbildung 3.3: „Angepasste Empfehlung“ zur Anwendung von DIN EN ISO 13849-1 und DIN EN 62061

4 Report und Norm im Überblick

Dieses Kapitel stellt für den Leser 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.

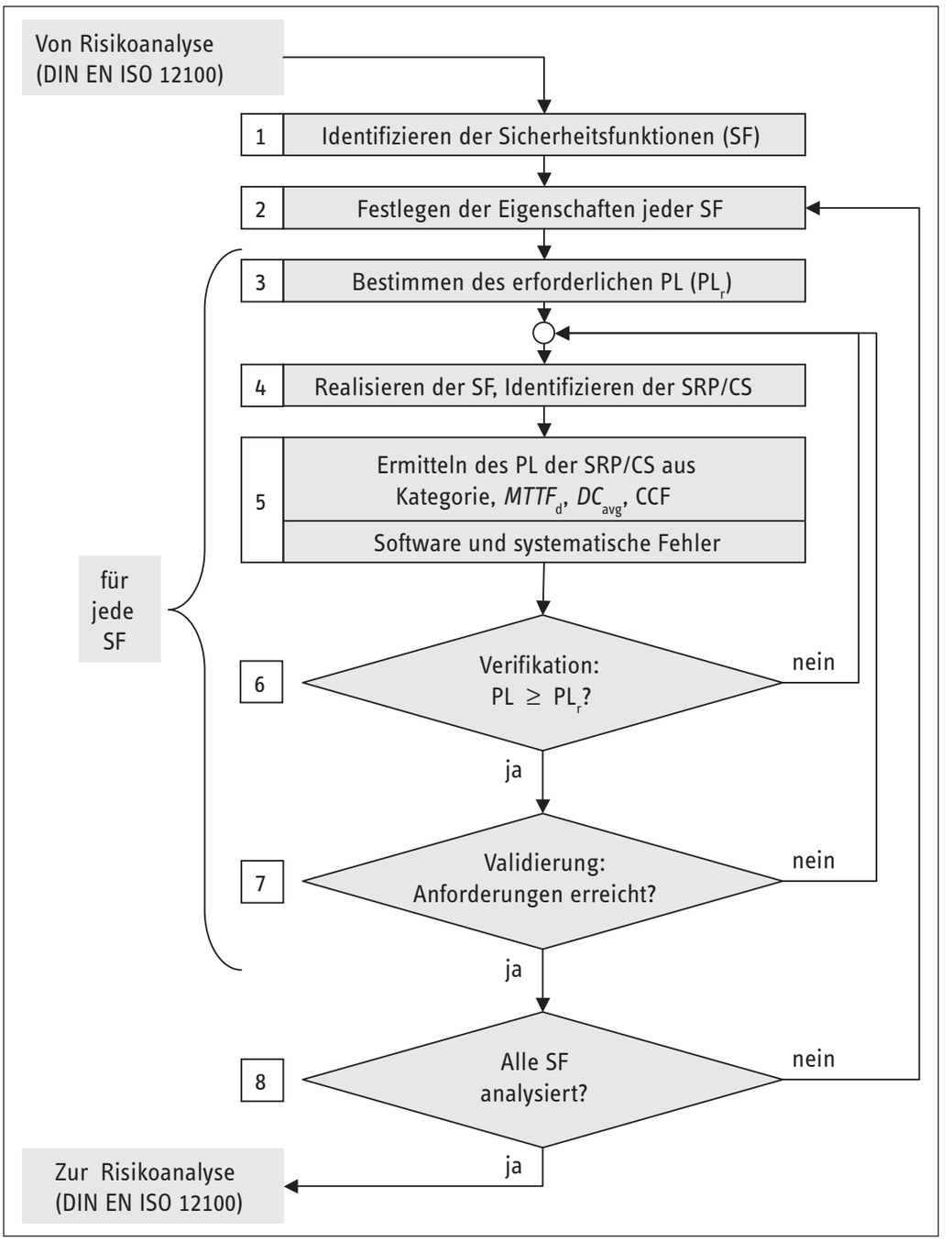


Abbildung 4.1: Iterativer Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen: SF = Sicherheitsfunktion; PL = Performance Level; PL_r = erforderlicher Performance Level; SRP/CS = Safety-Related Parts of Control Systems (sicherheitsbezogene Teile der Steuerung); $MTTF_d$ = Mean Time 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)

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?

Eine Maschine soll zunächst derart gebaut sein, dass für den Nutzer 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 heute meistens von der Steuerung durchgeführt werden. Damit diese Schutzmaßnahmen, man spricht bei der technischen Umsetzung auch von Schutzeinrichtungen, abhängig vom Risiko eine bestimmte Qualität erreichen, ist die Risikobeurteilung ein wesentlicher Schritt. Die Schutzeinrichtung führt dann als sicherheitsbezogener Teil einer Steuerung die Sicherheitsfunktion vollständig oder zumindest teilweise aus. Sie kann zum Beispiel den unerwarteten Anlauf verhindern, wenn ein Bediener einen Gefahrenraum betritt. Da es an einer Maschine durchaus mehrere Sicherheitsfunktionen geben kann (z.B. für Automatik- und Einrichtbetrieb), ist eine sorgfältige Betrachtung jeder einzelnen Gefährdung und der mit ihr verbundenen Sicherheitsfunktion sehr wichtig.

Die Sicherheitsfunktion kann von Teilen der Steuerung oder von zusätzlich notwendigen Komponenten übernommen werden. Beides sind 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 Steuerung anteilig leisten muss, dann hilft ein einfaches Diagramm, der „Risikograph“, bei der schnellen und direkten Bestimmung des geforderten Performance Levels PL_r (Beispiele im Anhang A). Ist die Verletzung irreversibel (z.B. Tod, Verlust von Körperteilen) oder reversibel (z.B. Quetschungen, die verheilen können)? Hält sich der Bediener häufig und lange im Gefahrenbereich auf (z.B. öfter als einmal pro Stunde) oder selten und kurz? Hat er eine Möglichkeit, den Unfall noch zu vermeiden (z.B. wegen langsamer Maschinenbewegung)? Diese drei Fragen entscheiden über den PL_r. Details findet der Leser in Abschnitt 5.4.

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 des BIA-Reports 6/97 enthält auch dieser Report im Kapitel 8 viele gerechnete Schaltungsbeispiele für alle Steuerungstechnologien und jede Kategorie. Ein ausführlich beschriebenes Schaltungsbeispiel begleitet zusätzlich die allgemeinen Ausführungen in den Kapiteln 5, 6 und 7. Dadurch werden dem Entwickler die nachfolgend beschriebenen Methoden und Parameter anschaulich vermittelt.

Sicherheitsbezogene Teile von Steuerungen sind voraussichtlich nur so gut wie zunächst die Sinnfälligkeit ihrer Sicherheitsfunktion. Danach folgen als Qualitätskriterien die Güte der verwendeten Bauteile (Lebensdauer), ihr Zusammenspiel (Dimensionierung), die Wirksamkeit der Diagnose (z.B. Selbsttests) und die Fehlertoleranz (Fehlersicherheit) der Struktur. Aus diesen Parametern bestimmt sich die Wahrscheinlichkeit eines gefährlichen Ausfalls und somit der erreichte PL. Die Revision der 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 Benutzung eines Säulendiagramms (siehe Abbildung 6.10), in dem diese Modellierung des PL schon vorweggenommen ist. Für Experten: Die Herleitung des Säulendiagramms findet sich in Anhang G.

Die Kategorien bleiben auch nach der Revision der Norm das Fundament bei der Bestimmung des PL. An ihrer Definition hat sich im Wesentlichen nichts geändert, allerdings werden 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, in der die drei rechten Spalten die Neuerungen in der Norm aufzeigen. 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, 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“ FMEA (Failure Mode and Effects Analysis, Ausfalleffektanalyse) werden in DIN EN ISO 13849-1 vereinfachte Rechenmethoden wie z.B. das „Parts Count“-Verfahren angeboten. Eine detaillierte Beschreibung dieser Thematik findet sich in Anhang B.

Tabelle 4.1:
Deterministische und probabilistische Merkmale der Kategorien; Ergänzungen nach der Revision 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
Diagnosedeckungsgrad – DC_{avg}	kein	kein	niedrig bis mittel	niedrig bis mittel	hoch
Maßnahmen gegen CCF			X	X	X
Hauptsächlich charakterisiert durch	Bauteilauswahl		Struktur		

Eine der meistgestellten Fragen zur Ausfallwahrscheinlichkeit betrifft die Beschaffung zuverlässiger Ausfalldaten, der $MTTF_d$-Werte (Mean Time to Dangerous Failure), für die sicherheitsbezogenen Komponenten. Hier ist der Bauteile- oder Komponentenhersteller mit seinem technischen Datenblatt allen anderen Quellen vorzuziehen. Viele Komponentenhersteller, auch im Bereich der Pneumatik, haben bereits signalisiert, dass solche Daten künftig erhältlich sein werden. Aber auch wenn es (noch) wenig Herstellerangaben 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.

Die Wirksamkeit der Diagnose, als Wert des mittleren Diagnosedeckungsgrades DC_{avg} (average Diagnostic Coverage), ermittelt sich sehr einfach: 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 und schließlich berechnet. Weitere Informationen liefern Abschnitt 6.2.14 sowie Anhang E. Eine nur scheinbar komplexe, aber trotzdem einfache Mittelungsformel hilft, daraus die Kenngröße DC_{avg} zu berechnen.

Sehr 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 kann. 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, bei dem mindestens 65 von 100 möglichen Punkten erreicht werden müssen (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. Wie in der Einleitung erwähnt, sind die Anforderungen an die sicherheitsbezogene Software in der Norm zwar neu, aber im Einzelnen bereits 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 sogenannten 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 Künftige Entwicklung von DIN EN ISO 13849-1

Nach Erscheinen der überarbeiteten EN ISO 13849-1 im November 2006 gibt es eine dreijährige Übergangsfrist, in der die Vorgängerfassung EN 954-1 parallel gültig bleibt. Damit ist einer der meistgenannten Kritikpunkte, der Umfang der Neuerungen, die erst ihren Weg in die Köpfe der Entwickler und Anwender finden müssen, entkräftet. Dieser Prozess wird, wie zuletzt durch den BIA-Report 6/97, vom BGIA auch diesmal durch frei verfügbare Anwendungshilfen unterstützt. 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). Bereits kostenlos verfügbar ist der vom BGIA entworfene „Performance Level Calculator“ [16], der das Säulendiagramm in Form einer Drehscheibe, mit der der PL jederzeit einfach und genau ermittelt werden kann, detailliert darstellt. Weiterführende Hilfen und Literatur finden sich auf den Internetseiten des BGIA unter der Adresse www.dguv.de/bgia/13849.

5 Sicherheitsfunktionen und ihr Beitrag zur Risikominderung

Der vorliegende BGIA-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 [1] ist in Deutschland im Rahmen des Geräte- und 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 Normenreihe DIN EN ISO 12100 [2; 3] „Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze“ hervorzuheben. Dem Maschinenkonstrukteur 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 [17], 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 eine Norm mit Vermutungswirkung nicht 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 12100-1 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 auf Seite 24). 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.

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

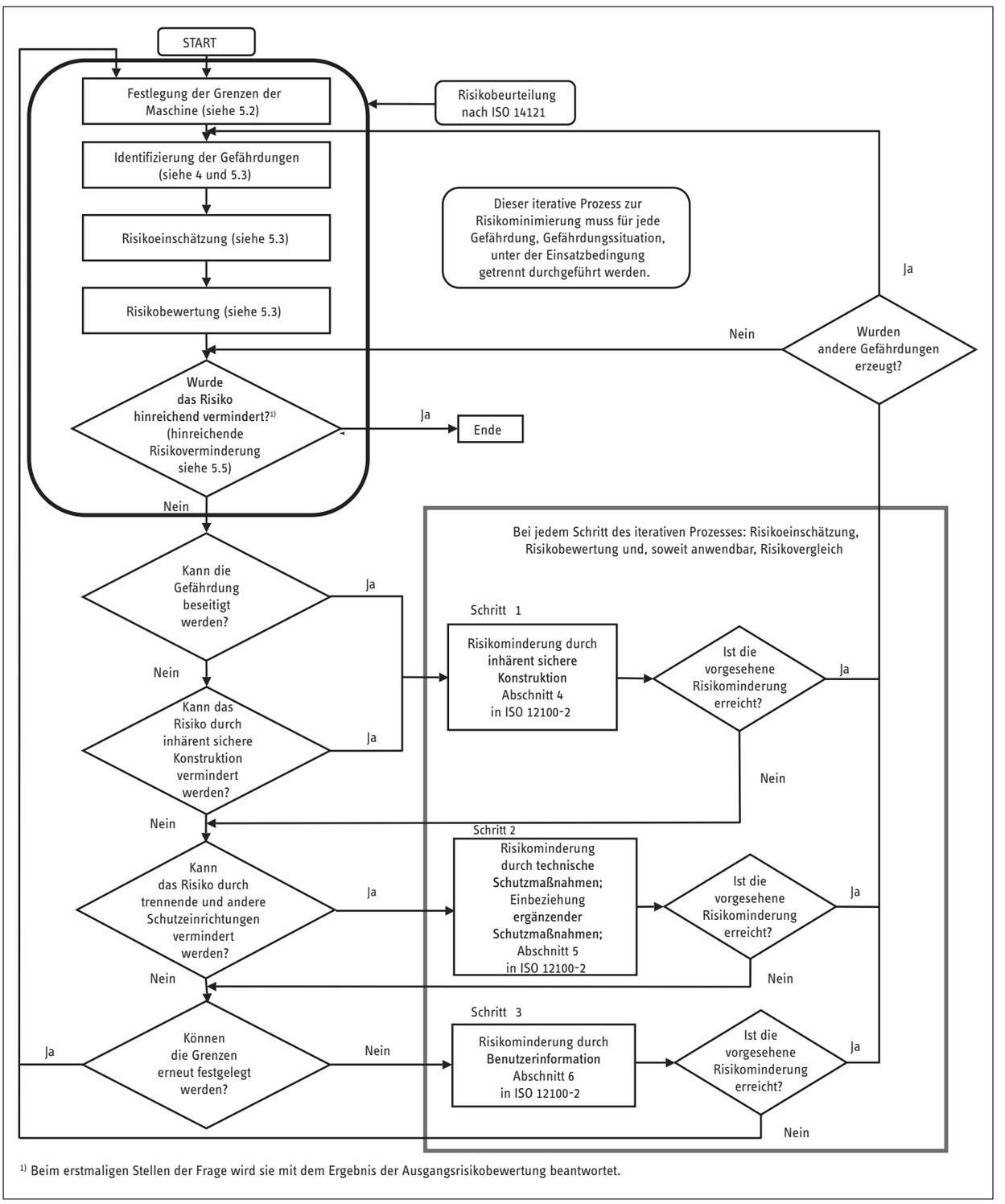
- das Einrichten,
- das Prüfen,
- das „Teachen“/Programmieren,
- die Inbetriebnahme,
- die Maschinenbeschickung,
- die Produktentnahme,
- die Fehlersuche und Fehlerbeseitigung,
- die Reinigung,
- die Instandhaltung.

Weitere Details zu diesem Prozessschritt sind in DIN EN ISO 12100-1 und DIN EN 14121-1 [4] zu finden. Für die systematische Identifizierung der Gefährdungen gibt es verschiedene Verfahren, Beispiele finden sich in ISO/DTR 14121-2 [5]. Darüber hinaus sind mögliche Gefährdungen ausführlich in [4] aufgelistet, einen Auszug zeigt Abbildung 5.2 (siehe Seite 25).

---

[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 nicht mehr dazugehört.*

Abbildung 5.1:
Iterativer Prozess zur Risikominderung



1) Beim erstmaligen Stellen der Frage wird sie mit dem Ergebnis der Ausgangsrisikobewertung beantwortet.

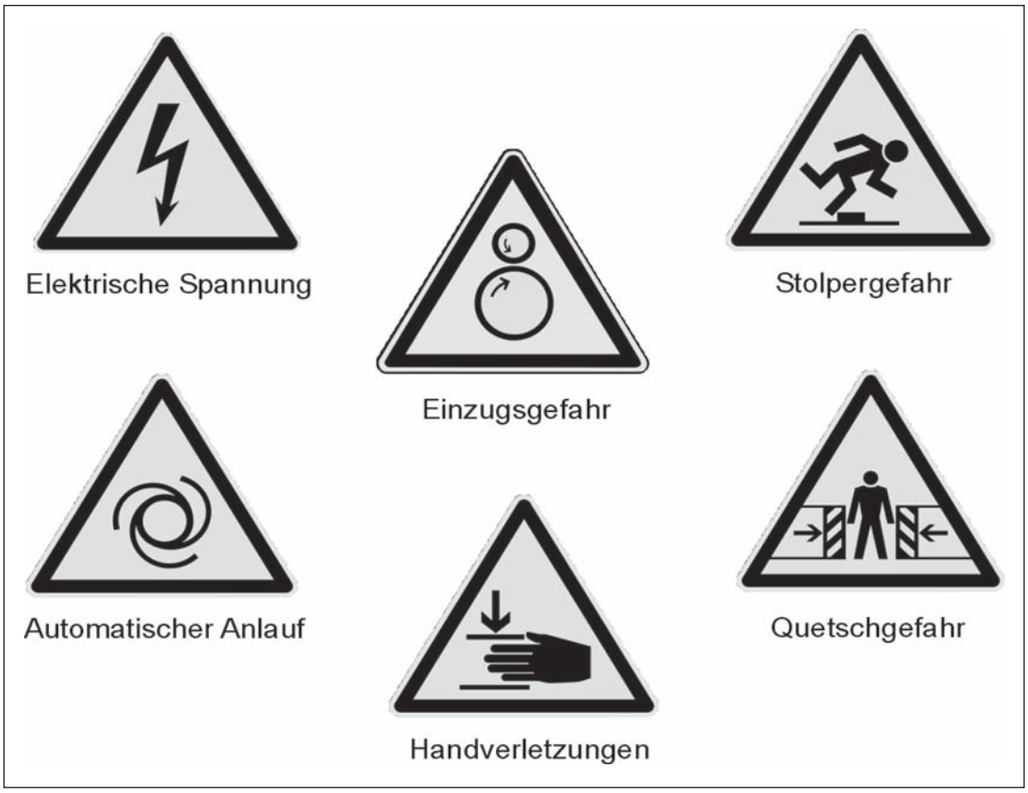


Abbildung 5.2: Beispiele für Gefährdungen (Quelle: Wikipedia)

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

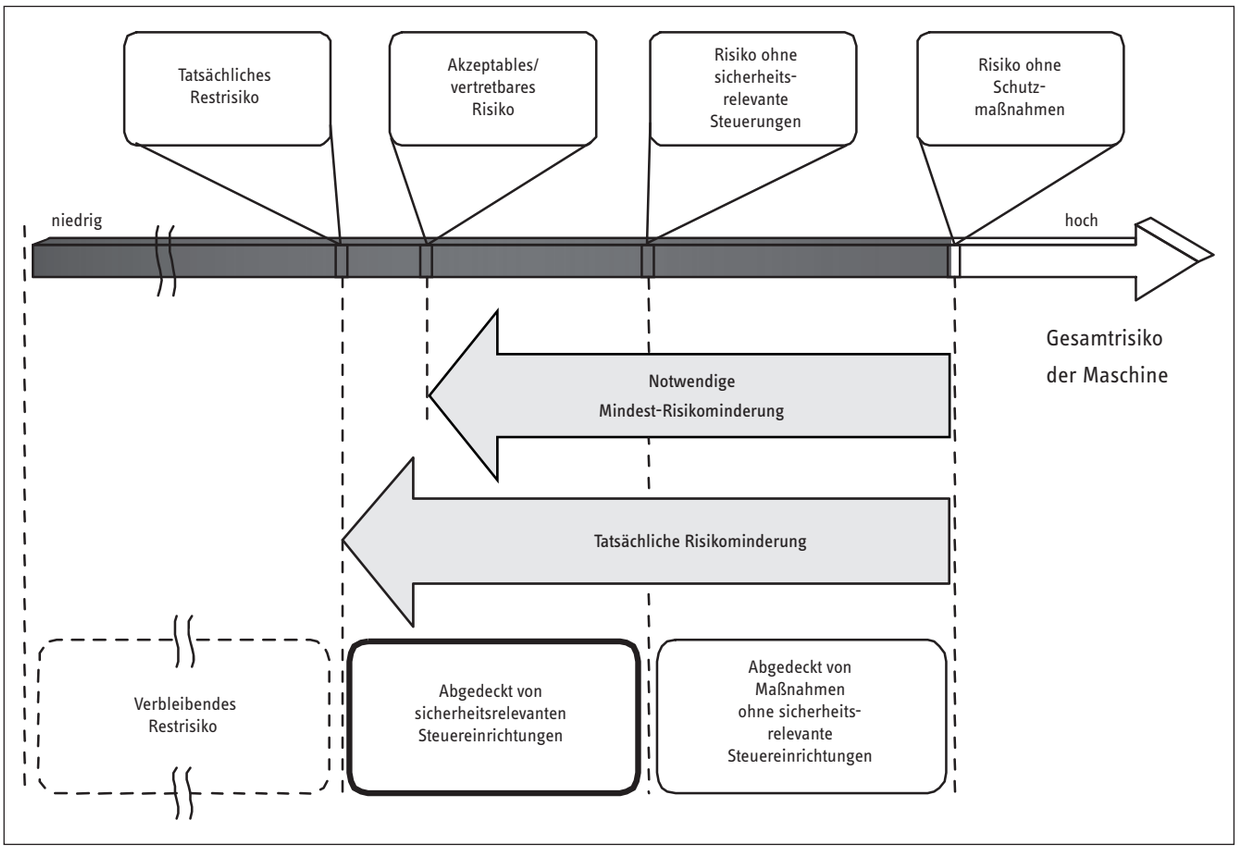
Ziel des weiteren Vorgehens ist es, das Risiko auf ein akzeptables Maß zu reduzieren. Abbildung 5.3 (siehe Seite 26) zeigt hierzu die Anteile der Risikoreduzierung mit und ohne sicherheitsrelevante Teile einer Steuerung. Weitere Informationen zum Thema Risiko enthält das BGIA-Handbuch [18].

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 12100-1 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 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?
- 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?
- Ist sichergestellt, dass die durchgeführten Schutzmaßnahmen die Arbeitsbedingungen der Bedienpersonen oder die Benutzerfreundlichkeit der Maschine nicht negativ beeinflussen?

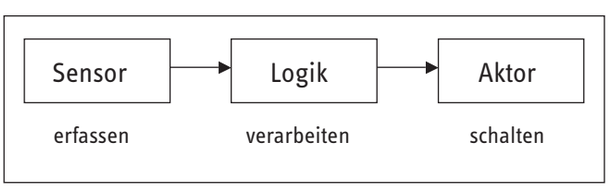
Abbildung 5.3:
Risikoeinschätzung und Risikominderung



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).

Abbildung 5.4:
Sicherheitsfunktionen werden von SRP/CS ausgeführt



Für die Gestaltung der sicherheitsbezogenen Teile von Steuerungen ist nach [6] ein iterativer Prozess vorgesehen (Abbildung 4.1). Abbildung 5.5 zeigt den für diesen Abschnitt des Reports relevanten Teil.

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) Verhinderung des Absturzes der Achse im Einrichtbetrieb

e) Ausweichen des Roboters bei Betreten seines Gefahrenbereiches

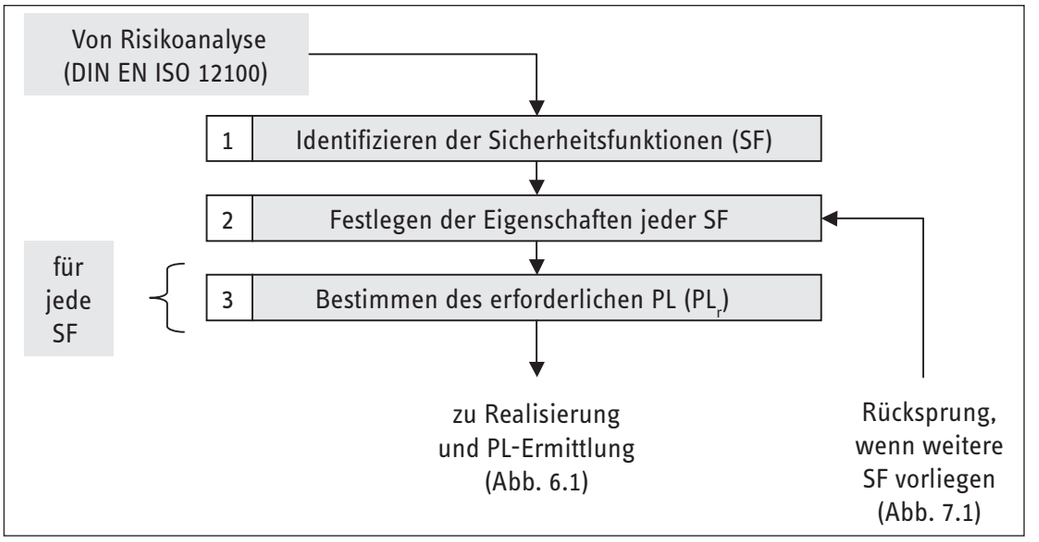


Abbildung 5.5: Ausschnitt aus dem iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP/CS)

f) Verhinderung des Einzugs von Personen

g) Unterbrechung der durch Zwei-Hand-Bedienung gesteuerten Schließbewegung bei Eingriff einer zweiten Person in den Gefahrenbereich (Auslösung durch Lichtgitter)

Häufig verwendet man zusammengesetzte Sicherheitsfunktionen wie im Beispiel in Abschnitt 5.7 (siehe Seite 32). 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 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 (siehe Seite 28) zeigt weitere Sicherheitsfunktionen für sichere Antriebssteuergeräte nach DIN EN 61800-5-2 (PDS/SR, Power Drive Systems/ Safety Related) [19]. Diese Norm enthält u.a. die häufig angewendeten Sicherheitsfunktionen zur Verhinderung eines unerwarteten Anlaufs STO (STO, Safe Torque Off; früher SH, Sicherer Halt), zum sicheren Stillsetzen SS1 und SS2 und zur sicheren Begrenzung einer Geschwindigkeit SLS (SLS, Safely-Limited Speed; früher SRG, Sicher Reduzierte Geschwindigkeit).

Tabelle 5.1:
Sicherheitsfunktionen aus DIN EN ISO 13849-1

Sicherheitsfunktion	Beispiel für mögliche Anwendung
Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung	Reaktion auf das Auslösen einer Schutzeinrichtung durch 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 12100-2
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

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	Safe Stop 1	Sicherer Stopp 1	Motor verzögert; Überwachung Bremsrampe und STO nach Stillstand oder STO nach Ablauf einer Verzögerungszeit; Stopp-Kategorie 1 nach DIN EN 60204-1
SS2	Safe Stop 2	Sicherer Stopp 2	Motor verzögert; Überwachung Bremsrampe und SOS nach Stillstand oder SOS nach Ablauf einer Verzögerungszeit; 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 Geschwindig-keitsüberwachung	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)
- 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

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

In späteren Kapiteln wird gezeigt, wie die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde für eine Sicherheitsfunktion berechnet werden kann. Die Grundlagen hierfür werden jedoch bereits hier bei der Definition der Sicherheitsfunktion festgelegt. Die 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 ein Maschinenbediener Zugang zu einem Gefahrenbereich, in dem fünf Antriebe Bewegungen von Maschinenteilen steuern. Das Öffnen der Schutztür bewirkt ein schnellstmögliches Stillsetzen aller fünf Antriebe. Das zugehörige funktionale Schaltbild ist in Abbildung 5.6 dargestellt.

Bei der späteren Berechnung des PL der Sicherheitsfunktion werden daher die PLs der folgenden Blöcke[1], z.B. nach Tabelle 6.6, verknüpft:

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

Das Resultat kann ein PL sein, der für die Anwendung nicht mehr ausreichend ist, obwohl vielleicht nur die Antriebe 1 und 3 für den Bediener 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 sind.

Beispiel 2: Sicherheitsfunktion
„Stillsetzen 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. Im Hinblick auf die spätere Bestimmung des PL ist jede Tür Bestandteil einer eigenen Sicherheitsfunktion SF1 bis SF5, die sich aus folgenden Blöcken[1] 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 5.6:
Stillsetzen beim Öffnen der Schutztür

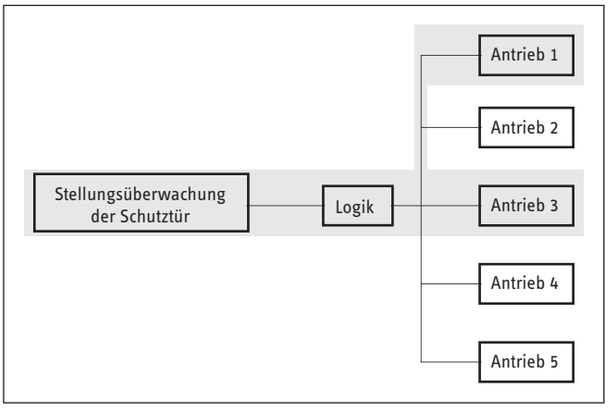
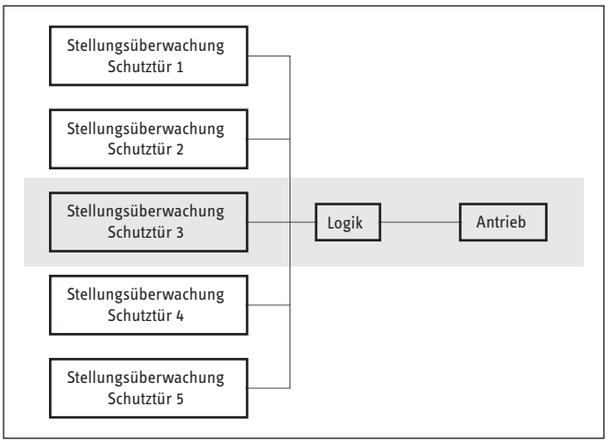


Abbildung 5.7:
Stillsetzen beim Öffnen der Schutztür 3



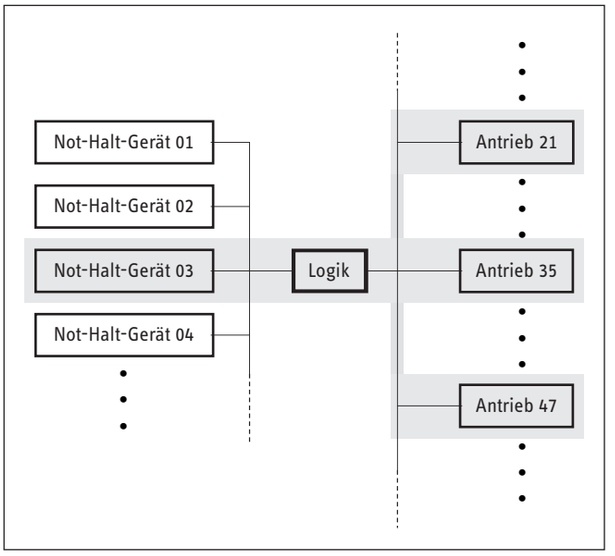
Beispiel 3: Sicherheitsfunktion „Not-Halt einer Gesamtmaschine" (siehe Abschnitt 5.5)

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 Sicherheitsfunktion zu berücksichtigen? Es ist nicht vorhersehbar, welches Not-Halt-Gerät zum Auslösen der Sicherheitsfunktion betätigt wird. Da der Bediener immer nur ein Not-Halt-Gerät betätigt, werden die Sicherheitsfunktionen 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 den schlechtesten PL, ist also u.a. abhängig von der Anzahl der Antriebe in der Sicherheitskette, die am ungünstigsten Standort gefahrbringende Bewegungen erzeugen, sowie den jeweiligen einzelnen PL. Das zugehörige Blockschaltbild ist in Abbildung 5.8 (siehe Seite 30) dargestellt.

---

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

Abbildung 5.8:
Not-Halt der Gesamtmaschine, ungünstigster Fall



Bei der späteren Bestimmung des PL für die Sicherheitsfunktion müssen die PL-Werte der folgenden Blöcke, z.B. nach Tabelle 6.6, berücksichtigt werden:

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

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?
- Welche Schutzeinrichtungen müssen die Sicherheitsfunktion auslösen? Ggf. sind mehrere alternativ benutzbare Schutzeinrichtungen zu berücksichtigen.

5.4 Bestimmung des erforderlichen Performance Level PL_r

Für jede vorgesehene Sicherheitsfunktion muss ein erforderlicher Performance Level PL_r[1] festgelegt werden – im technischen Sinne der Sollwert. Die Anforderungen ergeben sich aus der notwendigen Risikominderung, bei deren Festlegung u.a. ein ggf. bekanntes Unfallgeschehen zu berücksichtigen ist. ISO/DTR 14121-2 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

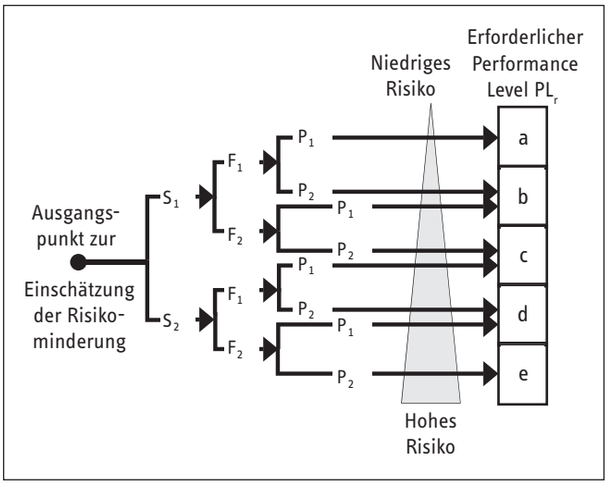
Das Diagramm im Anhang A der Norm führt direkt zum erforderlichen Performance Level PL_r und wird im Folgenden erläutert (siehe Abbildung 5.9). Weitere Beispiele zur Bestimmung des PL_r finden sich in Anhang A.

Beginnend am Ausgangspunkt werden die Risikoparameter[2]

- 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.

Abbildung 5.9:
Risikograph zur Bestimmung des PL_r für jede Sicherheitsfunktion



---

[1] *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 $PL \geq PL_r$ ist. „>“ bedeutet in diesem Zusammenhang: PL = e > PL = d > PL = c > PL = b > PL = a*

[2] *Die Wahrscheinlichkeit für den Eintritt eines Gefährdungsereignisses ist in der Praxis kaum zu bestimmen. Zur Vereinfachung ist daher im Risikographen bereits der ungünstigste Fall eingearbeitet und eine weitere Bewertung nicht mehr erforderlich.*

Schwere der Verletzung S1 und S2

Die Schwere der Verletzung 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

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

Eine feste Grenze zur Auswahl zwischen F1 und F2 kann leider nicht angegeben werden. Die Norm gibt in einer Anmerkung den nicht normativen Hinweis, dass bei Eingriffen, die häufiger als einmal pro Stunde erfolgen, F2 gewählt werden sollte, sonst F1. Dieser Hinweis passt aber in der Regel auf alle in der Praxis vorkommenden Fälle. Bei der Bewertung ist ein durchschnittlicher Wert der Gefährdungsexposition im Verhältnis zur gesamten Nutzungszeit einer Maschine zu berücksichtigen. Eindeutige Fälle liegen jedoch vor, z.B. bei einer manuell beschickten Presse in der Metallbearbeitung, bei der zyklisch zwischen die Werkzeuge der Maschine gegriffen werden muss (F2). 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

An dieser Stelle soll bewertet werden, ob 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 und die mögliche Reaktion des Bedieners 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: Der Bediener 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 des Bedieners 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 des Bedieners 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.

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

5.4.2 Übergang von einer erforderlichen Kategorie nach DIN EN 954-1 zu einem PL_r

Für die Anwendung der DIN EN ISO13849-1:2007 ist es notwendig, den PL_r zu kennen. Wie im vorherigen Abschnitt beschrieben, ist zu dessen Bestimmung eine Risikoeinschätzung erforderlich. Für Normensetzer und Maschinenhersteller wäre es jedoch einfacher, wenn man den PL_r aus einer bekannten **erforderlichen Kategorie** nach DIN EN 954-1:1997 ableiten könnte. Eine solche Übertragung ist jedoch nur zulässig, sofern an einer Maschine gleiche Gefährdungen mit gleichen Risiken vorliegen. Kann man also den PL_r ohne erneute Risikoeinschätzung ermitteln?

Sowohl die erforderliche Kategorie nach DIN EN 954-1 als auch der PL_r nach der neuen Norm werden durch eine Risikoeinschätzung ermittelt. Unterstellt man, dass die erforderliche Kategorie anhand des Risikographen aus DIN EN 954-1 bestimmt wurde und überträgt die hierbei verwendeten Parameter S, F und P (siehe Abschnitt 5.4.1) auf den Risikographen der neuen Norm, so stellt man fest, dass es nicht für alle erforderlichen Kategorien eine eindeutige Zuordnung zum PL_r gibt.

Weiterhin ist zu berücksichtigen, dass bei der Überführung einer erforderlichen Kategorie nach DIN EN 954-1 in einen PL_r die Anforderung an die zu realisierende Struktur der SRP/CS verloren geht. Kapitel 6 erläutert, mit welchen vorgesehenen Architekturen die Kategorien verbunden sind, z.B. die Testung mit Kategorie 2 und die Einfehlersicherheit mit Kategorie 3. Würde man einer erforderlichen Kategorie 3 nach DIN EN 954-1 einen PL_r = d zuordnen, so könnte eine Sicherheitsfunktion nun auch in der Kategorie 2 realisiert werden (siehe Abbildung 6.10). Die bisherige hochwertige Einfehlersicherheit der Kategorie 3 würde also bei dieser einfachen Umsetzung durch eine funktional einkanalige Struktur mit Testeinrichtung realisierbar sein.

Dies ist ein beabsichtigter Freiheitsgrad der neuen Norm, der jedoch bei der Festlegung des PL_r berücksichtigt werden muss. So ist bei der Auswahl einer erforderlichen Kategorie u.a. das entstehende Risiko im Fall eines Fehlers der SRP/CS zu beachten (siehe DIN EN 954-1, Abschnitt 6.3, bzw. DIN EN ISO 13849-1, Abschnitt 6.1). Diese Anforderung könnte in dem betrachteten Beispiel zur Festlegung der erforderlichen Kategorie 3 nach DIN EN 954-1 geführt haben.

Aus diesen Überlegungen ergibt sich, dass beim Übergang von einer erforderlichen Kategorie nach DIN EN 954-1 in einen erforderlichen PL_r zusätzliche Informationen nowendig sein können, die in der Regel nicht mehr verfügbar sind. Wird keine neue Risikoanalyse durchgeführt, bietet sich als Ausweg ein Worst-case-Ansatz mit gleichzeitiger Festlegung von PL_r und erforderlicher Kategorie an, wie Tabelle 5.3 (siehe Seite 32) zeigt. Hierbei wird vorausgesetzt, dass ggf. zusätzliche Maßnahmen, die entsprechend DIN EN 954-1 zu einer Auswahl der „möglichen Kategorie“ anstelle der „bevorzugten Kategorie“ geführt haben, weiterhin wirksam sind.

Erforderliche Kategorie nach DIN EN 954-1:1997		Erforderlicher Performance Level PL_r und erforderliche Kategorie nach DIN EN ISO 13849-1:2007
B	➔	b
1	➔	c
2	➔	d, Kategorie 2
3	➔	d, Kategorie 3
4	➔	e, Kategorie 4

Tabelle 5.3: Worst-case-Ansatz zum Übergang von einer erforderlichen Kategorie nach DIN EN 954-1 zu einem erforderlichen Performance Level PL_r

5.5 Ergänzende Schutzmaßnahmen

Die Anforderungen an ergänzende Schutzmaßnahmen sind in DIN EN ISO 12100-2 [3], Abschnitt 5.5, 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, für deren Realisierung ein bestimmter Performance Level erforderlich wäre. Allerdings sollen diese ergänzenden Schutzmaßnahmen dann greifen, wenn technische Schutzmaßnahmen (trennende und/oder nicht trennende Schutzeinrichtungen) versagt haben bzw. durch Manipulation unwirksam gemacht wurden. Besonders in diesen Fällen erwartet man, dass z.B. ein Not-Halt auch funktionsfähig ist. Insofern sind die Anforderungen der DIN EN 60204-1 [20] 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. Die Anforderungen der DIN EN ISO 13849 gelten letztlich also auch für diese ergänzenden Schutzmaßnahmen. 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 Diagramm der Berufsgenossenschaft der chemischen Industrie [21].

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

Das folgende Beispiel 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 den Bediener auch genügend Platz zur Bereitstellung von Schneidgut, Abfuhr bzw. Lagerung der geschnittenen Papierstapel und 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 Bewegung verlängern. Die daraus resultierende Überschreitung des Nachlaufwegs muss daher detektiert werden und zu einer Stillsetzung der Maschine führen.

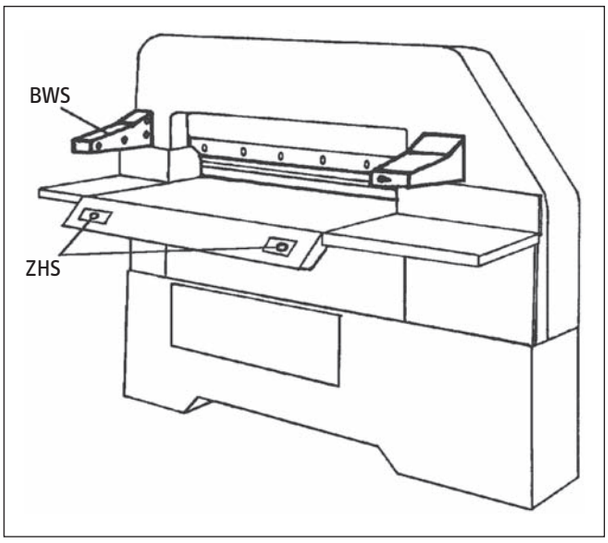
Verwendungsgrenzen

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

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



In den ersten drei Betriebsarten ist eine alleinige Bewegung des Pressbalkens möglich, um die Schnittlinie anzuzeigen (Schnitt andeuten). Hierzu betätigt der Bediener 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 den Bediener praktisch keine Möglichkeit besteht, die Gefahr abzuwenden. Bei stillstehendem Messer (Gefährdung G3) hat der Bediener die Möglichkeit, den Schaden zu vermeiden oder zu begrenzen.

Die Eintrittswahrscheinlichkeit eines Schadens als Funktion des Eintritts eines Gefährdungsereignisses wird an dieser Stelle nicht bewertet, da hierfür im Folgenden der Worst-case angenommen wird.

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 der Bediener in den Gefahrenbereich eingreifen kann, ist nicht möglich, da er 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.

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 des Bedieners 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

SF7 – Abdeckung des Messers durch den Pressbalken

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 DIN EN 1010-3).

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

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. Abbildung 5.11 zeigt hierzu Dokumentation und Risikograph in der Software SISTEMA für die Sicherheitsfunktion SF1.

Für die Gefährdung G3 „Schneiden durch das Schneidmesser im Ruhezustand“ ist die Sicherheitsfunktion SF7 vorgesehen. Folgende Risikoparameter werden hierfür festgesetzt:

S1 – leichte, üblicherweise reversible Verletzung

F2 – Zeit der Gefährdungsexposition ist lang

P1 – Vermeidung einer Gefährdungssituation möglich unter bestimmten Bedingungen

Entsprechend dem Risikographen in Abbildung 5.9 ergibt sich aus dieser Bewertung ein erforderlicher Performance Level PL_r = b. Abbildung 5.12 zeigt hierzu Dokumentation und Risikograph in der Software SISTEMA für die Sicherheitsfunktion SF7.

Abbildung 5.11:
Dokumentation und Risikograph für SF1

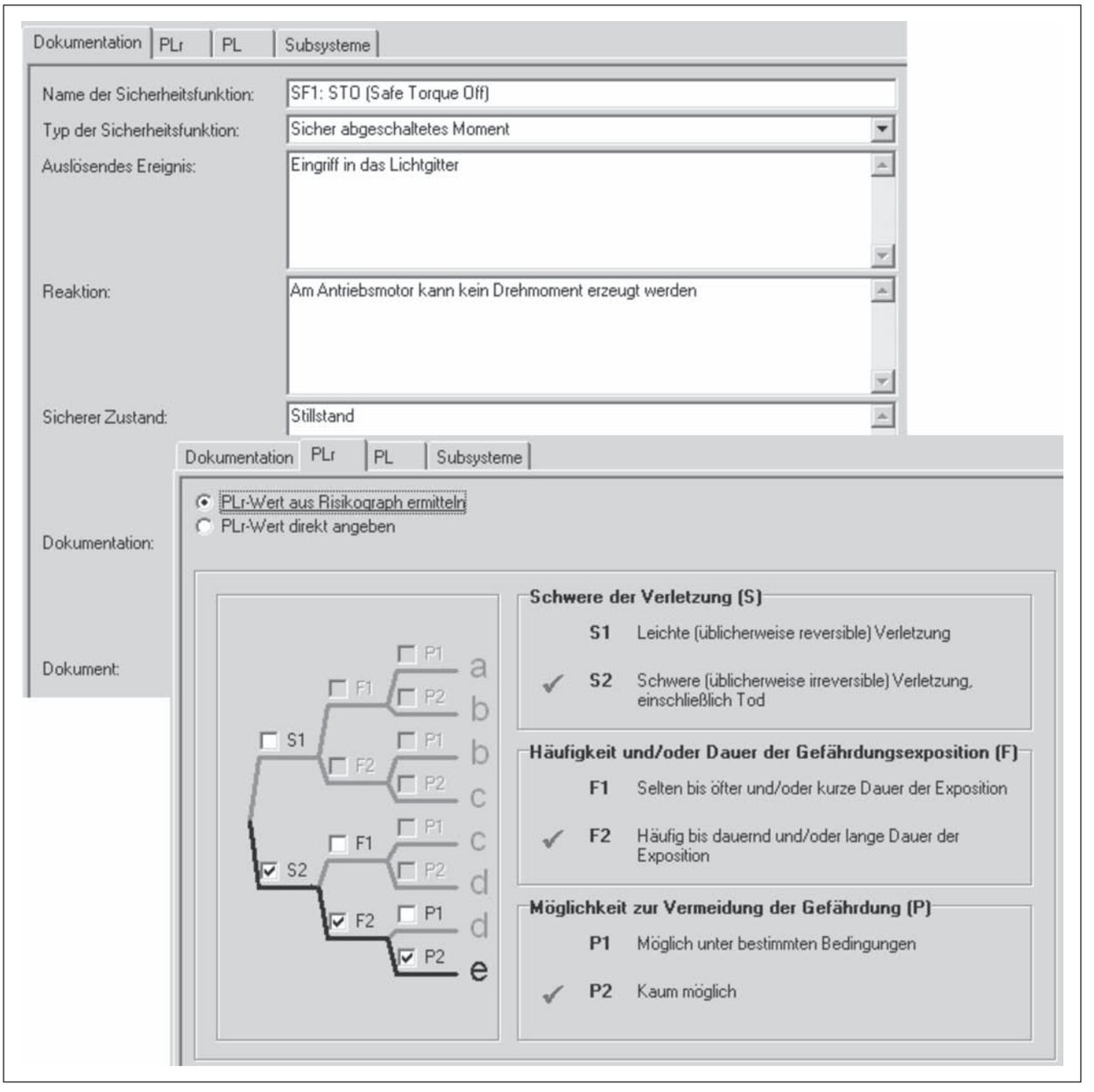
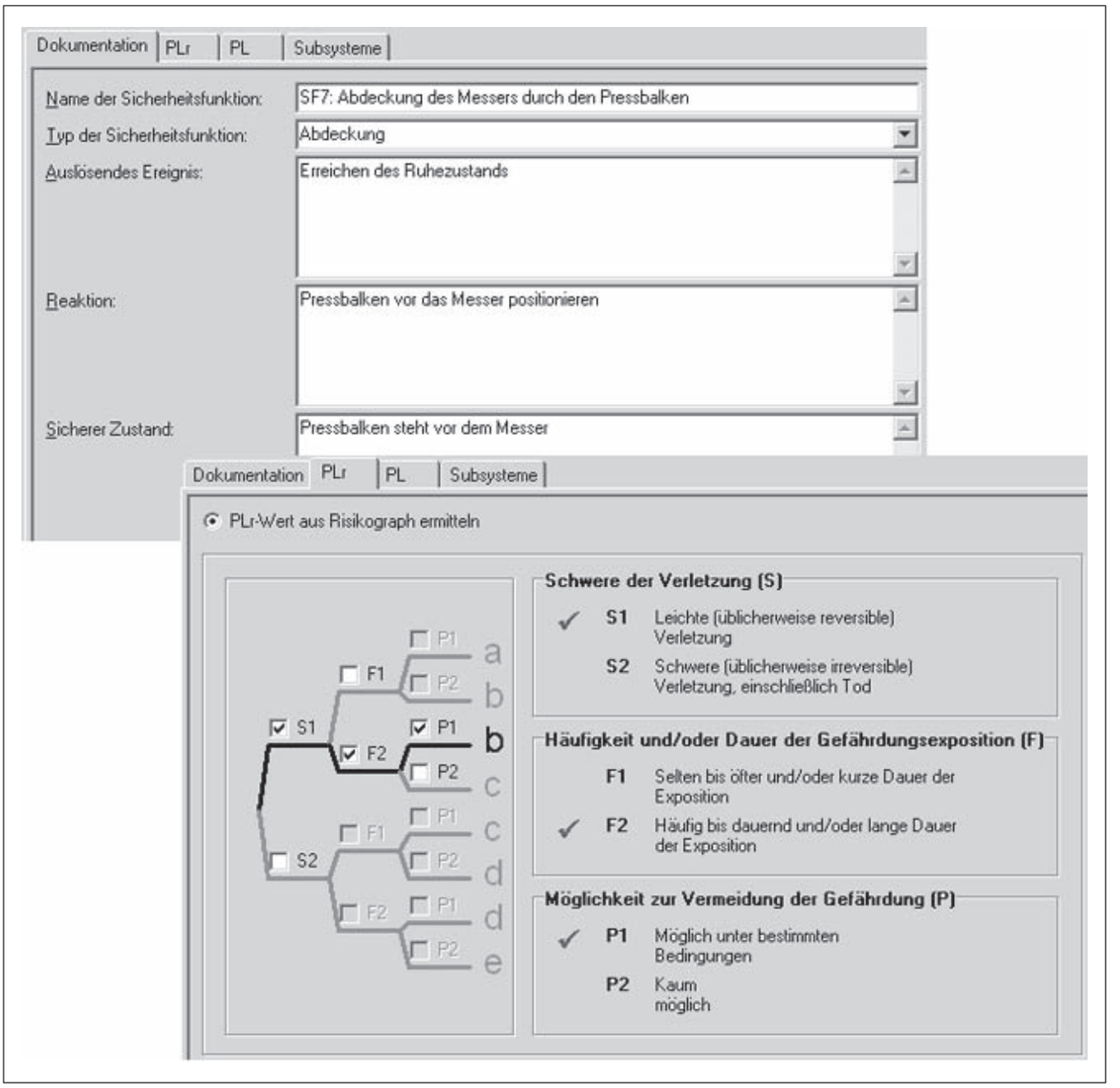


Abbildung 5.12:
Dokumentation und Risikograph für SF7



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-Befehlsgerätes 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

6.1 Einleitung

Wenn die genaue Sicherheitsfunktion und ihre geforderte 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.

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). Neben der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde, die auch als *PFH* (Probability of a Dangerous Failure per Hour) bezeichnet wird, sind weitere Maßnahmen, z.B. zur Ertüchtigung von Software oder gegen systematische Ausfälle, notwendig, um den entsprechenden PL zu erreichen.

Tabelle 6.1:
Zuordnung der Ausfallwahrscheinlichkeit zu den Performance Level

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (*PFH*) 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 $< 10^{-7}$

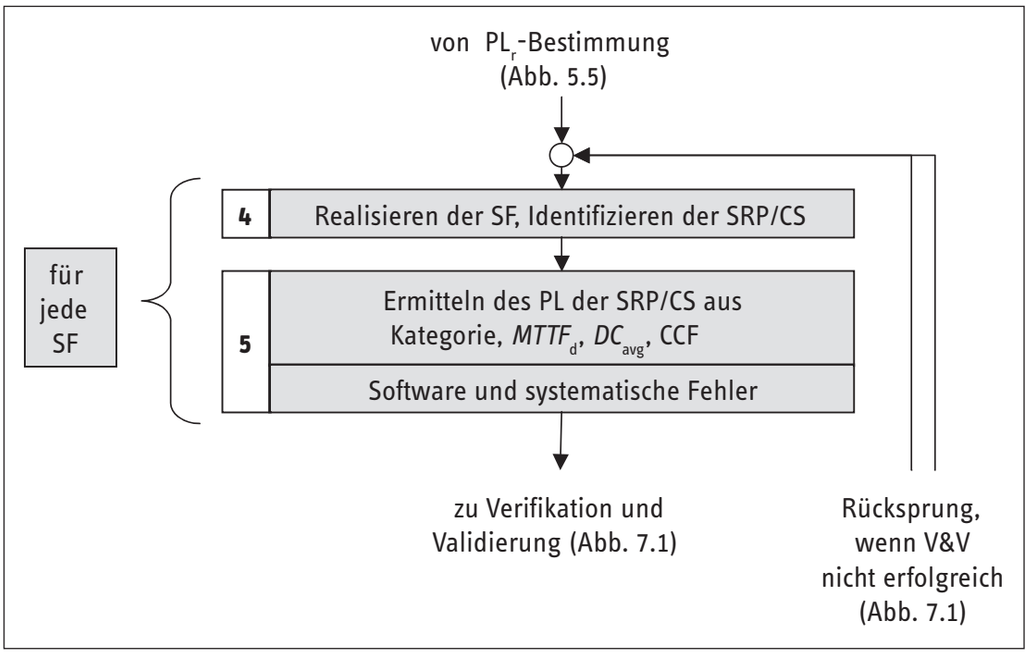


Abbildung 6.1: Ermittlung des erreichten PL in der Realisierungsphase der SRP/CS als Ausschnitt aus dem iterativen Gestaltungsprozess, siehe Abbildung 4.1

Das Verfahren 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 Selbsttests, 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 Fremdkräfte (z.B. an Vertikalachsen), so müssen die Leistungselemente zusätzlich sicherheitstechnisch ertüchtigt sein (z.B. Rückschlagventil an Zylindern, zusätzliche mechanische Bremse). Abschnitt 6.5 schließlich beschreibt – wie schon im Abschnitt 5.7 – die konkrete Umsetzung am praktischen Beispiel einer Planschneidemaschinensteuerung.

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 12100-1 muss, wie in Abbildung 6.3 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 Abschnitt 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.

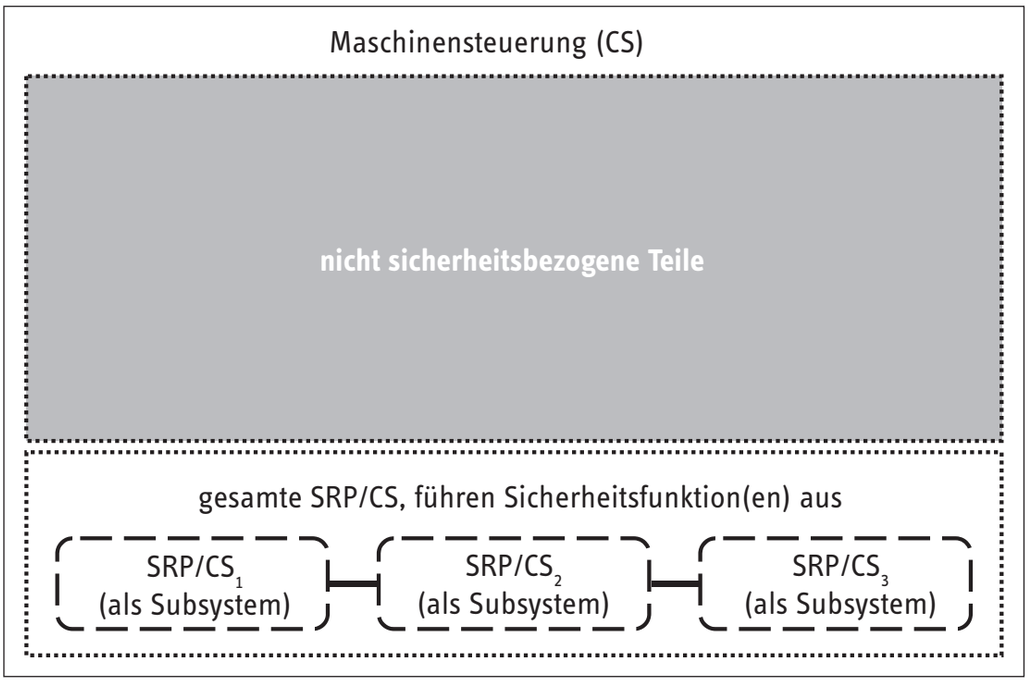
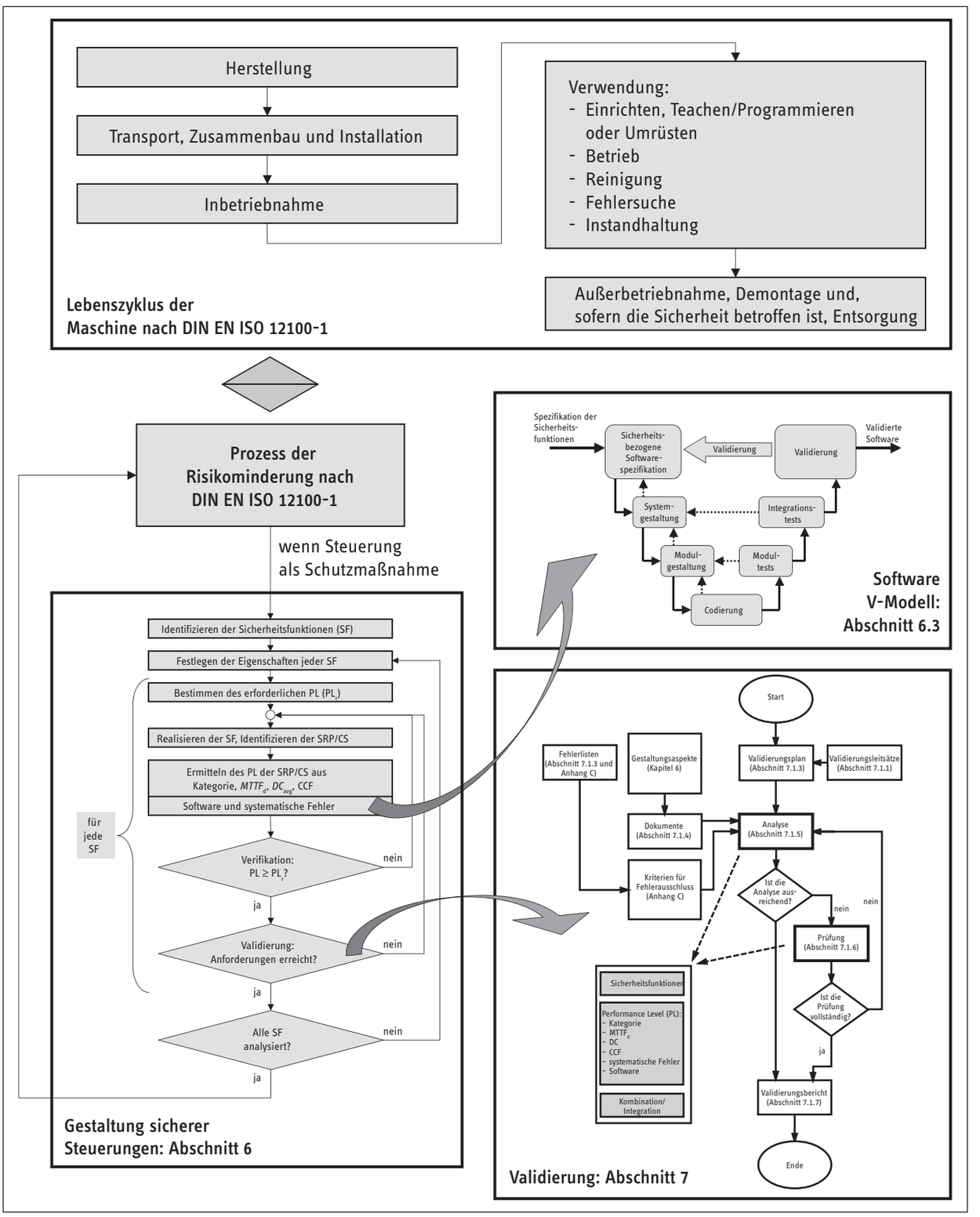


Abbildung 6.2: SRP/CS und Subsysteme innerhalb der Maschinensteuerung

Abbildung 6.3:
Lebenszyklen von Maschine und SRP/CS



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. SRP/CS, die nicht speziell für eine 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 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.

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 jemand anderem als dem Entwickler 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 sogenannte 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 Kapitel 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 (siehe Seite 42) zeigt den Inhalt der erforderlichen technischen Unterlagen für Maschinen aus der zukünftigen (neuen) europäischen Maschinenrichtlinie 2006/42/EG [8], die ab 29. Dezember 2009 anzuwenden ist.

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)
2.4 Kenndaten, z.B. Zykluszeiten, Reaktionszeiten, Nachlaufwege
2.5 Sonstige Eigenschaften der Maschine
2.6 Sicherer Zustand der Maschine
2.7 Wechselwirkung zwischen Prozessen (siehe auch 2.2) und manuellen Aktionen (Reparatur, Einrichten, Reinigen, Fehlersuche usw.)
2.8 Handlungen im Notfall

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)
- Funktionsbeschreibung („Erfassen – Verarbeiten – Ausgeben“) einschließlich aller funktionaler 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
- 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, Bedienerschnittstellen, 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

Kasten 6.2:

Technische Unterlagen für Maschinen: Auszug aus zukünftiger 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

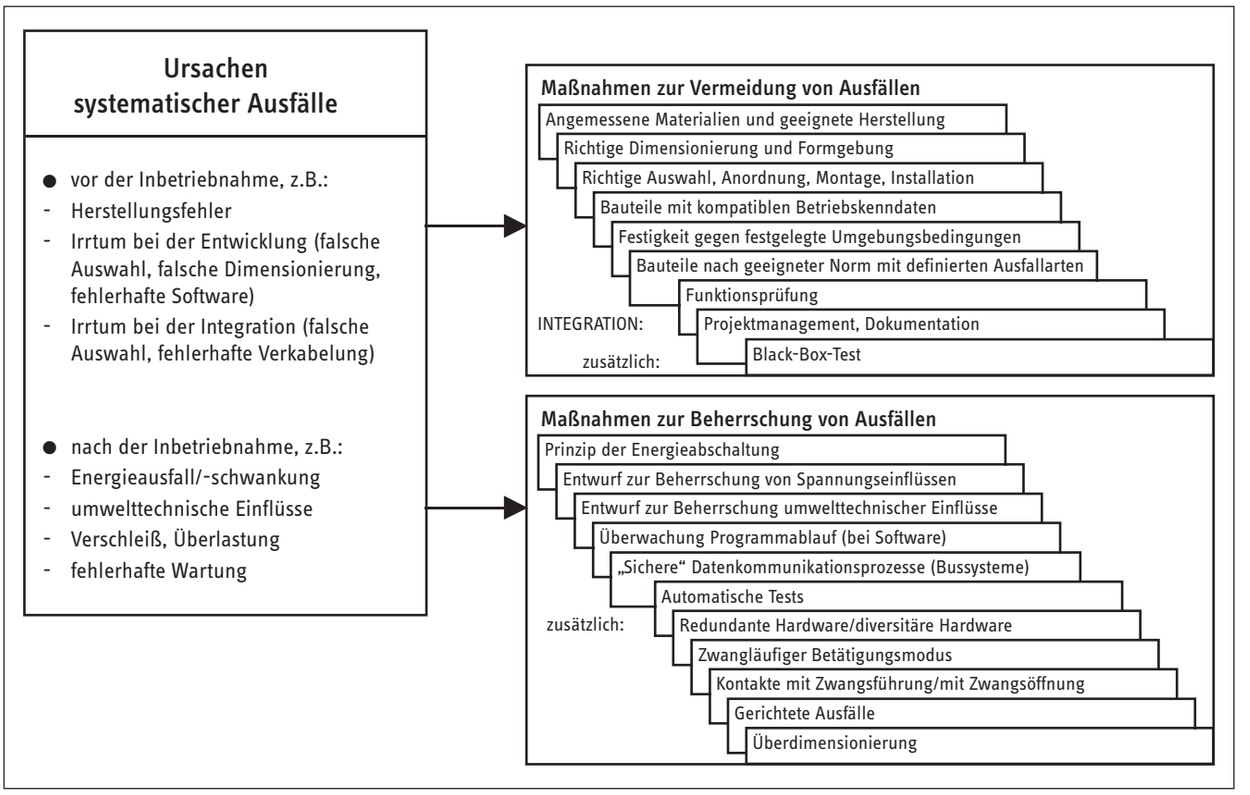
Systematische Ausfälle haben im Gegensatz zu zufälligen Bauteilausfällen Ursachen, die nur durch eine Änderung z.B. der Gestaltung oder des Herstellungsprozesses, der Betriebsverfahren oder der Dokumentation beseitigt werden können. Sie entstehen irgendwann im Laufe des Lebenszyklus eines Produktes, 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 BGIA ein großer Nutzen unterstellt wird – vergleiche dazu auch die Ausführungen zu Anforderungen an Software im Abschnitt 6.3.10.

Der aufmerksame Leser 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 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.

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



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 Anforderungen auf einen geringeren PL_r zu reduzieren, z.B. weil der Ausfall der Energieversorgung selten vorkommt, ist nicht zulässig, da die für die Risikobeurteilung relevanten Parameter S, F und P durch die Berücksichtigung eines Energieausfalls nicht verändert werden.

Beispiel 2:
Versagen von Pneumatik- bzw. Hydraulikventilen

DIN EN ISO 13849-2, Tabelle B.1 „Grundlegende Sicherheitsprinzipien der Pneumatik“ und Tabelle 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 ist in Tabelle C.1 „Grundlegende Sicherheitsprinzipien der Hydraulik“ festgelegt, dass bei der Konstruktion von hydraulischen Bauteilen auch auf die *„richtige Dimensionierung und Formgebung“* geachtet werden muss: Dies bezieht sich z.B. vor allem auf Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Toleranzen und Herstellungsverfahren.

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) bei längerem Verbleiben in einer Schaltstellung quellen oder der Schmierfilm kann durch die Dichtkantenpressung 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 Schmutzpartikeln 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 durch entsprechende Schaltzyklen bzw. Testzyklen im Abstand von z.B. < 8 Stunden zu 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 sind 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 dem Konstrukteur 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 98/37/EG (MRL) fordert im Anhang I Abschnitt 1.1.2d vom Maschinenhersteller, dass Belästigung, Ermüdung und psychische Belastungen der Maschinenbediener unter Berücksichtigung ergonomischer Prinzipien bereits bei der Konzeption der Maschine auf ein Minimum zu reduzieren sind. Dies gilt daher auch für die Schnittstellen zwischen dem Bediener 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.

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, das zeigt der HVBG-Report „Manipulation von Schutzeinrichtungen an Maschinen“ [22] auf.

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, wurde im BGIA die Checkliste „Ergonomische Maschinengestaltung“ entwickelt. Im Oktober 2006 wurden diese Checkliste und weitere Dokumente als BG-Informationen BGI 5048-1 und BGI 5048-2 veröffentlicht [23]. 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 [24].

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 BGIA 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. Neben dieser „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, von denen sich jeder einzeln auf eine vorgesehene Architektur abbilden lässt. Wie diese Abschnitte 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.

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.

Tabelle 6.2:
Zusammenfassung der Anforderungen für Kategorien; die drei rechten Spalten zeigen die wesentlichen Änderungen gegenüber der Kategoriedefinition der alten Normfassung

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	keine	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	keine	nicht relevant

Tabelle 6.2:
(Fortsetzung)

Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_d$ jedes Kanals	DC_{avg}	CCF
2	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung getestet werden.	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	niedrig bis mittel	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	niedrig bis mittel	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

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 ein zweikanaliges System 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.

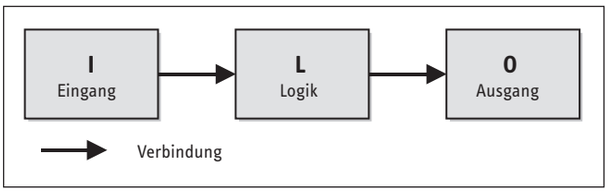
Diese allgemeinen Grundsätze lassen sich in den in Anhang C aufgeführten grundlegenden Sicherheitsprinzipien allgemein, aber auch technologiebezogen, darstellen. Die allgemeinen grundlegenden Sicherheitsprinzipien gelten dabei vollständig für alle Technologien, während die technologiebezogenen Prinzipien 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.

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 können bei einkanaligen Steuerungen nicht berücksichtigt werden, 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 nicht als gleichwertig bewährt betrachtet werden. Als Konsequenz daraus können einfache elektronische Bauteile wie Transistoren, Dioden usw. als bewährt angesehen 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 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 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
- einen Ausgang für die Einleitung geeigneter Steuerungsmaßnahmen erzeugen, wenn ein Fehler erkannt wurde. Wann immer möglich, muss dieser Ausgang einen sicheren Zustand einleiten. Dieser muss aufrechterhalten bleiben, bis der Fehler behoben ist. Ist die Einleitung eines sicheren Zustandes nicht möglich (z.B. durch Verschweißen des Kontaktes eines Schaltgliedes), muss der Ausgang die Warnung vor der Gefährdung bereitstellen.

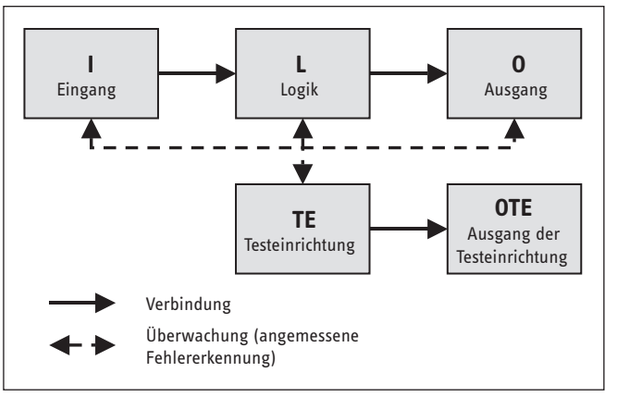
Für die vorgesehene Architektur der Kategorie 2 (Abbildung 6.6) berücksichtigt die Berechnung der $MTTF_d$ und DC_{avg} nur die Blöcke des Funktionskanals (d.h. I, L und O) und nur indirekt die $MTTF_d$ der Blöcke des Testkanals (d.h. TE und OTE). Für die $MTTF_d$ des Funktionskanals sind Werte von niedrig bis hoch erlaubt. DC_{avg} muss mindestens niedrig sein. Ausreichende Maßnahmen gegen CCF müssen angewendet werden (siehe Abschnitt 6.2.15 und Anhang F).

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. 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 ausfallen. Bei der vereinfachten Quantifizierung des PL mithilfe der vorgesehenen Architektur und des Säulendiagramms (Abbildung 6.10) wurde daher vorausgesetzt,

- dass der $MTTF_d$-Wert der Testeinrichtung TE nicht kleiner ist als der halbe $MTTF_d$-Wert der Logik L (siehe auch letzte Seite von Anhang E) und
- die Testrate mindestens 100-mal höher ist als die mittlere Anforderungsrate der Sicherheitsfunktion (siehe Abschnitt 6.2.14).

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.

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



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}. 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, siehe Seite 50). 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

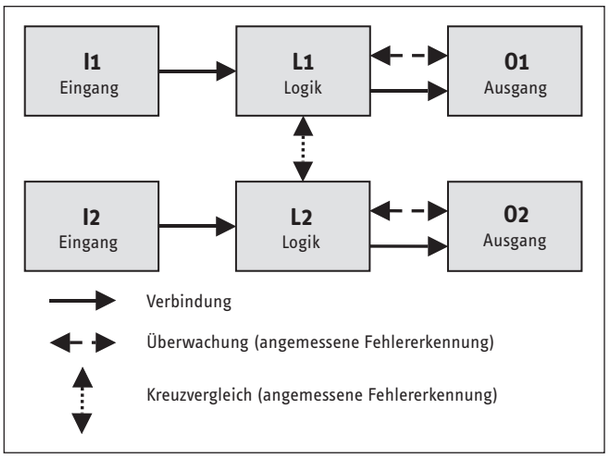
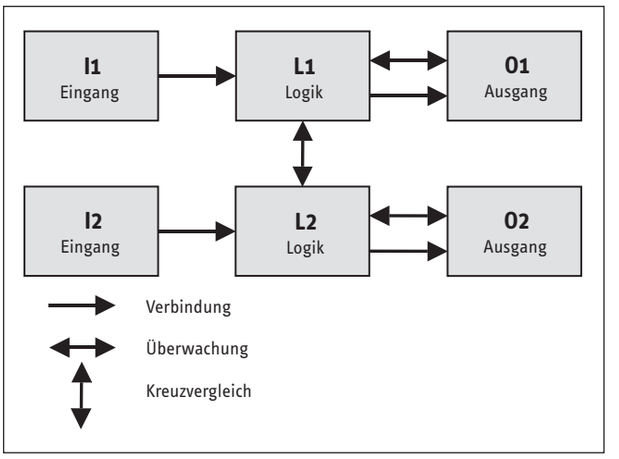


Abbildung 6.8:
Vorgesehene Architektur für Kategorie 4



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 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}.

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 Steuerungselemente 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 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 separate Blöcke eines zusätzlichen Testkanals zusammengefasst werden.

Die Norm stellt für die Kategorien 3 und 4 keine direkten Anforderungen an die Zuverlässigkeit externer Testeinrichtungen, aber in Anlehnung an Kategorie 2 sollten die Testeinrichtungen mindestens die halbe $MTTF_d$ des einzelnen (symmetrisierten, siehe unten) Kanals haben, und auch systematische Ausfälle und CCF sollten berücksichtigt werden.

6.2.9 Sicherheitsbezogenes Blockdiagramm

Das sicherheitsbezogene Blockdiagramm ist dem bekannteren Zuverlässigkeitsblockdiagramm [25] 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.

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

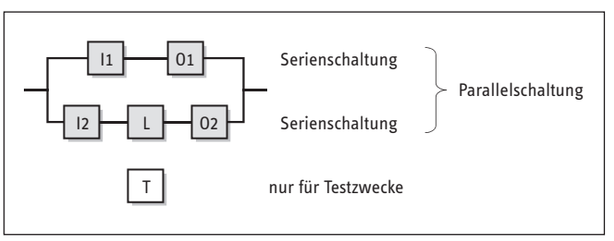
- Die Serienschaltung von Blöcken als sogenannter „Kanal" (z.B. I, L und O) bringt zum Ausdruck, dass der Ausfall eines Blocks zu einem Ausfall der gesamten Kette führen kann. Fällt z.B. eine Hardwareeinheit in einem Kanal gefährlich aus, kann der gesamte Kanal die Sicherheitsfunktion nicht weiter ausführen.

- 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 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).

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



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, 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. 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 bzw. 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 Voraussetzungen 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, haben bereits signalisiert, dass solche Daten künftig erhältlich sein werden. Aber auch wenn es (noch) 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.

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 den $MTTF_d$-Werten der beteiligten Bauteile (N Bauteile mit Laufindex i) in folgender Weise die $MTTF_d$ des Blocks:

$$\lambda_d = \sum_{i=1}^{N} \lambda_{di} \text{ bzw.} \frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} \qquad (1)$$

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
nicht zulässig	100 Jahre < $MTTF_d$

Weniger als drei Jahre mittlere (nicht garantierte!) Lebensdauer wird für Komponenten der Sicherheitstechnik als nicht angemessen betrachtet. Mehr als 100 Jahre dürfen nicht 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 noch 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 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):

$$MTTF_d = \frac{2}{3}\left(MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right) \qquad (2)$$

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 $MTTF_d$ gekappt wurde und der symmetrisierte Wert dadurch weniger als 100 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:

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}} = \frac{\sum \lambda_{dd}}{\sum \lambda_{d}} \qquad (3)$$

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 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.
- Sowohl das Auslösen eines Tests, dessen Ausführung als auch die erforderliche Abschaltung sollten bevorzugt automatisch von SRP/CS durchgeführt werden. Nur in Ausnahmefällen erscheint es angeraten, hier auf eine manuelle Intervention, z.B. des Maschinenbedieners, 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 sind ein hoher organisatorischer Aufwand und Disziplin nötig, um manuelle Tests wirksam umzusetzen. Gleichwohl berücksichtigt die Bestimmung des *DC* für zweikanalige Systeme 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.
- 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. 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 zweikanaligen Systemen hat sich ein Test einmal pro Schicht in der Praxis bewährt. Anders ist es beim einkanalig getesteten System der Kategorie 2: Hier 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 beiden Fällen wird ein Faktor von 100 als ausreichend angesehen, also eine mindestens 100-mal höhere Testrate als die gefahrbringende Ausfallrate λ_d (= $1/MTTF_d$) bzw. als die mittlere Anforderungsrate der Sicherheitsfunktion. Bis hinunter zu einem Faktor von 25 ergibt sich demgegenüber eine maximale Erhöhung der Ausfallwahrscheinlichkeit von ca. 10 %. 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 die Tests so schnell ausgeführt werden, dass der sichere Zustand erreicht wird, bevor es zu einer Gefährdung kommt, dann werden keine Bedingungen an die Testhäufigkeit gestellt.

- Ein weiterer Punkt ist die Zuverlässigkeit der Testeinrichtung selbst: Grundsätzlich sollte 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 der Testeinrichtung nicht mehr als doppelt so hoch sein wie die gefahrbringende Ausfallrate der davon überwachten Komponenten - im Zweifel lässt sich dieser Vergleich kanalweise durchführen, sodass der $MTTF_d$-Wert des gesamten Testkanals nicht kleiner sein sollte als der halbe $MTTF_d$-Wert des 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.

- 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.

- 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):

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}} \qquad (4)$$

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

DC (Diagnosedeckungsgrad)	
Bezeichnung	Bereich
kein	$DC < 60\ \%$
niedrig	$60\ \% \leq DC < 90\ \%$
mittel	$90\ \% \leq DC < 99\ \%$
hoch	$99\ \% \leq DC$

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 [27] wird dazu das sogenannte Beta-Faktor-Modell bemüht, das die Ausfälle gemeinsamer Ursache als β mal λ_d ins Verhältnis setzt zur gefahrbringenden Ausfallrate eines Kanals λ_d. 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 der Konstrukteure/Monteure hinsichtlich CCF und ihrer Vermeidung (5 Punkte)
- Schutz vor durch Verunreinigung (mechanische und fluidische Systeme) bzw. elektromagnetische Beeinflussung (elektrische Systeme) ausgelöste Ausfälle infolge gemeinsamer Ursache (25 Punkte)
- Schutz vor durch ungünstige Umgebungsbedingungen ausgelöste Ausfälle 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 von 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).

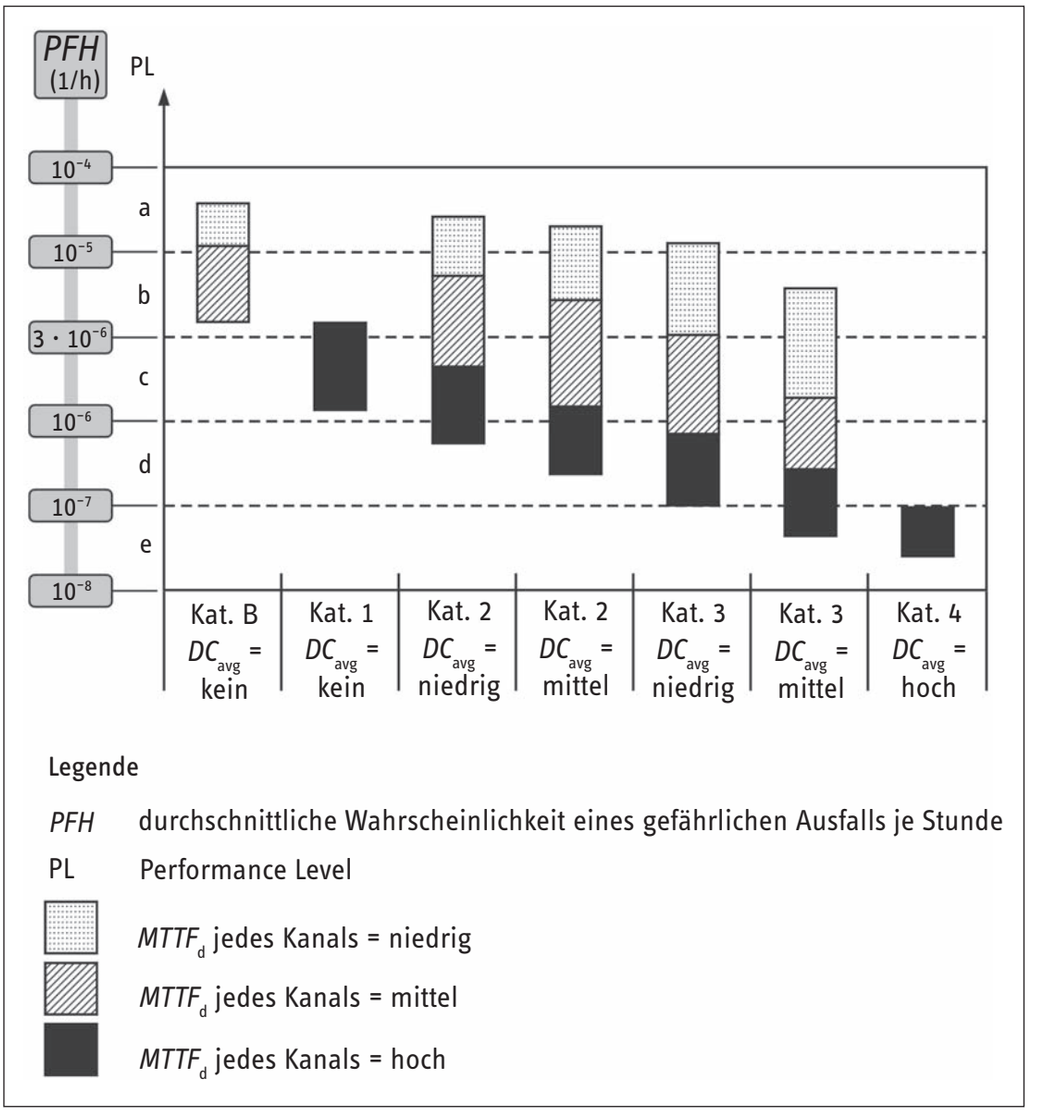


Abbildung 6.10: Säulendiagramm zur vereinfachten PL-Bestimmung aus der Kategorie (inklusive Maßnahmen gegen CCF), dem DC_{avg} und der $MTTF_d$

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 Kategorien 2, 3 und 4 ausreichende Maßnahmen gegen CCF vorhanden sein - 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, so helfen die Tabellen in Anhang K der Norm weiter. Ähnliches leistet auch die BGIA-Software SISTEMA (siehe Anhang H), die das Säulendiagramm quantitativ auswertet.

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

- Als Gebrauchsdauer der SRP/CS wurden 20 Jahre unterstellt, innerhalb derer die Bauteilzuverlässigkeiten durch konstante Ausfallraten beschrieben bzw. 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. Dem Anwender sind diese Informationen in geeigneter Form mitzuteilen, zum Beispiel über die Benutzerinformationen und durch Kennzeichnung auf den SRP/CS.

- Bei den Säulen für Kategorie 2 wurde unterstellt, dass die Testhäufigkeit mindestens 100-mal größer ist als die mittlere Häufigkeit der Anforderung der Sicherheitsfunktion und dass außerdem die Testeinrichtung mindestens halb so zuverlässig ist wie Logik (siehe auch Anhang E).

Durch die Begrenzung der anrechenbaren $MTTF_d$ jedes Kanals auf 100 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 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 sogenannte „Verbindungsmittel“, die als Teil der SRP/CS betrachtet werden. Der Name Verbindungsmittel erscheint zunächst aus der Sicht eines Experten 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 [28]) und eine Norm (DIN EN 61784-3 [29]) 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 bereits mehrere Bussysteme, die für den sicherheitstechnischen Einsatz geeignet sind.

In den oben erwähnten Publikationen wird ein spezielles Fehlermodell verwendet, um dem Einsatz eines Black-Box-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 sogenannte 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. [30].

Sollen ein in der Regel von unabhängiger Stelle geprüftes Bussystem bzw. dessen Komponenten für die Realisierung von Sicherheitsfunktionen eingesetzt werden, so ist 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.

6.3 Entwicklung sicherheitsbezogener Software

„Der Programmierer einer Software, der 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 sich der „Power-User" 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 verträgt? Dagegen sind Hardwarefehler eher selten. Normale, das heißt einfache Software für einfache Funktionen hat nach [31] etwa 25 Fehler pro 1 000 Programmzeilen. Gute Software hat nach [31] etwa zwei bis drei Fehler pro 1 000 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 ihr Programmierer.

Als eine der wesentlichen Neuerungen in der Revision der DIN EN ISO 13849-1 wurden die schon im Anwendungsbereich der DIN EN 954-1 einbezogenen programmierbaren SRP/CS erstmals mit Anforderungen an die Software und deren Entwicklung ausgestattet. 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 Anwendungsprogrammierer, die Sicherheitsfunktionen für eine Maschine, z.B. in einer applikationsorientierten Sprache auf einer speicherprogrammierbaren Steuerung (SPS), entwickeln. Für Entwickler 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 [32] (und aller weiteren sieben Teile).

Die Grundgedanken dieses Abschnitts können auf beide Softwaretypen bezogen werden. Einzelne Anforderungen werden aber eher für Anwendungsprogrammierer von SRASW (Safety-Related Application Software – sicherheitsbezogene Anwender-Software) 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 in der Praxis diese Phasen der Anwendungsprogrammierung 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 sogenannte „V-Modell" referenziert [32]. 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 werden von einem Programmierer, der üblicherweise nicht sicherheitsrelevante Software erstellt, als mühsam empfunden, geben ihm aber andererseits die Bestätigung, die Software hinreichend gut entwickelt zu haben.

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

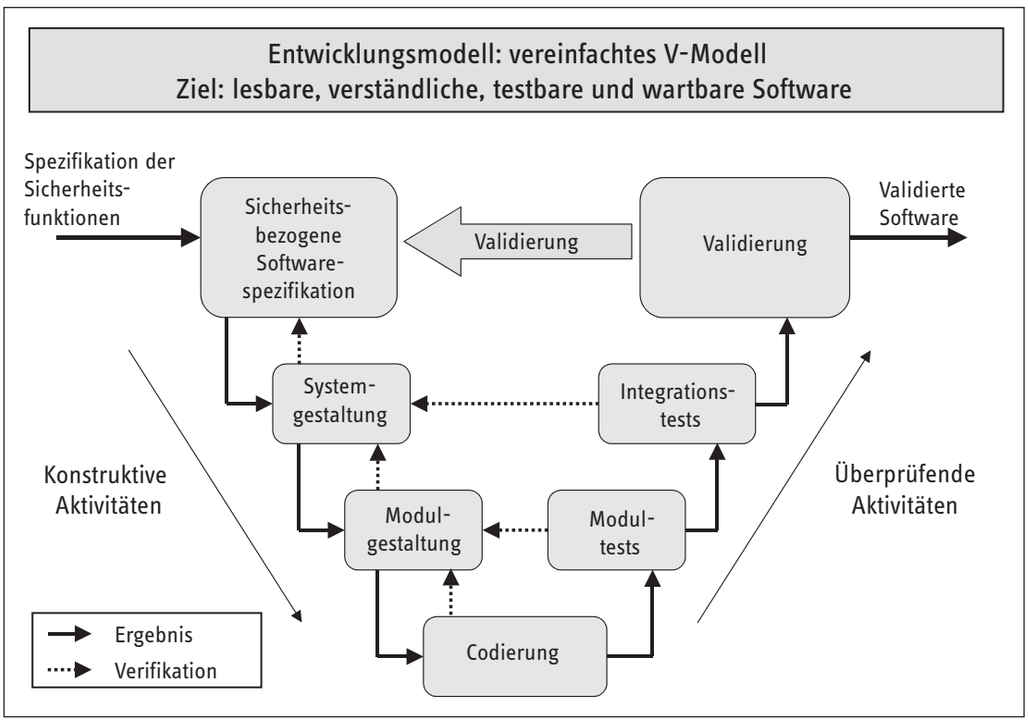


Abbildung 6.11: Vereinfachtes V-Modell für die Entwicklung sicherheitsbezogener Software

Ergebnis

Bezeichnet das, was in einer Phase erstellt wurde, z.B. die Spezifikation, das Gestaltungsdokument, 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 bzw. Maschinenanlage wird es eine Teilmenge von Arbeiten für den Programmierer geben. Die Softwarespezifikation ist damit Teil des Gesamtkonzepts und folglich als „Vertrag“ mit einem „Unterauftragnehmer“, dem Programmierer, 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. Es ist zu entscheiden, 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

Nun freut sich der Programmierer: Endlich 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, Integrationtest 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 Fehlern 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. DIN EN ISO 13849-1 nennt aber keine Minimalanforderungen, die für jede Software - unabhängig vom PL - notwendig wären.

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 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 fehlervermeidende 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).

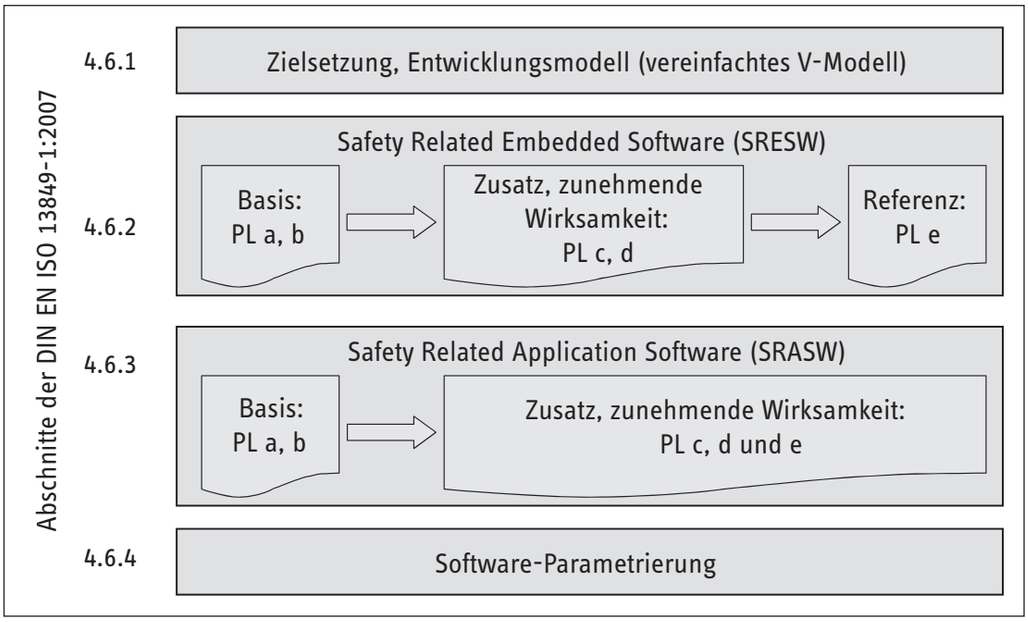


Abbildung 6.12: Abstufung der Anforderungen an sicherheitsbezogene Software

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 der Programmierer die Spezifikation selbst verfasst und ein anderer Programmierer sie gegenliest („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 der Programmierer selbst die Spezifikation schreibt, sondern z.B. der „Projektleiter Software“. Darüber hinaus könnte das Review dieser Spezifikation gemeinsam vom Programmierer und einer unabhängigeren Person, z.B. dem Hardware-Projekteur, durchgeführt werden. Mehr Personen sehen (meist) mehr Fehler. Im Rahmen dieses BGIA-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 wie z.B. d oder e realisiert. Dementsprechend gelten die Anforderungen des höchsten PL_r auch für die Software dieses einen Kanals (siehe auch Abschnitt 6.3.10).

- Verwendung von Standard-SPS: Die Schaltungsbeispiele in diesem BGIA-Report (siehe Kapitel 8, Seite 85 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* (mindestens 99 %) zu erreichen – sofern diese Diagnose durch die SRASW realisiert werden muss. Für PL a bis d werden die Anforderungen an die Standard-SPS im Abschnitt 6.3.10 beschrieben. Zusätzlich muss der Anwendungsprogrammierer die Anforderungen zur Fehlervermeidung bei SRASW (Abschnitte 4.6.1 und 4.6.3 der Norm) entsprechend des PL_r erfüllen.

- Bonus bei 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 den Programmierer und erhöhen die Softwarequalität.

- Bibliotheken mit Softwarefunktionen:
  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 vom Inbetriebnehmer oder einer externen Organisation noch selbst zu validieren. Der Systemintegrator ist 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 [33], empfohlen. Selbst diese Sprachen sind bereits über das notwendige Maß hinaus sehr umfangreich und enthalten teilweise fehlerträchtige Konstrukte. Daher sollte der Programmierer die Syntax nur eingeschränkt einsetzen. Entsprechende Sprachteilmengen werden meist durch das Werkzeug vorgegeben.

- Programmierrichtlinien:
  Zur Codierung der Softwarefunktionen sind geeignete Programmierrichtlinien zu beachten [34; 35]. Dies sollten bestehende und akzeptierte Regeln einer anerkannten Organisation 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 beinhaltet, 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 fünf 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, der ursprüngliche Programmierer hat dringendere Aufgaben oder ist bereits in einem 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 Programmierer.

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/r Kollegen/in, 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, sollte frühzeitig 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. Folgende Kategorien bzw. Performance Level (PL) können durch elektronische programmierbare Standardkomponenten nicht beansprucht werden:

- Kategorie 1: Ausschluss durch die Norm
- Kategorie 4 bzw. PL e kann in der Regel beim Einsatz von Standardkomponenten wegen des geforderten hohen Diagnosedeckungsgrades *DC* in der Praxis nicht erreicht werden. Eine individuelle Beurteilung des Einzelfalls ist notwendig.

Anforderungen an SRESW

Alle betrachteten Standardkomponenten müssen für den industriellen Einsatz entwickelt worden sein. Für die SRESW (Firmware, Betriebssystem) gelten mindestens die Basismaßnahmen für PL a bis b. In den meisten Anwendungsfällen gibt es (siehe Tabelle 6.5) zwei Alternativen, um dies nachzuweisen:

- entweder durch eine Bestätigung des Komponentenherstellers dafür, dass die Basismaßnahmen erfüllt wurden,
- oder durch Angaben des Komponentenherstellers darüber, dass er eine qualitätssichernde Entwicklung (z.B. nach DIN EN ISO 900x) nach relevanten Produktstandards (z.B. DIN EN 61131-2 für SPS) durchgeführt hat. Dies wird für die meisten Standardkomponenten zutreffen.

Im Folgenden wird an einigen Stellen „diversitäre SRESW" vorausgesetzt. Als „diversitär" werden hier die SRESW zweier Komponenten bezeichnet, wenn

- es sich um unterschiedliche Komponenten mit unterschiedlichen Betriebssystemen zweier verschiedener Hersteller handelt oder
- wenn es sich um unterschiedliche Komponenten aus verschiedenen Baureihen/Produktfamilien desselben Herstellers handelt, für die vom Hersteller bestätigt wird, dass sie sich in der SRESW signifikant voneinander unterscheiden. Beispiele bei SPS: eine Komponente ist eine Kompakt-SPS (z.B. 16-bit-CPU, proprietäres Betriebssystem), die zweite Komponente ist eine Modular-SPS (z.B. 32-bit-CPU, Embedded Windows) oder als weiteres Beispiel: eine SPS und ein programmierbares Schaltrelais.

Sofern der Hersteller die Diversität nicht bestätigt, wird in allen anderen Fällen (zwei gleiche SPS oder zwei vergleichbare aus derselben Baureihe vom selben Hersteller) die SRESW beider Komponenten als nicht diversitär - und somit homogen - angenommen. Falls für die Erreichung des erforderlichen *DC* notwendig muss der Hersteller zusätzlich den *DC* der fehlererkennenden/-beherrschenden Maßnahmen, die in der SRESW implementiert sind, bestätigen. Die $MTTF_d$ der Komponenten gehört natürlich zu den grundsätzlich erforderlichen Angaben des Herstellers.

Bei Verwendung von nur einer Standardkomponente in Kategorie 2 oder 3 in Kombination mit einer anderen Technologie sowie bei diversitären Standardkomponenten für jeden Kanal werden aufgrund der geringeren Wahrscheinlichkeit eines gefährlichen Ausfalls durch systematische Fehler in der SRESW die Anforderungen abgesenkt. Tabelle 6.5 zeigt die verschiedenen Kombinationen und wie die Anforderungen an SRESW erfüllt werden.

Tabelle 6.5:
Anforderungen an die SRESW von Standardkomponenten

Nr.	PL	Kategorie, Redundanz	SRESW
1	a b	Kategorie B/2/3	Es gelten die Basismaßnahmen für PL a bis b. Zwei Alternativen: a) Bestätigung durch Hersteller b) abgedeckt durch qualitätssichernde Entwicklung nach relevanten Produktstandards, dann ist keine Herstellerbestätigung über die Einhaltung der Anforderungen nach DIN EN ISO 13849-1 erforderlich
2	c d	Zwei Komponenten für zwei Kanäle in Kategorie 2/3 diversitäre SRESW oder diversitäre Technologie	Bonus durch die Diversität der SRESW oder der Technologien. Es gelten die Basismaßnahmen für PL a bis b. Zwei Alternativen: a) Bestätigung durch Hersteller b) abgedeckt durch qualitätssichernde Entwicklung nach relevanten Produktstandards, dann ist keine Herstellerbestätigung über die Einhaltung der Anforderungen nach DIN EN ISO 13849-1 erforderlich
3	c d	Zwei Komponenten für zwei Kanäle in Kategorie 2/3 SRESW homogen	Kein Bonus durch Diversität. Es gelten die Basismaßnahmen für PL a bis b und zusätzliche Maßnahmen für PL c bzw. d. Eine Herstellerbestätigung über die Einhaltung aller Anforderungen nach DIN EN ISO 13849-1 ist erforderlich.

Zusammenfassend wird der Einsatz von elektronischen programmierbaren Standardkomponenten in SRP/CS hinsichtlich der Anforderungen an die SRESW wie folgt beurteilt:

- PL e kann nach heutigem Stand der Technik durch eine Realisierung mit softwaregestützten Standardkomponenten im Allgemeinen nicht erreicht werden.
- PL c/d kann bei Diversität der SRESW bzw. bei diversitärer Technologie zweier Kanäle mit reduzierten Anforderungen hinsichtlich der Anforderungen an SRESW realisiert werden. Zwar wird der Nutzen von Diversität in der Norm nicht explizit formuliert, ist aber gängige Praxis und wird auch in der zukünftigen zweiten Fassung der DIN EN 61508 ähnlich dargestellt.
- PL a/b können mit geeigneten Standardkomponenten realisiert werden.

Anforderungen an SRASW

Die Anforderungen an SRASW orientieren sich an dem PL, den das Subsystem mit der programmierbaren Standardkomponente erreichen soll. Wird eine Standardkomponente in einem Kanal in diversitärer Redundanz mit einer anderen Technologie (z.B. fluidtechnisch) in dem anderen Kanal eingesetzt, dann werden aufgrund der geringeren Wahrscheinlichkeit eines gefährlichen Ausfalls durch systematische Fehler in der SRASW die Anforderungen für SRASW im PL um eine Stufe abgesenkt (z.B. von PL d auf PL c).

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 bzw. 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 bzw. 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 dargestellt. Einer der großen Vorteile des PL-Konzepts gegenüber den Kategorien ist es, dass nun ein Verfahren existiert, um Subsysteme verschiedener Kategorien, aber ähnlichen Performance Level 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:

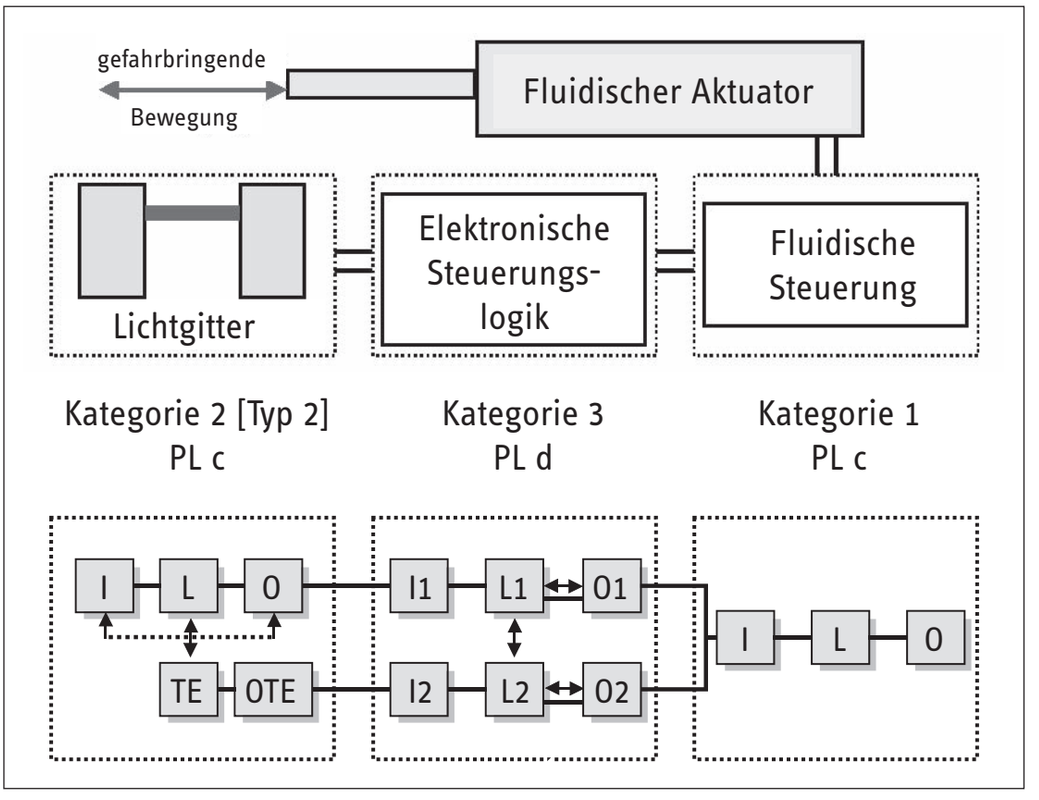


Abbildung 6.13: Reihenschaltung von Subsystemen zur Realisierung einer Sicherheitsfunktion

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

- Teilsteuerung/Subsystem in einer Kategorie: Für diesen Fall gelten ebenfalls die oben angeführten Erläuterungen, z.B. hinsichtlich der 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) den PL des Gesamtsystems zu ermitteln. Dabei ist ebenfalls die genaue Definition des Anteils an der Sicherheitsfunktion und der Schnittstellen zu beachten.

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

Die Reihenschaltung mehrerer Subsysteme auch unterschiedlicher Technologie sieht typischerweise aus wie in Abbildung 6.13 beispielhaft skizziert: Lichtgitter, elektronische Steuerung und Pneumatikventil werden hintereinander geschaltet, um insgesamt die Sicherheitsfunktion (Stillsetzung der gefahrbringenden Bewegung bei Unterbrechung eines Lichtstrahls) auszuführen. Der Pneumatikzylinder 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 an der Häufigkeit des niedrigsten PL in der Serienschaltung und nicht an der niedrigsten Einzelkategorie. Mit der Anzahl der Steuerungselemente steigt auch die Gesamt-Ausfallwahrscheinlichkeit, daher kann der PL der Reihenschaltung gegenüber dem niedrigsten Subsystem-PL noch um eine Stufe verringert sein, wenn z.B. davon mehr als drei Elemente hintereinander geschaltet werden. Als grobe Abschätzung des erreichten Gesamt-PL auf der Basis der Subsystem-PL lässt sich folgendes Verfahren der DIN EN ISO 13849-1 verwenden:

- 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 6.6 der Gesamt-PL bestimmen.

Tabelle 6.6:
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

Dieses vereinfachte Verfahren unterstützt die Bestimmung des Gesamt-PLs, wenn von den Subsystemen nur der PL und nicht der dahinter stehende Wert der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde bekannt ist. Als Näherung wird dabei für die Subsysteme eine Ausfallwahrscheinlichkeit genau in der Mitte des für den jeweiligen $PL_{niedrig}$ gültigen Bereichs angenommen.

Liegen hingegen die Werte der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde für alle Subsysteme vor (geeignet sind auch Werte für SIL und Ausfallwahrscheinlichkeit nach DIN EN 61508 [12] oder DIN EN 62061 [13]), so kann daraus durch Aufaddieren der für den Gesamt-PL relevante Wert gebildet werden:

$$PFH_{gesamt} = \sum_{i=1}^{N} PFH_i = PFH_1 + PFH_2 + \ldots + PFH_N \quad (5)$$

mit

N = Zahl der an der Sicherheitsfunktion beteiligten Subsysteme

PFH_i = durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde des i-ten Subsystems

Da 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. D.h., jeder Ausgangsstatus eines ansteuernden Subsystems, der die Anforderung der Sicherheitsfunktion signalisiert, muss als auslösendes Ereignis für die Einleitung des sicheren Zustands des nachgeordneten Subsystems geeignet sein.

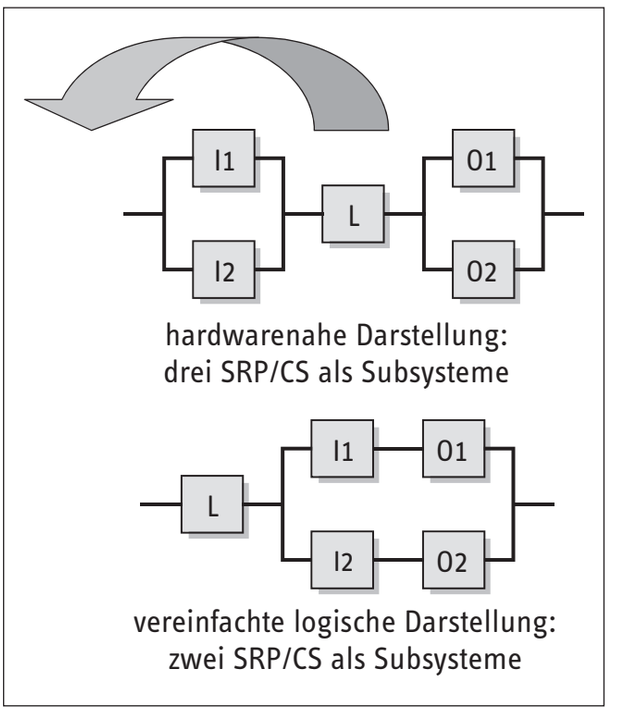
Bei hintereinander geschalteten zweikanaligen Systemen können bei der Addition der Subsystem-PFH-Werte geringe Rechenfehler zur unsicheren Seite auftreten. Streng genommen müssten die beiden Ausgänge des ersten Subsystems zusätzlich über Kreuz in die Eingänge des zweiten Subsystems eingelesen und verglichen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

Mit den bisher beschriebenen Regeln lassen sich Subsysteme bereits viel flexibler kombinieren, als dies vor der Revision der DIN EN ISO 13849-1 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 zeigt beispielhaft ein 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 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



Einen weiteren Spezialfall stellt die Integration von bereits mit einem PL (oder SIL) oder einer durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde 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 als Block-$MTTF_d$ angesetzt werden. Da alle unter Umständen intern realisierten Diagnosemaßnahmen des Subsystems bereits in der Ausfallwahrscheinlichkeit berücksichtigt sind, können für die *DC* des Blocks nur zusätzliche, von außen auf das Subsystem wirkende Diagnosemaßnahmen herangezogen 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 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 des Bedieners außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung

6.5.2 Realisierung

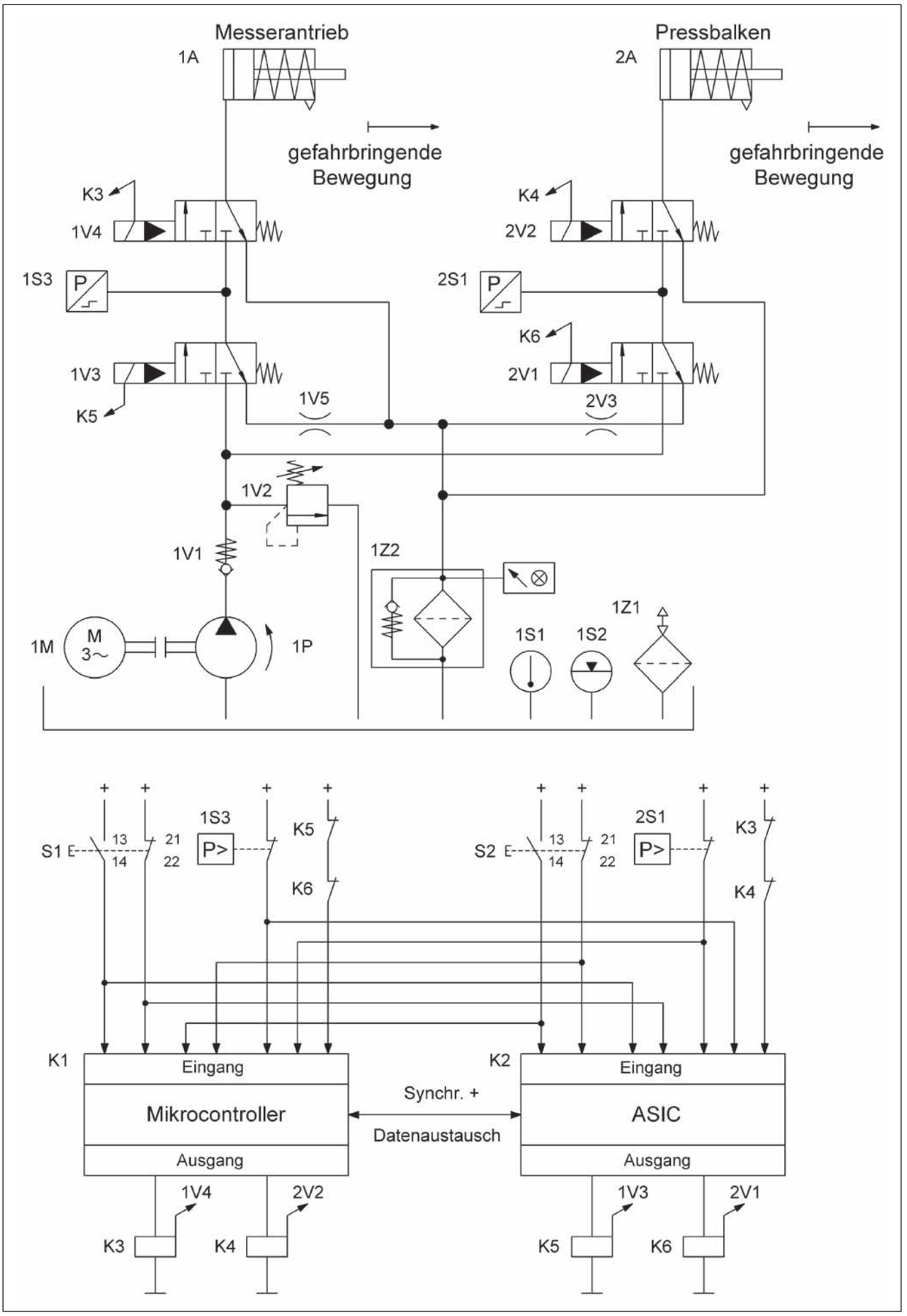
Realisiert als Zweihandschaltung lässt sich diese Sicherheitsfunktion folgendermaßen beschreiben: Beim Loslassen mindestens eines der beiden Stellteile S1 und S2 wird die gefahrbringende Bewegung von Pressbalken und Messer unterbrochen und sowohl Messer als auch Pressbalken kehren durch Federkraft in 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 (siehe Seite 68) zeigt in einem 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 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.

Abbildung 6.15:

Prinzipschaltplan der elektronischen Ansteuerung eines hydraulischen Messerantriebes und eines hydraulischen Pressbalkens (wesentliche Bauelemente)



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 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.

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 abgearbeitet wird, daher kommt Kategorie 3 oder 4 in Betracht. Wegen der hochwertigen Testmaßnahmen, 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 Abschnitt 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?“ und dann über die Logik bis zu den Sensoren zu gelangen. In diesem Beispiel ist zu beachten, dass die Stellteile S1 und S2 nicht zueinander redundant sind, auch wenn dies auf den ersten Blick so erscheinen mag, denn jeder Taster schützt unabhängig eine Hand des Bedieners. 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.

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)

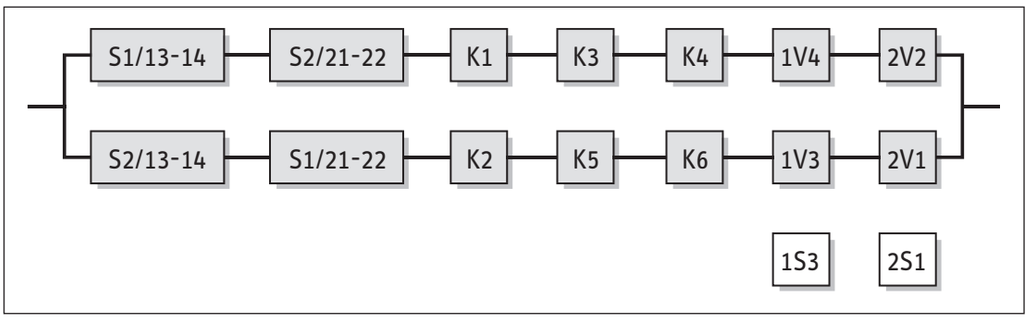


Abbildung 6.16: Sicherheitsbezogenes Blockdiagramm zum SRP/CS für die ausgewählte Sicherheitsfunktion SF2 an der Planschneidemaschine

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.

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 1 142 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 Ventile 1V3, 1V4, 2V1 und 2V2 wird eine $MTTF_d$ von jeweils 150 Jahren [N] angenommen. 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 Drucksensor) 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.

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 207) 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 6.7 gezeigt wird (Abbildung B.3 auf Seite 209 zeigt im Vergleich das Vorgehen bei einer Ausfalleffektanalyse).

Tabelle 6.7:
„Parts Count"-Verfahren für den „Mikrocontroller"-Block K1, basierend auf Ausfallraten λ, die der Datensammlung SN 29500 [36] entnommen wurden (angegeben in FIT, d.h. 10^{-9}/h)

Bauteil	Ausfallrate λ [FIT] nach SN 29500	Anzahl	Gesamtausfallrate λ [FIT]	Gesamtrate gefahrbringender Ausfälle λ_d [FIT]	$MTTF_d$ in Jahren als Kehrwert der Gesamtrate 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
Relais kunststoffdicht	10	1	10	5	22 831
				↓	
Summe für den „Mikrocontroller"-Block K1				141,7 FIT	→ 806 Jahre

Die in der zweiten Spalte genannten Ausfallraten der Elemente wurden mithilfe der **D**atensammlung SN 29500 [35] ermittelt, was unter „Berechnung der Ausfallwahrscheinlichkeit“ durch das Kürzel „[D]“ gekennzeichnet wird (siehe Abschnitt 7.6). 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 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.

Für die Blöcke S1/S2 und K3 bis K6 werden **H**erstellerdaten (Kürzel „[H]“) verwendet. Da Zuverlässigkeitsdaten nur für S1/S2 insgesamt (Betätigungsmechanik plus Öffner- **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.

$$T_{10d} = \frac{B_{10d}}{n_{op}} = \frac{2\,000\,000\ \text{Zyklen}}{86\,400\ \text{Zyklen/Jahr}} = 23{,}15\ \text{Jahre} \tag{8}$$

Die $MTTF_d$-Werte für die Ventile 1V3, 1V4, 2V1 und 2V2 können nach dem Verfahren guter ingenieurmäßiger Praxis aus der **N**orm (Kürzel „[N]“) selbst abgeleitet werden, wenn die dort genannten Voraussetzungen eingehalten werden.

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 den SRP/CS nach Abschnitt 6.2.14 ein DC_{avg} von 98,6 %, der unter Ausnutzung der 5-%-Toleranz im Bereich von „hoch“ liegt:

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

Die im grauen Kasten auf Seite 70 oben 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 BGIA [16] liefern folgendes Ergebnis:

Kategorie	CCF	DC_{avg}	$MTTF_d$	durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde
4	OK	„hoch“	„hoch“ (abgerundet 30 Jahre)	$9{,}54 \cdot 10^{-8}$/Stunde (PL e)

Sehr viel mehr Komfort bei der Verwaltung, Dokumentation und Berechnung aller Zwischenergebnisse bietet die vom BGIA 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 (für die Toleranzen bei DC und $MTTF_d$ vgl. Anmerkungen 2 in den Tabellen 5 und 6 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 hingegen eine leichte Verbesserung gegenüber dem abgerundeten Wert von 30 Jahren für $MTTF_d$ „hoch“. Damit ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde von $9{,}7 \cdot 10^{-8}$/Stunde (siehe Abbildung 6.18), was nur geringfügig von dem oben ermittelten Wert abweicht.

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.:

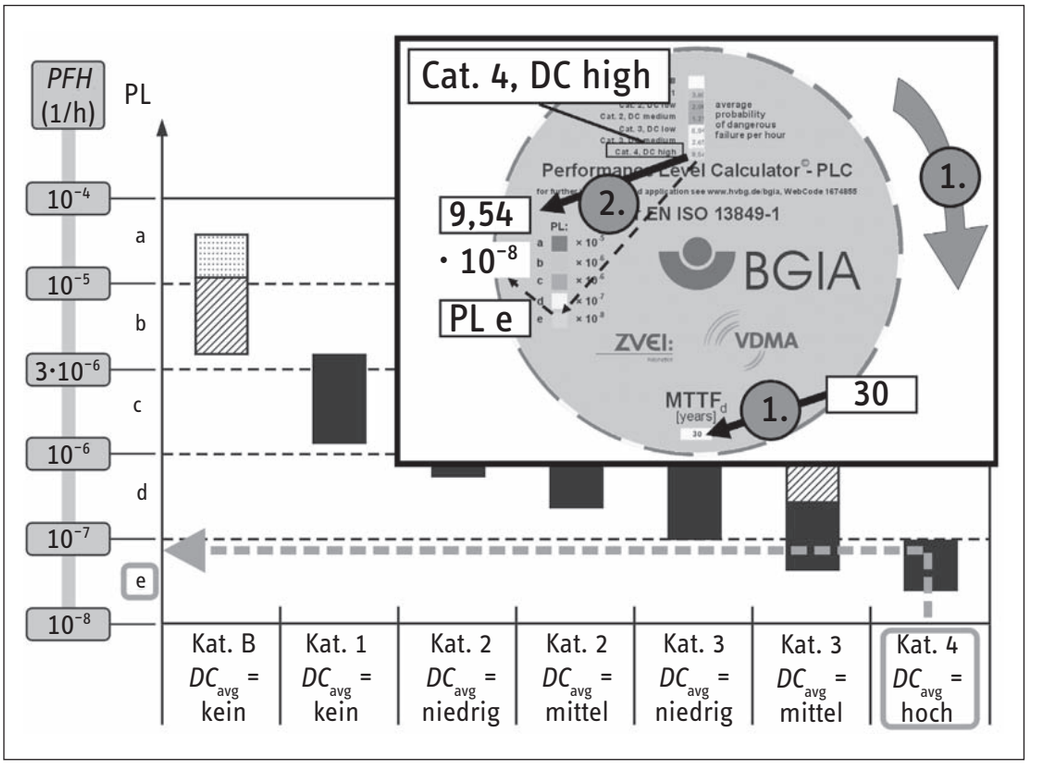


Abbildung 6.17: PL-Bestimmung mithilfe des Säulendiagramms

- 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.

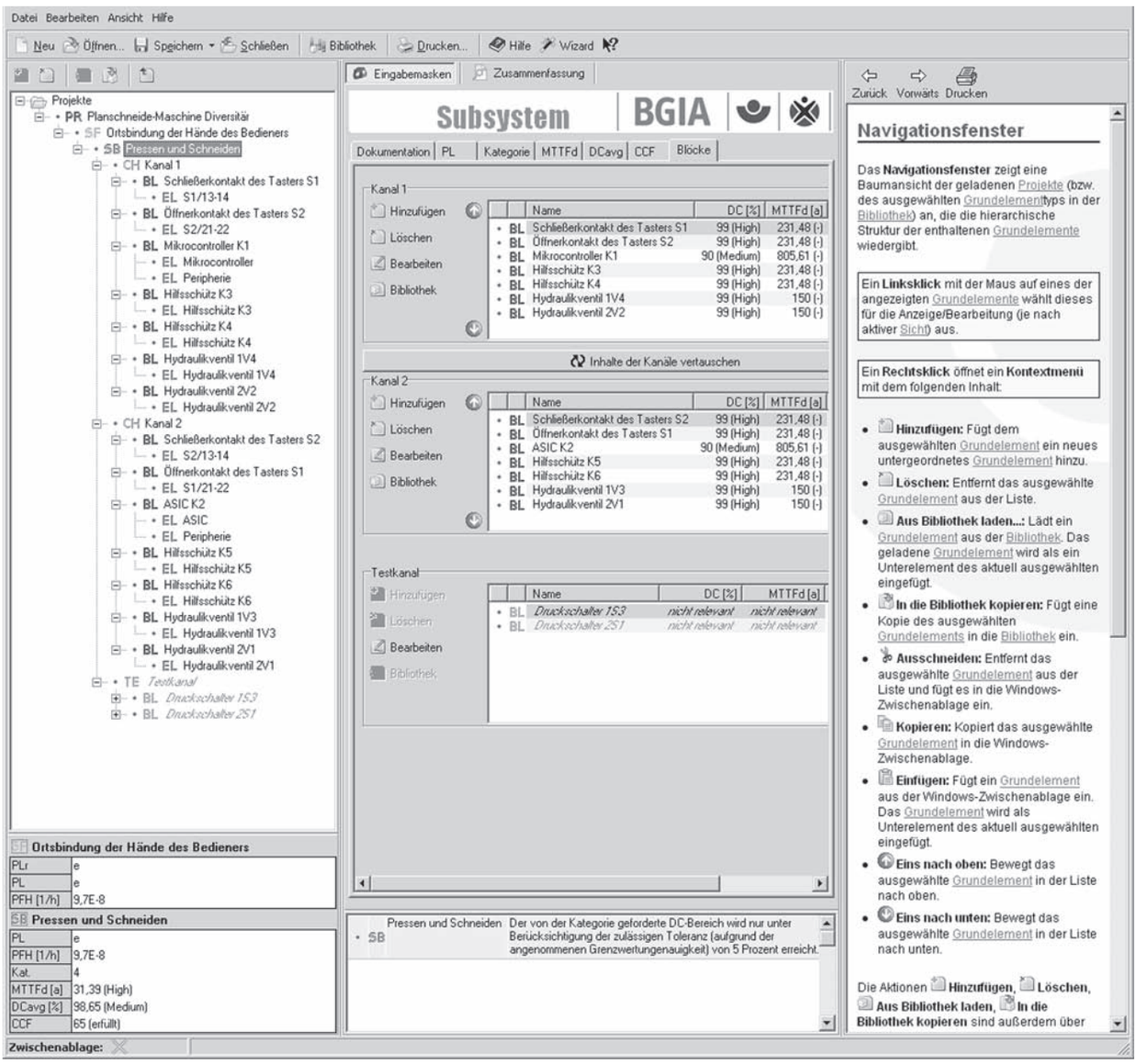
- Verwendung von Hilfsschützen mit zwangsgeführten Kontakten; durch das Rücklesen entsprechender Kontakte können gefährliche Ausfälle der Hilfsschütze und unter Umständen anderer Schaltungsteile erkannt werden.

- 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.

Abbildung 6.18:
PL-Bestimmung mithilfe von SISTEMA



- Fehlervermeidende Maßnahmen bei der ASIC-Entwicklung gemäß ASIC-Entwicklungs-Lebenszyklus des Normentwurfs DIN IEC 61508-2:2006. In diesem Normentwurf 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 den BG-Informationen 5048 „Ergonomische Maschinengestaltung", Teile 1 und 2 [23], überprüft werden. Folgende Aspekte sind dabei u.a. zu betrachten:

- Höhe und Orientierung der Stellteile in Bezug auf den Bediener
- 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 der Programmierer mit Kollegen 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 bzw. 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 (12.02). Beuth, Berlin 2002
- DIN IEC 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (Normentwurf). Beuth, Berlin 2006
- DIN EN 574: Sicherheit von Maschinen - Zweihandschaltungen - Funktionelle Aspekte; Gestaltungsleitsätze (02.97). Beuth, Berlin 1997

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

7 Verifikation und Validierung

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 [7] 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 Entwicklungsabschnittes den Vorgaben für diese Phase entsprechen, also z.B. ob das Schaltungslayout dem Schaltungsentwurf entspricht.

Als Validierung wird der Nachweis der Eignung – bezogen auf den realen Einsatzzweck –, der während oder am Ende des Entwicklungsprozesses erfolgt, bezeichnet. Es wird also überprüft, ob die spezifizierten Sicherheitsanforderungen an den sicherheitsrelevanten Teil der Maschinensteuerung erreicht wurden.

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 im Folgenden auch als V&V-Aktivitäten bezeichnet.

7.1 Ablauf

Abbildung 7.1 zeigt den relevanten Ausschnitt aus Abbildung 4.1, der sich mit den Aktivitäten des Verifizierens und Validierens befasst.

Ein wichtiger erster Prüfungsschritt geschieht beim Durchlaufen der oberen Raute (Block 6): Wenn der Performance Level (PL) jeder realisierten Sicherheitsfunktion nicht mindestens dem nach Kapitel 5 bestimmten erforderlichen Performance Level PL_r entspricht, so ist es erforderlich, in die Phase der Gestaltung und Realisierung zurückzukehren. Anderenfalls gelangt man in die zweite Raute (Block 7).

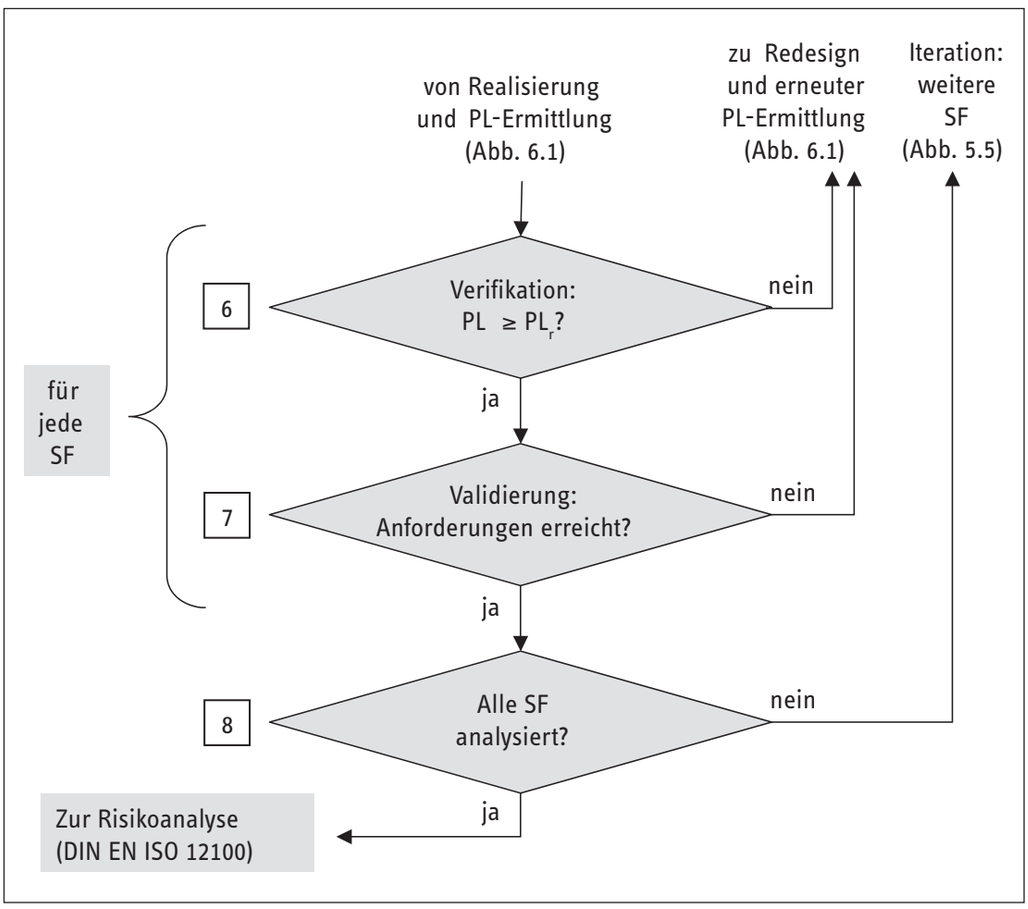


Abbildung 7.1: V&V-Aktivitäten; Ausschnitt aus Abbildung 4.1

Zur Planung der dort erforderlichen Schritte kann der Ablauf in Abbildung 7.2 herangezogen werden. Abbildung 7.2 stammt aus Teil 2 der 2003 veröffentlichten DIN EN ISO 13849 und wurde grafisch aufbereitet, um die V&V-Aktivitäten deutlicher herauszustellen.

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

7.1.1 Leitsätze für die Verifikation und Validierung

Verifikation und Validierung sollen die Konformität der Gestaltung der SRP/CS mit der Maschinenrichtlinie sicherstellen.
Da DIN EN ISO 13849-1 als Sicherheitsnorm für Maschinensteuerungen unter der Maschinenrichtlinie gelistet 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, sofern die Vermutungswirkung der Norm beansprucht werden soll. Diese Aktivitäten sollten so früh wie möglich während der Entwicklung begonnen werden, sodass Fehler rechtzeitig erkannt und behoben werden können. Die Prüfungen sollten nach Möglichkeit von Personen durchgeführt werden, die nicht in den Gestaltungsprozess der sicherheitsbezogenen Teile einbezogen sind, d.h. unabhängig von Entwurf und Realisierung sind. Dies können 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 können durch alleinige Analyse oder durch eine Kombination aus Analyse und Prüfung erfolgen.

7.1.2 Verifikations- und Validierungsplan

In einem Verifikations- und Validierungsplan (V&V-Plan) müssen alle geplanten Aktivitäten verbindlich festgelegt werden; er sollte folgende Angaben enthalten:

- Produktidentifikationen der zu prüfenden SRP/CS
- Identifikation der Sicherheitsfunktionen mit Zuordnung der beteiligten SRP/CS

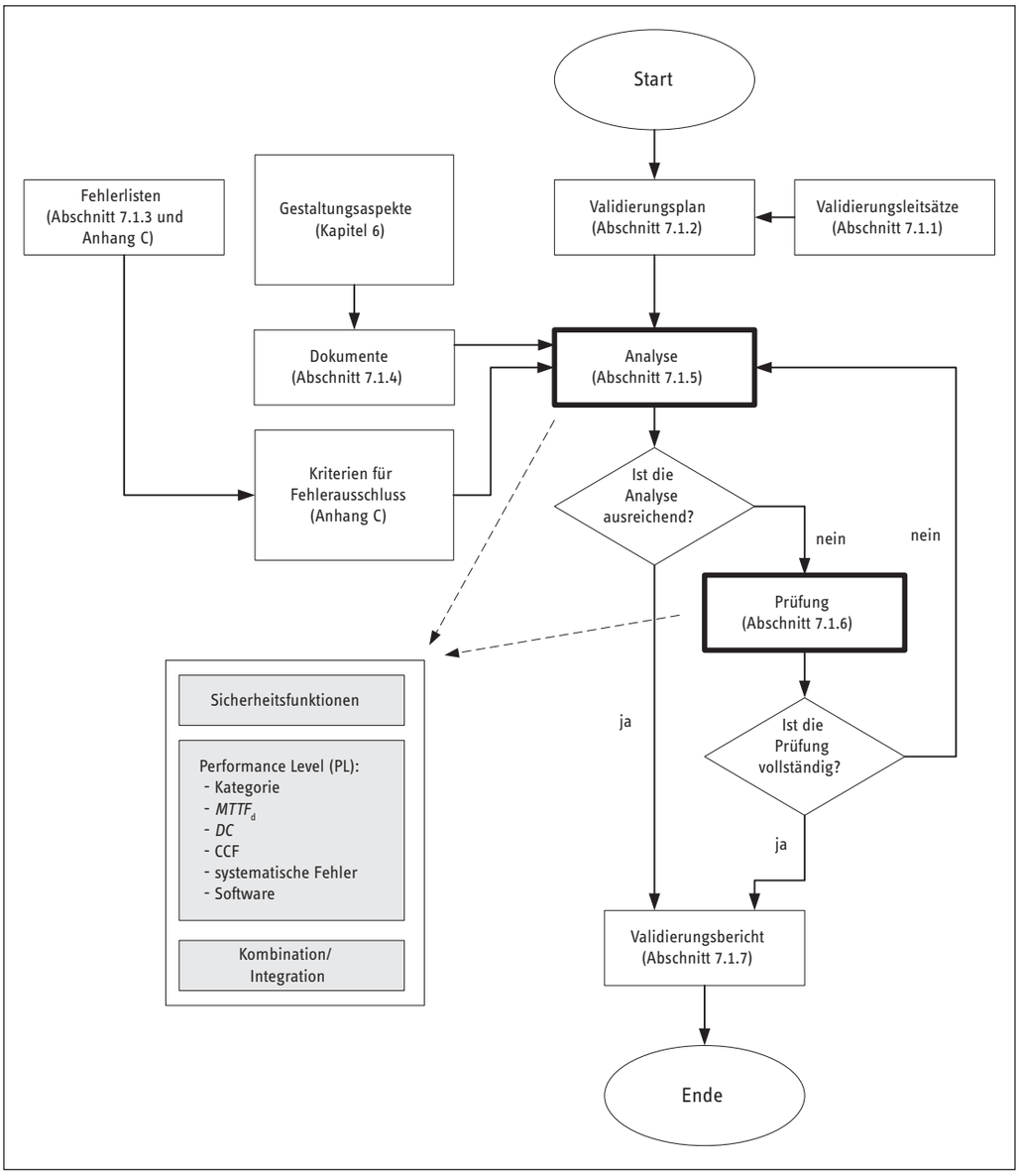


Abbildung 7.2: Übersicht zum Verifikations- und Validierungsablauf nach DIN EN ISO 13849-2

- Liste der Dokumente mit Anforderungsbeschreibungen/ Spezifikationen, auch bekannt als Spezifikation der Sicherheitsanforderungen SRS (Safety Requirements Specification)
- anzuwendende Prüfgrundlagen (Normen) und firmeninterne Festlegungen, z.B. eigene Standards, Designregeln und Programmierrichtlinien
- durchzuführende Analysen und Prüfungen einschließlich Identifikation der Prüfspezifikationen
- anzuwendende Fehlerlisten
- weitere Bezugsdokumente (z.B. QM-Handbuch, Verfahrensanweisungen)
- für die Analysen und Prüfungen verantwortliches Personal (Prüfer, Abteilung oder Stelle)
- vorgesehene Ausrüstung und Hilfsmittel (kann auch in den Ergebnisdokumenten aufgelistet sein)
- vorgesehene Ergebnisdokumentation (zu erstellende Prüfberichte/-protokolle)
- Festlegung von Kriterien dafür, wann Prüfungen erfolgreich/ nicht erfolgreich sind, einschließlich der Maßnahmen, die durchzuführen sind, wenn eine Prüfung nicht bestanden wurde
- formale Aspekte wie Freigabevermerke oder Prüferunterschrift
- erforderliche erneute V&V-Aktivitäten bei Modifikationen am Produkt

7.1.3 Fehlerlisten

Im Prüfverfahren sind Überlegungen zum Verhalten der SRP/CS bei Ausfällen vorzunehmen. Die Grundlage für die Fehlerbetrachtung ist in den Anhängen der DIN EN ISO 13849-2 zu finden (siehe auch Anhang C dieses Reports). Die Fehlerlisten stützen sich auf langjährige Erfahrungen.

Eine vollständige Referenzierung der zur Anwendung kommenden Fehlerlisten und Fehlerausschlüsse ist erforderlich. Je nach Produkt und angewandter Technologie sollen eigene Fehlerlisten und Fehlerausschlüsse in vergleichbarer Weise ergänzt werden. Dies trifft insbesondere auf Bauteile und Baugruppen zu, die in den Fehlerlisten der DIN EN ISO 13849-2 nicht enthalten sind. Alle Fehlerausschlüsse müssen ausreichend begründet sein.

7.1.4 Dokumente

Wie Abbildung 7.2 zeigt, sind für V&V-Aktivitäten eingehende Dokumentationen erforderlich. Dies sind Dokumente, die im Rahmen der Entwicklung entstanden sind und die sich je nach angewendeter Technologie unterscheiden können. Zusammengefasst sollten in ausreichendem Maße folgende Inhalte berücksichtigt sein:

- Spezifikation aller Anforderungen an die Sicherheitsfunktionen sowie die Anforderungen an SRP/CS, die diese Sicherheitsfunktionen ausführen sollen, Leistungskriterien, Auflistung aller realisierter Betriebsarten, ausführliche Funktionsbeschreibungen, Ablaufbeschreibungen
- Betriebs- und Umgebungsbedingungen mit Schärfegraden (Bemessungsdaten) der anzuwendenden Normen, die sich aus den angestrebten Anwendungen ergeben
- Konstruktionsbeschreibung der SRP/CS (mit Spezifika für eingesetzte mechanische, elektrische, elektronische, hydraulische und pneumatische Komponenten), Verdrahtungspläne und Anschluss- bzw. Schnittstellenbeschreibungen, Schaltpläne, Montagepläne, technische Daten bzw. Bemessungsdaten für Komponenten, ggf. Datenblätter
- Analyse aller relevanten Fehler, z.B. als Ausfalleffektanalyse (FMEA), unter Berücksichtigung der angewandten Fehlerlisten
- Daten zur Ermittlung des PL (Quantifizierungsdokumentation)
- vollständige Softwaredokumentation (siehe Abschnitt 6.3)
- eingehaltene Qualitätssicherungsregeln für den Entwurf und die Realisierung wie Designregeln für Analog- und Digitalschaltungen, Programmierrichtlinien
- Prüfnachweise zu bereits geprüften Bauteilen, Modulen oder SRP/CS

Die Dokumente müssen vollständig, die Inhalte widerspruchsfrei, logisch aufgebaut, leicht verständlich und nachvollziehbar sein. In den nachfolgenden Beschreibungen der V&V-Aktivitäten finden sich detaillierte Informationen zu allen Dokumenten.

7.1.5 Analyse

Die Beurteilung der SRP/CS bzw. von Teilaspekten erfolgt zunächst durch Analyse. Dabei soll anhand der Durchsicht von Unterlagen und ggf. durch den Einsatz von Analysewerkzeugen, z.B. Schaltungssimulatoren, Tools zur statischen und dynamischen Softwareanalyse oder FMEA-Tools, festgestellt werden, ob die spezifizierten Anforderungen erreicht wurden. Die Beurteilung der Aspekte $MTTF_d$, *DC* und CCF erfolgt ausschließlich durch Analyse auf der Basis vorliegender Unterlagen.

7.1.6 Prüfung

Prüfungen müssen immer dann durchgeführt werden, wenn 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 der Validierung durch Prüfung müssen angemessen sein. DIN EN ISO 13849-2 gibt Hinweise auf einzuhaltende Grenzen.

Zu den Analyse- und Prüfaktivitäten gehört jeweils auch ein Review aller für den Abschnitt relevanten Unterlagen. Falls negative Prüfergebnisse festgestellt wurden, sind Verfahren und Maßnahmen erforderlich, um diese Ergebnisse in der Entwicklung der SRP/CS entsprechend zu behandeln.

7.1.7 Dokumentation der V&V-Aktivitäten

Alle Analyse- und Prüfaktivitäten müssen inklusive ihrer Ergebnisse (erfolgreich oder nicht bestanden) dokumentiert werden. In den folgenden Abschnitten werden die Schritte zur Validierung der Sicherheitsfunktionen, der SRP/CS sowie für Teilaspekte wie u.a. PL, Kategorie, $MTTF_d$, *DC* und CCF beschrieben.

Wurden nicht alle in der Spezifikation der SRP/CS festgelegten Anforderungen erfüllt, muss man auch an dieser Stelle in den Gestaltungs- und Realisierungsprozess zurückkehren. Ansonsten ist als Abschluss der V&V-Aktivitäten in der dritten Raute (Block 8) von Abbildung 7.1 zu bewerten, ob alle Sicherheitsfunktionen analysiert wurden. Ist dies der Fall, so ist die Bewertung der SRP/CS nach DIN EN ISO 13849-1 abgeschlossen, ansonsten muss die Prüfung mit den noch offenen Sicherheitsfunktionen fortgesetzt werden.

7.2 Validieren der Sicherheitsfunktion

Ein wichtiger Schritt ist die Validierung der realisierten Sicherheitsfunktion auf vollständige Übereinstimmung mit den in der Spezifikation geforderten Eigenschaften und Leistungskriterien. Folgende Fragen sollen dem Prüfer helfen zu beurteilen, ob die Sicherheitsfunktion korrekt umgesetzt wurde:

- Wurde die Sicherheitsfunktion korrekt und vollständig definiert?
- Wurde die richtige Sicherheitsfunktion umgesetzt?
- Passen die Festlegungen der Sicherheitsfunktion zur Konstruktion?
- Wurden alle erforderlichen Betriebsarten berücksichtigt?
- Wurden die Betriebseigenschaften der Maschine berücksichtigt (einschließlich der vernünftigerweise vorhersehbaren Fehlanwendungen)?
- Wurden Handlungen bei Notfällen berücksichtigt?
- Werden alle sicherheitsbezogenen Eingangssignale korrekt und logisch richtig zu sicherheitsgerichteten Ausgangssignalen verarbeitet?
- Sind die Ergebnisse der Risikobeurteilung für jede bestimmte Gefährdung oder Gefährdungssituation in die Definitionen der Sicherheitsfunktion eingeflossen?

Um eine Aussage darüber treffen zu können, ob die funktionalen Anforderungen erfüllt wurden, sollten folgende typische Teilprüfungen durchgeführt werden:

- Funktionstest (in redundanten Systemen für jeden Kanal)
- Test zum Verhalten der SRP/CS bei unüblichen, nicht erwarteten oder außerhalb der Spezifikation liegenden Eingangssignalen, Bedienungsabläufen oder Eingaben mittels sogenanntem erweiterten Funktionstest
- Black-Box-Test
- Leistungstests (funktionale Aspekte)

Im Fokus der in diesem Kapitel beschriebenen V&V-Aktivitäten stehen SRP/CS, die Sicherheitsfunktionen ausführen. Zur vollständigen Prüfung der Sicherheitsfunktion an der kompletten Maschine gehört allerdings eine Reihe weiterer Aspekte wie z.B. die Bemessung von Nachläufen und Sicherheitsabständen.

7.3 Validieren des PL der SRP/CS

Dieser Abschnitt beschreibt die Prüfung einzelner SRP/CS. Die Vorgehensweise zur Prüfung einer Kombination mehrerer SRP/CS zu einer Sicherheitsfunktion wird in Abschnitt 7.5 erläutert.

Für die SRP/CS muss der PL (Quantifizierung der Ausfallwahrscheinlichkeit) abgeschätzt werden. In den folgenden Abschnitten werden die Validierungsschritte der Teilaspekte benannt, die in die Berechnung des PL einfließen. Dies sind zum einen quantifizierbare Aspekte wie $MTTF_d$-Werte für einzelne Bauteile, *DC*, CCF und die Kategorie und zum anderen qualitative Aspekte wie das Verhalten der Sicherheitsfunktion unter Fehlerbedingungen sowie sicherheitsbezogene Software, systematische Ausfälle und das funktionale Verhalten unter Umgebungsbedingungen. Im Anschluss an die Beurteilung der Einzelaspekte wird beschrieben, wie die Abschätzung des PL kontrolliert werden kann.

7.3.1 Validieren der Kategorie

Ziel der Kategorievalidierung ist die Bestätigung aller gestellten Anforderungen an die durch die SRP/CS realisierte Kategorie (siehe Abschnitt 6.2). Dazu notwendige Dokumente sind insbesondere:

- Spezifikationen der SRP/CS
- Konstruktionsbeschreibungen
- Blockdiagramme bzw. Strukturbeschreibungen
- Schaltpläne
- Fehlerlisten

Um eine Aussage darüber treffen zu können, ob die Anforderungen erfüllt wurden, sollten folgende typische Teilprüfungen durchgeführt werden:

- Tests zum Verhalten der SRP/CS im Fehlerfall mit Ausfalleffektprüfung bzw. Test durch Fehlereinbau
- Tests zum Verhalten der SRP/CS bei fehlerhaften Zuständen von Eingangssignalen und fehlerhaften Abläufen/Eingaben bei der Bedienung mit sogenannten erweiterten Funktionstests

Diese Teilprüfungen sollten durch folgende Analysen ergänzt werden:

- Struktur-/Signalpfadanalyse
- 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 deren hinreichender Begründung

Die Anhänge im Teil 2 der Norm (siehe auch Anhang C dieses Reports) geben detaillierte Hilfe bei den vier letztgenannten Analysen.

7.3.2 Validieren der $MTTF_d$-Werte

Die zur Bestimmung des PL herangezogenen $MTTF_d$-Werte sollten mindestens auf ihre Plausibilität überprüft werden. Dazu zählt typischerweise die Beurteilung, ob geeignete Quellenangaben zur Herkunft der Werte benannt werden. 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.

7.3.3 Validieren der DC-Werte

Der den Blöcken durch Testmaßnahmen zugewiesene Diagnosedeckungsgrad *DC* muss nachvollziehbar begründet sein. Geprüft werden auch hier typischerweise die Angaben zur Herkunft der Werte, d.h. darüber, ob die ermittelten Werte glaubwürdig oder eher zweifelhaft sind. Wie bei den $MTTF_d$-Werten ist stichprobenartig oder für die dominanten Bauteile das Nachvollziehen der Begründung sinnvoll. In Anhang E sind Hinweise zur Abschätzung der DC-Werte zu finden.

Für die realisierte Konstruktion gilt es zu prüfen, ob die beschriebenen Diagnosemaßnahmen umgesetzt wurden. Dazu ist es zumeist erforderlich, in der Entwicklungsdokumentation die Diagnosefunktionen und -module zu identifizieren und deren Wirksamkeit einzuschätzen. Zusätzlich sollten Tests zum Verhalten der SRP/CS im Fehlerfall (Ausfalleffektprüfung bzw. Test durch Fehlereinbau) zeigen, dass durch die Diagnosefunktionen eine korrekte Fehleraufdeckung gegeben ist.

7.3.4 Validieren der Maßnahmen gegen CCF

Zur Validierung der ausgewählten Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache CCF (Common Cause Failure) enthält Anhang F ein mögliches Verfahren, basierend auf einem Punkteschema. Neben dem Erreichen der Gesamtpunktzahl wird untersucht, ob die ausgewählten Maßnahmen in den entsprechenden Dokumenten hinreichend beschrieben sind. Durch Analyse bzw. Prüfung ist zu zeigen, dass die Maßnahmen tatsächlich umgesetzt wurden. Zu den hierzu typischen V&V-Aktivitäten zählen die statische Hardwareanalyse und die Funktionsprüfung unter Umgebungsbedingungen (Grenzbedingungen).

7.3.5 Verifizieren und Validieren der Maßnahmen gegen systematische Ausfälle

Als Verifikation der Maßnahmen zur Vermeidung systematischer Ausfälle sollen die Entwicklungsdokumente dahingehend inspiziert werden, ob die in Abschnitt 6.1.2 beschriebenen erforderlichen Konstruktionsmaßnahmen umgesetzt wurden. Ein entsprechender Nachweis erfolgt typischerweise durch

- Ausfalleffektprüfung bzw. Test durch Fehlereinbau zu den Versorgungseinheiten (z.B. Spannungsversorgung, Takt, Druck)

- Prüfung der Störfestigkeit gegen Umgebungseinflüsse bzw. Test bei spezifizierten Umgebungsbedingungen

- Analyse zur Implementierung der Programmlaufüberwachung

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

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

7.3.6 Validieren der Software

Die im Rahmen des Entwurfs und der Codierung der Software stattfindenden Verifikationsmaßnahmen werden ausführlich in Abschnitt 6.3 beschrieben.

Für die Entwicklung von sicherheitsbezogener Software ist mit Ausnahme der unten beschriebenen Embedded-Lösung im PL e das vereinfachte „V-Modell“ anzuwenden (siehe Abbildung 6.11). Die letzte Entwicklungsaktivität hierbei ist die Softwarevalidierung. Zu prüfen ist, ob die Anforderungen der sicherheitsbezogenen Softwarespezifikation an das funktionale Verhalten sowie die Leistungskriterien (z.B. zeitbezogene Vorgaben) korrekt umgesetzt 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 „Black box“ betrachtet, die Validierung hierzu ist der sogenannte Black-Box-Test.

Bei sicherheitsrelevanter Anwendungssoftware (SRASW) müssen „I/O-Tests“ sicherstellen, dass die sicherheitsbezogenen Eingangs- und Ausgangssignale korrekt verwendet werden. Für PL d und e wird bei der Validierung auch eine erweiterte Testfallausführung auf der Basis von Grenzwertanalysen empfohlen. Hierbei wird auch die Reaktion auf vorher analytisch bestimmte und im Test durchgeführte Fehlerfälle beobachtet, um so die Fehlererkennung und -beherrschung durch die Software zu testen. 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.

Für sicherheitsbezogene Embedded-Software (SRESW) muss für das Erreichen des PL überprüft werden, ob die erforderlichen konstruktiven Maßnahmen zur Softwarerealisierung gemäß Abschnitt 6.3 korrekt umgesetzt und implementiert wurden. Im besonderen Fall von SRESW, die in SRP/CS mit PL e eingesetzt und nicht diversitär für beide Kanäle entwickelt wurde, müssen die SIL-3-Anforderungen nach Abschnitt 7 der DIN EN 61508-3 [32] vollständig erfüllt werden. Dies schließt die darin geforderten V&V-Aktivitäten ein.

Bei einer späteren Modifikation der sicherheitsbezogenen Software ist in jedem Fall deren Validierung in geeignetem Umfang zu wiederholen.

7.3.7 Kontrolle der Abschätzung des PL

Die Kontrolle der korrekten Abschätzung des PL für jeden SRP/CS besteht insbesondere aus dem Nachvollziehen der richtigen Anwendung des eingesetzten Abschätzungsverfahrens, einschließlich der korrekten Berechnungen. Zum Beispiel beinhalten Abschnitt 6.2.11 und Anhang D vereinfachte Verfahren zur Bestimmung der $MTTF_d$, der durchschnittliche Diagnosedeckungsgrad DC_{avg} kann mit der Formel in Anhang E nachvollzogen werden.

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

7.4 Prüfen der Benutzerinformation

Wichtige Informationen zur sicheren Verwendung der SRP/CS sind dem Benutzer in Form von Betriebsanleitungen, Montageanleitungen und Typenschild an die Hand zu geben. Diese gesamtheitlich Benutzerinformationen genannten Dokumente sollten daraufhin geprüft werden, ob sie alle in Abschnitt 11 der Norm genannten Inhalte enthalten. Dazu zählen u.a. verständliche Beschreibungen der/des

- bestimmungsgemäßen Verwendung (Einsatz- und Anwendungsbereich)
- Information zum Performance Level und der Kategorie sowie die datierte Verweisung auf die Norm
- Sicherheitsfunktionen und Standardfunktionen
- Betriebsarten
- Ansprechzeiten
- Mutings (zeitweiliges Aufheben der Sicherheitsfunktionen)
- Grenzen für den Betrieb (einschließlich Umgebungsbedingungen)
- Schnittstellen
- Anzeigen und Alarme
- sicheren Montage und Inbetriebnahme, ggf. des sicheren Parametrierens und Programmierens
- Instandhaltung inklusive dafür geeigneter Checklisten
- Wartungs- und Wechselintervalle
- Zugänglichkeit und Ersatz interner Teile
- Mittel und Verfahren zur leichten und sicheren Fehlersuche

7.5 Validieren der Kombination und Integration von SRP/CS

Die einzelnen SRP/CS sind vor der Kombination separat zu prüfen. 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 Sicherheitsfunktion beschreiben
- Abgleich der Kenndaten der Schnittstellen zwischen den SRP/CS (z.B. Spannungen, Ströme, Drücke, Informationsdaten, Signalpegel)
- FMEA, bezogen auf die Kombination bzw. Integration
- Funktionstest/Black-Box-Test
- erweiterter Funktionstest
- Kontrolle der vereinfachten Bestimmung des Gesamt-PL aus den PLs der einzelnen SRP/CS wie in Abschnitt 6.4 beschrieben

7.6 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 werden in diesem Abschnitt die V&V-Aktivitäten am praktischen Beispiel einer Planschneidemaschine, das schon in den Abschnitten 5.7 und 6.5 beschrieben wurde, erläutert.

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

Anhand einer Risikoanalyse wurde ermittelt, dass für die auszuführende Sicherheitsfunktion SF2 ein erforderlicher Performance Level PL_r = e gilt. In der Berechnung der Ausfallwahrscheinlichkeit unter Berücksichtigung aller quantifizierbarer Aspekte wird dieser erreicht. Auch werden alle Anforderungen an die qualitativen Aspekte wie das Verhalten der Sicherheitsfunktion unter Fehlerbedingungen, sicherheitsbezogene Software, systematische Ausfälle und das Verhalten unter Umgebungsbedingungen für PL e hinreichend erfüllt.

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

Fehlerlisten

Bei der PL-Bestimmung werden die Fehlerlisten nach DIN EN 13849-2 [7] zugrunde gelegt.

Dokumente

Wie bereits genannt, bilden Schaltpläne, Stücklisten, Spezifikation und Funktionsbeschreibung die Grundlage für die Analyse bzw. Prüfung.

Dokumentation

Alle Analyse- und Prüfergebnisse bedürfen der Dokumentation in schriftlicher Form.

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 wäre die Überprüfung der Reaktion der SRP/CS, wenn eine weitere Person in den Gefahrenbereich durch eine dort vorhandene BWS (Lichtgitter) eingreift, während ein Mitarbeiter gerade die Zweihandschaltung bedient. Leistungstests zu funktionalen Aspekten werden durchgeführt. Dazu zählt die Überprüfung der nach der Norm DIN EN 574 [37] 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 abgeschlossen.

Validieren des PL der SRP/CS

- Validieren der Kategorie

Unter Einbeziehung der Entwicklungsunterlagen finden an einem Prototypen Tests zum Verhalten im Fehlerfall statt. Dies geschieht durch gezielten Einbau von Fehlern. Die Reaktion der SRP/CS auf die eingebauten Fehler sollte 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 von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.

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.

- Validieren der $MTTF_d$-Werte

Beispielhaft für die Validierung der $MTTF_d$-Werte wird hier der für die Ventile 1V3, 1V4, 2V2 und 2V1 angesetzte Wert von 150 Jahren aus Tabelle C.1 der DIN EN ISO 13849-1 [6] überprüft (siehe Tabelle D.2 dieses Reports). Es wurde der richtige Wert ausgewählt, und er entstammt einer zuverlässigen Quelle. Die für die Annahme von $MTTF_d$ = 150 Jahre geltenden Sicherheitsprinzipien (z.B. Ölwechsel) werden eingehalten und auch dem Betreiber in der Betriebsanleitung mitgeteilt.

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 Drucksensoren, 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 [38]. 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) des Normentwurfs DIN IEC 61508-2:2006 [39] durchgeführt.

- Validieren 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 Ausfällen und Kurzschlüssen. 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 Prüfungen muss gezeigt werden, dass die beschriebenen Maßnahmen in hinreichendem Maße umgesetzt wurden.

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

- Validieren 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.

- Verifizieren und Validieren der Maßnahmen gegen systematische Ausfälle

Die Einhaltung grundlegender und bewährter Sicherheitsprinzipien wirkt stark gegen systematische Ausfälle. Die Aktivitäten zur Validierung der Kategorie beinhalten ebenfalls die Überprüfung der Einhaltung beider 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 Dokumentation, 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 Ausfälle 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.

- Validieren der Software

Die Verifikation der Software wird ausführlich in Abschnitt 6.3 beschrieben. An dieser Stelle wird ergänzend die Validierung der Software durchgeführt, d.h. die Prüfung der Funktion und auch der Reaktionszeiten der auf der Hardware integrierten Software. Geprüft wird mit funktionalen Tests und einem erweiterten Funktionstest, bei dem 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 validieren.

- 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.

Prüfen der Benutzerinformation

Die Benutzerinformation muss zu Belangen der SRP/CS auf folgende Punkte erfolgreich überprüft werden: Beschreibung der bestimmungsgemäßen Verwendung; Angabe von Informationen zum PL und der Kategorie (einschl. 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.

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.

7.6.3 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 SF7) 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 Teil 1 und Teil 2 abgeschlossen.

8 Schaltungsbeispiele für SRP/CS

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. Sie lassen sich aufgrund der Vielfalt möglicher Sicherheitsfunktionen und ihrer Realisierung auch nur schwer allgemein beschreiben. Daher wird nun in diesem Kapitel die Bewertung einer Vielzahl von Schaltungsbeispielen vorgestellt, die Sicherheitsfunktionen in verschiedenen Kategorien bzw. Performance Leveln 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 nur als Anregung für eine Realisierung. Bei deren Auswahl wurde auf ein breites Spektrum von Technologien und möglichen Anwendungen Wert gelegt. Leser des Reports zu den Kategorien für sicherheitsbezogene Steuerungen nach EN 954-1 aus dem Jahre 1997 [40] werden das eine oder andere Beispiel angereichert u.a. um die Berechnung der Ausfallwahrscheinlichkeit wiedererkennen. 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 dem Konstrukteur eine wirksame Hilfestellung für eigene Entwicklungen zu geben. Da sie von verschiedenen Autoren erstellt wurden, ist naturgemäß eine Varianz, z.B. in 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 1.0 ausgeführt.

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 Beispieles, 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 Sensorsignale z.B. 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. In den technologiebezogenen Bemerkungen zur Fluidtechnik sind weitere Beispiele aufgeführt. Selbstverständlich muss gemäß den Fehlerlisten aus DIN EN ISO 13849-2 z.B. auch der Einfluss von Leitungskurzschlüssen im Zusammenhang mit der jeweiligen Sicherheitsfunktion 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.

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 **H**ersteller), typische Werte aus Datenbanken (Kennzeichnung „[D]“ für **D**atenbank) oder als Werte aus der Norm DIN EN ISO 13849-1 ((Kennzeichnung „[N]“ für **N**orm) markiert. Die Norm sieht eine Priorisierung von Herstellerdaten vor. Für einige Komponenten, z.B. Drehgeber oder Frequenzumrichter, waren zum Zeitpunkt der Erstellung des Reports weder verlässliche Herstellerangaben noch Datenbankwerte zu erhalten. Hier wurden Hersteller gezielt angesprochen oder das „Parts Count“-Verfahren zu Hilfe genommen, um typische Beispielwerte abzuschätzen (Kennzeichnung „[G]“ für **g**eschätzt). 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 hinsichtlich *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“ und den „rechnerischen“ Methoden zur Bestimmung des PL. Einige Teilschritte, z.B. Fehlerauschlüsse, 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 [20] 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 [38], Anhang K.

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. Auch die ausgeführten 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).

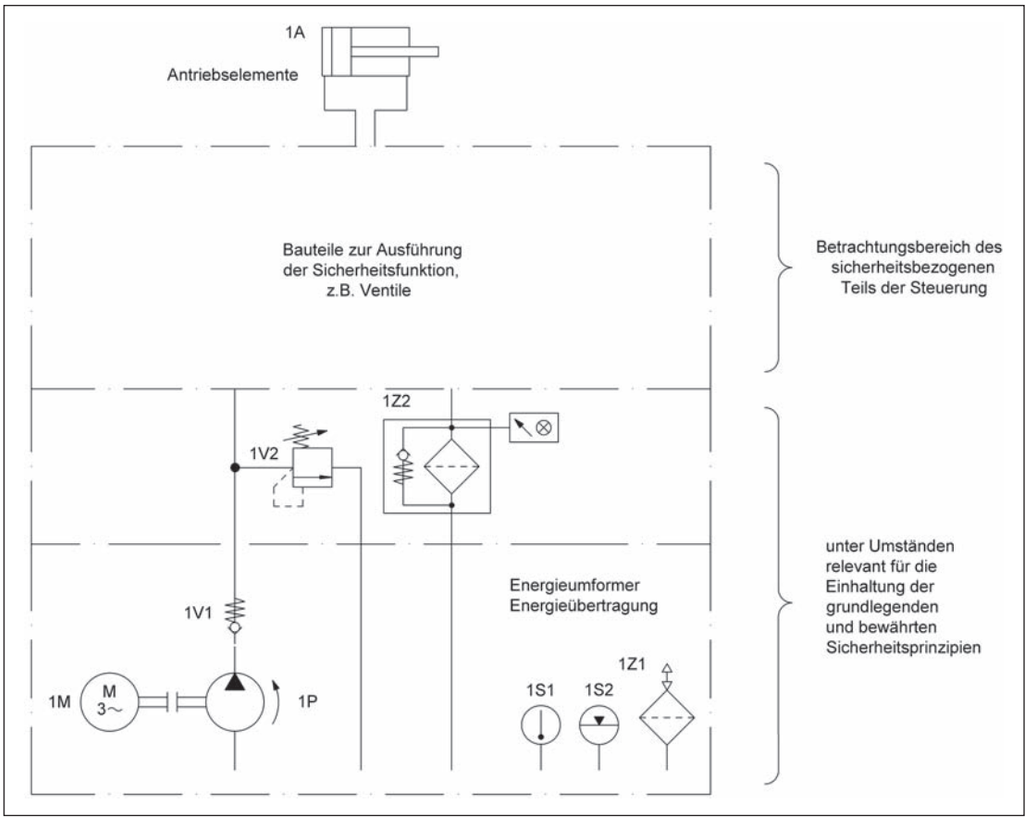


Abbildung 8.1: Anwendungsbereich der DIN EN ISO 13849 bei hydraulischen Anlagen

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 auf Seite 88) 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 [41; 42] zu entnehmen. Als weitere zutreffende Normen sind [43 bis 47] zu nennen.

Die meisten Steuerungsbeispiele sind elektrohydraulische bzw. 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.

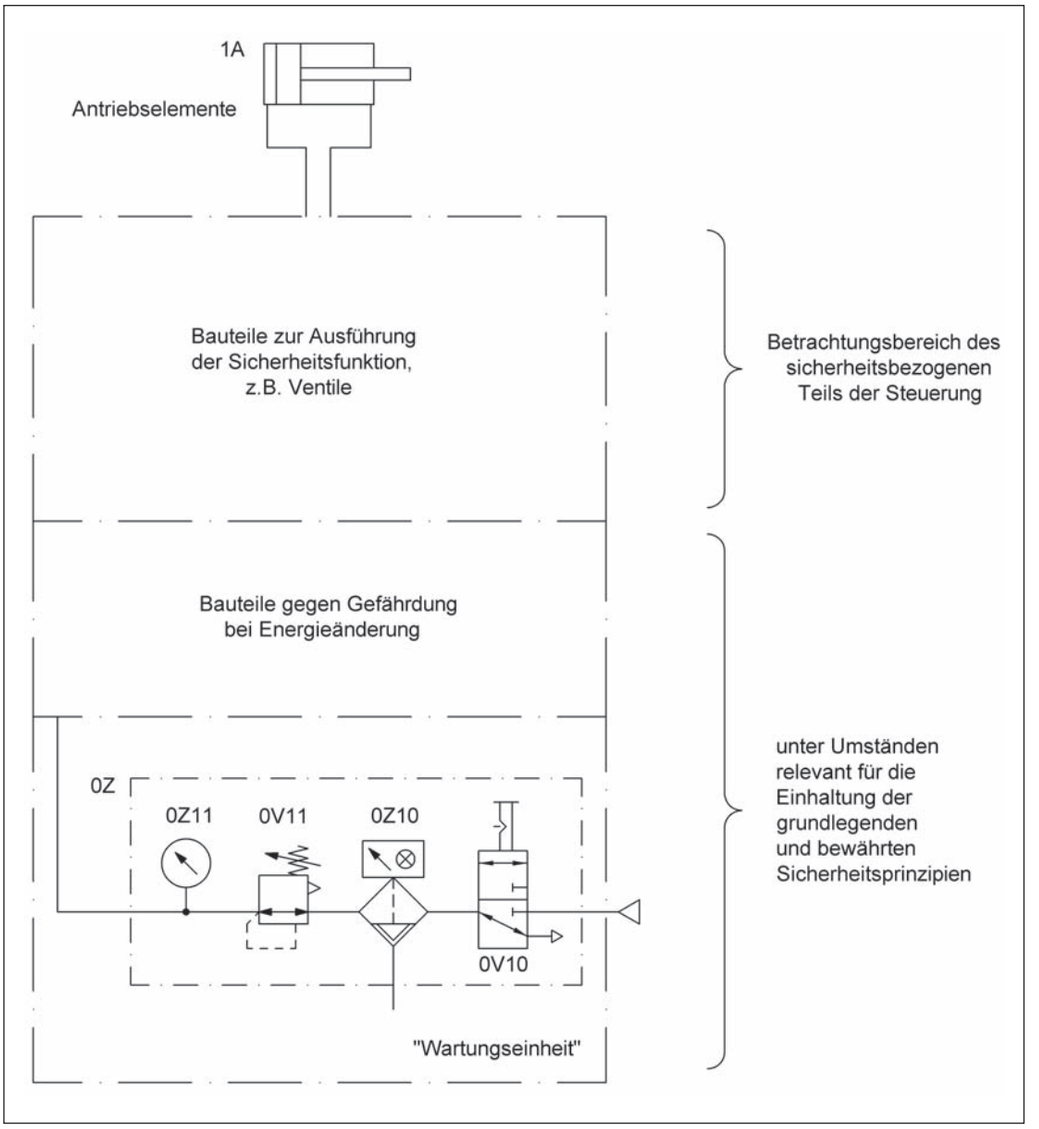


Abbildung 8.2: Anwendungsbereich der DIN EN ISO 13849 bei pneumatischen Anlagen

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 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 Schütz elektrisch nicht angesteuert, d.h. wird seine Spule nicht vom Strom durchflossen, gibt es keinen Grund dafür, dass sich die Kontakte des Schützes schließen. 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-prozentiger 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. Durch Anwendung von Prinzipien, z.B. Ruhestrom, Diversität oder Überdimensionierung, können auch elektronische Schaltungen so robust gestaltet werden, dass ein systematischer Ausfall ausreichend sicher verhindert ist. 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 siehe Abschnitt 6.3. Werden im Rahmen einer Entwicklung ASICs eingesetzt, so sind im Entwicklungsprozess fehlervermeidende Maßnahmen erforderlich. Solche enthält zum Beispiel der Normentwurf DIN IEC 61508-2:2006 [39], der 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 37. Tabelle 8.2 (siehe Seite 90) nennt alphabetisch sortiert die wichtigsten in den Schaltungsbeispielen verwendeten Abkürzungen.

Tabelle 8.1:
Übersicht der Schaltungsbeispiele

Erreichter PL	Realisierte Kategorie	Technologie/Beispiel Nr.		
		Pneumatik	Hydraulik	Elektrotechnik
b	B			1
c	1	2	3	4, 5, 6, 7, 8
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, 26	27	29, 30
e	4	31	32, 33	28, 33, 34, 35, 36, 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. Anhang D, Abschnitt D2.6)
[G]	Geschätzte B_{10d}- oder $MTTF_d$-Werte
[H]	B_{10d}- oder $MTTF_d$-Werte auf der Basis von Herstellerangaben
[N]	B_{10d}- oder $MTTF_d$-Werte auf der Basis von gelisteten Angaben in der Norm DIN EN ISO 13849-1 (siehe z.B. Tabelle D.2 dieses Reports)
µC	Mikrocontroller
B_{10}	Nominale Lebensdauer, die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der bis zu 10 % der betrachteten Einheiten ausgefallen sind
B_{10d}	Nominale Lebensdauer, die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der bis zu 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 Bauteilstunden (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	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)
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	Sicherer Stopp 1 (Safe Stop 1, siehe Tabelle 5.2)
SS2	Sicherer Stopp 2 (Safe Stop 2, siehe Tabelle 5.2)
STO	Sicher abgeschaltetes Moment (Safe Torque Off, siehe Tabelle 5.2)
T_{10d}	Mittlere Zeit, nach der bis zu 10 % der betrachteten Einheiten gefährlich ausgefallen sind
ZHS	Zweihandschaltung

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

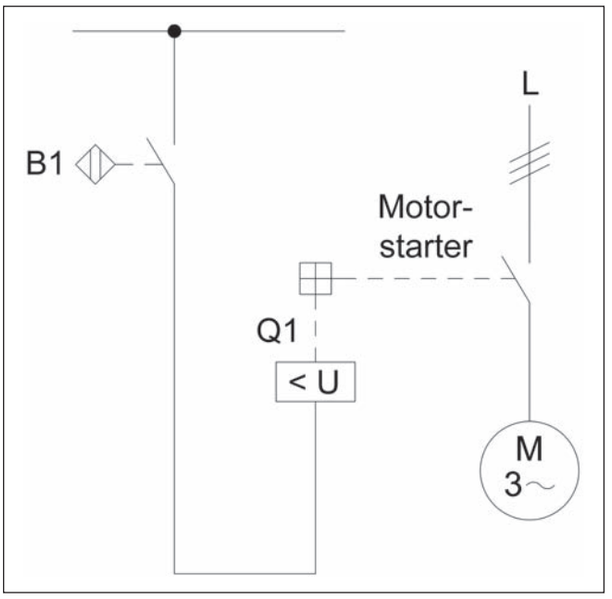


Abbildung 8.3:
Stellungsüberwachung beweglicher trennender Schutzeinrichtungen mittels Näherungsschalter

Sicherheitsfunktion

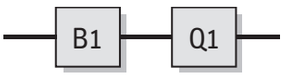
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Die Betätigung des Näherungsschalters beim Öffnen der beweglichen trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der beweglichen 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 verdeckter Einbau (siehe auch DIN EN 1088/A1 Anhang J).
- 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 $MTTF_d$ = 40 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 B10-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 $MTTF_d$ = 37 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 $4{,}23 \cdot 10^{-6}$/Stunde. Dies entspricht PL b.

Weiterführende Literatur

- DIN EN 1088/A1: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (07.07). Beuth, Berlin 2007

- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

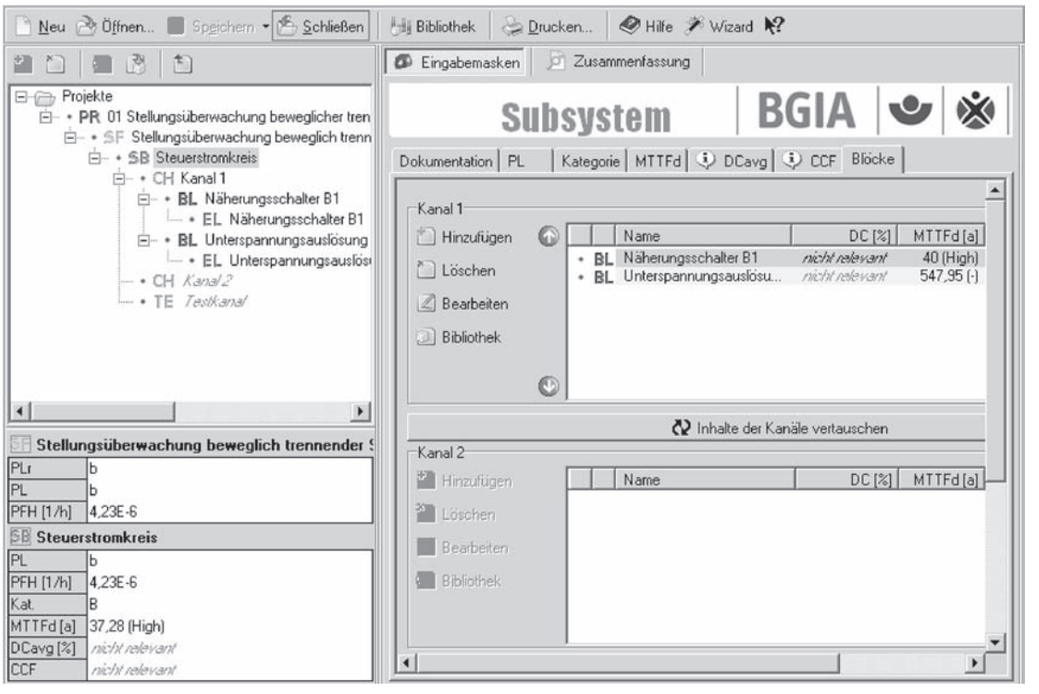


Abbildung 8.4: PL-Bestimmung mithilfe von SISTEMA

8.2.2 Pneumatisches Ventil (Subsystem) – Kategorie 1 – PL c (für PL-b-Sicherheitsfunktionen) (Beispiel 2)

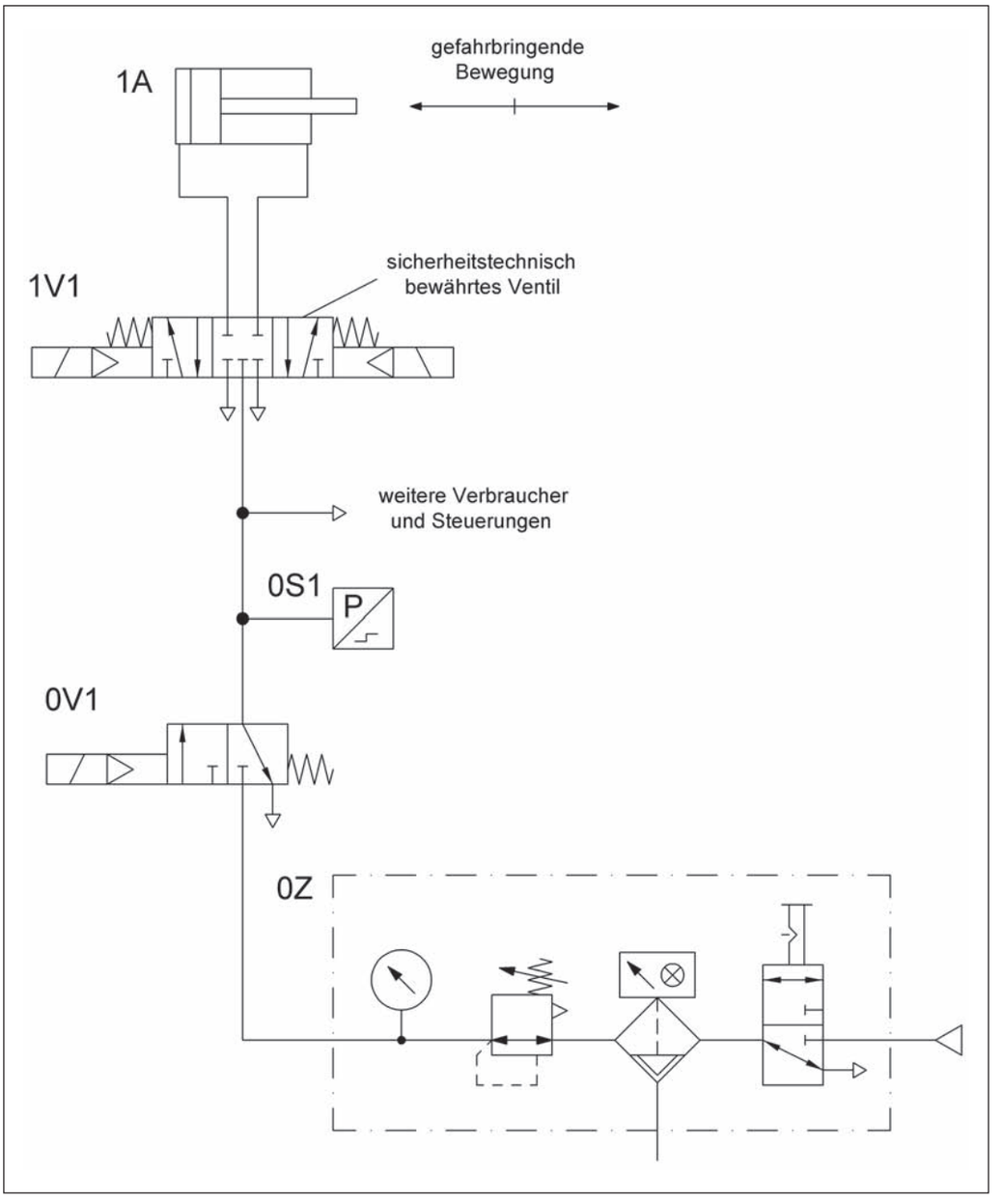


Abbildung 8.5: Pneumatisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- 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 bei Bedarf 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 40 000 000 Schaltspielen [G] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 5 Sekunden Zykluszeit ist n_{op}=2 764 800 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 $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Wegeventil 1V1 ein Wert von 14 Jahren (T_{10d}) Betriebszeit bis zum vorgesehenen Austausch.

8.2.3 Hydraulisches Ventil (Subsystem) – Kategorie 1 – PL c (für PL-b-Sicherheitsfunktionen) (Beispiel 3)

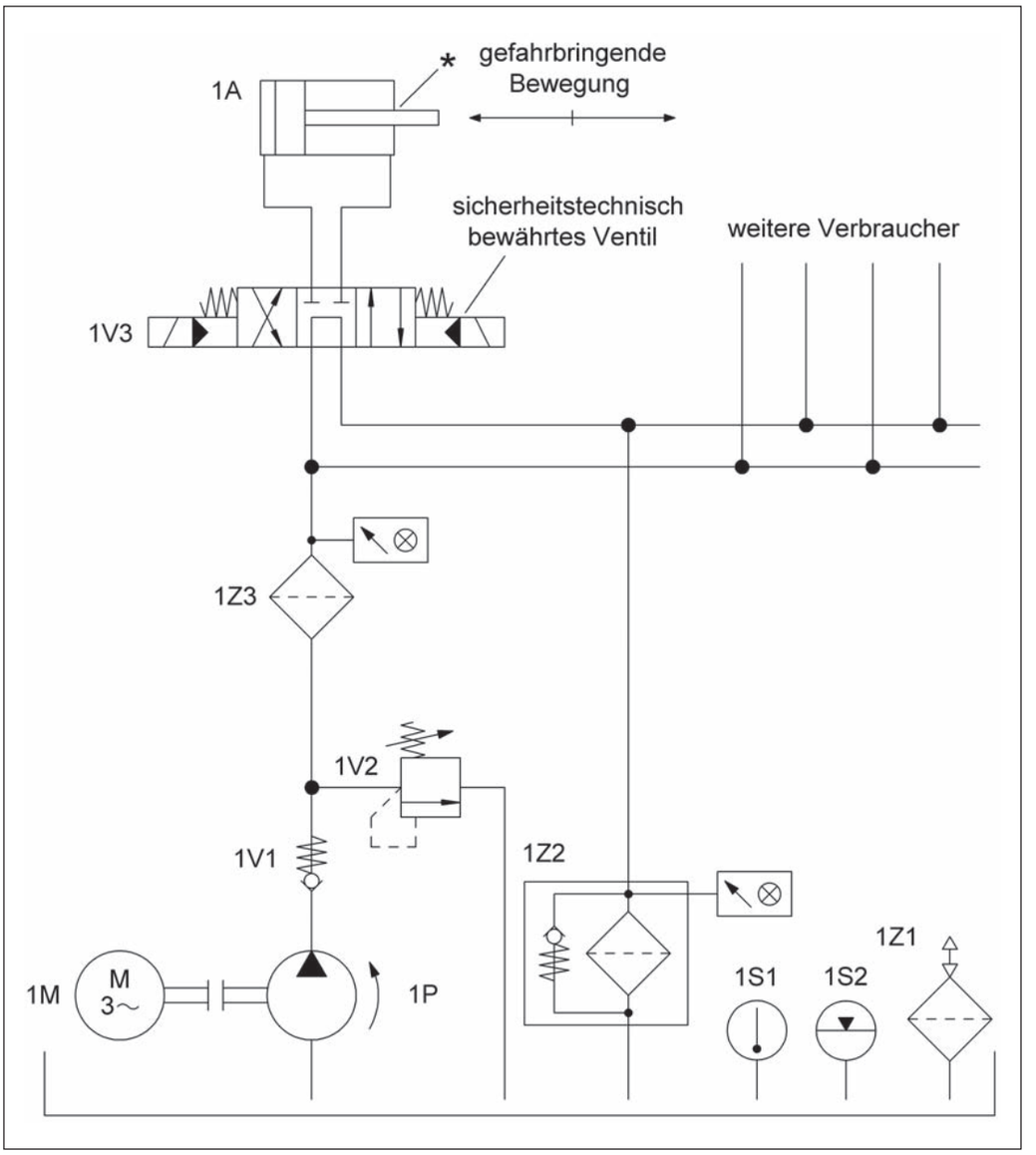


Abbildung 8.6: Hydraulisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten 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 8.6) vorgesehen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für das Wegeventil 1V3 wird eine $MTTF_d$ von 150 Jahren angenommen [N]. 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 $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

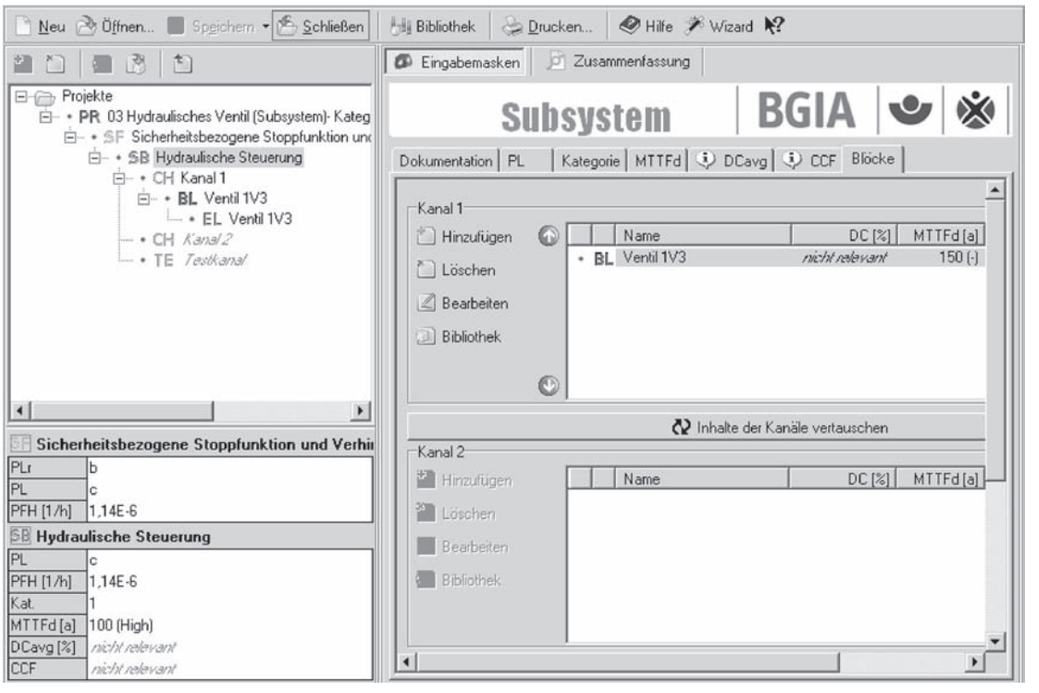


Abbildung 8.7: PL-Bestimmung mithilfe von SISTEMA

8.2.4 Stillsetzen von Holzbearbeitungsmaschinen – Kategorie 1 – PL c (Beispiel 4)

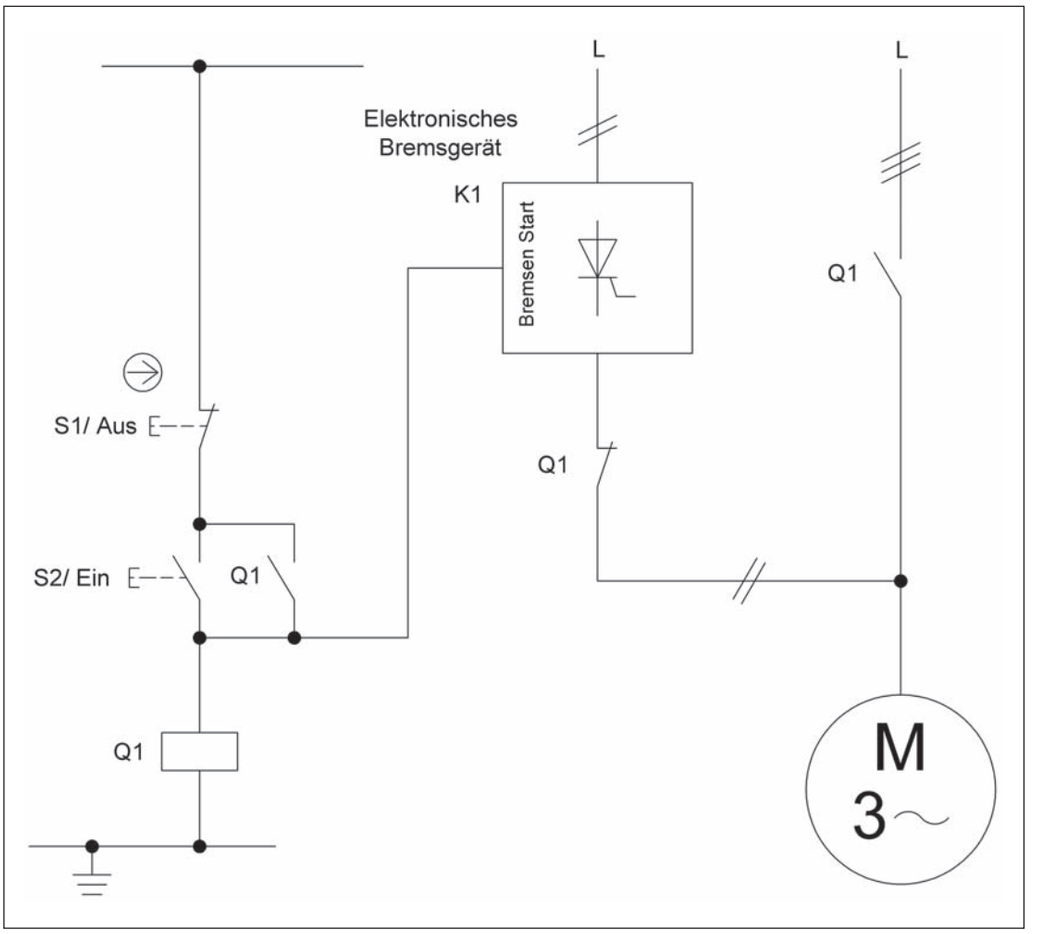


Abbildung 8.8: Kombination von elektromechanischer Befehlseinrichtung und einfachem elektronischen Bremsgerät zum Stillsetzen von Holzbearbeitungs-maschinen

Sicherheitsfunktion

- Die Betätigung des Aus-Tasters führt zu SS1 – Sicherer Stopp 1, 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.4 der DIN EN 13849-2.

- Das Bremsgerät K1 ist ausschließlich unter Verwendung einfacher elektronischer Bauelemente wie z.B. Transistoren, Kondensatoren, Dioden, Widerstände, Thyristoren aufgebaut, die als bewährte Bauteile angesehen werden. Die fehlerfreie Durchführung der sicherheitsrelevanten Bremsfunktion wird durch die Auswahl der Bauteile charakterisiert. Interne Maßnahmen zur Fehlererkennung sind nicht vorgesehen. Es kommen keine komplexen elektronischen Bauteile (z.B. Mikroprozessoren) zum Einsatz, die gemäß DIN EN ISO 13849-1, Abschnitt 6.2.4, nicht als gleichwertig zu bewährt betrachtet werden.

Anwendung

- Bei Holzbearbeitungsmaschinen oder ähnlichen Maschinen, bei denen das ungebremste Stillsetzen zu einem unzulässig langen Auslaufen der gefahrbringenden Werkzeugbewegungen führen würde. Die Steuerung muss so ausgeführt sein, dass mindestens PL b erreicht wird (Prüfgrundsätze Holzbearbeitungsmaschinen GS-HO-01).

Berechnung der Ausfallwahrscheinlichkeit

- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung). Beim Einsatz eines solchen Tasters als Befehlsgerät kann ein Fehlerausschluss für das Nichtöffnen des elektrischen Kontakts inklusive der Mechanik innerhalb des Tasters erfolgen.

- $MTTF_d$: Für das Schütz Q1 wird bei nominaler Last ein B_{10d}-Wert von 2 000 000 Schaltspielen [N] angenommen. Bei 300 Arbeitstagen, 8 Arbeitsstunden und 2 Minuten Zykluszeit ist n_{op} = 72 000 Zyklen/Jahr und $MTTF_d$ = 277 Jahre. 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 [36] ergibt sich eine $MTTF_d$ = 518 Jahre [D]. Die Kombination von Q1 und K1 ergibt $MTTF_d$ = 180 Jahre 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 $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Damit ist der PL_r = b übertroffen.

Weiterführende Literatur

- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01. Ausg. 12/2007 www.dguv.de/bgia, Webcode d14898

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

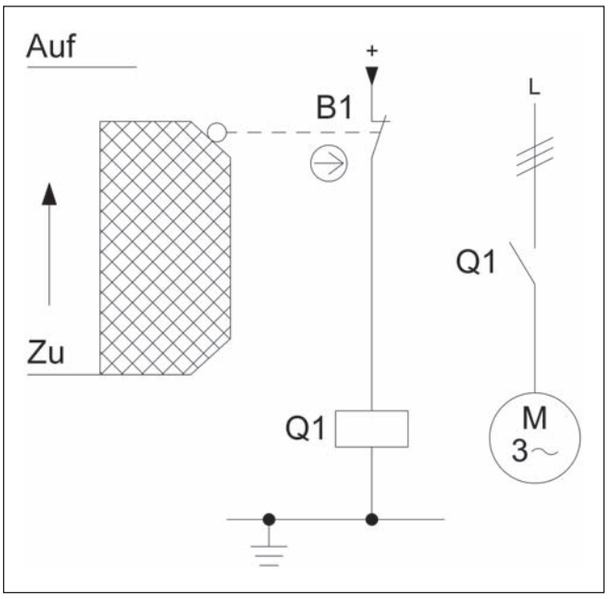


Abbildung 8.9:
Stellungsüberwachung beweglicher trennender Schutzeinrichtungen zur Verhinderung von gefahrbringenden Bewegungen (STO – Sicher abgeschaltetes Moment)

Sicherheitsfunktion

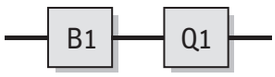
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der beweglichen 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.4 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 kann ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt erfolgen. Für den mechanischen Teil von B1 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op}= 35 040 Zyklen/Jahr und $MTTF_d$ = 285 Jahre. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 300 000 Schaltspiele [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 $MTTF_d$ = 206 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 $1{,}14 \cdot 10^{-6}$/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 (02.05). Beuth, Berlin 2005

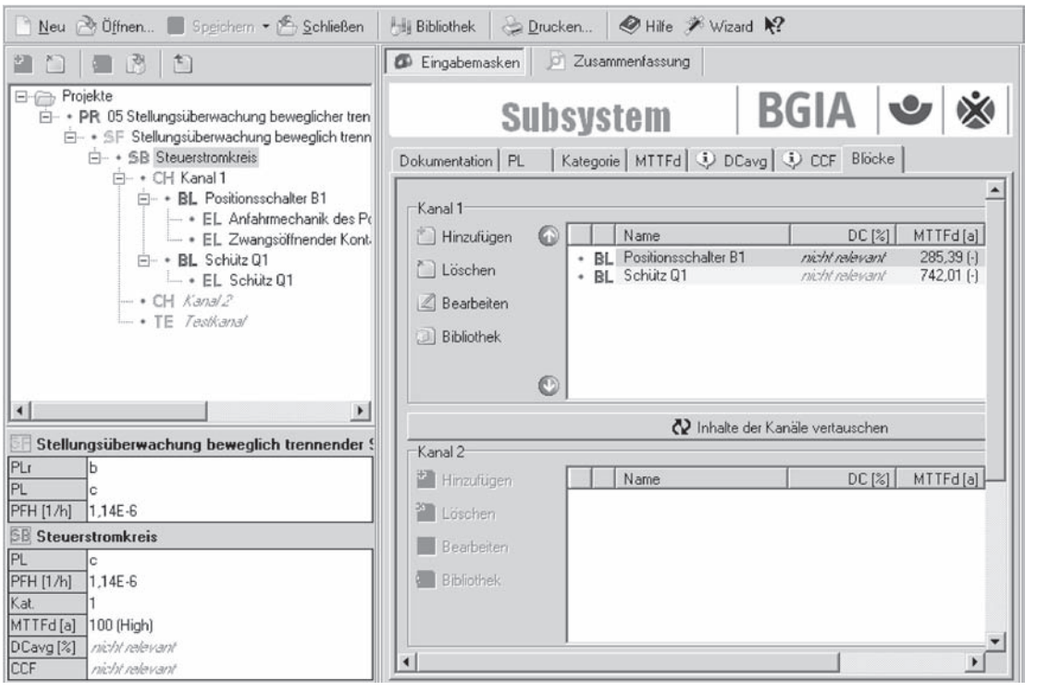


Abbildung 8.10.: PL-Bestimmung mithilfe von SISTEMA

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

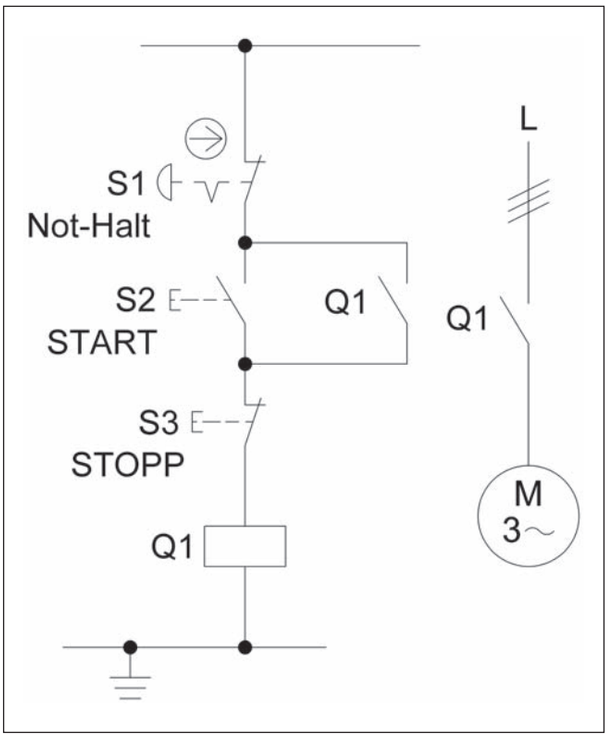


Abbildung 8.11:
Kombinierte Start-Stopp-Einrichtung mit Not-Halt-Gerät

Sicherheitsfunktion

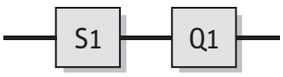
- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes

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 60947-5-1, Anhang K, und daher ein bewährtes Bauteil nach Tabelle D.4 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.4 der DIN EN ISO 13849-2.



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 erfolgt ein Fehlerausschluss für den zwangsöffnenden Kontakt und die Mechanik, sofern die in Tabelle D.2 dieses Reports angegebene Anzahl der Betätigungen nicht überschritten wird. Für das Schütz Q1 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. Werden an 365 Arbeitstagen täglich zwei Betätigungen der Start-Stopp-Einrichtung und jährlich drei Betätigungen des Not-Halt-Geräts angenommen, so ergibt sich mit n_{op} = 733 Zyklen/Jahr für Q1 eine $MTTF_d$ von 35 470 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 $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (03.07). Beuth, Berlin 2007
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

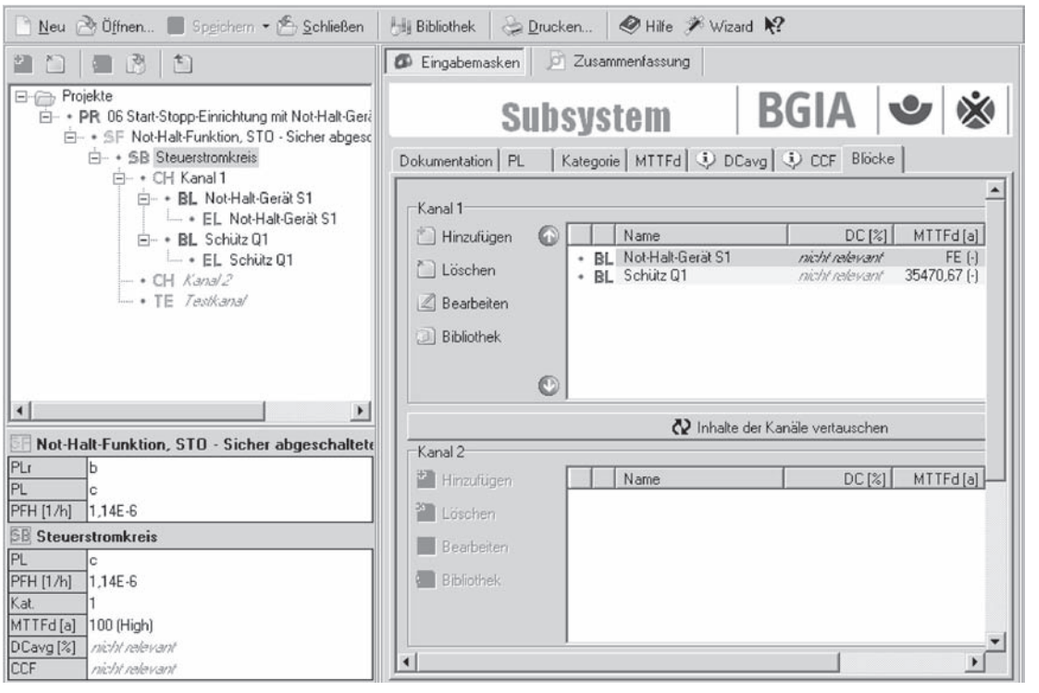


Abbildung 8.12: PL-Bestimmung mithilfe von SISTEMA

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

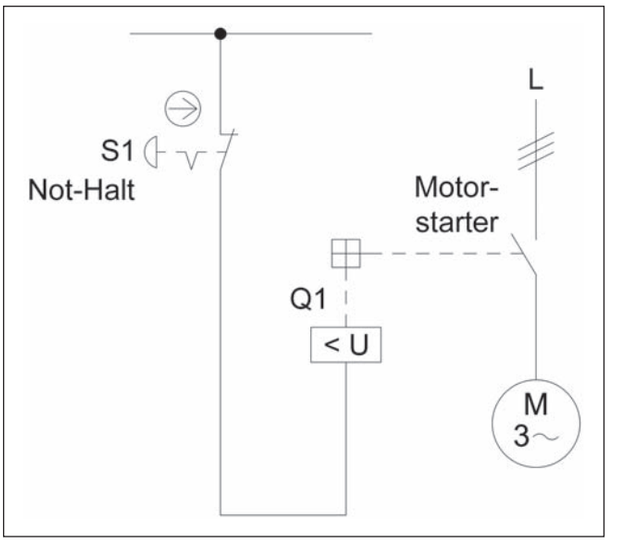


Abbildung 8.13:
Not-Halt-Gerät auf Unterspannungsauslösung der Netztrenneinrichtung (Motorstarter) wirkend

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

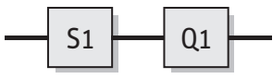
- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Gerätes S1 durch Unterspannungsauslösung der Netztrenneinrichtung – hier in Form eines Motorstarters Q1 – unterbrochen.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der 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 60947-5-1, Anhang K, und daher ein bewährtes Bauteil nach Tabelle D.4 der DIN EN ISO 13849-2.
- Der Motorstarter Q1 ist einem Leistungsschalter nach Tabelle D.4 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).

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 erfolgt ein Fehlerausschluss für den zwangsöffnenden Kontakt und die Mechanik, sofern die in Tabelle D.2 dieses Reports angegebene Anzahl der Betätigungen nicht überschritten wird. 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 drei Betätigungen des Not-Halt-Geräts ergibt sich mit n_{op} = 3 Zyklen/Jahr für Q1 eine $MTTF_d$ von 66 666 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 $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (03.07). Beuth, Berlin 2007
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

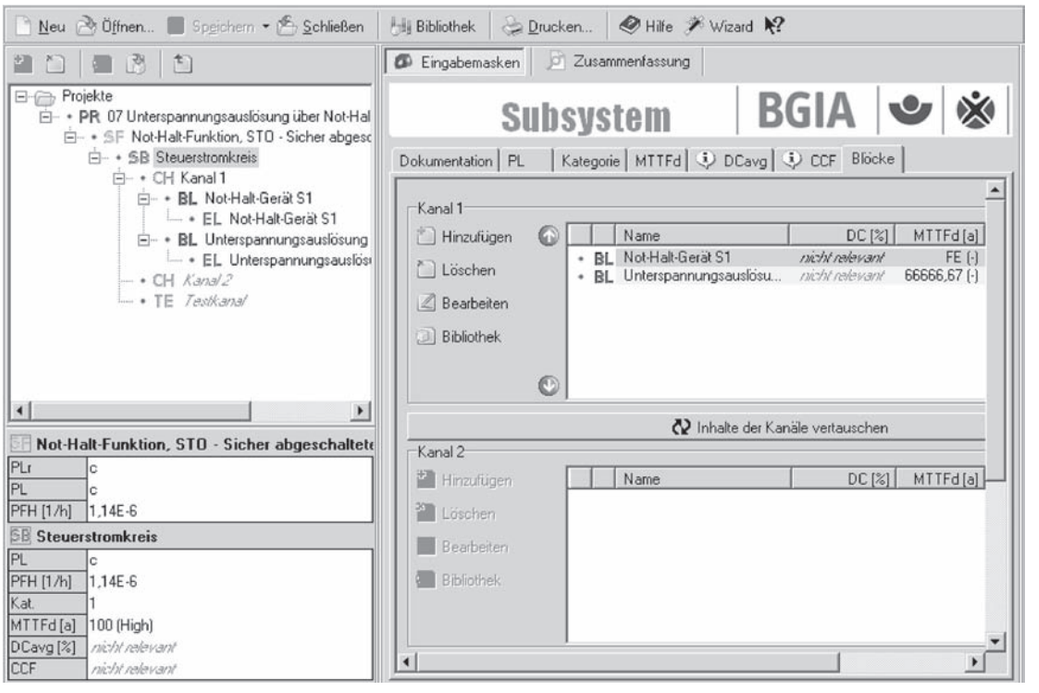


Abbildung 8.14: PL-Bestimmung mithilfe von SISTEMA

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

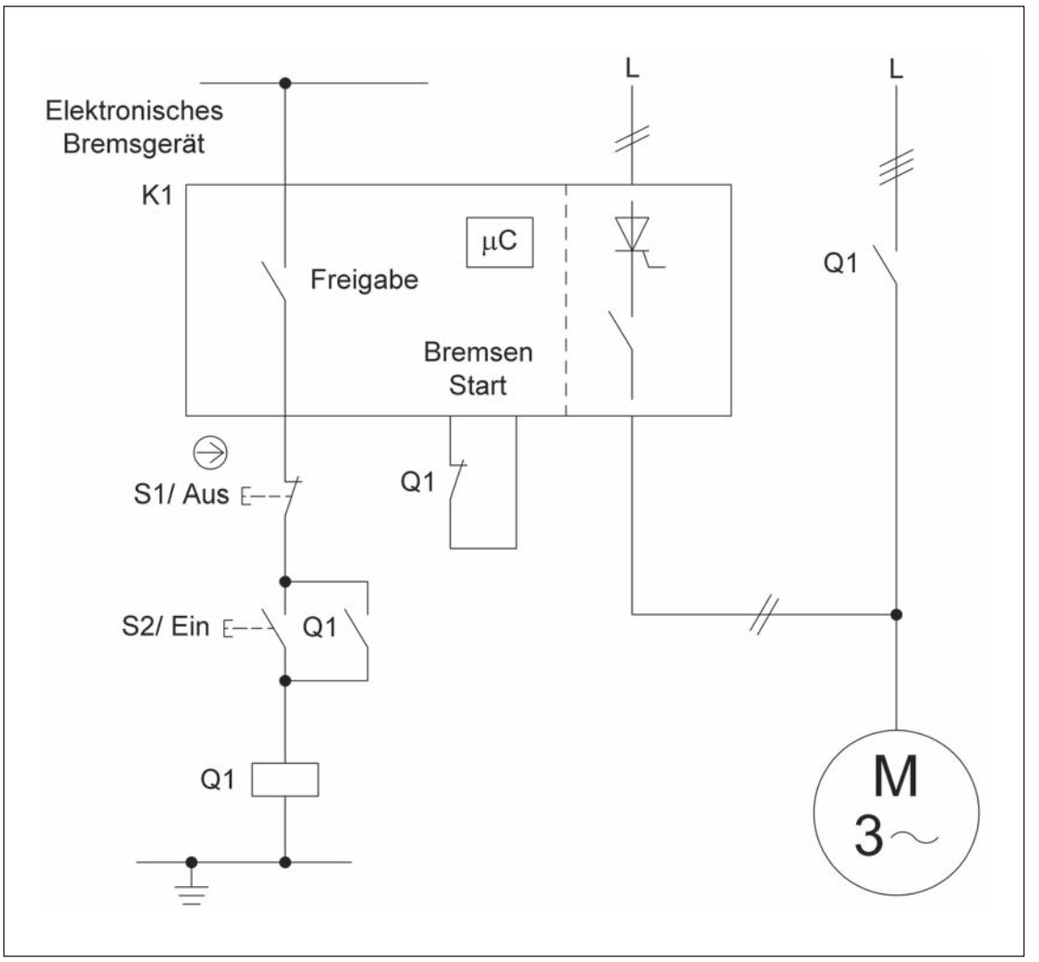


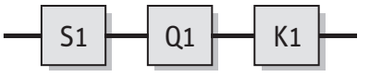
Abbildung 8.15: Kombination von elektromechanischer Befehlseinrichtung und programmierbar elektronischem Bremsgerät zum Stillsetzen von Holzbearbeitungsmaschinen

Sicherheitsfunktion

- Die Betätigung des Aus-Tasters führt zu SS1 – Sicherer Stopp 1, 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 Thyristoren erzeugt und über interne Relais auf die Motorwicklung geschaltet wird.
- Die Stillsetzzeit darf einen maximalen Wert, z.B. 10 Sekunden, nicht überschreiten. Die gewünschte Bremszeit und evtl. andere erforderliche Parameter (z.B. Bremsstrom, Schwelle für Stillstandserkennung) können am Bremsgerät eingestellt werden.
- Nach erfolgtem Stillstand bzw. nach Ablauf der maximalen Bremszeit schaltet das Bremsgerät den Bremsstrom ab und trennt den Motor wieder vom Netz. 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.
- Die fehlerfreie Durchführung der Bremsfunktion wird vom Bremsgerät K1 regelmäßig überwacht. Sollte ein Fehler festgestellt werden, z.B. eine Überschreitung der maximal zulässigen Bremszeit, wird über den Freigabekontakt im Gerät ein erneutes Starten des Motors verhindert. Maßnahmen zur Fehlererkennung in S1 oder Q1 sind nicht 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.4 der DIN EN ISO 13849-2.

- Das von einem Mikrocontroller gesteuerte Bremsgerät K1 erfüllt alle Anforderungen für Kategorie 2 und PL c. Die sicherheitsrelevanten Funktionen werden in regelmäßigen Abständen getestet. Der zeitliche Programmablauf des Mikrocontrollers wird durch einen separaten Watchdog überwacht.

Anwendung

- Bei Holzbearbeitungsmaschinen oder ähnlichen Maschinen, bei denen das ungebremste Stillsetzen zu einem unzulässig langen Auslaufen der gefahrbringenden Werkzeugbewegungen führen würde. Die Steuerung muss so ausgeführt sein, dass mindestens Performance Level b erreicht wird (Prüfgrundsätze Holzbearbeitungsmaschinen GS-HO-01).

Berechnung der Ausfallwahrscheinlichkeit

- Da das elektronische Bremsgerät K1 als handelsüblicher Baustein zum Einsatz kommt, wird dessen Ausfallwahrscheinlichkeit ($5{,}28 \cdot 10^{-7}$/Stunde [H]) am Ende der Berechnung mit SISTEMA addiert. Für den übrigen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.

- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung). Bei Einsatz eines solchen Tasters als Befehlsgerät kann ein Fehlerausschluss für das Nichtöffnen des elektrischen Kontakts inklusive der Mechanik innerhalb des Tasters erfolgen.

- $MTTF_d$: Für das Schütz Q1 wird bei nominaler Last ein B_{10d}-Wert von 2 000 000 Schaltspielen [N] angenommen. Bei 300 Arbeitstagen, 8 Arbeitsstunden und 2 Minuten Zykluszeit ist n_{op} = 72 000 Zyklen/Jahr und $MTTF_d$ = 277 Jahre. 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, bestehend aus S1 und Q1, entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $1{,}67 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Damit ist der PL_r = b übertroffen.

Weiterführende Literatur

- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01. Ausg. 12/2007 www.dguv.de/bgia, Webcode d14898

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

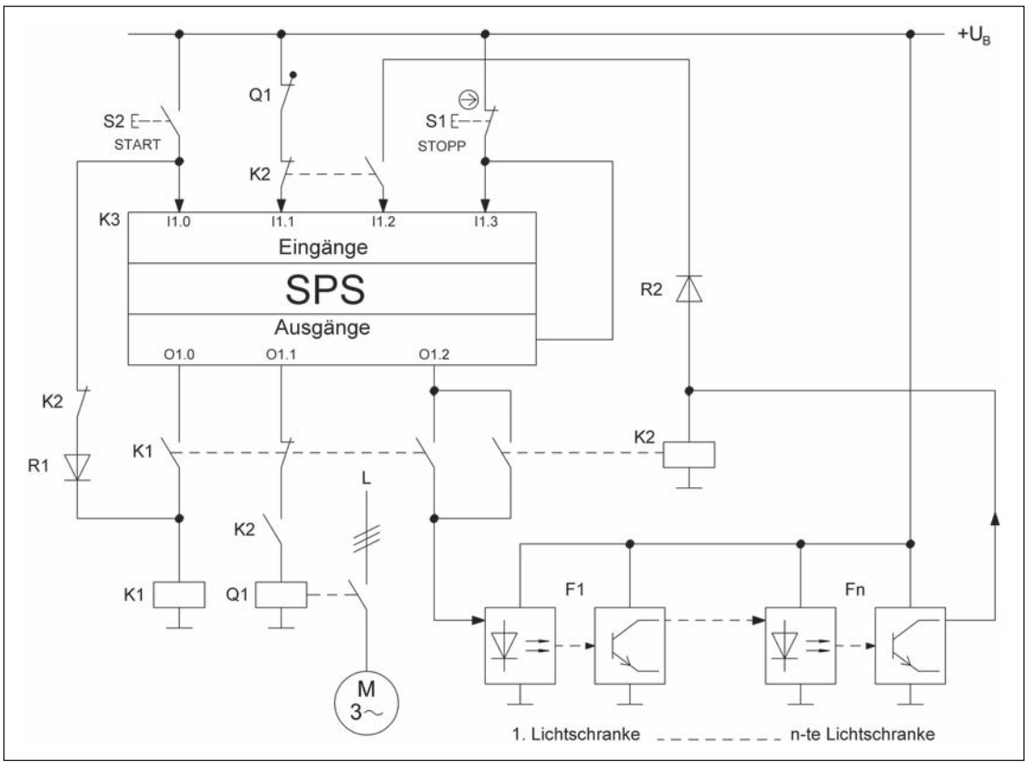


Abbildung 8.16: Testung von Lichtschranken mit einer Standard-SPS

Sicherheitsfunktion

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

Funktionsbeschreibung

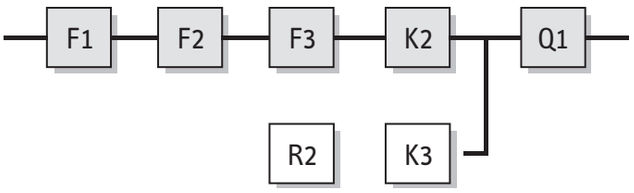
- Bei einer Lichtstrahlunterbrechung der *n* kaskadierten Lichtschranken F1 bis Fn wird sowohl kontaktbehaftet durch das Entregen des Hilfsschützes K2 als auch durch den SPS-Ausgang (O1.1) des Testkanals ein Abschaltbefehl erzeugt. Das Stillsetzen der gefahrbringenden Bewegung erfolgt dann über das Leistungsschütz 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 ausreichenden optischen Eigenschaften (optischer Öffnungswinkel, Fremdlichtsicherheit usw.) nach DIN CLC/TS 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 Schütz 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 (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.
- 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 999 und DIN IEC 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 $MTTF_d$ = 1 302 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 61,0 % („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 $MTTF_d$ pro Kanal (32,5 Jahre) und niedrigem DC_{avg} (61,0 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}85 \cdot 10^{-6}$/Stunde.

Für das Subsystem „Hauptschütz" wird angenommen:

- B_{10d} = 2 000 000 Zyklen [N] mit n_{op} = 76 800 Zyklen/Jahr. Dies führt zu einer $MTTF_d$ von 260,4 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 mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde.

- Die Addition der mittleren Wahrscheinlichkeit gefährlicher Ausfälle beider Subsysteme ergibt $3{,}0 \cdot 10^{-6}$/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 5 Stunden), so kann dies gemäß Anhang G 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 Ausfallwahrscheinlichkeit von $2{,}04 \cdot 10^{-6}$/Stunde. Die mittlere Gesamtwahrscheinlichkeit gefährlicher Ausfälle von $3{,}18 \cdot 10^{-6}$/Stunde erreicht allerdings nur noch PL b. Um PL c zu erreichen, müssten z.B. die Anzahl der Lichtschranken reduziert oder Komponenten höherer $MTTF_d$ eingesetzt werden.

Weiterführende Literatur

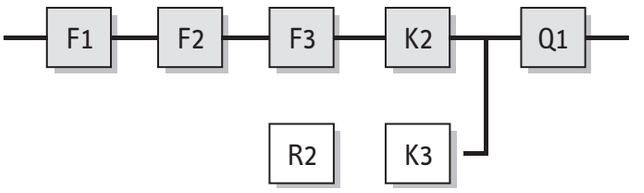
- *Grigulewitsch, W.; Reinert, D.:* Lichtschranken mit Testung. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 228. 22. Lfg. V/94. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/330228

- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (01.05). Beuth, Berlin 2005

- DIN CLC/TS 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (02.08). Beuth, Berlin 2008

- DIN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zum Erkennen von Personen (Normentwurf) (08.06). Beuth, Berlin 2006

- DIN EN 999: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (12.98). Beuth, Berlin 1998



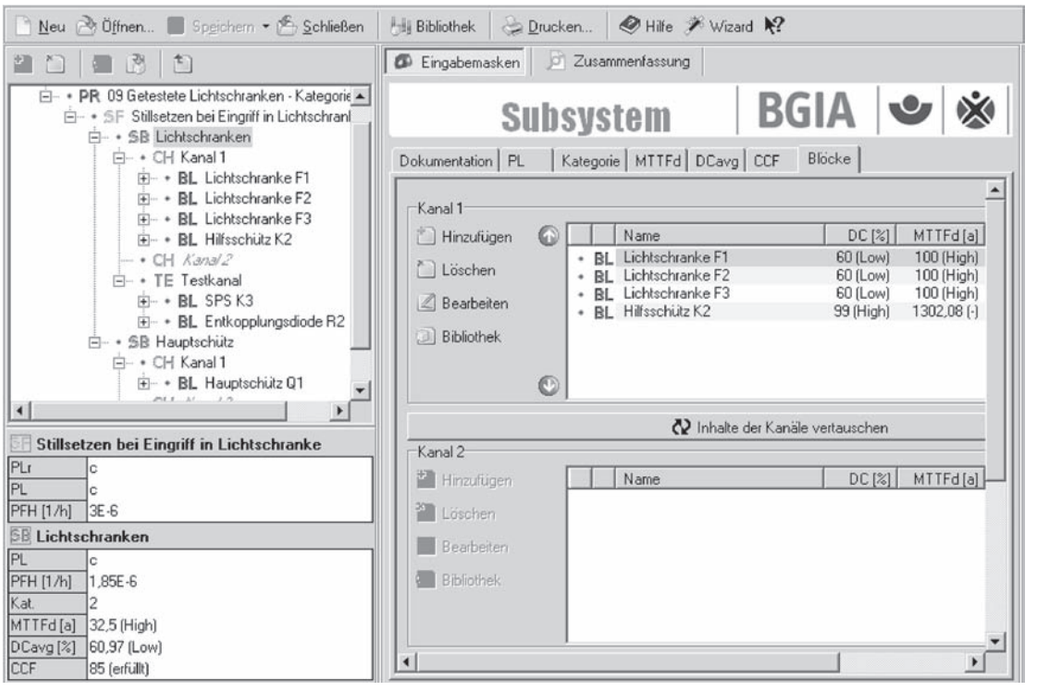


Abbildung 8.17: PL-Bestimmung mithilfe von SISTEMA

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

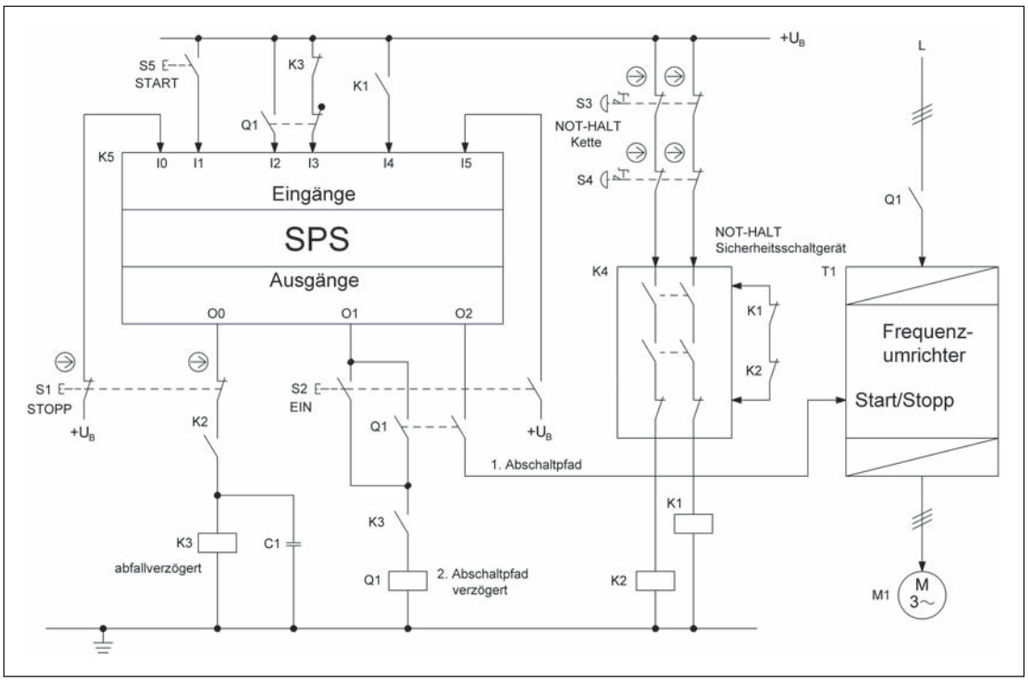


Abbildung 8.18: Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl

Sicherheitsfunktion

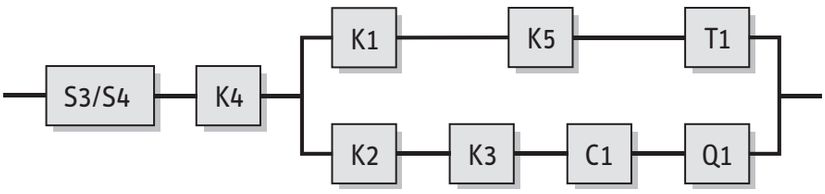
- Sicherheitsbezogene Stoppfunktion bzw. Not-Halt-Funktion: Nach einem Stopp- oder Not-Halt-Befehl wird der Antrieb angehalten (SS1 – Sicherer Stopp 1).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird redundant unterbrochen, falls entweder die Stopp-Taste S1 oder eines der Not-Halt-Geräte S3 bzw. S4 betätigt wird. Das Stillsetzen des Antriebs im Notfall erfolgt nach Betätigung von S3/S4 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 jeweils 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.



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 b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.
- Die verzögerte Einleitung des Stillstands im Fehlerfall nur über den zweiten Abschaltpfad darf nicht mit einem verbleibenden inakzeptabel hohen Risiko 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. Für die Berechnung der sicherheitsbezogenen Stoppfunktion müssen S3/S4 und K4 durch S1 ausgetauscht sowie K1 und K2 weggelassen werden.

- Für die Not-Halt-Geräte S3/S4 wird ein Fehlerausschluss angenommen, da die in Tabelle D.2 genannte maximale Anzahl von 6 050 Schaltzyklen innerhalb der Gebrauchsdauer des Schaltgerätes nicht überschritten wird. 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. Der Wert gilt für eine maximale Anzahl von 6 050 Schaltzyklen innerhalb der Gebrauchsdauer des Schaltgerätes.

Für die Ausfallwahrscheinlichkeit der nachfolgenden zweikanaligen Struktur gilt:

- $MTTF_d$: Folgende $MTTF_d$-Werte werden geschätzt: 25 Jahre für K5 und 50 Jahre für T1 [G]. 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 400 000 Zyklen [N] und Schalthäufigkeit von täglichem Einschalten an 240 Arbeitstagen eine $MTTF_d$ von 16 667 Jahren. Für K3 und Q1 ergibt sich bei einem B_{10d}-Wert von 400 000 Zyklen [N] und bei 240 Arbeitstagen, 16 Arbeitsstunden und 3 Minuten Zykluszeit eine n_{op} = 76 800 Zyklen/Jahr und jeweils eine $MTTF_d$ von 52 Jahren. Diese Werte ergeben eine symmetrisierte $MTTF_d$ des Kanals von 21 Jahren („mittel“).
- DC_{avg}: Fehlererkennung durch den Prozess bei Ausfall der Ansteuerung der Bremsrampe führt auf DC = 30 % 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 K3 DC = 99 % wegen Fehlererkennung durch K5. Für C1 gilt DC = 60 % durch Testung des Zeitglieds bei spannungsfreiem FU. Für Q1 folgt DC = 99 % durch direkte Überwachung in K5. Die Mittelungsformel für DC_{avg} ergibt 63 % („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 mit mittlerer $MTTF_d$ pro Kanal (21 Jahre) und niedrigem DC_{avg} (63 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}04 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Die Gesamtausfallwahrscheinlichkeit wird durch Addition der Wahrscheinlichkeit gefährlicher Ausfälle von K4 ermittelt und beträgt $1{,}34 \cdot 10^{-6}$/Stunde. Dies entspricht dann ebenfalls PL c.

- Die verschleißbehafteten Elemente K3 und Q1 sollten nach jeweils ca. fünf Jahren (T_{10d}) ausgetauscht werden.

Weiterführende Literatur

- *Apfeld, R.; Zilligen, H.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003
  www.dguv.de/bgia, Webcode d6428

- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

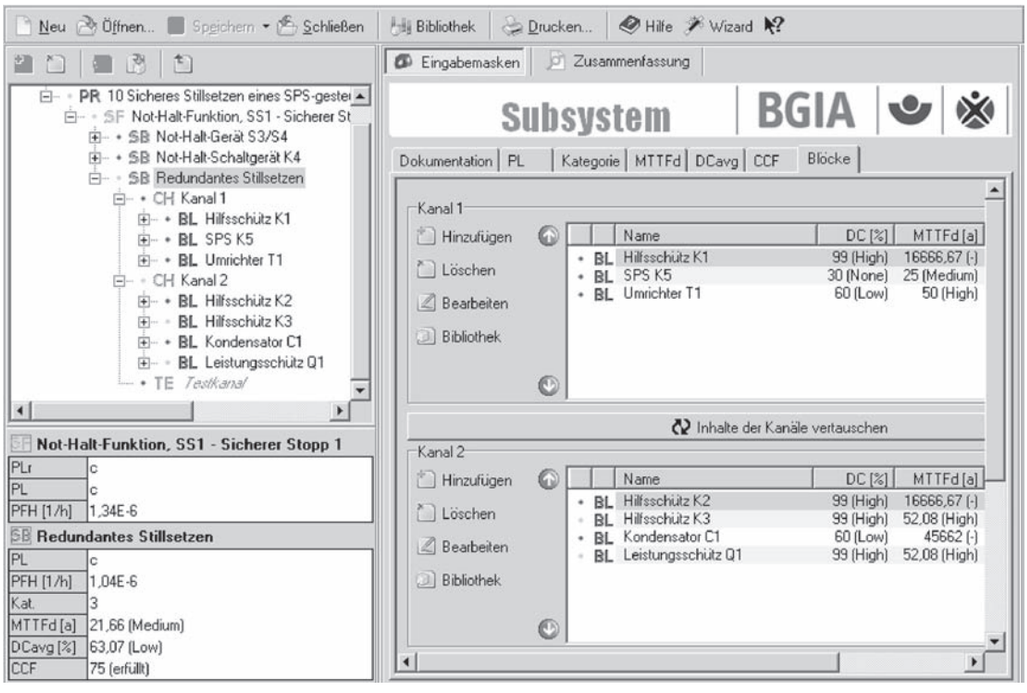


Abbildung 8.19: PL-Bestimmung mithilfe von SISTEMA

8.2.11 Getestetes pneumatisches Ventil (Subsystem) – Kategorie 2 – PL d (für PL-c-Sicherheitsfunktionen) (Beispiel 11)

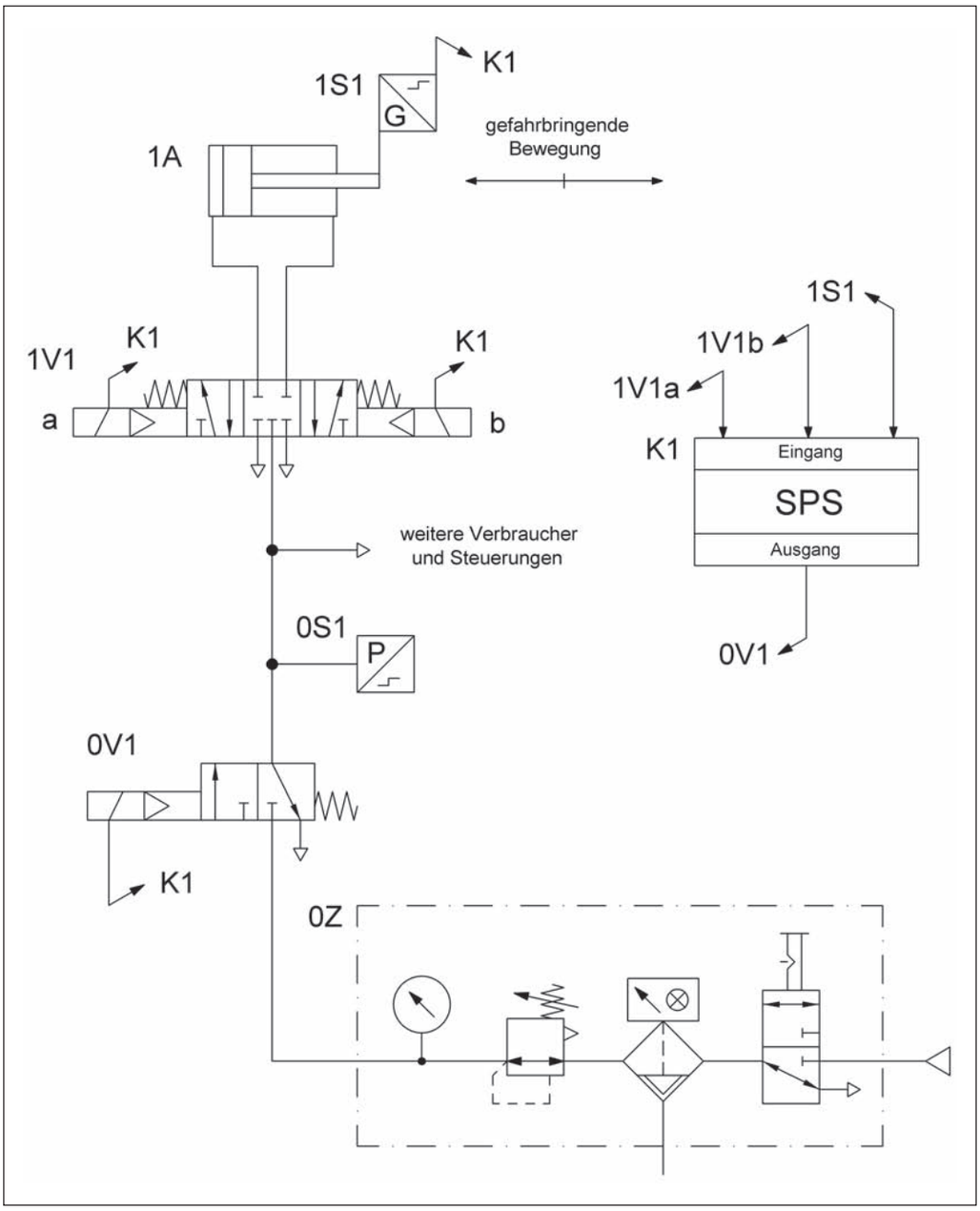
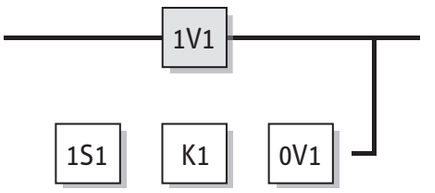


Abbildung 8.20: Pneumatisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- 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 Schutzfunktion. 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).
- 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, nämlich „Testung sehr viel häufiger als Anforderung der Sicherheitsfunktion“ (vgl. Anhang G), erfüllt werden.
- 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 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 $7{,}62 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile (Subsysteme) zur Vervollständigung der Sicherheitsfunktion wird sich in der Regel PL c für die komplette Sicherheitsfunktion ergeben.

- Das verschleißbehaftete Element 1V1 sollte nach jeweils ca. sieben Jahren (T_{10d}) ausgetauscht werden.

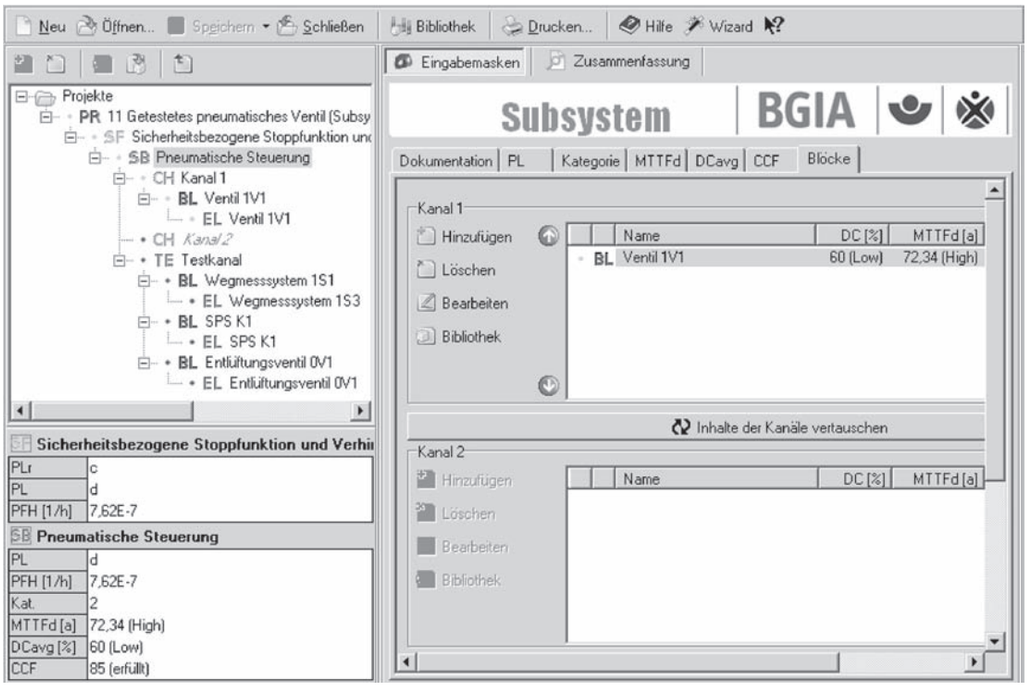


Abbildung 8.21: PL-Bestimmung mithilfe von SISTEMA

8.2.12 Getestetes hydraulisches Ventil (Subsystem) – Kategorie 2 – PL d (für PL-c-Sicherheitsfunktionen) (Beispiel 12)

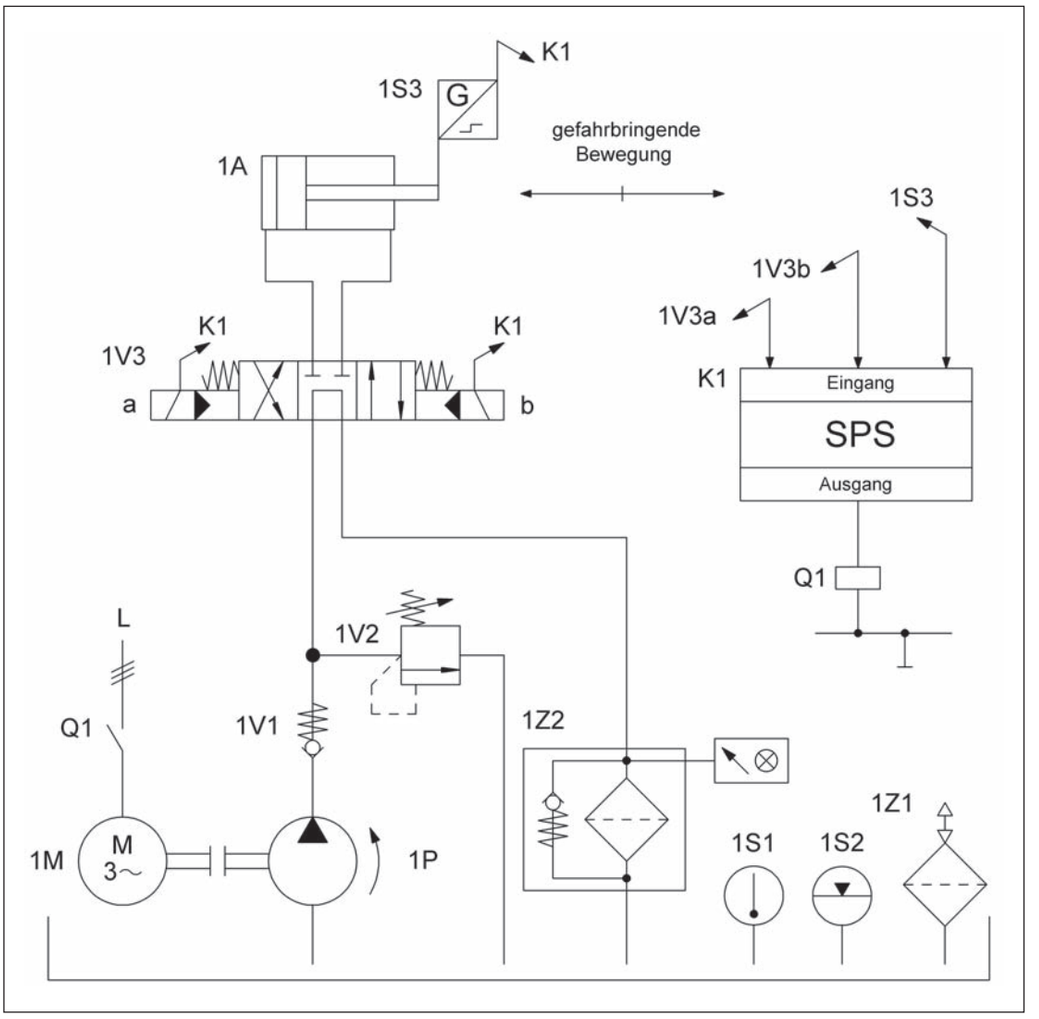


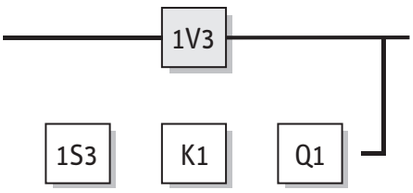
Abbildung 8.22: Hydraulisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des ungewollten 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 Schutzfunktion. 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).

- 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, nämlich „Testung sehr viel häufiger als Anforderung der Sicherheitsfunktion“ (vgl. Anhang G), erfüllt werden.

- 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 [N]. 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 150 Jahren [G] 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 2 000 000 Zyklen [N]. Bei täglichem Einschalten an 240 Arbeitstagen ergibt sich ein $MTTF_d$-Wert für Q1 von 83 333 Jahren. Damit beträgt die $MTTF_d$ des Testkanals 37,5 Jahre. Die $MTTF_d$ des Funktionskanals muss deshalb nach dem zugrunde liegenden Berechungsmodel auf 75,0 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 $MTTF_d$ (75,0 Jahre) und niedrigem DC_{avg} (60 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}31 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile (Subsysteme) zur Vervollständigung der Sicherheitsfunktion wird sich in der Regel PL c für die komplette Sicherheitsfunktion ergeben.

8.2.13 Unterlast-Erkennung für Leuchtenhänger – Kategorie 2 – PL d (Beispiel 13)

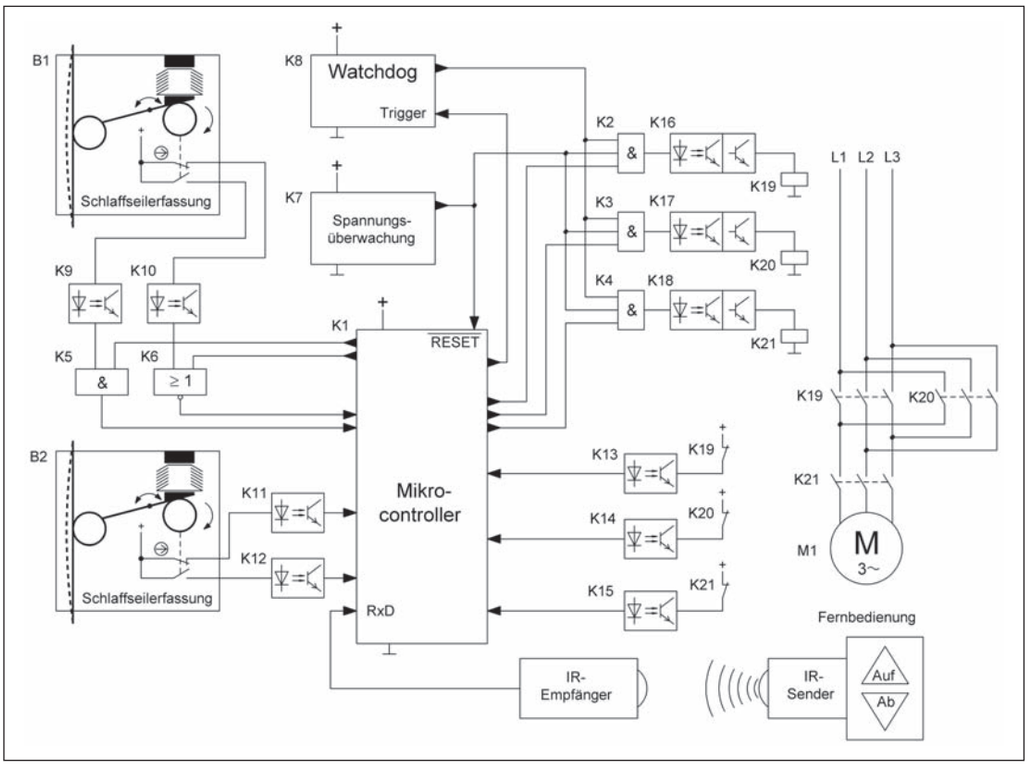


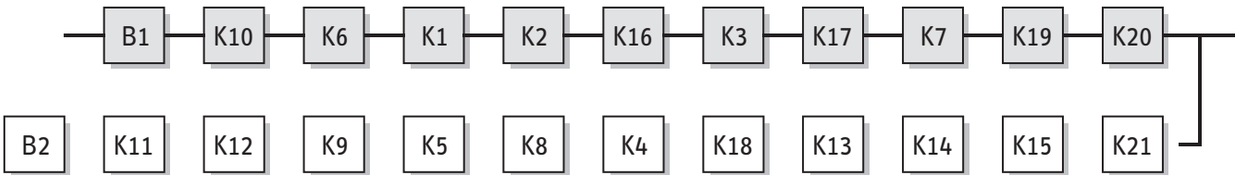
Abbildung 8.23: Kombinierte elektromechanische und programmierbare elektronische Steuerung zur Verhinderung der Unterlast von Leuchtenhängern

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 im Gefahrenbereich 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 bemerkt Fehler in der 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

- Der Entwurf zu DIN 15560-46 fordert in Abschnitt 5.1.2 mindestens 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 ungewollte Bewegungen des Leuchtenhängers (unerwarteter Anlauf) 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 15560-46, Abschnitt B.1.1.3.3, 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 8.23 Bauteile zu Blöcken zusammengefasst. K9 bis K15 beinhalten je einen Optokoppler und zwei Widerstände. K16 bis K18 beinhalten 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, K7
  O: K19, K20
  TE: B2, K11, K12, K9, K5, K8, K4, K18, K13, K14, K15
  OTE: K21

- $MTTF_d$: Die für die Berechnung benötigten $MTTF_d$-Werte stammen 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 1 141 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, 38 051 Jahre für die Spannungsüberwachung K7 und 45 662 Jahre für Transistoren bzw. 228 310 Jahre für Widerstände. Durch Aufsummierung der Ausfallraten aller Bauteile des funktionalen Kanals (Blöcke I, L und O) ergibt sich eine $MTTF_d$ von 288 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 393 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 K7 ist DC = 0 %. Die Mittelungsformel für DC_{avg} ergibt 85 % („niedrig“).

- 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 $MTTF_d$ pro Kanal (100 Jahre) und niedrigem DC_{avg} (85 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}72 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN 15560-46: Scheinwerfer für Film, Fernsehen, Bühne und Fotografie – Teil 46: Bewegliche Leuchtenhänger; Sicherheitstechnische Anforderungen und Prüfung (Normentwurf) (06.07). Beuth, Berlin 2007

- Sicherheit bei Produktionen und Veranstaltungen – Leitfaden BGI 810. Hrsg.: Verwaltungs-Berufsgenossenschaft, Hamburg 2006, http://www.vbg.de/imperia/md/content/produkte/broschueren/bgi_810_.pdf

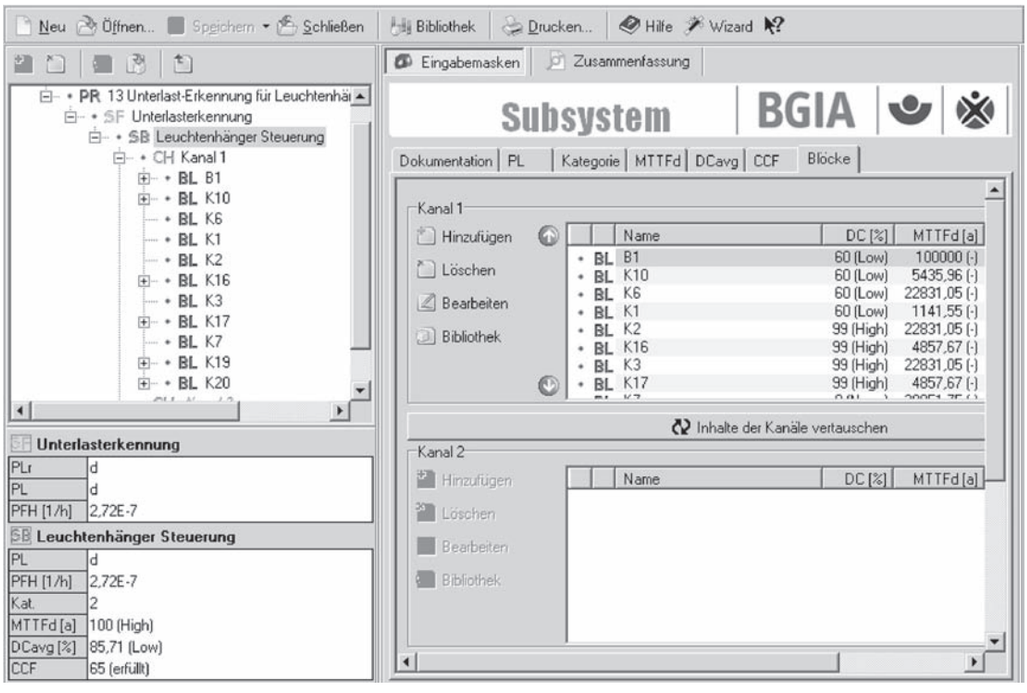


Abbildung 8.24: PL-Bestimmung mithilfe von SISTEMA

8.2.14 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 3 – PL d (Beispiel 14)

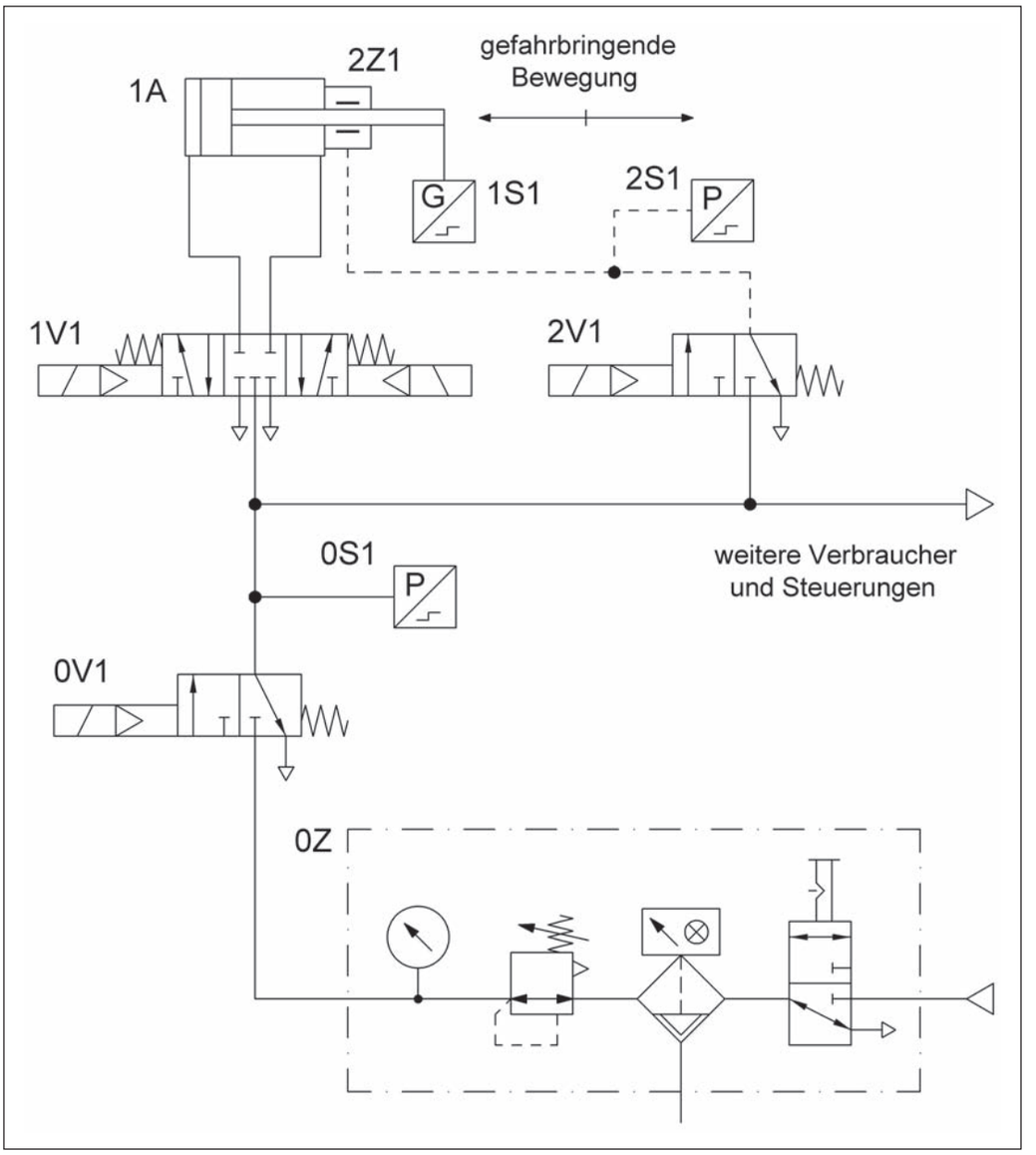


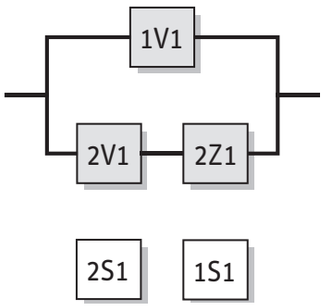
Abbildung 8.25: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- 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 Ventil 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 8 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.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für die Wegeventile 1V1 und 2V1 werden B_{10d}-Werte von 40 000 000 Zyklen [G] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr. Für 1V1 und 2V1 ergibt sich damit eine $MTTF_d$ = 289 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 $MTTF_d$ = 36 Jahre. Insgesamt ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 71 Jahren („hoch“).

- DC_{avg}: DC = 99 % für das Ventil 2V1 ergibt sich aus der Drucküberwachung des Steuersignals für die Bremse. DC = 60 % für das Ventil 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 75 % („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 (71 Jahre) und niedrigem DC_{avg} (75 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}21 \cdot 10^{-7}$/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. drei Jahren (T_{10d}) ausgetauscht werden.

8.2.15 Schutzeinrichtung und SPS-gesteuerte Hydraulik – Kategorie 3 – PL d (Beispiel 15)

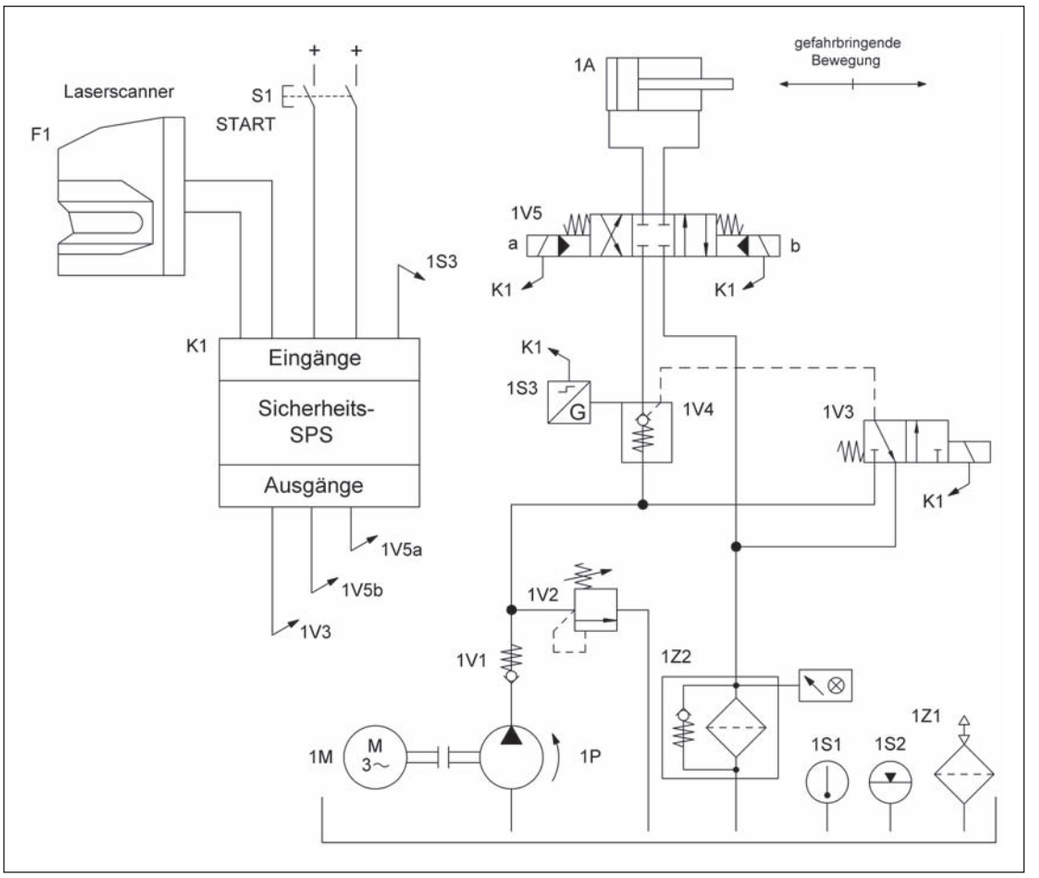


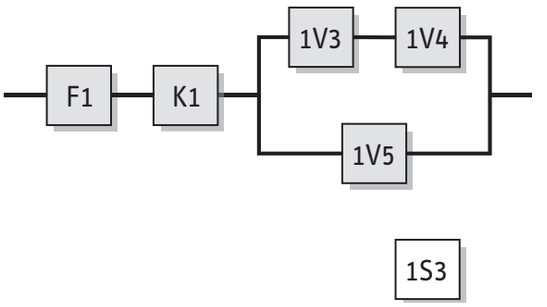
Abbildung 8.26: Schutzfeld-Überwachung durch Laserscanner mit elektrohydraulischer Abschaltung der gefahrbringenden Bewegung

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 den Bediener 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 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 angesteuert, 1V3 und 1V4 schließen nur bei einer Verletzung des Schutzfeldes.
- 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: $3{,}0 \cdot 10^{-7}$/Stunde [G], K1: $1{,}5 \cdot 10^{-7}$/Stunde [G]). Für den hydraulischen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_d$: Für die Ventile 1V3 bis 1V5 werden Werte von 150 Jahren [N] angenommen. Damit ergibt sich insgesamt ein symmetrisierter $MTTF_d$-Wert pro Kanal von 88 Jahren („hoch“).
- 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 $(3{,}0 + 1{,}5 + 0{,}62) \cdot 10^{-7} = 5{,}12 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- *Bömer, T.:* Hinweise zum praktischen Einsatz von Laserscannern. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 310 243. 36. Lfg. XII/99. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/310243

8.2.16 Erdbaumaschinensteuerung mit Bussystem – Kategorie 3 – PL d (Beispiel 16)

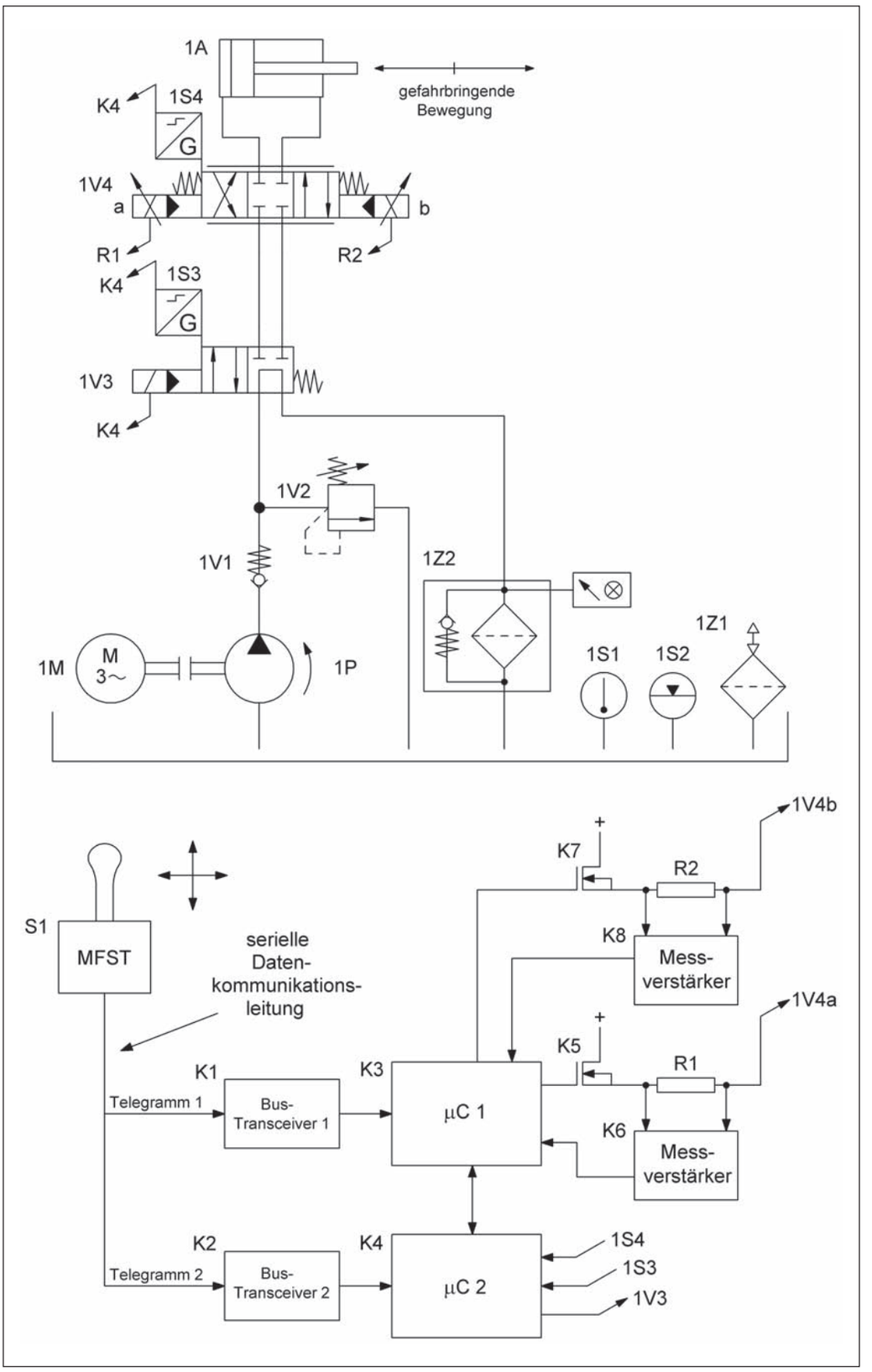
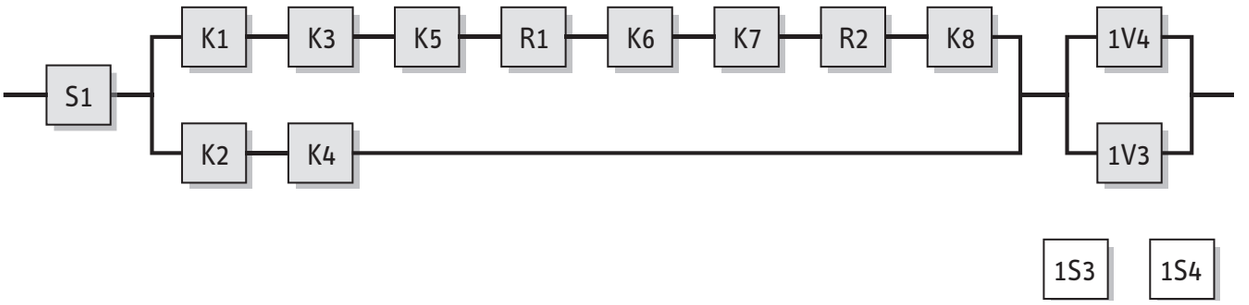


Abbildung 8.27: Ansteuerung von gefahrbringenden Bewegungen einer Erdbaumaschine



Sicherheitsfunktion

- Verhinderung des unerwarteten Anlaufs: Vermeidung unerwarteter Bewegungen der Arbeitsgeräte von Erdbaumaschinen

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 vom Bediener 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 prüft die korrekte Auslenkung des Proportionalventils 1V4 über das in 1V4 integrierte Weg-Messsystem 1S4 auf Plausibilität gegen die aus Telegramm 2 ermittelte Sollstellung. Bei erkannten Fehlern schaltet K4 übergeordnet über ein 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.

- 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 beinhaltet redundante Telegramme und Maßnahmen, um folgende Übertragungsfehler zu erkennen: Wiederholung, Verlust, Einfügung, falsche Abfolge, Verfälschung und Verzögerung (siehe auch Abschnitt 6.2.17). 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. Dieser geringe Anteil ist in der Berechnung der Gesamtausfallwahrscheinlichkeit 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 Berechung addiert ($PFH_{MFST} = 3{,}0 \cdot 10^{-7}$/Stunde [G]). Für den übrigen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.

- $MTTF_d$ der Logiksteuerung: Für die Bus-Transceiver K1 und K2 wird eine $MTTF_d$ von 11 415 Jahren [D] angesetzt. Für die Mikrocontroller K3 und K4 einschließlich ihrer Peripherie wird nach SN 29500-2 eine $MTTF_d$ von 878 Jahren [D] berücksichtigt. Für die restlichen Bauteile werden folgende Kenndaten angesetzt [D]: 45 662 Jahre für die Schalttransistoren K5 und K7, 228 310 Jahre für die Widerstände R1 und R2 und 1 141 Jahre für die Messverstärker K6 und K8. Die $MTTF_d$ der Kanäle beträgt damit 329 Jahre und 815 Jahre. Nach Kürzen auf 100 Jahre ergibt dies einen symmetrisierten $MTTF_d$-Wert von 100 Jahren.

- DC_{avg} der Logiksteuerung: DC = 99 % für K1 und K2 durch Kreuzvergleich der Telegramme in den Mikrokontrollern K3 und K4; DC = 60 % für K3 und K4 durch Kreuzvergleich und Selbsttests einfacher Wirksamkeit durch Software; DC = 90 % für die restlichen Bauteile durch Fehlererkennung in K4 mittels Weg-Messsystem 1S4. Die Mittelungsformel für DC_{avg} ergibt 74 % („niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10)

- Die Logiksteuerung entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und niedrigem DC_{avg} (74 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}36 \cdot 10^{-8}$/Stunde.

- $MTTF_d$ des hydraulischen Teils der Steuerung: Für das Proportionalventil 1V4 und das Wegeventil 1V3 wird eine $MTTF_d$ von 150 Jahren [N] angesetzt. Nach Kürzen ergibt dies einen symmetrisierten $MTTF_d$-Wert von 100 Jahren.

- DC_{avg} des hydraulischen Teils der Steuerung: DC = 99 % für 1V4 und 1V3 durch direkte Überwachung der Stellung über 1S4 bzw. 1S3 in K4. Die Mittelungsformel für DC_{avg} ergibt 99 % („hoch“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), Verwendung bewährter Bauteile (5), Schutz gegen Überdruck (15) und Umgebungsbedingungen (25 + 10).

- Der hydraulische Teil der Steuerung entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde.

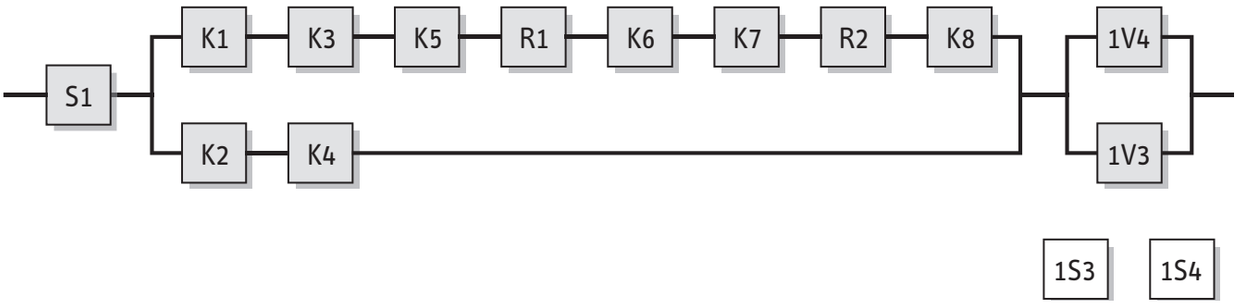
- Die mittlere Wahrscheinlichkeit gefährlicher Ausfälle der Sicherheitsfunktion ergibt sich durch Addition der Anteile des MFST, der Logiksteuerung und des hydraulischen Teils. Die Summe beträgt $3{,}98 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- ISO 15998: Earth-moving machinery – Machine control systems (MCS) using electronic components – Performance criteria and tests (Normentwurf) (11.03). Beuth, Berlin 2003

- DIN EN 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2007) (11.08). Beuth, Berlin 2008

- Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Hrsg.: Fachausschuss Elektrotechnik, Köln 2002
  www.dguv.de, Webcode d14884



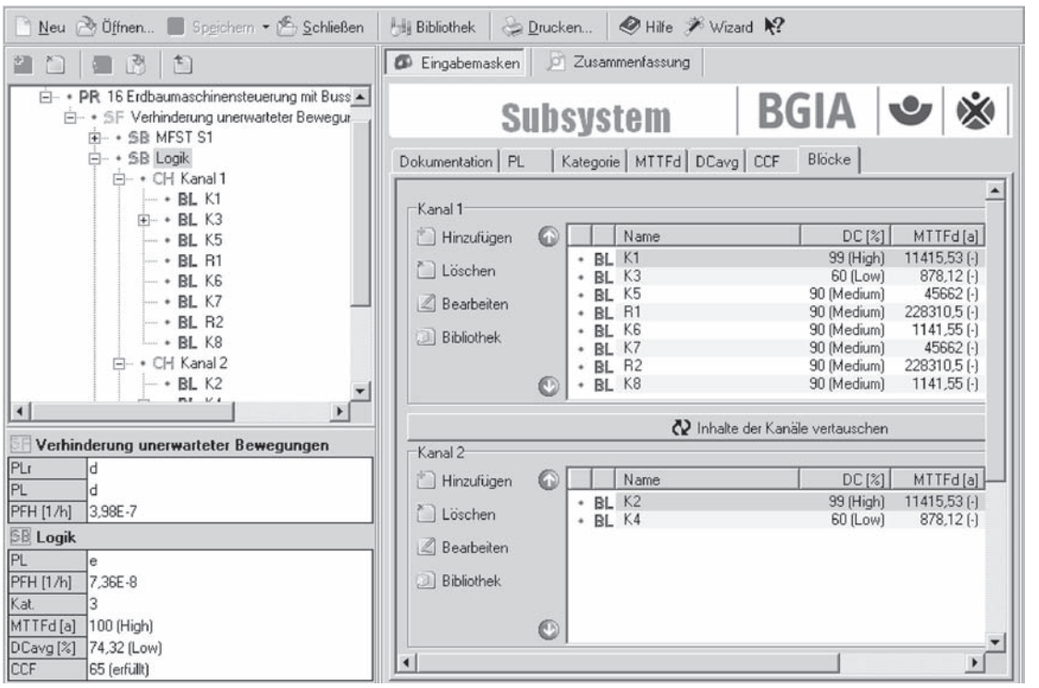


Abbildung 8.28: PL-Bestimmung mithilfe von SISTEMA

8.2.17 Kaskadierung von Schutzeinrichtungen mittels Sicherheitsbausteinen – Kategorie 3 – PL d (Beispiel 17)

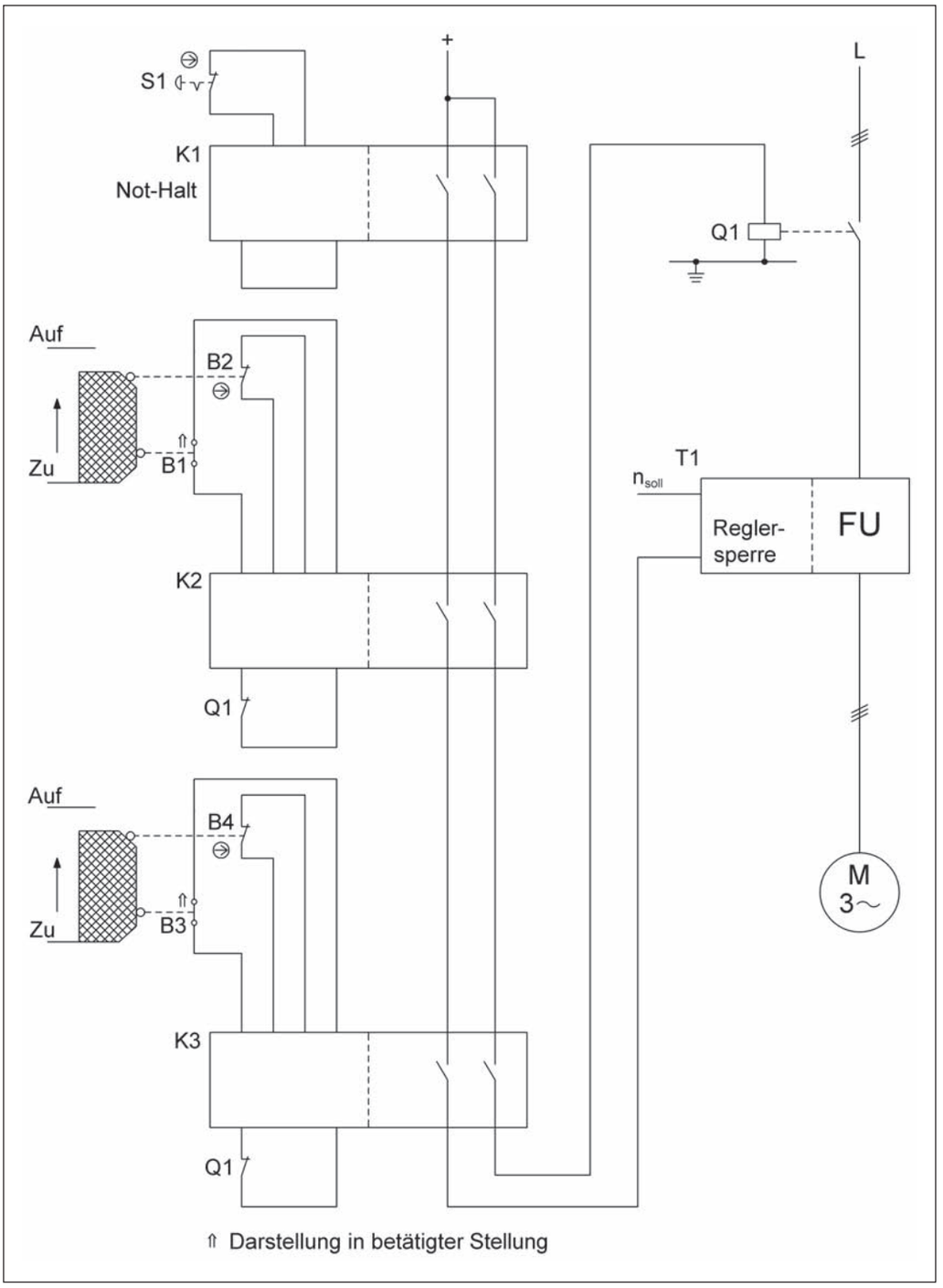
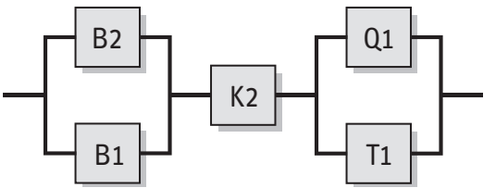


Abbildung 8.29: Kaskadierung von Schutzeinrichtungen mittels Sicherheitsbausteinen (Not-Halt-Funktion, STO)



Sicherheitsfunktionen

- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Geräts S1 über den Sicherheitsbaustein 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 eines Schutzgitters wird durch zwei Positionsschalter B1/B2 in Öffner-Schließer-Kombination erfasst und in einem zentralen Sicherheitsbaustein K2 ausgewertet. Dieser kann in gleicher Weise wie K1 gefahrbringende Bewegungen oder Zustände unterbrechen bzw. verhindern. Die Überwachung des zweiten Schutzgitters erfolgt in der gleichen Weise mit den zwei Positionsschaltern B3/B4 und einem Sicherheitsbaustein 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. Beide Positionsschalter an einem Schutzgitter werden im zugehörigen Sicherheitsbaustein, der auch über interne Diagnosemaßnahmen verfügt, auf Plausibilität überwacht. Fehler im Schütz Q1 werden über zwangsgeführte Kontakte 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 werden durch den Prozess erkannt. Einige wenige Fehler werden von der Steuerung nicht erkannt.

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 entspricht DIN EN ISO 13850, B2 und B4 sind Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern B1 bis B4 sind getrennt oder geschützt verlegt.
- Das Schütz Q1 besitzt zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Sicherheitsbausteine K1, K2 und K3 erfüllen alle Anforderungen für Kategorie 4 und PL d.
- Der Frequenzumrichter T1 verfügt über keine integrierte Sicherheitsfunktion.

Bemerkungen

- Die Not-Halt-Funktion ist eine ergänzende Schutzmaßnahme nach DIN EN ISO 12100-2:2004.

Berechnung der Ausfallwahrscheinlichkeit

- Die Schaltung lässt sich in drei Sicherheitsfunktionen und jeweils drei Subsysteme aufteilen. Das sicherheitsbezogene Blockdiagramm zeigt die sicherheitsbezogene Stoppfunktion beispielhaft für eine Schutzeinrichtung, da zu einem Zeitpunkt immer nur eine Schutzeinrichtung geöffnet wird. Für die zweite Schutzeinrichtung gilt die gleiche Sicherheitsfunktion und eine identische Berechnung der Ausfallwahrscheinlichkeit. Bei der Not-Halt-Funktion treten das Not-Halt-Gerät S1 und der Sicherheitsbaustein K1 an die Stelle der ersten beiden Subsysteme. Die Ausfallwahrscheinlichkeit der fertigen Sicherheitsbausteine K1, K2 und K3 wird am Ende der Berechnung addiert ($2{,}31 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für die übrigen Subsysteme wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.

- Bei S1 handelt es sich um ein handelsübliches Not-Halt-Gerät nach DIN EN ISO 13850. Es erfolgt ein Fehlerausschluss für den zwangsöffnenden Kontakt und die Mechanik, sofern die in Tabelle D.2 dieses Reports angegebene Anzahl der Betätigungen nicht überschritten wird. Für n_{op} wird von drei Betätigungen im Jahr ausgegangen. Hinsichtlich der Gesamtschaltungen von Q1 und dem Frequenzumrichter wird dieser Wert bei der weiteren Berechnung für beide Sicherheitsfunktionen vernachlässigt.

- $MTTF_d$: Für den Positionsschalter B2 mit zwangsöffendem Kontakt ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt des Positionsschalters B1 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B2 und B1 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 35 040 Zyklen/Jahr und $MTTF_d$ beträgt 285 Jahre für B2 bzw. 142 Jahre für B1. 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 285 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“).

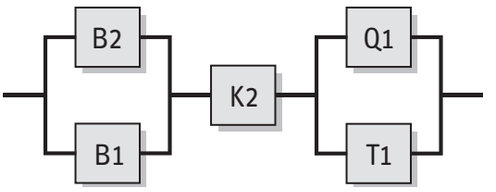
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in K2. Dies entspricht der DC_{avg} für das Subsystem. DC = 99 % für das Schütz Q1 ergibt sich aus der Rücklesung der Kontaktstellung in den Sicherheitsbausteinen. Für den Frequenzumrichter 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“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Subsystemen B2/B1 bzw. Q1/T2 (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)

- Das Subsystem B1/B2 entspricht Kategorie 3 mit hoher $MTTF_d$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Das Subsystem Q1/T1 entspricht Kategorie 3 mit hoher $MTTF_d$ (68 Jahre) und niedrigem DC_{avg} (62 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}73 \cdot 10^{-7}$/Stunde.

- Für die sicherheitsbezogene Stoppfunktion ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}00 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für Not-Halt-Funktion ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}75 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.



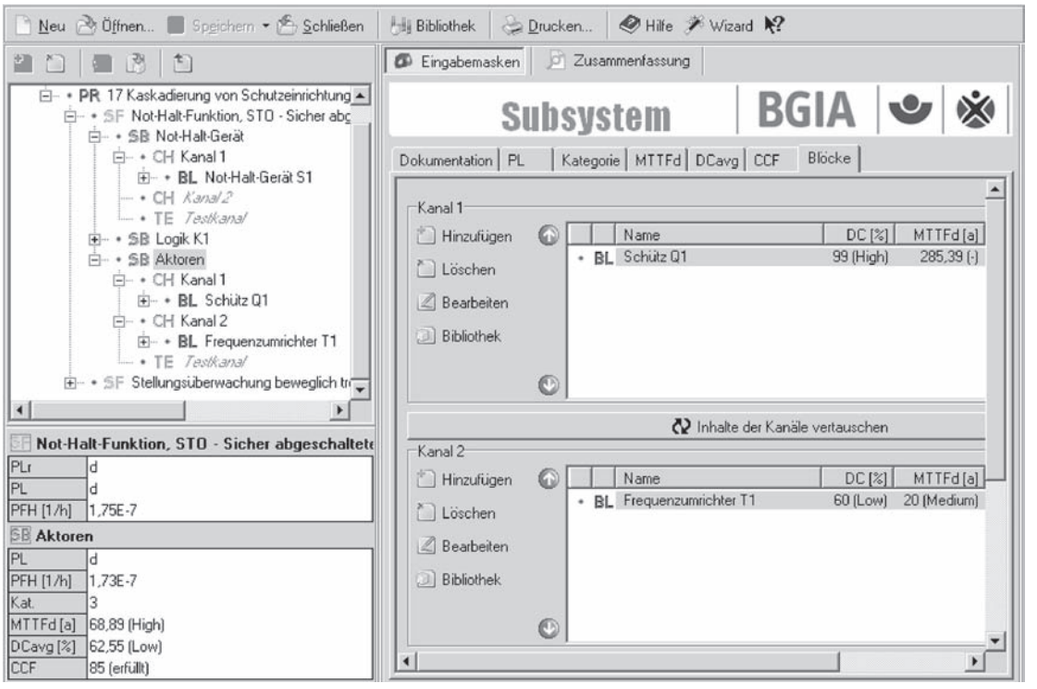


Abbildung 8.30: PL-Bestimmung mithilfe von SISTEMA

8.2.18 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen – Kategorie 3 – PL d (Beispiel 18)

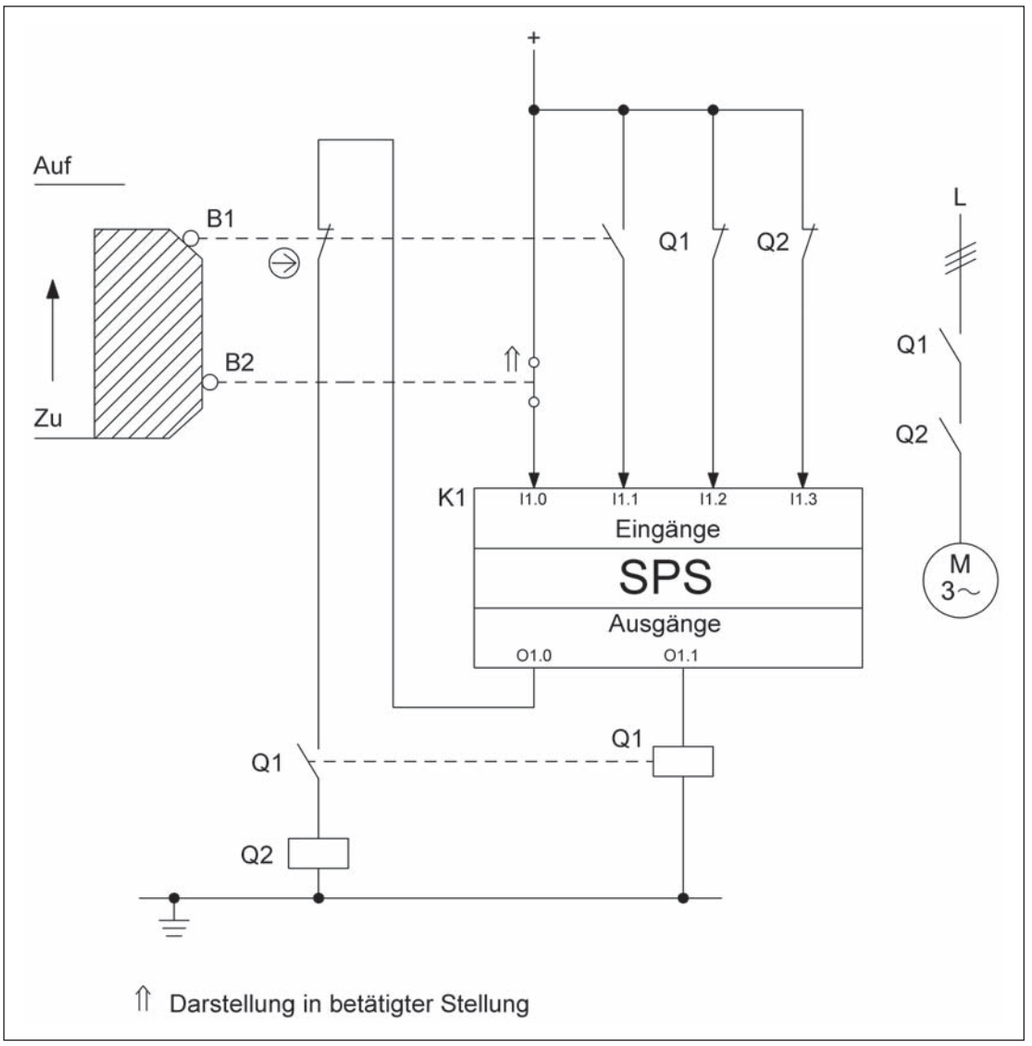


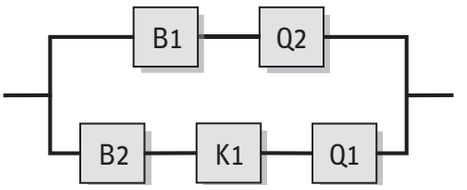
Abbildung 8.31: Redundante Stellungsüberwachung beweglicher trennender Schutzeinrichtung in diversitärer Technologie (elektromechanisch und programmierbar elektronisch)

Sicherheitsfunktion

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

Funktionsbeschreibung

- Das Öffnen der beweglichen 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 zwangsgeführte Rücklesekontakte 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 zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die programmierbare SPS K1 erfüllt die normativen Anforderungen gemäß Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für den Positionsschalter B1 ist ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt von Positionsschalter B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 1 Stunde Zykluszeit ist für diese Komponenten n_{op}= 5 840 Zyklen/Jahr und $MTTF_d$ beträgt 1 712 Jahre für B1 bzw. 856 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 $MTTF_d$ = 1 236 Jahre für den ersten Kanal, B2, K1 und Q2 tragen zur $MTTF_d$ = 28 Jahre im zweiten Kanal bei. Insgesamt ergibt sich über beide Kanäle ein symmetrisierter $MTTF_d$-Wert pro Kanal von 70 Jahren („hoch“).
- 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 zwangsgeführte Kontaktelemente 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 62 % („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} (62 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}66 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

8.2.19 Verriegelungseinrichtung mit Zuhaltung – Kategorie 3 – PL d (Beispiel 19)

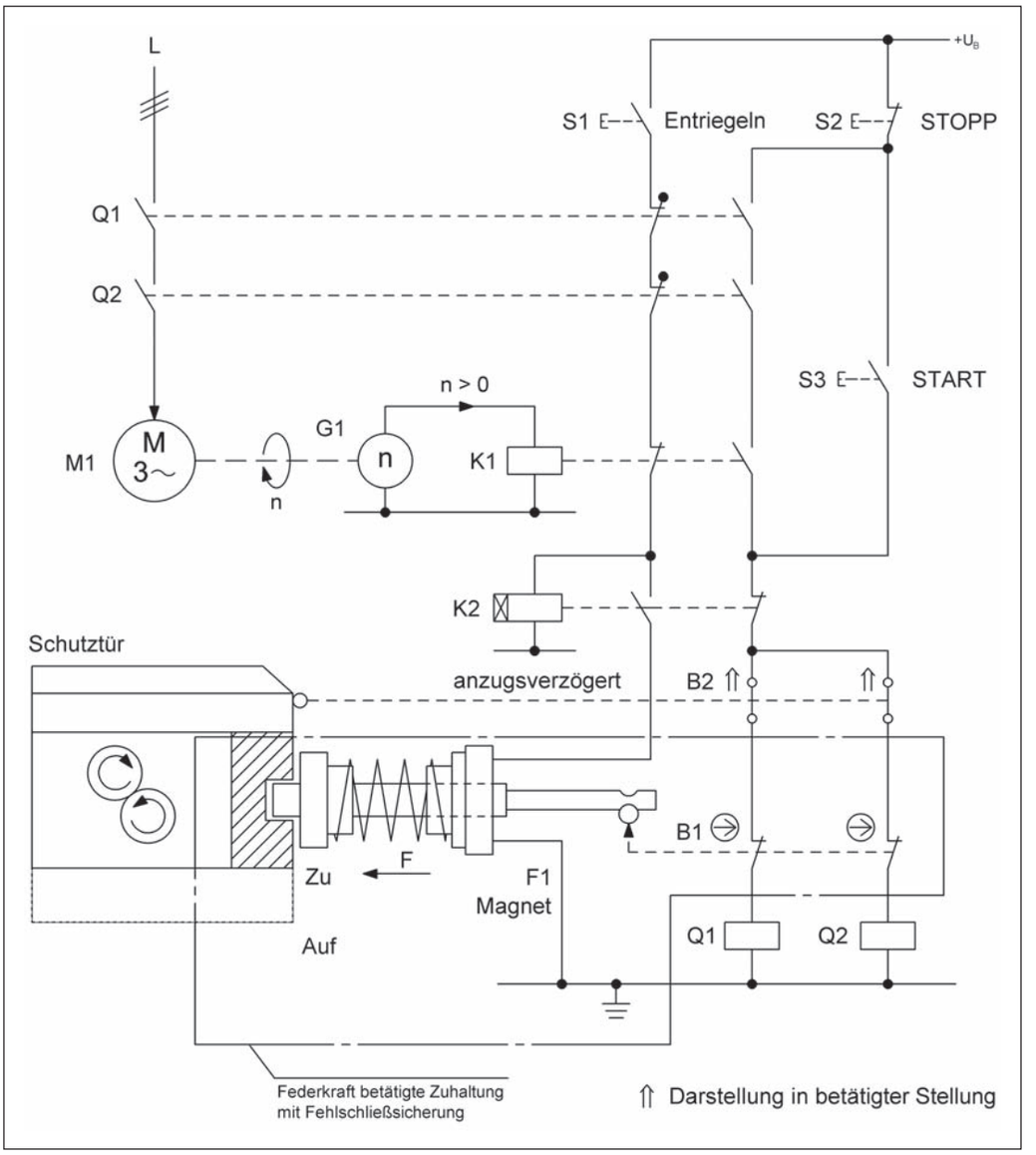


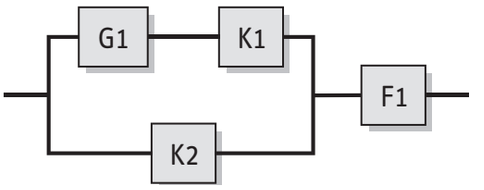
Abbildung 8.32: Zuhaltung einer Schutztür in kontaktbehafteter Technik – Kategorie 3

Sicherheitsfunktionen

- Kein Entriegeln der Zuhaltung bei Drehzahl größer Null
- Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür

Funktionsbeschreibung

- Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung solange versperrt, bis die Bewegung zum Stillstand gekommen ist. Das Schließen der Tür erfolgt durch formschlüssiges federkraftbetätigtes Einrücken eines Sperrbolzens, der zum Öffnen elektromagnetisch gezogen wird. Die Stellung des Sperrbolzens wird über den integrierten Positionsschalter B1 überwacht, die Stellung der Schutztür zusätzlich zur Erhöhung der Manipulationssicherheit über den Positionsschalter B2. Die Verriegelungseinrichtung mit integrierter federkraftbetätigter Zuhaltung besitzt zusätzlich eine Fehlschließsicherung.



- Die gefahrbringende Bewegung kann nur bei geschlossener Schutztür und per Federkraft eingerücktem Sperrbolzen über den Starttaster S3 in Gang gesetzt werden. Der Positionsschalter B1 ist dann entlastet, Positionsschalter B2 ist betätigt. Damit sind die Öffnerkontakte von B1 geschlossen, ebenso die Schließerkontakte von B2. Ihre Reihenschaltung gibt die Ansteuerung für die Motorschütze Q1 und Q2 frei. Das sicherheitsbezogene Blockdiagramm für die Sicherheitsfunktion „Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür“ (hier nicht dargestellt) besteht daher bei Vereinfachung zur sicheren Seite aus zwei redundanten Kanälen B1-Q1 und B2-Q2. Alternativ kann B1-Q2 und B2-Q1 gewählt werden. Ergeben sich aus diesen beiden Modellen unterschiedliche Werte der $MTTF_d$ pro Kanal, kann für die Bestimmung der Ausfallwahrscheinlichkeit der höhere $MTTF_d$-Wert verwendet werden.

- Das Öffnen der Schutztür während der gefahrbringenden Bewegung ist durch die Einbindung je eines Öffnerkontaktes (Spiegelkontaktes) der Schütze Q1, Q2 und des auf der Drehzahlinformation des Tachogenerators G1 basierenden Stillstandswächters K1 sowie des Schließerkontaktes des anzugsverzögerten Schützes K2 im Ansteuerkreis des Magneten F1 einfehlersicher verhindert.

- Ein Öffnen der Schutztür während des Austrudelns des Motors nach Betätigen des Stopptasters S2 und des Entriegelungstasters S1 ist durch die Einbindung des Öffnerkontaktes des Stillstandswächters K1 (basierend auf der Drehzahlinformation von G1) und des Schließerkontaktes des anzugsverzögerten Schützes K2 im Ansteuerkreis des Magneten F1 einfehlersicher verhindert (siehe sicherheitsbezogenes Blockdiagramm).

- Mit dem Betätigen der Entriegelungstaste S1 wird nach dem Stillstand des Motors (Q1, Q2 und K1 abgefallen) das anzugsverzögerte Schütz K2 angesteuert, der Magnet F1 aktiviert und damit der Sperrbolzen aus der Schutztür gezogen. Der Positionsschalter B1 verbleibt während der geöffneten Schutztür manipulationssicher formschlüssig zwangläufig betätigt. Ein unerwarteter Anlauf aus dem Stillstand wird auch über den Positionsschalter B2 (unbetätigt) verhindert.

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 Leitungen sind im elektrischen Einbauraum verlegt oder in getrennten Mantelleitungen ausgeführt.

- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.

- Die Schütze Q1 und Q2 besitzen Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F.

- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.

- Der Positionsschalter B1 ist ein zwangsöffnender Positionsschalter entsprechend DIN EN 60947-5-1, Anhang K.

- Die in der Schaltung vorgesehene Verriegelungseinrichtung (in Abbildung 8.32 gestrichelt dargestellt) enthält – in einem Gehäuse untergebracht und damit von außen nicht zugänglich – sowohl die Zuhaltung mit dem federrückgestellten Entriegelungsmagneten als auch den zur Stellungsüberwachung des Sperrbolzens und der Schutztür notwendigen Positionsschalter B1.

- Die Feder der Zuhaltung ist eine bewährte Feder nach DIN EN ISO 13849-2, Anhang A.3. Außerdem ist die Feder dauersicher nach DIN EN 13906-1. Die Kriterien nach GS-ET-19, Abschnitt 5.5.1, werden eingehalten. Der Magnet F1 zieht ohne Spannung nicht an, sodass bei gleichzeitigem Fehlerausschluss für die Fehlerannahme „Bruch des Sperrmittels“ für diese Elemente insgesamt ein Fehlerausschluss in Bezug auf gefahrbringende Fehler erfolgt.

- Die Fehlschließsicherung der Zuhaltung stellt konstruktiv sicher, dass der Sperrbolzen bei geöffneter Schutztür nicht die Sperrstellung (Zuhaltestellung) einnehmen kann.

- In Abbildung 8.32 sind nicht gezeichnet die in einer Zuhaltung zusätzlich integrierbaren Funktionen „Fluchtentriegelung“ und „Notentsperrung“ zum gewollten handbetätigten Öffnen der Schutzeinrichtung im Gefahrenfall – ohne Hilfsmittel und unabhängig vom Betriebszustand jeweils zwangläufig auf das Sperrmittel wirkend, siehe hierzu Prüfgrundsätze GS-ET-19.

- Die Standardkomponente G1 wird nach den Hinweisen in Abschnitt 6.3.10 eingesetzt.

Berechnung der Ausfallwahrscheinlichkeit

Zunächst wird die Wahrscheinlichkeit der ungewollten Aufhebung der Zuhaltung bzw. der Sicherheitsfunktion „Kein Entriegeln der Zuhaltung bei Drehzahl größer Null“ (siehe auch sicherheitsbezogenes Blockdiagramm) berechnet.

- $MTTF_d$: Für K1 und K2 gilt der B_{10d}-Wert von 400 000 Zyklen [N]. Bei 240 Arbeitstagen, 8 Arbeitsstunden und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 11 520 Zyklen/Jahr und $MTTF_d$ = 347 Jahre. Für den elektronischen Teil der Anzugsverzögerung in K2 wird eine $MTTF_d$ von 1 000 Jahren angenommen [G], sodass K2 insgesamt eine $MTTF_d$ von 257 Jahren besitzt. Für G1 liegt keine Herstellerangabe vor, es wird eine $MTTF_d$ von 30 Jahren angenommen [G]. Diese Werte ergeben eine symmetrisierte $MTTF_d$ pro Kanal von 70 Jahren.

- DC_{avg}: Fehlerhafte Zustände von K1 oder K2 führen aufgrund der Zwangsführung der Kontakte zu einem dauerhaften Ausfall der Entriegelung der Zuhaltung oder der Motorenergie, sodass eine Fehlererkennung durch den Prozess gegeben ist und ein *DC* von 99 % angenommen wird. Eine Drift der Schaltschwelle von G1 kann durch den Prozess erkannt werden, sodass ein *DC* von 60 % angenommen wird. Für den Ausfall der Anzugsverzögerung von K2 ist keine Fehlererkennung gegeben. Dies ergibt einen DC_{avg} von 57 %, der im Toleranzbereich von „niedrig“ liegt.

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15), Verwendung bewährter Bauteile (5) und Umgebungsbedingungen (25 + 10)

- Bei gleichzeitigem Fehlerausschluss für die weiteren Elemente der Zuhaltung (siehe oben) entspricht die Kombination der Steuerungselemente Kategorie 3 mit hoher $MTTF_d$ pro Kanal (70 Jahre) und niedrigem DC_{avg} (57 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}83 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Die Berechnung der Wahrscheinlichkeit für die Sicherheitsfunktion „Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür“ führt zu folgendem Ergebnis.

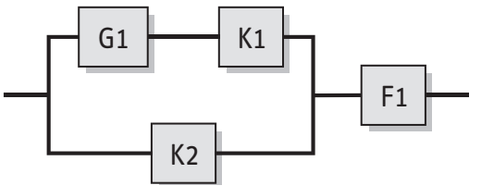
- $MTTF_d$: Für den Positionsschalter B1 wird aufgrund der Zwangsöffnung ein B_{10d}-Wert von 20 000 000 Zyklen [N] angenommen. Mit der oben angenommenen n_{op} = 11 520 Zyklen/Jahr beträgt der zugehörige $MTTF_d$-Wert 17 361 Jahre. Für den Positionsschalter B2 wird ein B_{10d}-Wert von 100 000 Zyklen [G] (siehe auch Tabelle D.2) angenommen, der zugehörige $MTTF_d$-Wert beträgt 86 Jahre. Für Q1 und Q2 gilt der B_{10d}-Wert von 400 000 Zyklen [N]. Mit der gleichen n_{op} ergibt sich jeweils eine $MTTF_d$ von 347 Jahren. Diese Werte ergeben eine symmetrisierte $MTTF_d$ pro Kanal von 85 Jahren.

- DC_{avg}: Fehlerhafte Zustände aller Elemente werden bei der angenommenen hohen Schalthäufigkeit jeweils mit einem *DC* von 99 % z.B. über Fehlererkennung durch den Prozess erkannt, was somit auch zu einem DC_{avg} von 99 % führt.

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): siehe oben

- Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (85 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}93 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Damit ist der PL_r = d übertroffen, was bei erforderlicher zweikanaliger Ausführung der Hardware mit wenigen Bauteilen, der Verwendung von B_{10d}-Werten nach Norm, einem *DC* von „hoch“ sowie einer „moderaten“ Schalthäufigkeit nahezu immer der Fall sein wird.

- Das verschleißbehaftete Element B2 sollte nach jeweils ca. 8 Jahren (T_{10d}) ausgetauscht werden.



Weiterführende Literatur

- *Reudenbach, R.:* Maßnahmen gegen das Umgehen von Verriegelungseinrichtungen an Schutztüren. die BG 2003 Nr. 7, S. 275-281
  www.diebg.info/download/reudenbach.pdf
- *Lüken, K., et al.*: Manipulation von Schutzeinrichtungen an Maschinen. HVBG-Report. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006
  www.dguv.de/bgia, Webcode d6303
- GS-ET-19: Grundsätze für die Prüfung und Zertifizierung von Verriegelungseinrichtungen mit elektromagnetischen Zuhaltungen (4/04)
  www.dguv.de, Webcode d14884
- BGI 575: Merkblatt für die Auswahl und Anbringung elektromechanischer Verriegelungseinrichtungen für Sicherheitsfunktionen. Carl Heymanns, Köln 2003
- DIN EN 1088: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (02.96). Beuth, Berlin 1996
- DIN EN 1088/A1: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (07.07). Beuth, Berlin 2007
- DIN EN 13906-1: Zylindrische Schraubenfedern aus runden Drähten und Stäben – Berechnung und Konstruktion – Teil 1: Druckfedern (07.02). Beuth, Berlin 2002

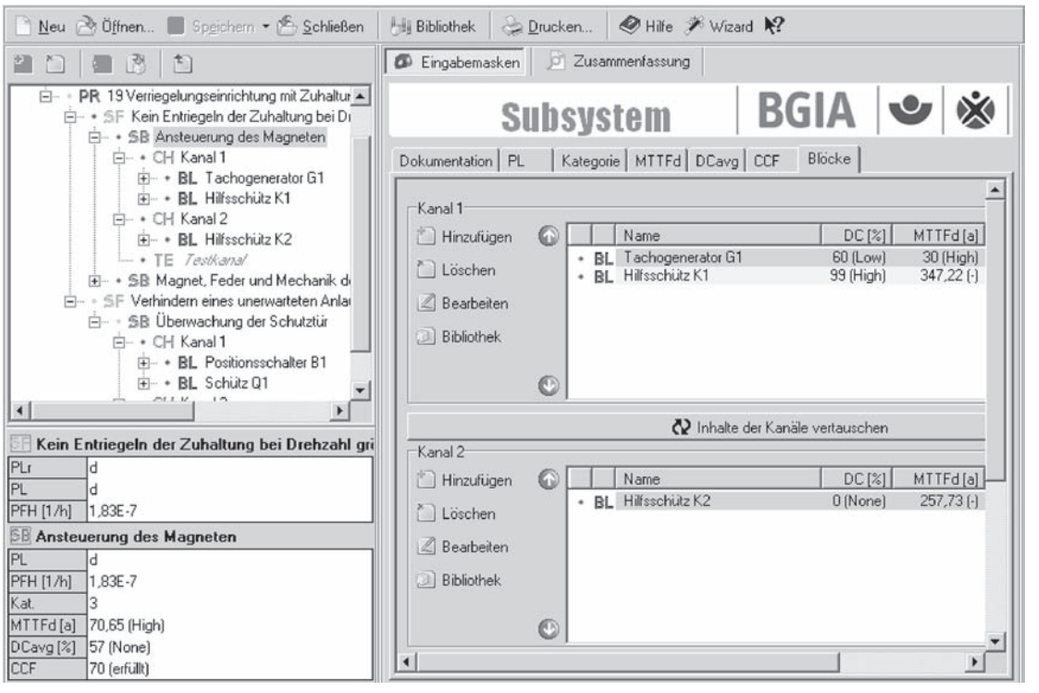


Abbildung 8.33: PL-Bestimmung mithilfe von SISTEMA

8.2.20 Sicheres Stillsetzen eines SPS-gesteuerten Antriebs – Kategorie 3 – PL d (Beispiel 20)

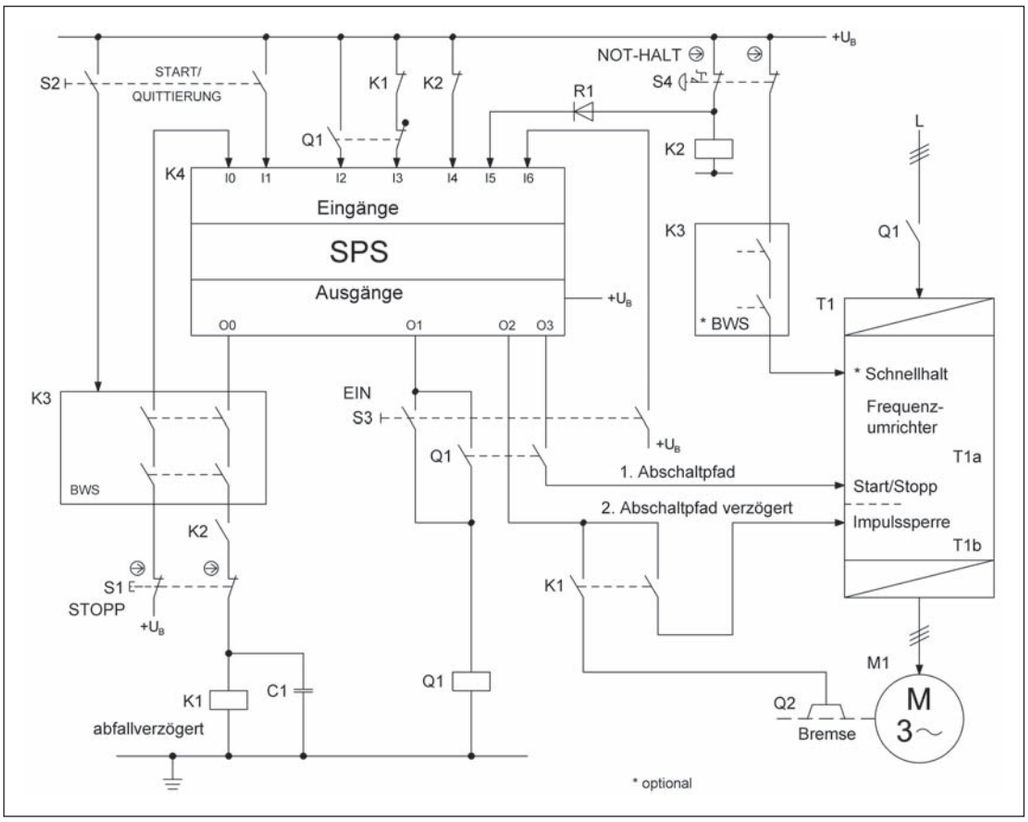


Abbildung 8.34: Sicheres Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung (hier: BWS)

Sicherheitsfunktion

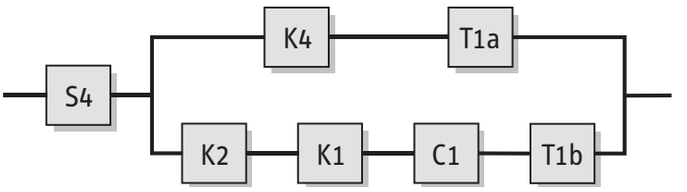
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung wird der Antrieb angehalten (SS1 – Sicherer Stopp 1).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird redundant unterbrochen, falls entweder die Stopp-Taste S1 oder die Schutzeinrichtung K3 (im Schaltbild als berührungslose 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“ (T1a) am Frequenzumrichter (FU) T1 die erste Bremszeitvorgabe realisiert. Redundant dazu wird als zweite Bremszeitvorgabe über das Entregen des Hilfsschützes K1 (abfallverzögert mithilfe des Kondensators C1) der Eingang „Impulssperre“ (T1b) an T1 deaktiviert und die Bremse Q2 fällt ein. 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 „Schnellhalt“ mit besonders kurzer Geschwindigkeitsabsteuerung am FU zur Verfügung, können Not-Halt-Gerät und 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 T1a/T1b, des abfallverzögerten Hilfsschützes K1 oder des Hilfsschützes K2 wird jeweils das Stillsetzen des Antriebes 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 Frequenzumrichters mit sicherer Impulssperre ist der Einsatz des Leistungsschützes Q1 zum Abschalten der Versorgungsspannung nicht unbedingt erforderlich. Der Frequenzumrichter muss zum Antreiben und Bremsen geeignet sein.
- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Kontakte der Taster S1 und S4 sind zwangsöffnend ausgeführt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Standardkomponenten K4 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.
- 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 von T1a (s.u.) und somit bei alleiniger Abschaltung über die Impulssperre 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 Karusselltürsteuerung (Beispiel 23, siehe Seite 156 ff.) beschrieben.
- Die BWS K3 erfüllt, z.B. als Lichtgitter, die Anforderungen für Typ 4 nach DIN EN 61496-1 und DIN CLC/TS 61496-2 sowie für PL e.

Berechnung der Ausfallwahrscheinlichkeit

- Es wird die Ausfallwahrscheinlichkeit des sicheren Stillsetzens ausgelöst durch das Not-Halt-Gerät S4 bzw. durch die BWS berechnet, die auch im sicherheitsbezogenen Blockdiagramm gezeigt wird. Die Funktion „Schnellhalt“ des FU und die Möglichkeit der Abschaltung der Spannungsversorgung des FU über Q1 werden bei der Berechnung der Ausfallwahrscheinlichkeit der Sicherheitsfunktion nicht berücksichtigt.
- Der Frequenzumrichter T1 wird in die Blöcke T1a und T1b zerlegt. Im Block T1a sind die Funktionen Start und Stopp sowie deren steuerungstechnische Umsetzung enthalten. Der Block T1b beinhaltet die mit einer geringen Anzahl von Bauteilen realisierte Impulssperre.

Sicheres Stillsetzen ausgelöst durch das Not-Halt-Gerät S4:

- Für das Not-Halt-Gerät wird ein Fehlerausschluss angenommen, da die in Tabelle D.2 genannte Betätigungsanzahl nicht überschritten wird.
- $MTTF_d$: Folgende $MTTF_d$-Werte werden geschätzt: 50 Jahre für K4, 100 Jahre für T1a und 1 000 Jahre für T1b [G]. Für K1 ergibt sich bei einem B_{10d}-Wert von 400 000 Zyklen [N] und 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* = 30 % für K4, auf *DC* = 90 % für T1a und auf *DC* = 60 % für T1b. *DC* = 99 % für K1 und *DC* = 60 % für C1 folgen durch Testung des Zeitglieds bei spannungsfreiem FU. Für K2 gilt *DC* = 99 % durch Plausibilitätstest in K4 mit dem Schaltzustand von S4. Die Mittelungsformel für DC_{avg} ergibt 56,9 % (im Toleranzbereich von „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} (57 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}76 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Sicheres Stillsetzen ausgelöst durch die BWS K3:

- Die BWS K3 liegt als geprüftes Sicherheitsbauteil vor. Ihre Ausfallwahrscheinlichkeit 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 beschrieben 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} = 56,8 % (im Toleranzbereich von „niedrig“). Für Kategorie 3 ergibt dies eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}77 \cdot 10^{-7}$/Stunde. Die Gesamtausfallwahrscheinlichkeit wird durch Addition ermittelt und ergibt $2{,}07 \cdot 10^{-7}$/Stunde. Dies entspricht ebenfalls PL d.

Weiterführende Literatur

- *Apfeld, R.; Zilligen, H.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003
  www.dguv.de/bgia, Webcode d6428

- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (01.05). Beuth, Berlin 2005

- DIN CLC/TS 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (02.08). Beuth, Berlin 2008

- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07). International Electrotechnical Commission (IEC), Genf 2007

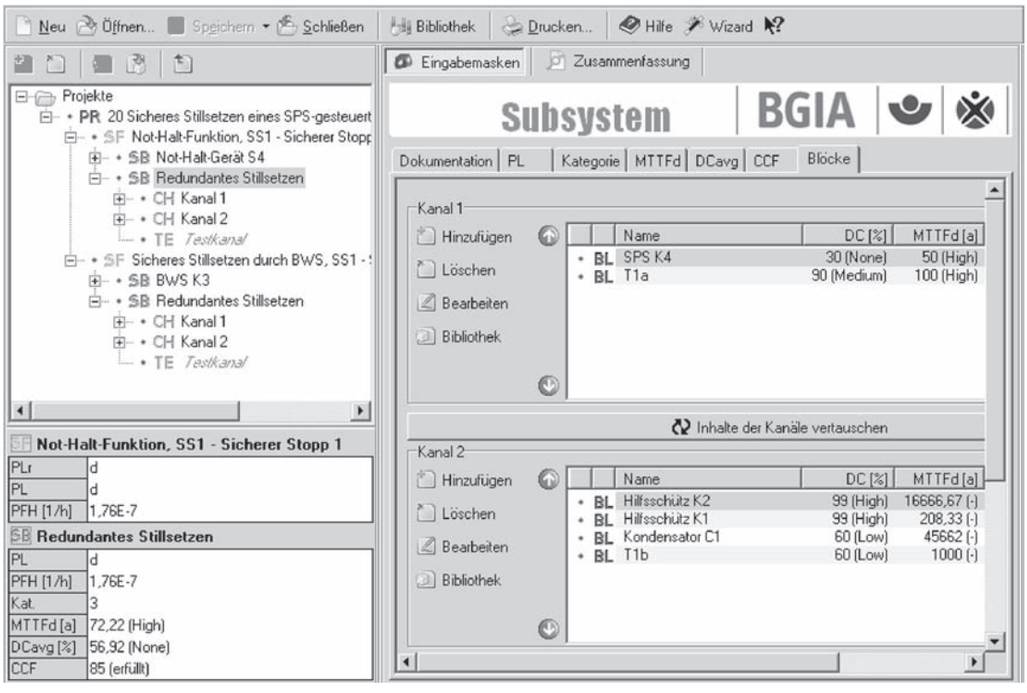


Abbildung 8.35:
PL-Bestimmung mithilfe von SISTEMA

8.2.21 Sicher begrenzte Geschwindigkeit für Tippbetrieb – Kategorie 3 – PL d (Beispiel 21)

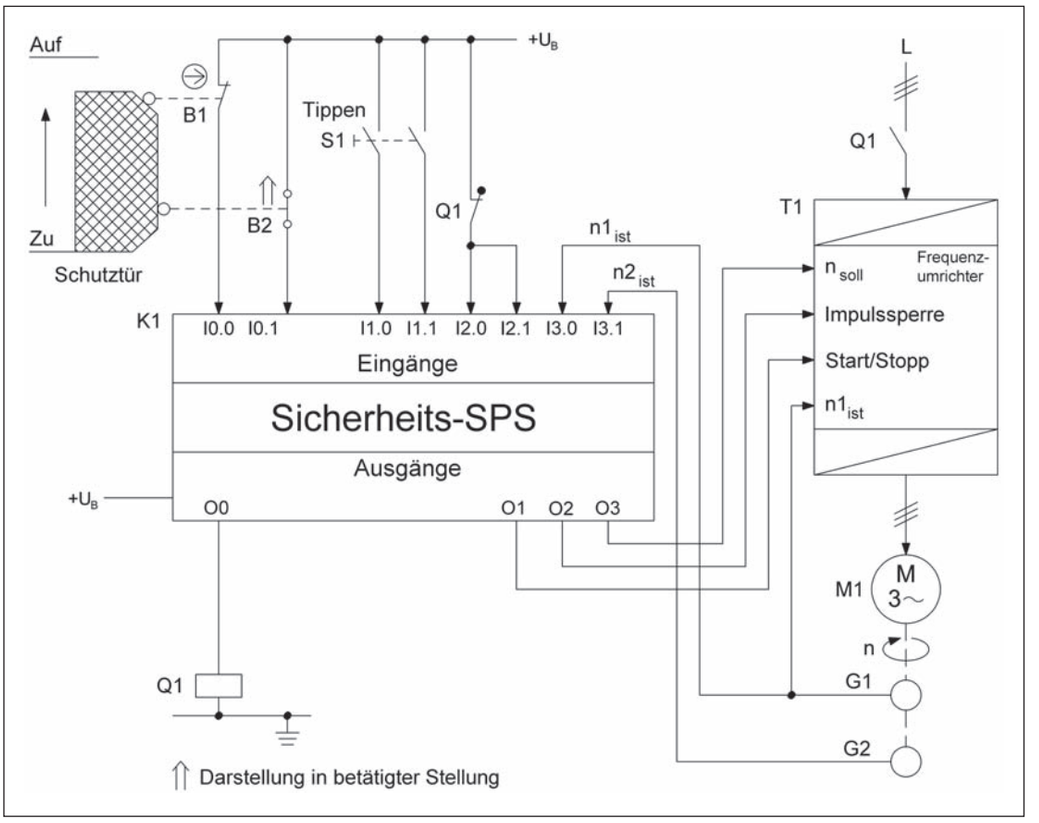


Abbildung 8.36: Tippbetrieb mit sicher begrenzter Geschwindigkeit bei geöffneter Schutztür, mit Soll-/Ist-Vergleich und Drehzahl-Grenzwertvorgabe innerhalb einer Sicherheits-SPS

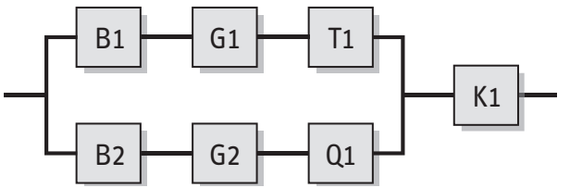
Sicherheitsfunktion

- Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür wird das Überschreiten einer zulässigen Drehzahl im Tipp-Betrieb verhindert.

Funktionsbeschreibung

- 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 sicher begrenzte Geschwindigkeit am Frequenzumrichter T1 eingestellt. Beide Verarbeitungskanäle innerhalb der SPS erhalten jeweils über ihre Anwendersoftware voneinander unabhängige Soll-Grenzwert-Vorgaben. Die Überwachung der Ist-Drehzahl der begrenzten Geschwindigkeit an den Eingängen I3.0 und I3.1 von K1 erfolgt über zwei separate Tachogeneratoren 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 Impulssperre am Umrichter einen Stillstand einleiten. Zusätzlich kann über ein Netzschütz Q1 die Energieversorgung zu T1 getrennt werden.

- Über eine intern in der Sicherheits-SPS K1 vorhandene Schnittstelle werden sicherheitsrelevante Daten ausgetauscht, z.B. zwecks Fehlererkennung durch Zustandsvergleich der beiden Verarbeitungskanäle. Versagt ein Verarbeitungskanal, so erfolgt die Abwärtssteuerung des Umrichters T1 sowie des Netzschützes Q1 jeweils durch den anderen noch funktionierenden Verarbeitungskanal. Ein Versagen des Umrichters, das z.B. zum unerwarteten Anlaufen, zum Weiterlaufen oder zu einer Erhöhung der Drehzahl führen kann, wird über die getrennte Erfassung der Drehzahlen durch die Tachogeneratoren 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 Impulssperre am Umrichter 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 gibt z.B. IEC 61800-5-2, Tabelle D.16.
- 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.
- Es wird davon ausgegangen, dass die Ausgänge der Sicherheits-SPS jeweils von beiden Verarbeitungskanälen der SPS angesteuert werden (Ausnahme O3).

Bemerkungen

- Nach DIN EN 1010-1 genügt bei Maschinen ohne betriebsmäßig regelmäßigen Eingriff in Gefahrstellen auch der Einsatz eines zwangsöffnenden Positionsschalters nach DIN EN 60947-5-1, Anhang K, je trennender verriegelter Schutzeinrichtung. Für den Fehlerausschluss in diesem Zusammenhang ist die Installation des Schalters nach DIN EN 60204-1 Bedingung.
- Für die vollständige Realisierung des Tippbetriebs ist zusätzlich die Sicherheitsfunktion „Kein unerwarteter Anlauf im Tippbetrieb“ zu betrachten.

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} = 1 920 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 104 116 Jahre. Für B2 wird aufgrund des definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) ein B_{10d}-Wert von 1 000 000 Zyklen [G] angenommen (siehe auch Tabelle D.2) und damit eine $MTTF_d$ = 5 208 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 Werte werden geschätzt: Für T1 $MTTF_d$ = 100 Jahre und für G1/G2 $MTTF_d$ = 50 Jahre [G]. Diese Werte ergeben eine symmetrisierte $MTTF_d$ pro Kanal von 41 Jahren („hoch“).

- DC_{avg}: Für die verwendeten Komponenten wird jeweils ein *DC* = 99 % angenommen. Dieser basiert für die Positionsschalter und die Tachogeneratoren auf einem Kreuzvergleich von Eingangssignalen in K1. Für den Umrichter T1 erfolgt 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 (41 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}56 \cdot 10^{-8}$/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 $2{,}16 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit programmierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Kennzahl 330 227. 27. Lfg. I/95. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/330227

- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebe mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

- DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Allgemeine Anforderungen (03.05). Beuth, Berlin 2005

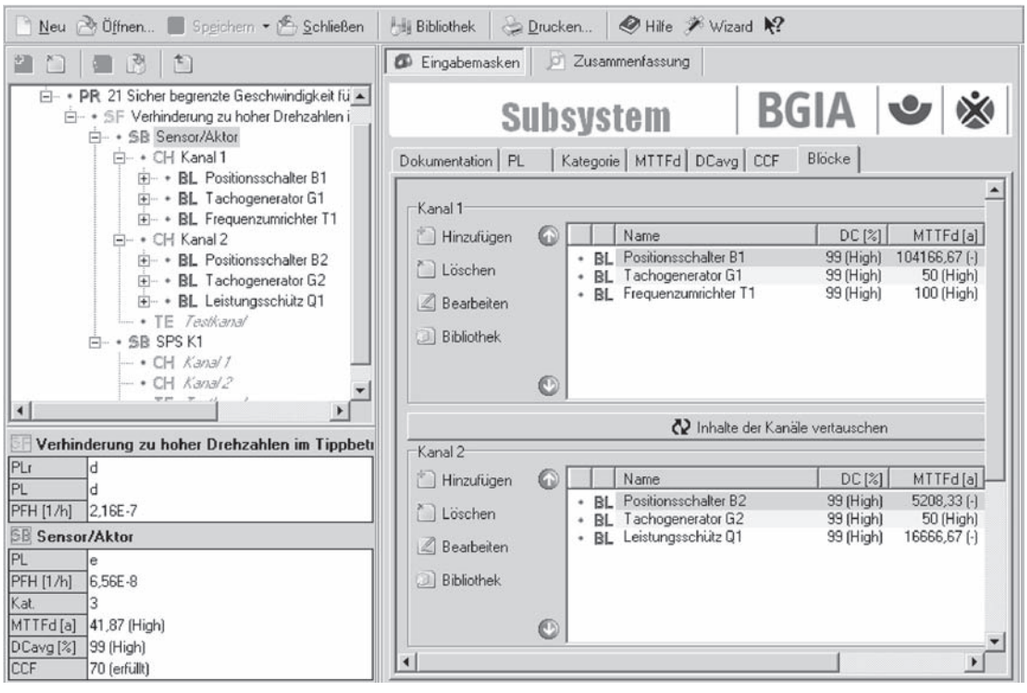


Abbildung 8.37: PL-Bestimmung mithilfe von SISTEMA

8.2.22 Muting einer Schutzeinrichtung – Kategorie 3 – PL d (Beispiel 22)

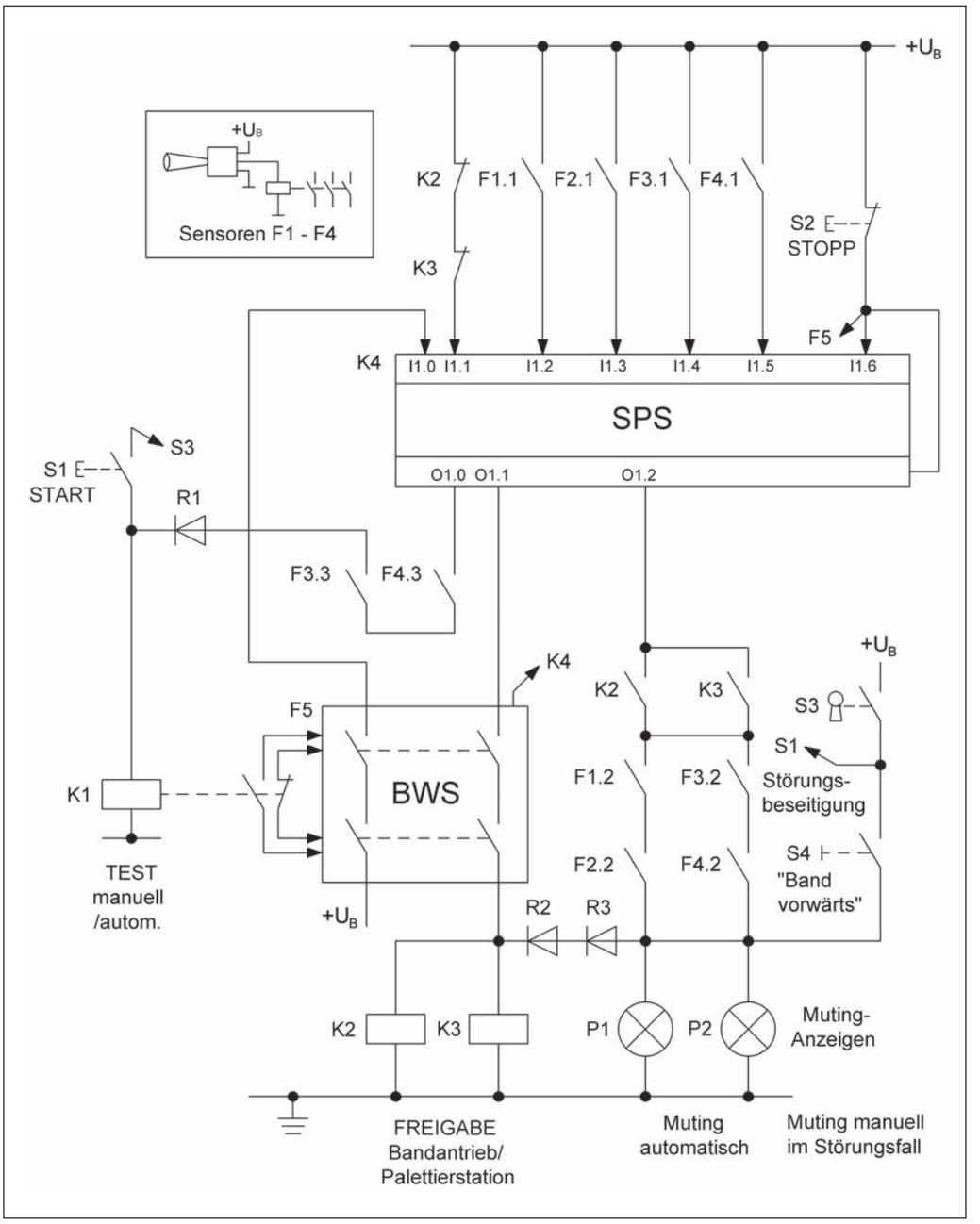
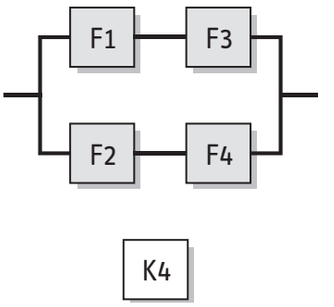


Abbildung 8.38: Überbrückung einer Schutzeinrichtung am Auslauf einer SPS-gesteuerten Palettieranlage

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 8.39) 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 ungewollten Muting (d.h. gefährlichem Ausfall der Mutingfunktion) führen.

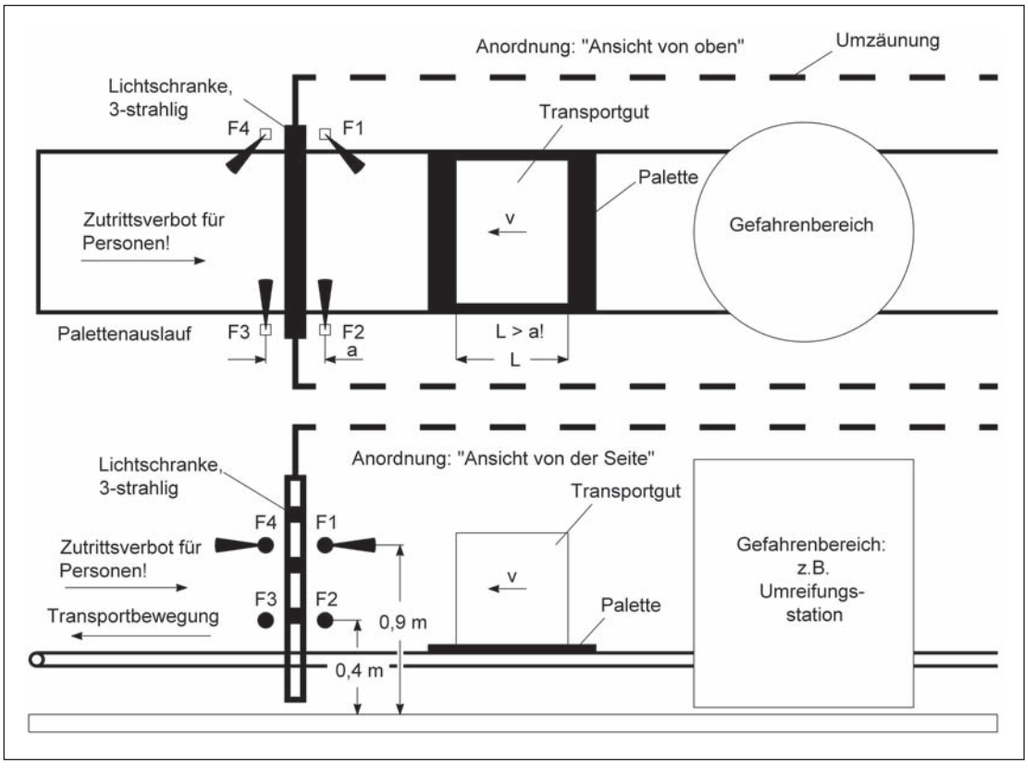


Abbildung 8.39: Automatisch gesteuerte Palettierstation – Prinzip der Absicherung des Palettenauslaufs mit Lichtschranke und Anordnung der Überbrückungssensoren F1 bis F4

- 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 Totmann-Tasters S4 kann eine Palette vom Bediener im Störfall aus dem Detektionsbereich der Lichtschranke und der Überbrückungssensoren herausgefahren werden.

  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 Schütze 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 den Benutzer.

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 Standardkomponenten F1 bis F4 werden, soweit zutreffend, entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.

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.

- 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 erforderlicher 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 [N]. Bei 300 Arbeitstagen, 16 Arbeitsstunden und 200 Sekunden Zykluszeit ist für diese Elemente n_{op} = 86 400 Zyklen/Jahr und $MTTF_d$ = 231 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 von $5{,}16 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- *Grigulewitsch, W.:* Speicherprogrammierbare Steuerung (SPS) zum zeitlich begrenzten, prozessabhängigen Aufheben einer Sicherheitsfunktion – Schaltungsbeispiel. Kennzahl 330 231. 36. Lfg. XII/99. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/330231

- *Kreutzkampf, F.; Hertel, W.:* Zeitbegrenztes Aufheben von Sicherheitsfunktionen. Kennzahl 330 214. 19. Lfg. X/92. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/330214

- 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 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (01.05). Beuth, Berlin 2005

- DIN CLC/TS 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (02.08). Beuth, Berlin 2008

- DIN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zum Erkennen von Personen (Normentwurf) (08.06). Beuth, Berlin 2006

- DIN EN 999: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (12.98). Beuth, Berlin 1998

8.2.23 Karusselltürsteuerung – Kategorie 3 – PL d (Beispiel 23)

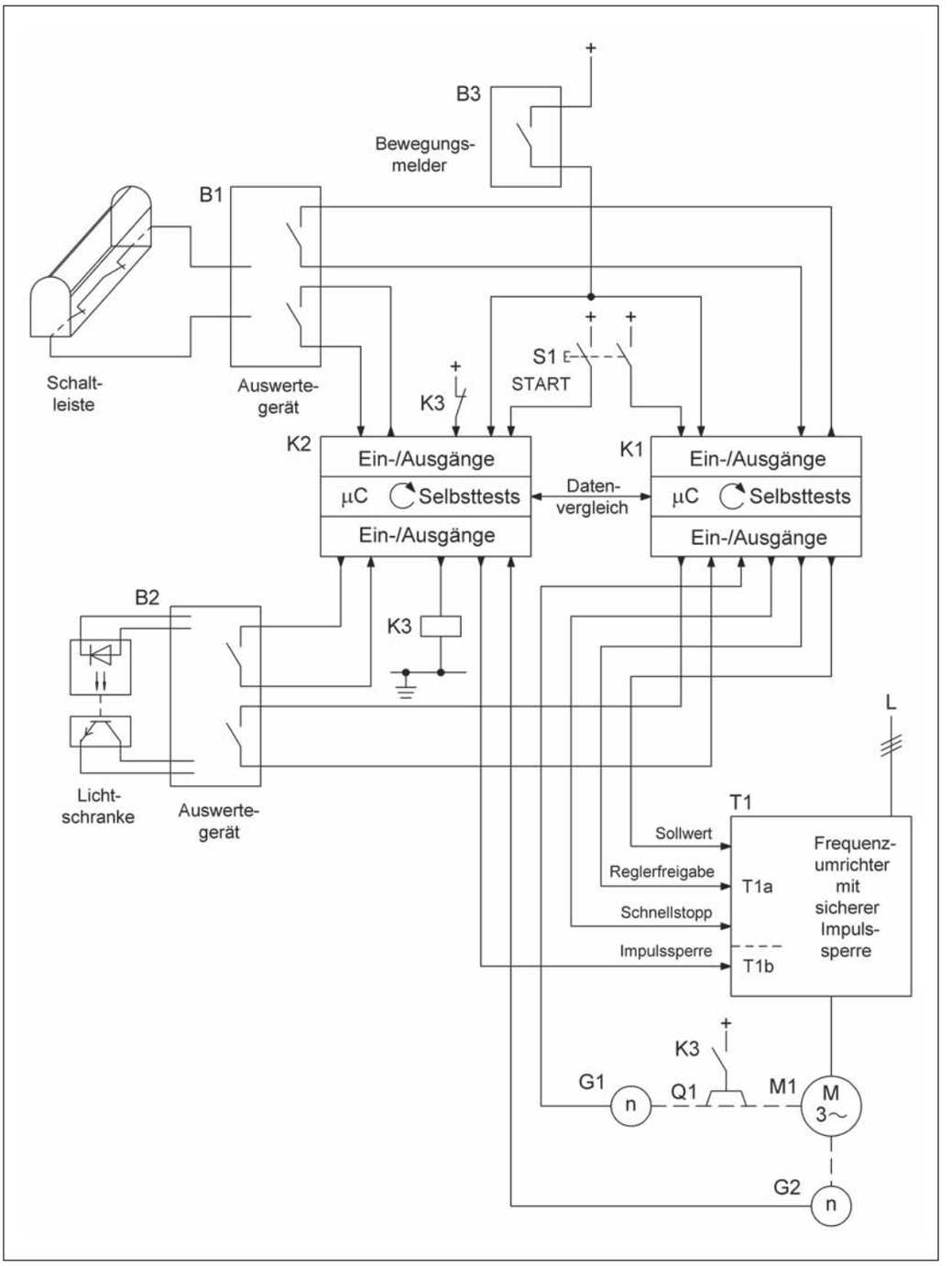
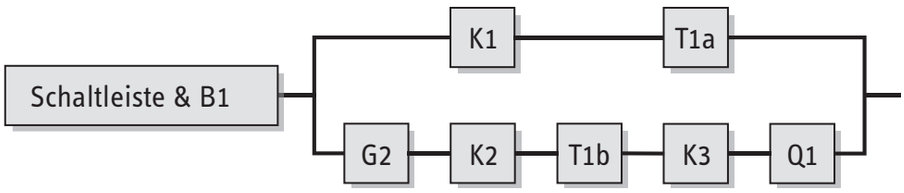


Abbildung 8.40: Karusselltürsteuerung mit Mikrocontrollern

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Bei Betätigung der Schaltleiste wird die Drehbewegung der Karusselltür stillgesetzt (SS1 – Sicherer Stopp 1).
- 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, Reglerfreigabe sowie des Schnellstopps. Durch K2 wird die Impulssperre angesteuert und die Haltebremse Q1 kann mithilfe des Hilfsschützes K3 gelöst werden. Die Drehgeber G1 und G2 übermitteln die Motordrehzahl an K1 bzw. K2.

- Fehler in der Schaltleiste bzw. der Lichtschranke werden in den zugehörigen Auswertegeräten B1 und B2 erkannt werden. Dies gilt auch für Fehler in B1 und B2, die durch interne Überwachung erkannt werden. Fehler in den Komponenten der Mikrocontroller werden über durchgeführte Selbsttests bzw. durch Datenvergleich erkannt. Die korrekte Funktion des Frequenzumrichters T1 wird mithilfe der Drehgeber G1 und G2 in K1 bzw. K2 überwacht. 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. Sie ist über B1 mit der Steuerung verbunden. Das Teilsystem aus Sensor und Auswertegerät erfüllt die Anforderungen nach DIN EN 1760-2 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. Sie erfüllt zusammen mit B2 mindestens die Anforderungen für Typ 2 nach DIN EN 61496-1 und DIN CLC/TS 61496-2 sowie nach DIN EN ISO 13849-1 für PL d. 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 Reglerfreigabe, der Schnellstoppfunktionalität sowie der Impulssperre). Ebenfalls findet ein Bremsentest statt, bei dem der Frequenzumrichter gegen die eingefallene Haltebremse 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 sicherer Impulssperre ist der Einsatz eines Schützes zum Abschalten der Versorgungsspannung nicht mehr 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 die Impulssperre aktiviert und die Reglerfreigabe weggenommen zur Vermeidung des unerwarteten Anlaufes. Bremszeit und Bremsweg werden von der Steuerung überwacht. Die Bremse Q1 ist im Fehlerfall erforderlich, damit es nach einem Fehler, wenn z.B. T1 die spezifizierte Funktion nicht mehr ausführen kann, zu keiner Gefährdung durch eine ungewollte 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 Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit“ wird ein Fehlerausschluss für den Fehler Geberwellenbruch (G1/G2) angenommen. Einzelheiten zur Möglichkeit eines Fehlerausschlusses siehe z.B. IEC 61800-5-2, Tabelle D.16

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

- Der Frequenzumrichter T1 wird für die Berechnung der Ausfallwahrscheinlichkeiten in die Blöcke T1a und T1b zerlegt. Im Block T1a sind die Funktionen Sollwertvorgabe, Reglerfreigabe und Schnellstopp sowie deren steuerungstechnische Umsetzung enthalten. Der Block T1b beinhaltet die mit einer geringen Anzahl von Bauteilen realisierte sichere Impulssperre.

Die detaillierte Berechnung der Ausfallwahrscheinlichkeit wird für die Sicherheitsfunktion „Sicherheitsbezogene Stoppfunktion (SS1)“, die auch im Blockdiagramm dargestellt ist, durchgeführt:

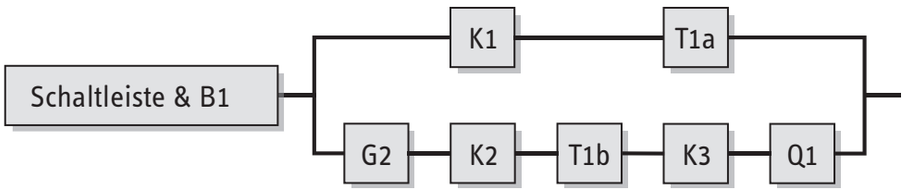
- Da die Schaltleiste mit zugehörigem Auswertegerät B1 als käufliches Sicherheitsbauteil vorliegt, wird deren Ausfallwahrscheinlichkeit am Ende der Berechnung addiert ($3{,}00 \cdot 10^{-7}$/Stunde [G]).

- $MTTF_d$: 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 G2 fließt ein Wert von 75 Jahren [G] in die Berechnung ein. Für T1a wird ein Wert von 100 Jahren [G] und für T1b ein Wert von 1 000 Jahren [G] 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. Q1 wird mit einer $MTTF_d$ von 50 Jahren [G] berücksichtigt. Die Haltebremse Q1 ist nur im Fehlerfall erforderlich und unterliegt keinem betriebsmäßigen Verschleiß. Insgesamt ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 64,3 Jahren („hoch“).

- DC_{avg}: Für K1 und K2 ergibt sich aufgrund der Auswahl geeigneter Testmaßnahmen ein *DC* von 60 %. Interne Selbsttests der Komponenten der Mikrocontroller werden durchgeführt. Für den Block T1a wird ein *DC* von 90 % angesetzt, da eine Fehleraufdeckung über den Prozess erfolgt. G2 wird mit einem *DC* von 90 % bemessen, die Fehleraufdeckung erfolgt auch hier durch den Prozess und den Vergleich mit G1 über K1 und K2. K3 wird mit einem *DC* = 99 % bemessen aufgrund der direkten Überwachung eines zurückgelesenen zwangsgeführten Kontaktes. Aufgrund des durchgeführten statischen Einschalttestes wird für T1b ein *DC* = 60 % und für Q1 ein *DC* = 30 % angesetzt. Durch Mittelung ergibt sich damit ein DC_{avg} von 62 % („niedrig“).

- 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 $MTTF_d$ (64,3 Jahre) und niedrigem DC_{avg} (62 %). Für die Kombination der Komponenten K1 und T1a im ersten Kanal sowie G2, K2, T1b, K3 und Q1 im zweiten Kanal ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}94 \cdot 10^{-7}$/Stunde. Zuzüglich der Sensoreinheit, bestehend aus Schaltleiste und Auswertegerät B1, beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle der Steuerung für diese Sicherheitsfunktion insgesamt $4{,}94 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.



Berechnung der Ausfallwahrscheinlichkeit für die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit (SLS)“:

- Für diese Berechnung muss zusätzlich G1 im ersten Kanal berücksichtigt werden. Dafür wird eine $MTTF_d$ von 75 Jahren [G] angesetzt. Der *DC* von 99 % ergibt sich aufgrund der Fehleraufdeckung durch den Prozess sowie den Vergleich mit G2 über K2 und K1. Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache wurden analog zur ersten Beispielberechnung gewählt. Mit 34,9 Jahren $MTTF_d$ und 70 % DC_{avg} ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}46 \cdot 10^{-7}$/Stunde. Nach Hinzufügen der Sensoreinheit, hier bestehend aus Lichtschranke und Auswertegerät B2 mit einem Wert von $2{,}00 \cdot 10^{-7}$/Stunde [G], beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle der Steuerung für diese Sicherheitsfunktion insgesamt $6{,}46 \cdot 10^{-7}$/Stunde. Dies entspricht ebenfalls PL d.

Weiterführende Literatur

- DIN EN 1760-2: Sicherheit von Maschinen – Druckempfindliche Schutzeinrichtungen – Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltleisten und Schaltstangen (07.01). Beuth, Berlin 2001
- DIN 18650-1: Schlösser und Baubeschläge – Automatische Türsysteme (12.05). Beuth, Berlin 2005
- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005
- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (01.05). Beuth, Berlin 2005
- DIN CLC/TS 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (02.08). Beuth, Berlin 2008
- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebe mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (07.07). Beuth, Berlin 2007

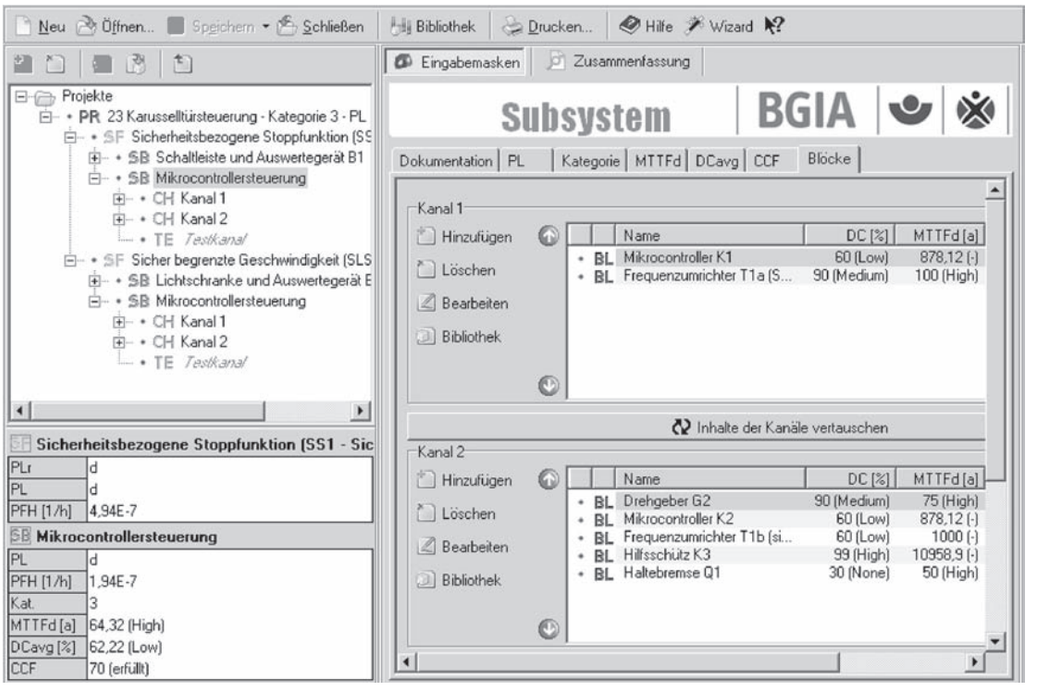
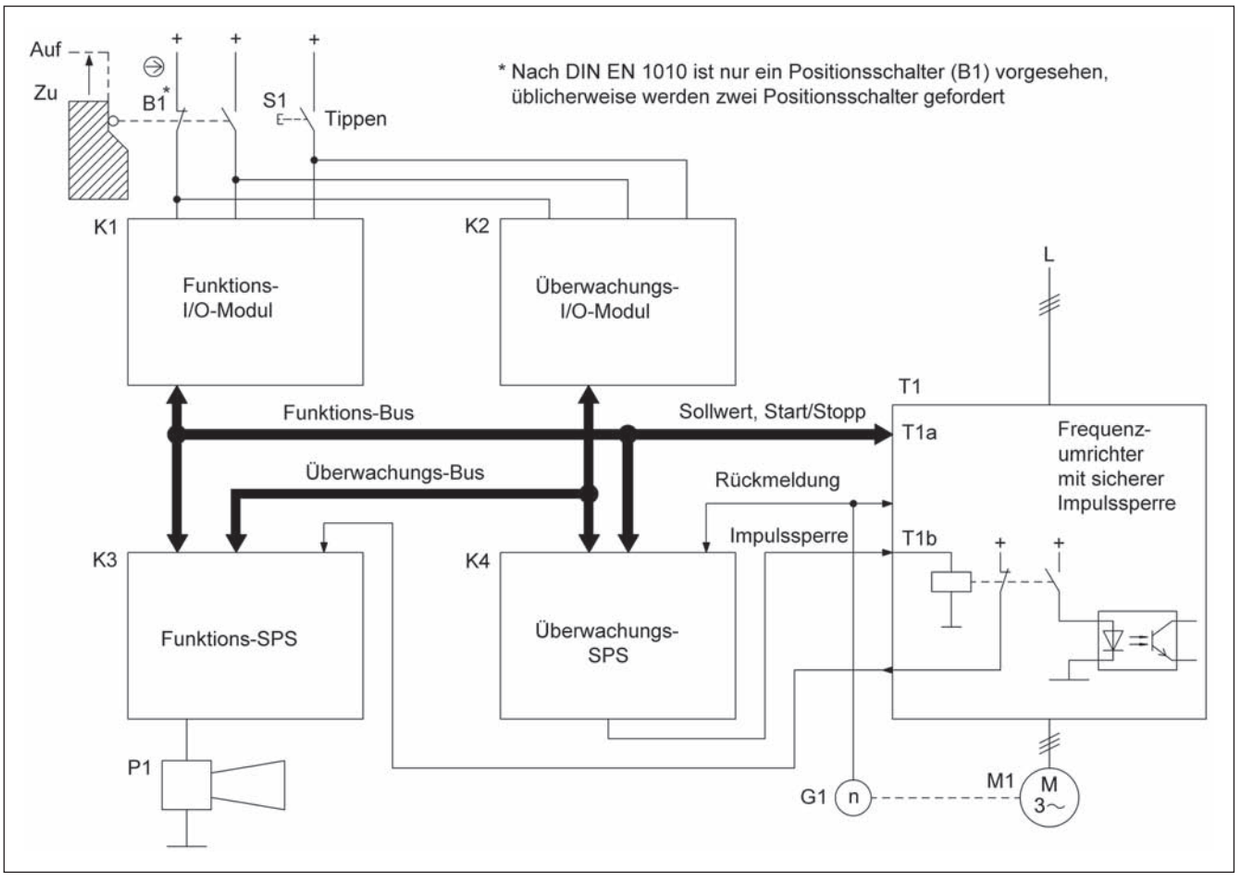


Abbildung 8.41: PL-Bestimmung mithilfe von SISTEMA

8.2.24 Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine – Kategorie 3 – PL d bzw. c (Beispiel 24)

Abbildung 8.42:
Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine durch eine zweikanalige Rechnersteuerung

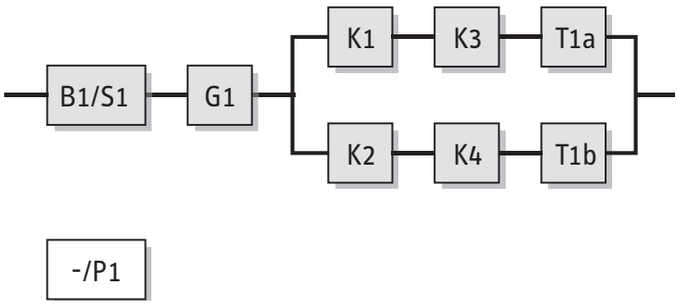


Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Beim Öffnen der Schutztür soll der Antrieb anhalten (SS1 – Sicherer Stopp 1).
- Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür dürfen Maschinenbewegungen nur mit begrenzten Drehzahlen 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 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 zur Ansteuerung des Frequenzumrichters T1 (Funktionsmäßige Ansteuerung T1a) über den Funktionsbus. Redundant zu K1 und K3 arbeiten das I/O-Modul K2 und die Überwachungs-SPS K4, die über einen eigenen Überwachungsbus kommunizieren. K4 kann durch Anwahl der sicheren Impulssperre von T1 eine ungesteuerte Stillsetzung (Austrudeln) herbeiführen (Sicherheitsabschaltung T1b).
- Bei geöffnetem B1 ist nur ein Tippbetrieb über S1 mit sicher begrenzter Geschwindigkeit erlaubt.



- Entsprechend DIN EN 1010-1 ist ein einziger Positionsschalter B1 ausreichend. Die meisten Fehler in S1 werden durch eine akustische Anlaufwarnung mittels P1 und Zwangsdynamisierung aufgedeckt und beherrscht: Nach erstmaliger Betätigung von S1 erfolgt eine akustische Warnung (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 werden 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 der Impulssperre und überwacht deren Rückmeldung durch den zwangsgeführten Öffnerkontakt des Impulssperrerelais 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). G1 wird zur Überwachung der sicher begrenzten Geschwindigkeit zusätzlich in K4 zurückgelesen und auf Plausibilität der Sin/Cos-Information ($Sin^2 + Cos^2 = 1$) sowie Übereinstimmung mit dem Sollwert für T1 überwacht.

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.

- Der Öffner von B1 entspricht DIN EN 60947-5-1, Anhang K. Maßnahmen zur Verhinderung der Lageänderung und der vernünftigerweise vorhersehbaren Manipulation sind realisiert (siehe DIN EN 1088 mit Anhang A1). Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.

- Trotz Anlaufwarnung und Zwangsdynamisierung kann S1 während des Tippbetriebs hängen bleiben. Daher muss in Reichweite des Bedieners 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 Antivalenzüberwachung des Öffner- und Schließerkontaktes in K1 und K2 erkannt.

- Die programmierbaren Komponenten K1 bis K4 erfüllen die normativen Anforderungen gemäß Abschnitt 6.3.

- G1 liefert redundante Positionsinformationen (z.B. Sin/Cos-Geber) und ist in den Regelkreis eingebunden (Gewinnung der Kommutierung).

- T1 besitzt eine sichere Impulssperre (T1b), deren erfolgreiche Anwahl durch einen zwangsgeführten Öffnerkontakt zurückgelesen wird.

- Der Einsatz der Standardkomponenten G1 und T1 erfolgt entsprechend den Hinweisen aus Abschnitt 6.3.10.

- Der Einsatz der Bussysteme (Funktionsbus, Überwachungsbus) erfolgt entsprechend den Hinweisen aus Abschnitt 6.2.17.

Bemerkungen

- Anwendung z.B. zur 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 (z.B. ein Öffner, ein Schließer).

- Für den Tippbetrieb unter der Voraussetzung bereits gewährleisteter sicher begrenzter Geschwindigkeit kann unter bestimmten Bedingungen von der Möglichkeit zur Vermeidung der Gefährdung ausgegangen werden.

Berechnung der Ausfallwahrscheinlichkeit

- Die Sensorebene B1, S1 und G1 liegt außerhalb der redundanten Logik- und Aktorebene und wird daher separat betrachtet.

- Für B1 kann ein Fehlerausschluss für den zwangsöffnenden Kontakt erfolgen. Für den mechanischen Teil 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. Dies entspricht rechnerisch einer mittleren Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}97 \cdot 10^{-10}$/Stunde. Um den Besonderheiten der DIN EN 1010-1 Rechnung zu tragen, wird dieser Wert auf den oberen Eckwert $1{,}00 \cdot 10^{-7}$/Stunde für PL d zurückgestuft, statt wie üblich die $MTTF_d$ für einen Kanal auf 100 Jahre zu begrenzen.

- S1 besitzt einen B_{10d}-Wert von 100 000 Zyklen [H]. Bei wöchentlich 10-facher Betätigung ist n_{op} = 520 Zyklen/Jahr und $MTTF_d$ = 1 923 Jahre. Wegen Zwangsdynamisierung und Anlaufwarnung wird ein *DC* von mindestens 60 % angenommen (ein Hängenbleiben nach wiederholtem Tippen wird aber nicht erkannt). S1 erreicht damit durch die Einbindung in eine Kategorie-2-Struktur eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}28 \cdot 10^{-7}$/Stunde.

- G1 ist durch Auswertung der Sin/Cos-Signale und Nutzung im Regelkreis (Verwendung für die Kommutierung) gemäß Kategorie 3 eingebunden. Mit 30 Jahren $MTTF_d$ pro Kanal [G] und 90 % *DC* durch Plausibilitätsprüfung und Fehlererkennung im Prozess ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}65 \cdot 10^{-7}$/Stunde.

- $MTTF_d$: Es werden 100 Jahre [G] für K1 und K2, 50 Jahre [G] für K4 und 30 Jahre [G] für K3 in Rechnung gestellt. Außerdem werden 30 Jahre [G] für T1a und 1 000 Jahre [G] für T1b angesetzt. Damit ergibt sich insgesamt ein symmetrisierter $MTTF_d$-Wert pro Kanal von 24 Jahren („mittel“).

- DC_{avg}: *DC* = 99 % für K1 und K2 ergibt sich durch den direkten Vergleich der bereitgestellten Zustandsinformationen in K4. *DC* = 99 % für K3 gründet sich auf der parallelen Verarbeitung aller sicherheitsrelevanter 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 Impulssperre führen für K4 auf einen *DC* von 60 %. *DC* = 99 % für T1a basiert auf dem Soll-/Ist-Wert-Vergleich der Achsposition in K4. Für T1b ergibt sich bei Annahme eines Fehlerausschlusses für den internen Optokoppler durch Rücklesung der Impulssperrenanwahl ein *DC* von 60 %. Durch Mittelung ergibt sich damit ein DC_{avg} von 91 % („mittel“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

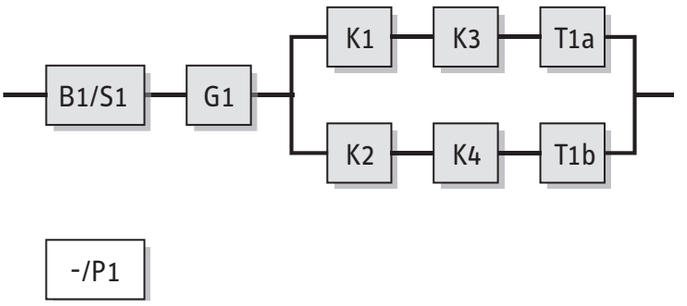
- Die Kombination von K1 bis K4 und T1 entspricht Kategorie 3 mit mittlerer $MTTF_d$ pro Kanal (24 Jahre) und mittlerem DC_{avg} (91 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $3{,}33 \cdot 10^{-7}$/Stunde. Für die sicherheitsbezogene Stoppfunktion und die sicher begrenzte Geschwindigkeit ist dazu der Wert von B1 und G1 zu addieren. So ergibt sich mit $(1{,}00 + 2{,}65 + 3{,}33) \cdot 10^{-7}$/Stunde = $6{,}98 \cdot 10^{-7}$/Stunde ein PL d. Für den Tippbetrieb muss der Wert von S1 und G1 hinzugefügt werden, womit sich ein Wert von $(5{,}28 + 2{,}65 + 3{,}33) \cdot 10^{-7}$/Stunde = $1{,}13 \cdot 10^{-6}$/Stunde errechnet. 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 (03.05). Beuth, Berlin 2005

- Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitungsmaschinen. Elektrische Ausrüstung und Steuerungen. Hrsg.: Berufsgenossenschaft Druck und Papierverarbeitung, Wiesbaden 2004
http://www.bgdp.de/pages/service/download/medien/220-2.pdf

- *Apfeld, R.; Zilligen, H.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. BGIA-Report 5/2003. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003
www.dguv.de/bgia, Webcode d6428



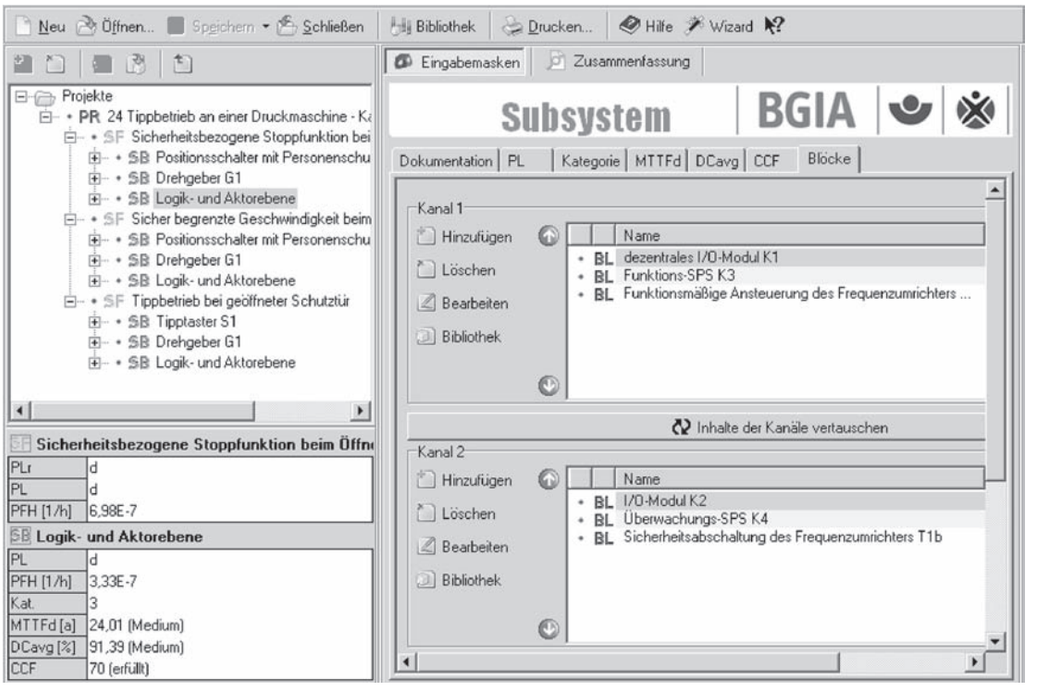


Abbildung 8.43: PL-Bestimmung mithilfe von SISTEMA

8.2.25 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 3 – PL e (für PL-d-Sicherheitsfunktionen) (Beispiel 25)

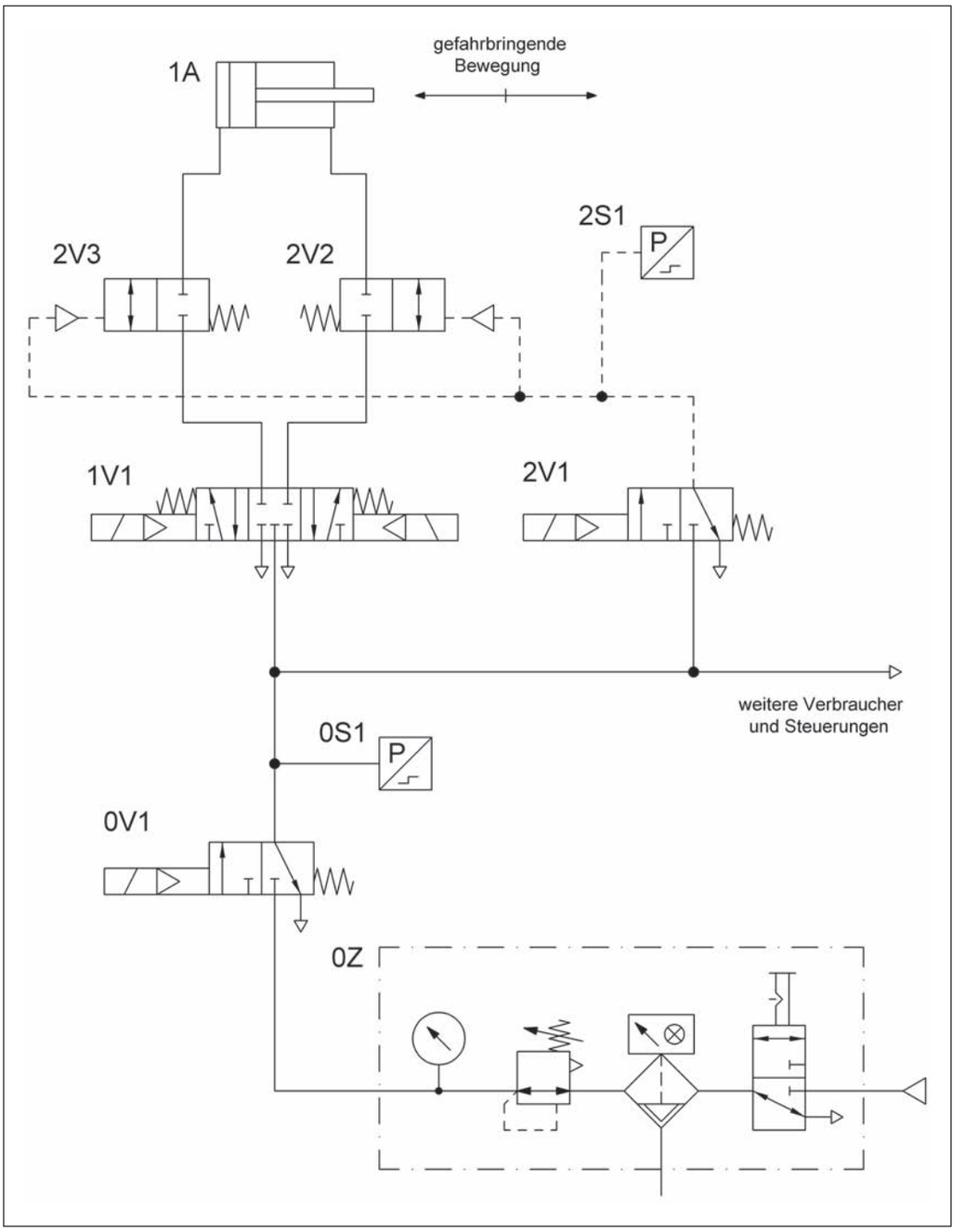
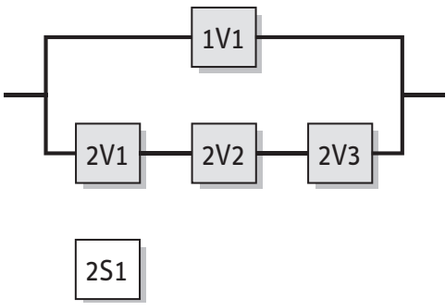


Abbildung 8.44: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- 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. Die 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 und 2V1 werden B_{10d}-Werte von 40 000 000 Zyklen [G] angenommen. Für die Ventile 2V2 und 2V3 werden B_{10d}-Werte von 60 000 000 Zyklen [G] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr. Damit beträgt die $MTTF_d$ für 1V1 und 2V1 289 Jahre und für 2V2 und 2V3 434 Jahre. Nach Kürzen beider Kanäle auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 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 71 % („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 $MTTF_d$ (100 Jahre) und niedrigem DC_{avg} (71 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}86 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

8.2.26 Pneumatische Ventilsteuerung – Kategorie 3 – PL e (Beispiel 26)

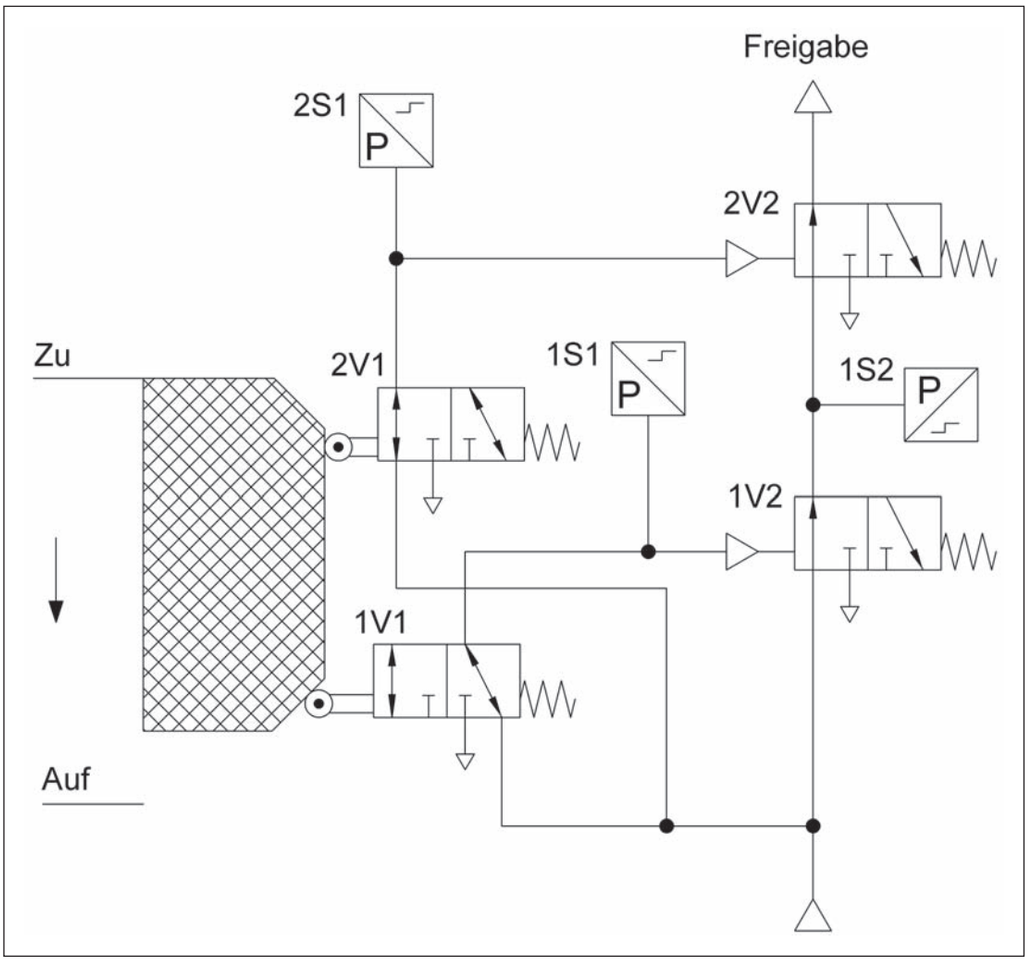


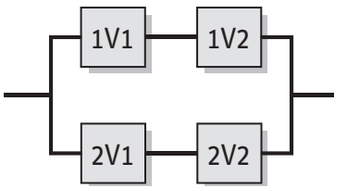
Abbildung 8.45: Redundante pneumatische Steuerung zur Verriegelung beweglicher trennender Schutzeinrichtungen

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Beim Öffnen der beweglichen trennenden Schutzeinrichtung erfolgt eine Energietrennung und Druckentlastung in der pneumatischen Steuerung.

Funktionsbeschreibung

- Die Verriegelung der beweglichen trennenden Schutzeinrichtung erfolgt durch zwei „pneumatische Positionsschalter“ (1V1 und 2V1). Diese geben jeweils einen Steuerbefehl an die Wegeventile 1V2 und 2V2.
- Pneumatische Energiezufuhr findet nur bei geschlossener Schutzeinrichtung statt.
- Der Ausfall eines „pneumatischen Positionsschalters“ oder Wegeventils führt nicht zum Verlust der Sicherheitsfunktion.
- Eine Fehlererkennung der Ventile 2V1 und 1V2 erfolgt über die Druckschalter 1S1, 2S1 und 1S2. Die entsprechenden Signale können in einer SPS verarbeitet werden. Bei einer Fehlererkennung kann z.B. die Energie abgeschaltet werden. Für das Ventil 2V2 ist keine Fehlererkennung vorhanden. Die Funktion dieses Ventils sollte regelmäßig überprüft werden. Die 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.
- 1V1 ist ein pneumatischer Positionsschalter mit zwangläufiger Betätigung durch die bewegliche trennende Schutzeinrichtung, entsprechend DIN EN 1088.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- Die sicherheitsgerichtete Schaltstellung der Wegeventile 1V2 und 2V2 wird durch Wegnahme der Steuersignale erreicht.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für Ventil 1V1 wird ein Fehlerausschluss angenommen, da eine zwangläufige Betätigung durch die beweglich trennende Schutzeinrichtung gegeben ist und da das Ventil als Positionsschalter mit Personenschutzfunktion ausgelegt ist (in Anlehnung an DIN EN 60947-5-1). Für die Ventile 2V1, 1V2 und 2V2 werden $B10_d$-Werte von 20 000 000 Zyklen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitstunden und 30 Sekunden Zykluszeit ist n_{op} = 460 800 Zyklen/Jahr und $MTTF_d$ = 434 Jahre. Nach Kürzen beider Kanäle auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“).
- DC_{avg}: DC = 99 % für die Wegeventile 2V1 und 1V2 ergibt sich aus der Fehlererkennung über die Druckschalter. Für das Wegeventil 2V2 wird ein DC = 0 % angenommen (Abschätzung zur sicheren Seite). Durch Mittelung ergibt sich damit ein DC_{avg} von 66 % („niedrig“).
- 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 3 mit hoher $MTTF_d$ (100 Jahre) und niedrigem DC_{avg} (66 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $8{,}95 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Weiterführende Literatur

- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005

8.2.27 Hydraulische Ventilsteuerung (Subsystem) – Kategorie 3 – PL e (für PL-d-Sicherheitsfunktionen) (Beispiel 27)

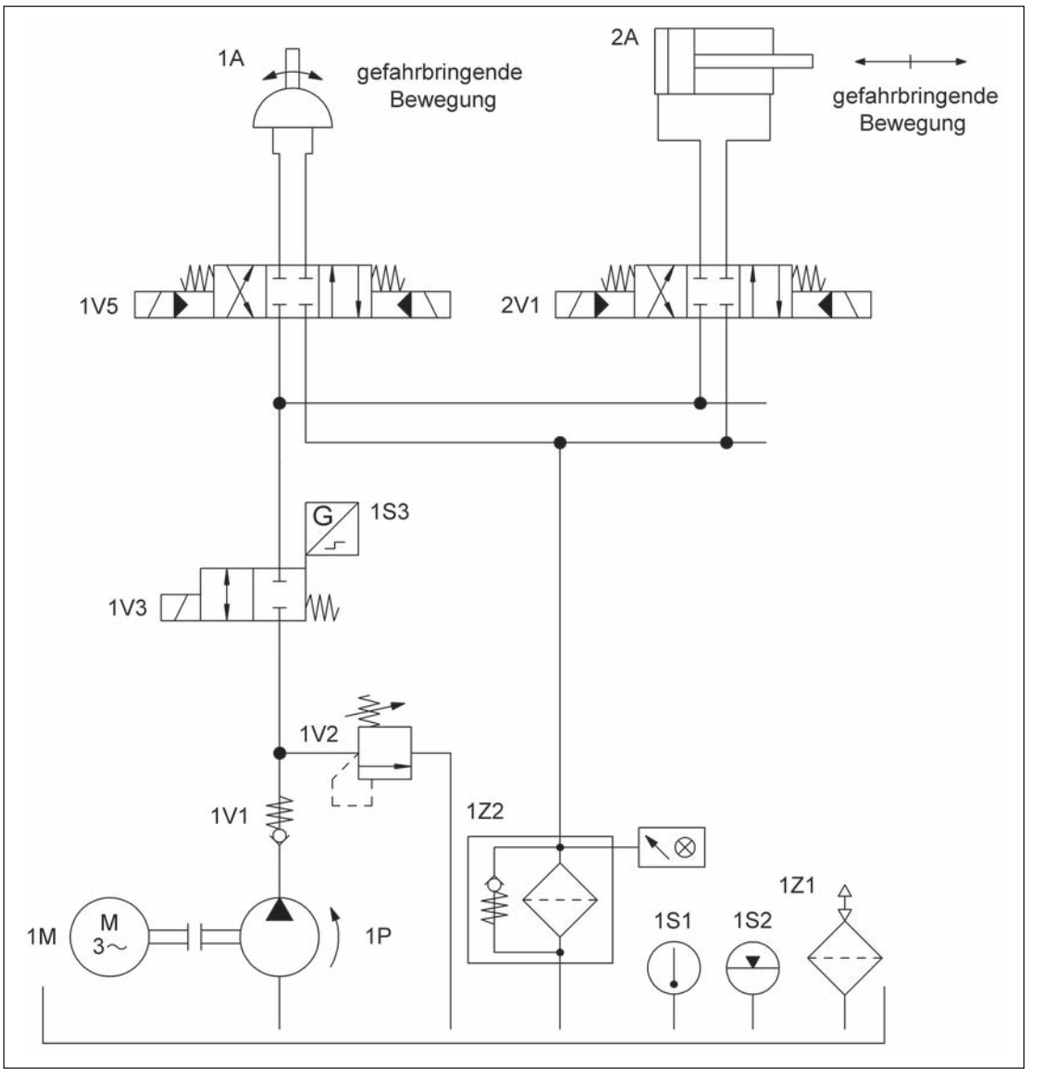


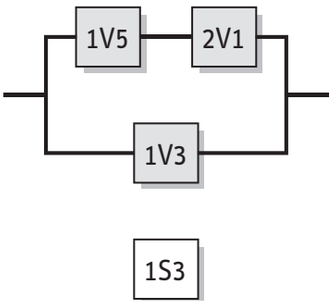
Abbildung 8.46: Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten 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 [N]. 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 $9{,}35 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

8.2.28 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen – Kategorie 4 – PL e (Beispiel 28)

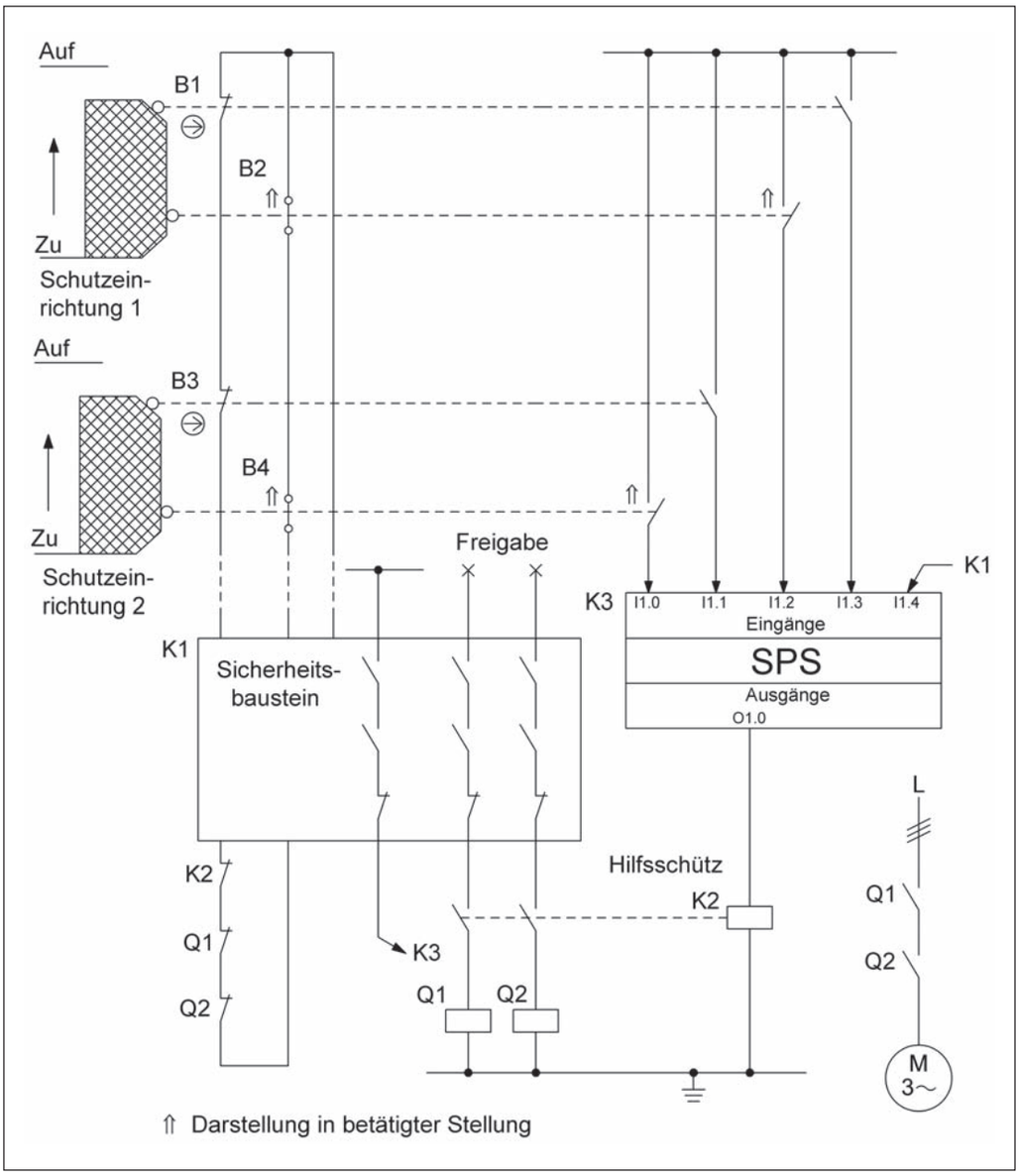


Abbildung 8.47: Stellungsüberwachung beweglicher trennender Schutzeinrichtungen zur Verhinderung von gefahrbringenden Bewegungen

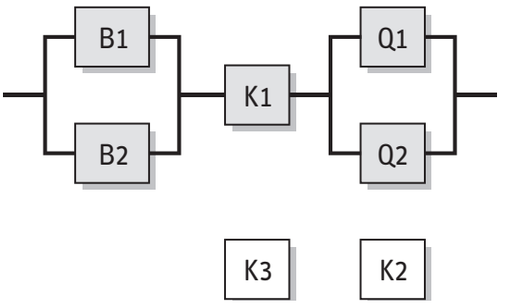
Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen einer beweglichen trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit zwei beweglichen 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 Sicherheitsbaustein 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 den Sicherheitsbaustein K1 erkannt. Einige wenige Fehler werden nicht erkannt (z.B. Nichtunterbrechung der Kontakte in B2 und B4).



- 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 (Kaskadierung).
- Der Sicherheitsbaustein K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Schütze K2, Q1, Q2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die programmierbare SPS K1 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 Sicherheitsbausteins K1 wird am Ende der Berechung addiert ($2{,}31 \cdot 10^{-9}$/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 Positionsschalter B1 ist ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt des Positionsschalters B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 1 Stunde Zykluszeit ist für diese Komponenten n_{op}= 5 840 Zyklen/Jahr und $MTTF_d$ beträgt 1 712 Jahre für B1 bzw. 856 Jahre für 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. Insgesamt ergibt sich in beiden Subsystemen ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“).
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in der SPS 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_{avg} 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 $2{,}47 \cdot 10^{-8}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $5{,}16 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

8.2.29 Kaskadierung von Not-Halt-Geräten mittels Sicherheitsbaustein – Kategorie 3 – PL e (Beispiel 29)

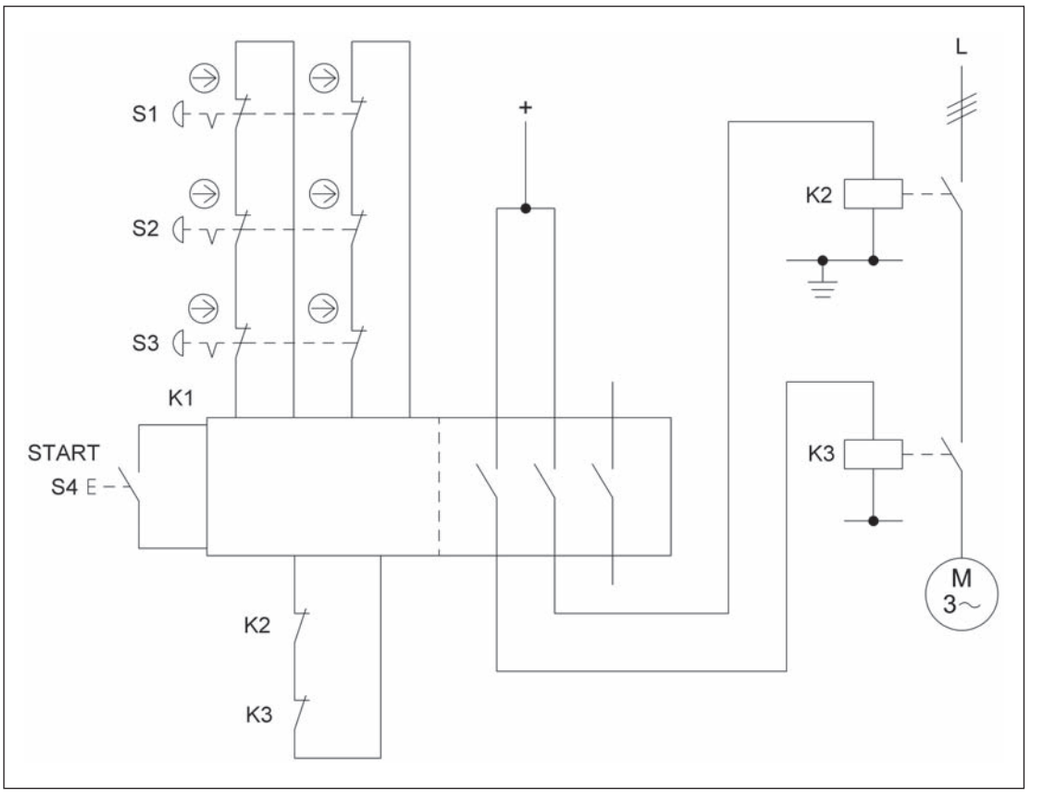


Abbildung 8.48: Kaskadierung von Not-Halt-Geräten mittels Sicherheitsbaustein (Not-Halt-Funktion, STO)

Sicherheitsfunktion

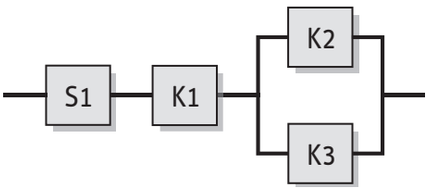
- Not-Halt-Funktion, STO durch Betätigung eines Not-Halt-Gerätes

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 Sicherheitsbaustein K1, der zwei redundante Hilfsschütze K2 und K3 ansteuert.
- Die Not-Halt-Geräte werden zur Fehlererkennung redundant in den Sicherheitsbaustein K1 eingelesen. Dieser 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 gedrückt 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, S3 handelt es sich um Schaltgeräte mit zwangsöffnenden Kontakten entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Schaltgeräten sind geschützt verlegt.



- Der Sicherheitsbaustein 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 12100-2:2004.

Berechnung der Ausfallwahrscheinlichkeit

- Bei S1, S2, S3 handelt es sich um handelsübliche Not-Halt-Geräte nach DIN EN ISO 13850. Es erfolgt jeweils ein Fehlerausschluss für den zwangsöffnenden Kontakt und die Mechanik, sofern die in Tabelle D.2 dieses Reports angegebene Anzahl der Betätigungen nicht überschritten wird.
- Die Ausfallwahrscheinlichkeit des fertigen Sicherheitsbausteins K1 wird am Ende der Berechung addiert ($2{,}31 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für das Subsystem K2/K3 wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_d$: 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 drei Anforderungen der Not-Halt-Funktion und 24 Startbefehlen ist n_{op}= 27 Zyklen/Jahr und $MTTF_d$ beträgt 740 740 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 beruht auf der Testung durch den Sicherheitsbaustein K1. Dies ist gleichzeitig DC_{avg} („mittel“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), bewährte Bauteile (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- 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 $4{,}29 \cdot 10^{-8}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $4{,}52 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Damit ist der PL_r = d übertroffen.

8.2.30 Schützüberwachungsbaustein – Kategorie 3 – PL e (Beispiel 30)

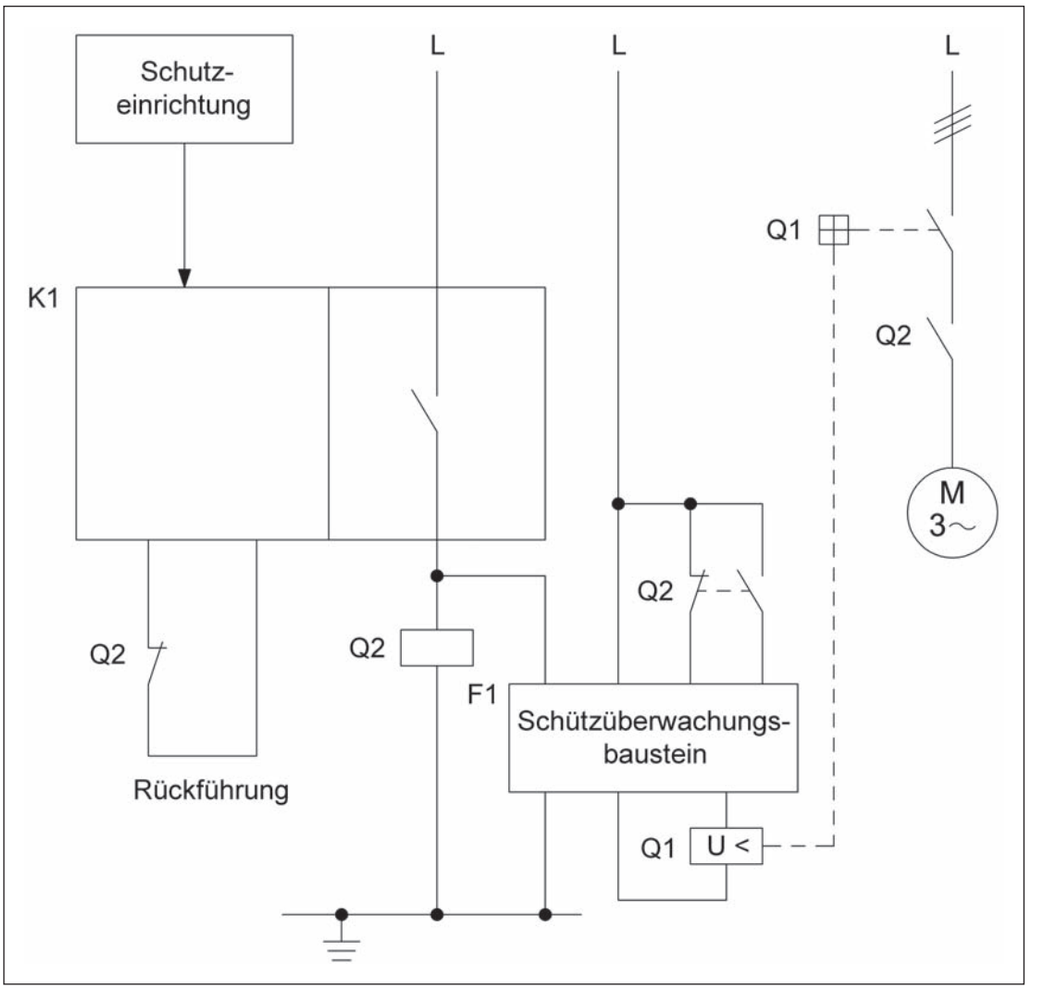


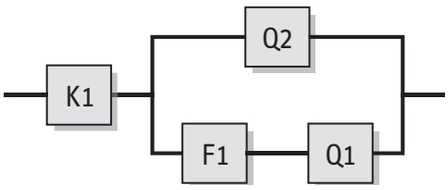
Abbildung 8.49: Einleitung des STO – Sicher abgeschaltetes Moment mittels Sicherheitsbaustein und Schützüberwachungsbaustein

Sicherheitsfunktion

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

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit einer Schutzeinrichtung, deren Öffnen durch einen Sicherheitsbaustein K1 detektiert wird. Dieser 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 einen Sicherheitsbaustein K1, der alle Anforderungen für Kategorie 3 oder 4 und PL e erfüllt.

- Das Schütz Q2 besitzt Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F, und ist in die Rückführung des Sicherheitsbausteins K1 zur Fehlerdetektion des Schützes eingebunden.

- 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 Sicherheitsbaustein 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 $MTTF_d$ beträgt 274 Jahre. Bei 365 Arbeitstagen, 16 Arbeitsstunden und 1 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 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 $4{,}45 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen des Subsystems, bestehend aus Schutzeinrichtung und Sicherheitsbaustein 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.

8.2.31 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 4 – PL e (Beispiel 31)

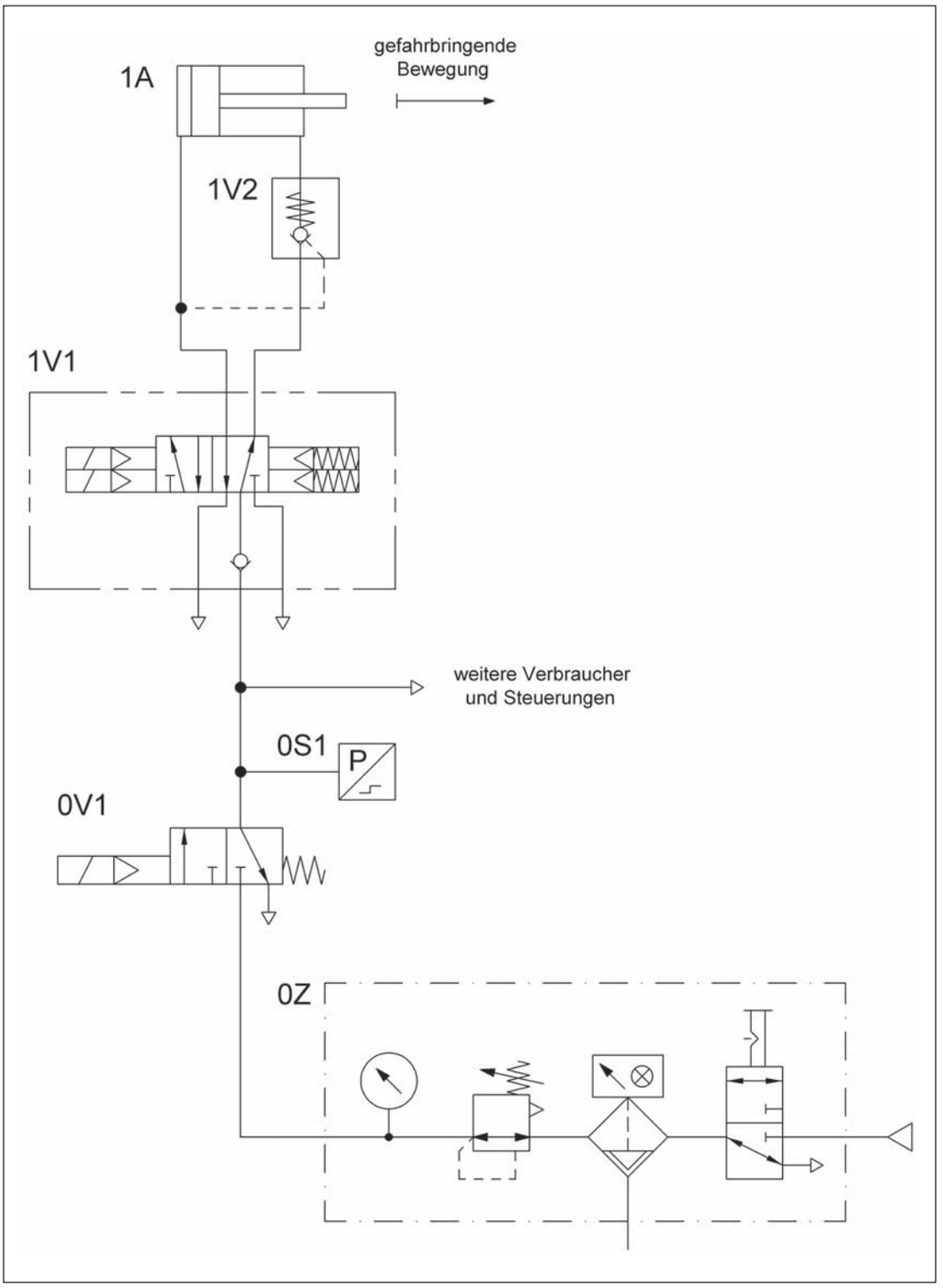
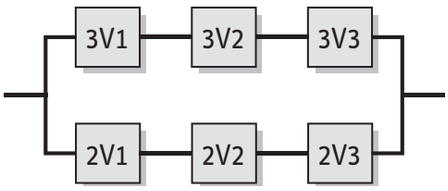


Abbildung 8.50: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Funktion: Reversieren der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- 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 eine selbstüberwachte Ventilkombination 1V1 gesteuert, in Verbindung mit einem entsperrbaren Rückschlagventil 1V2 (bei Ausfall der Druckluft und äußeren Kräften von Bedeutung).
- Ein Bauteilausfall innerhalb der Ventilkombination führt nicht zum Verlust der Sicherheitsfunktion.
- Beide in 1V1 enthaltenen Vorsteuerventile der Ventilkombination werden getrennt angesteuert. Nach Wegnahme mindestens eines Steuersignals erfolgt immer eine Reversierung der Bewegung.
- Der einzelne Fehler innerhalb der Ventilkombination führt zu einer Selbsthemmung im sicheren Zustand und wird daher im Arbeitsprozess erkannt; ein Einleiten der nächsten gefahrbringenden Bewegung wird verhindert.
- Die Ventilkombination 1V1 kann auch durch mehrere Ventile mit einer entsprechenden Verknüpfung und einer entsprechenden Stellungsabfrage der Schaltstellungen aufgebaut werden.
- 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.
- 1V1 ist eine selbstüberwachte Ventilkombination mit mechanisch getrennten integrierten Vorsteuerventilen und pneumatisch/mechanisch realisierter Fehlererkennung mit integriertem Rückschlagventil in der P-Leitung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme der Steuersignale erreicht.
- Das entsperrbare Rückschlagventil 1V2 ist möglichst im Zylinder eingeschraubt.
- Die Fehlererkennung innerhalb der Ventilkombination erfüllt entsprechende Anforderungen an den Fehlerfall.

Berechnung der Ausfallwahrscheinlichkeit

Die Ventilkombination1V1 besteht aus zwei Ventilkanälen mit jeweils drei verbundenen Ventilen. Diese sind im Blockschaltbild bezeichnet mit 2V1, 2V2 und 2V3 sowie 3V1, 3V2 und 3V3.

- $MTTF_d$: Für jedes der Ventile der Ventilkombination 1V1 wird ein B_{10d}-Wert von 20 000 000 Zyklen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr und $MTTF_d$ = 144 Jahre. Dies ergibt einen $MTTF_d$-Wert pro Kanal von 48 Jahren („hoch“).
- DC_{avg}: DC = 99 % für 1V1 ergibt sich über eine Zwangsführung der beiden Ventilkanäle bei gleichzeitigem internen Kreuzvergleich des Steuerdruckes(Steuerdrucküberwachung). 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 $MTTF_d$ (48 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}60 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für die verschleißbehaftete Ventilkombination 1V1 ein Wert von 14 Jahren (T_{10d}) für den vorgesehenen Austausch.

8.2.32 Hydraulische Ventilsteuerung (Subsystem) – Kategorie 4 – PL e (Beispiel 32)

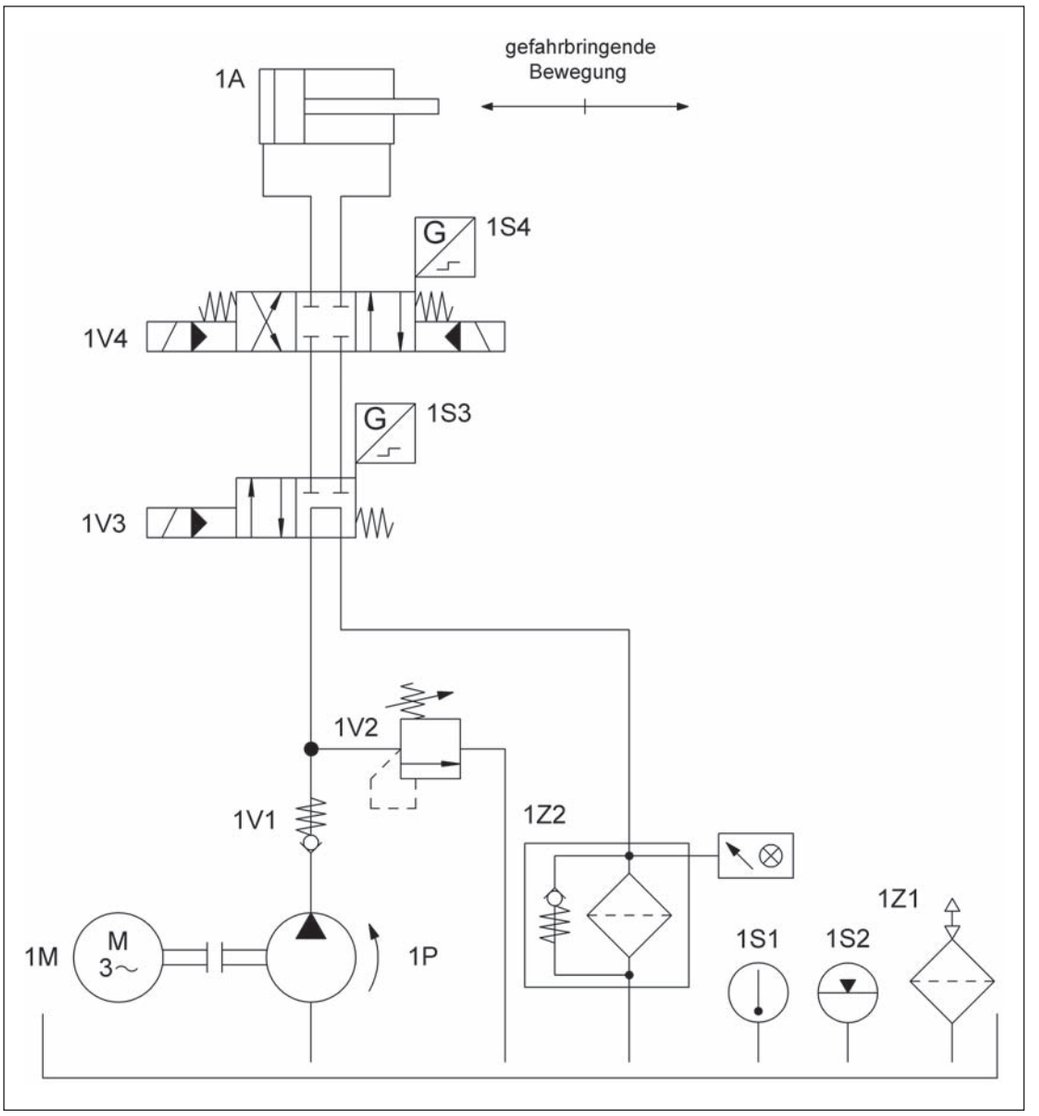


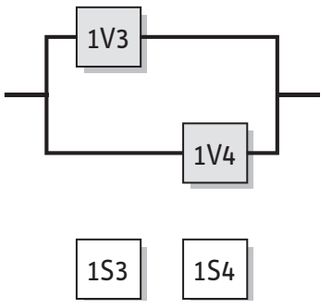
Abbildung 8.51: Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten 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 [N]. Dies ist gleichzeitig der $MTTF_d$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- 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 $MTTF_d$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

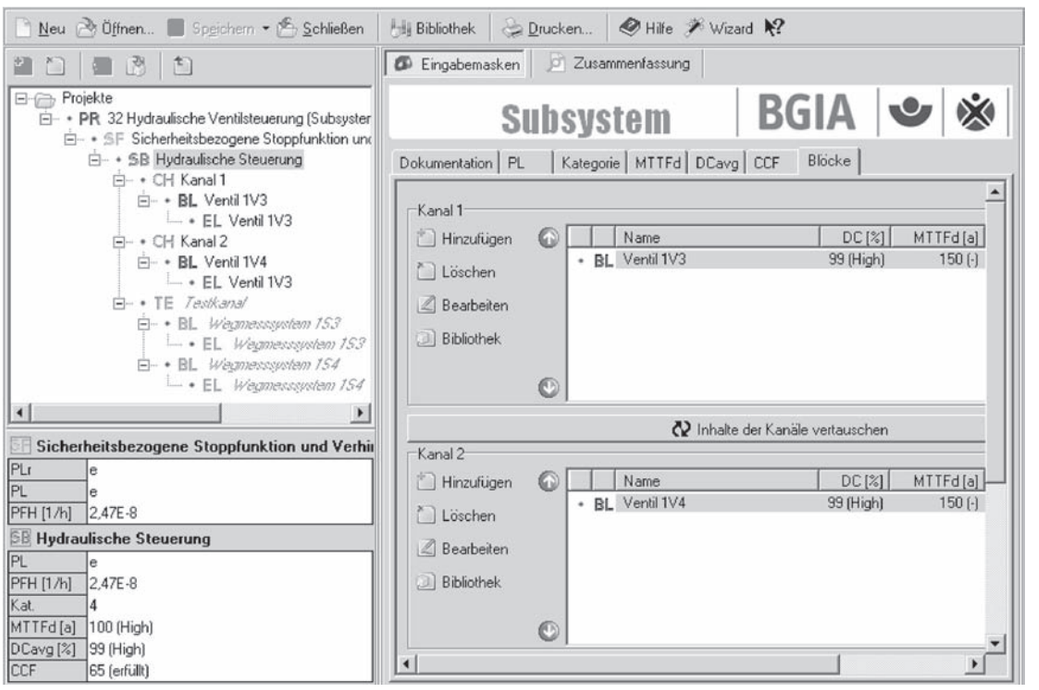


Abbildung 8.52: PL-Bestimmung mithilfe von SISTEMA

8.2.33 Elektrohydraulische Pressensteuerung – Kategorie 4 – PL e (Beispiel 33)

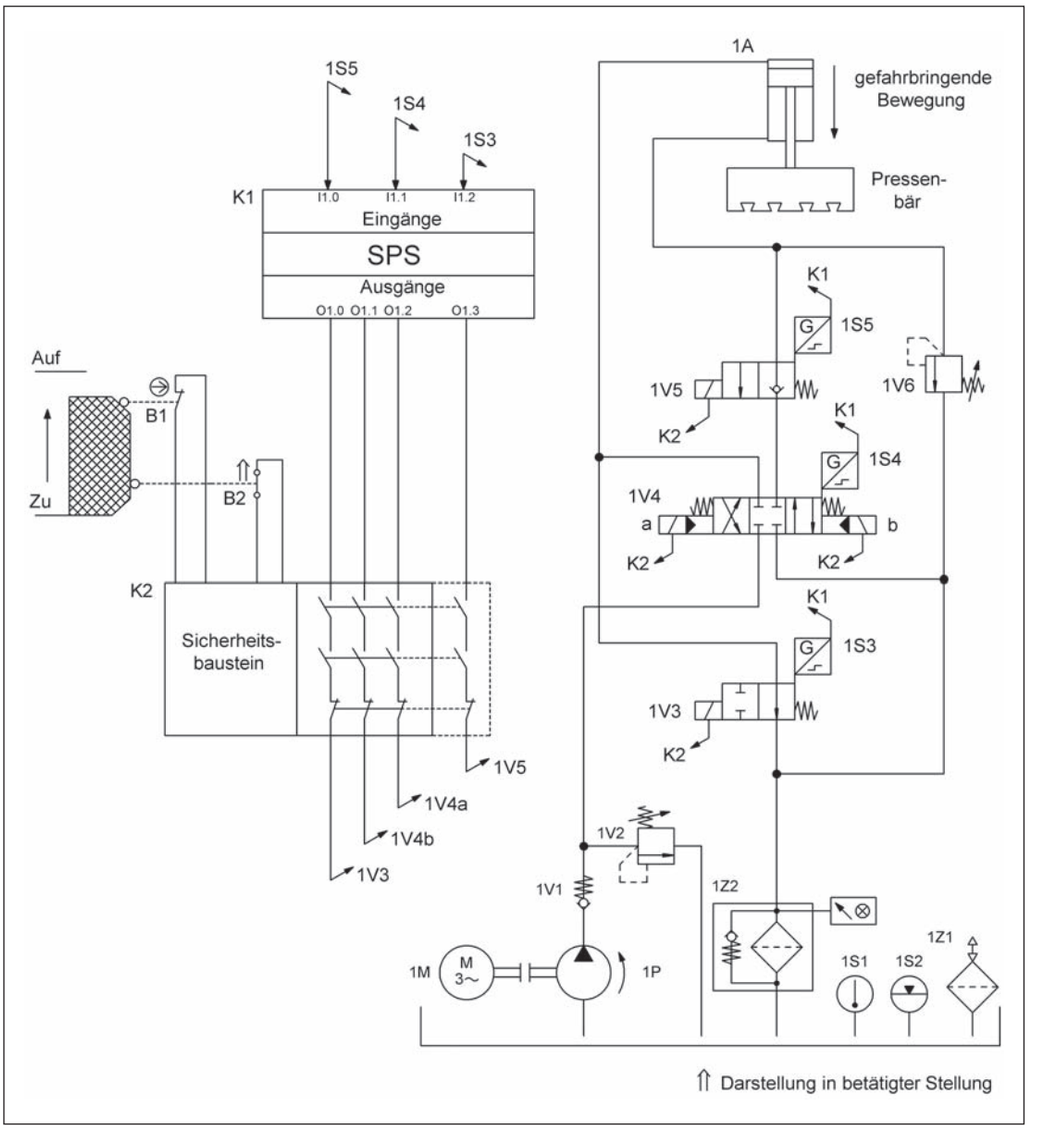


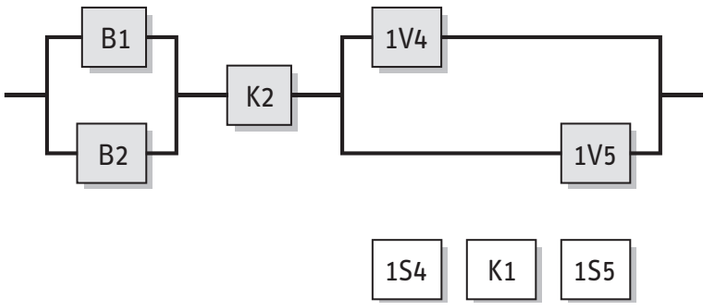
Abbildung 8.53: Pressensteuerung, elektrische Überwachung einer beweglichen trennenden Schutzeinrichtung mit hydraulischem Stillsetzen der gefahrbringenden Bewegung

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Stillsetzen der gefahrbringenden Bewegung

Funktionsbeschreibung

- Der Gefahrenbereich ist mittels einer beweglichen trennenden Schutzeinrichtung gesichert, deren Stellung von zwei Positionsschaltern B1 und B2 in Öffner-Schließer-Kombination erfasst wird. Die Signale werden in einen handelsüblichen Sicherheitsbaustein 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. Voraussetzung dafür ist ein Fehlerausschluss für das Druckbegrenzungsventil 1V6. Wenn z.B. die Feder bricht, wird die Abwärtsbewegung des Oberwerkzeugs nicht gestoppt. Die sicherheitsbezogene Stoppfunktion wird mittels der Ventile 1V4 und 1V5 realisiert. Das Ventil 1V3 wird z.B. für die Sicherheitsfunktion „Verhinderung eines unerwarteten Anlauf aus der Ruhelage“ benötigt. Diese und weitere Sicherheitsfunktionen werden hier jedoch nicht behandelt.



- Bei Anforderung der Sicherheitsfunktion werden beide Ventile durch K2 stromlos geschaltet und gehen aufgrund der vorhandenen Rückstellfedern in die Sperr-Mittelstellung (1V4) bzw. in die Sperr-Stellung (1V5). Dabei wird der Ölrückfluss von der Kolbenunterseite des Zylinders zum Tank durch die beiden Ventile gleichzeitig unterbrochen. Bei 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.
- Der Ausfall eines Ventils führt nicht zum Verlust der Sicherheitsfunktion. Beide Ventile werden zyklisch angesteuert.
- An beiden Ventilen ist jeweils eine Stellungsabfrage 1S4 bzw. 1S5 zur Fehlererkennung vorgesehen. Der Ausfall jedes der beiden 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.
- Der handelsübliche Sicherheitsbaustein 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 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.

Berechnung der Ausfallwahrscheinlichkeit

- K2 wird als Subsystem mit einer Ausfallwahrscheinlichkeit von $2{,}31 \cdot 10^{-9}$/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 ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt von Positionsschalter B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. 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 285 Jahre für B1 bzw. 142 Jahre für B2. Für die Ventile 1V4 und 1V5 wird jeweils eine $MTTF_d$ von 150 Jahren [N] angenommen. Daraus ergibt sich ein gekürzter $MTTF_d$-Wert pro Kanal von 100 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 $MTTF_d$ pro Kanal (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich jeweils eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Für die komplette Sicherheitsfunktion ergibt sich durch Addition inklusive K2 eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}16 \cdot 10^{-8}$ pro Stunde. Dies entspricht PL e.

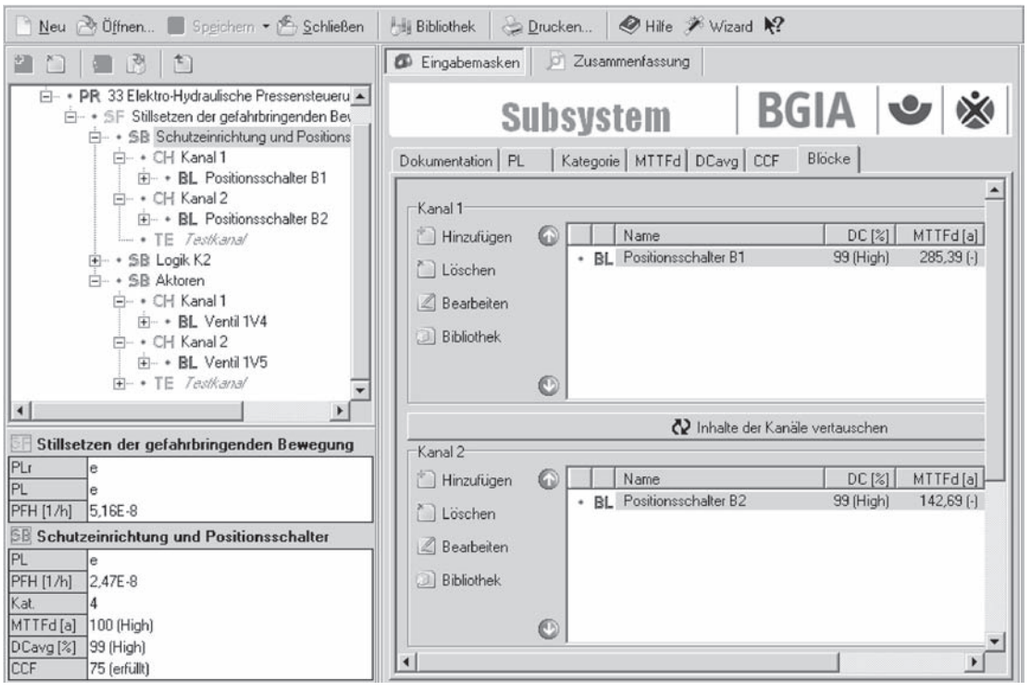


Abbildung 8.54: PL-Bestimmung mithilfe von SISTEMA

8.2.34 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen – Kategorie 4 – PL e (Beispiel 34)

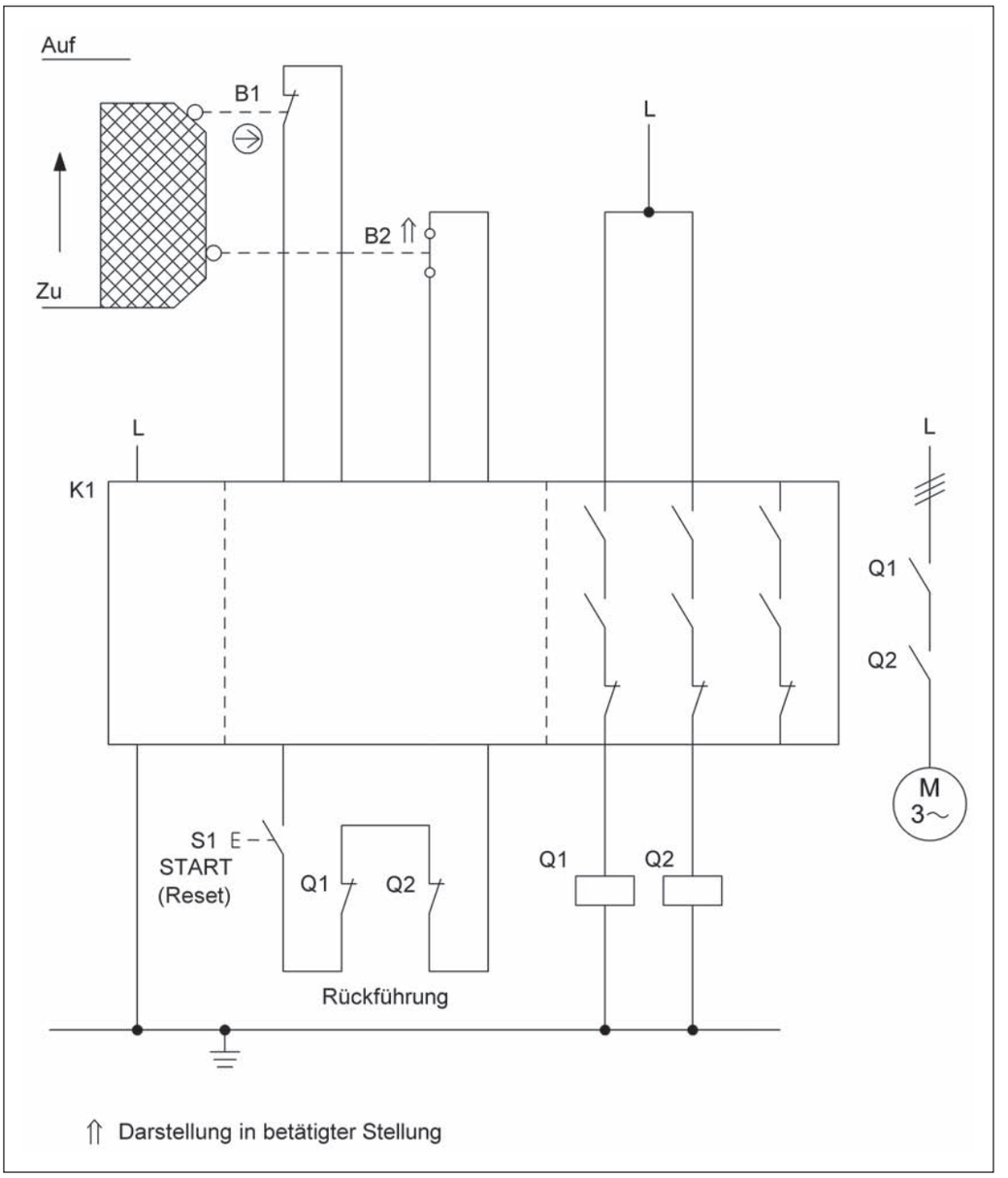


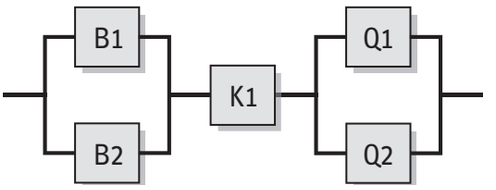
Abbildung 8.55: Stellungsüberwachung beweglicher trennender Schutzeinrichtung mittels Sicherheitsbaustein

Sicherheitsfunktion

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

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit einer beweglichen trennenden Schutzeinrichtung (Schutzgitter). Das Öffnen des Schutzgitters wird durch zwei Positionsschalter B1/B2 in Öffner-Schließer-Kombination erfasst und in einem zentralen Sicherheitsbaustein K1 ausgewertet. Dieser 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.
- Der Sicherheitsbaustein K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Schütze K2, Q1, Q2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.

Bemerkung

- Kategorie 4 wird nur eingehalten, wenn nicht mehrere mechanische Positionsschalter verschiedener Schutzeinrichtungen hintereinander geschaltet werden (keine Kaskadierung), da sonst keine Fehlererkennung in den Schaltern möglich ist.

Berechnung der Ausfallwahrscheinlichkeit

- Die Schaltung lässt sich in drei Subsysteme aufteilen, wie im sicherheitsbezogenen Blockdiagramm gezeigt. Die Ausfallwahrscheinlichkeit des handelsüblichen Sicherheitsbausteins K1 wird am Ende der Berechnung addiert ($2{,}31 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für die übrigen Subsysteme wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_d$: Für den Positionsschalter mit Zwangsöffnung B1 ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt des Positionsschalters B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden und 1 Stunde Zykluszeit ist für diese Komponenten n_{op}= 5 840 Zyklen/Jahr und $MTTF_d$ beträgt 1 712 Jahre für B1 bzw. 856 Jahre für 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. Insgesamt ergibt sich in beiden Subsystemen ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“).
- 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 (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 jeweils eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $5{,}16 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

8.2.35 Zweihandschaltung – Kategorie 4 – PL e (Beispiel 35)

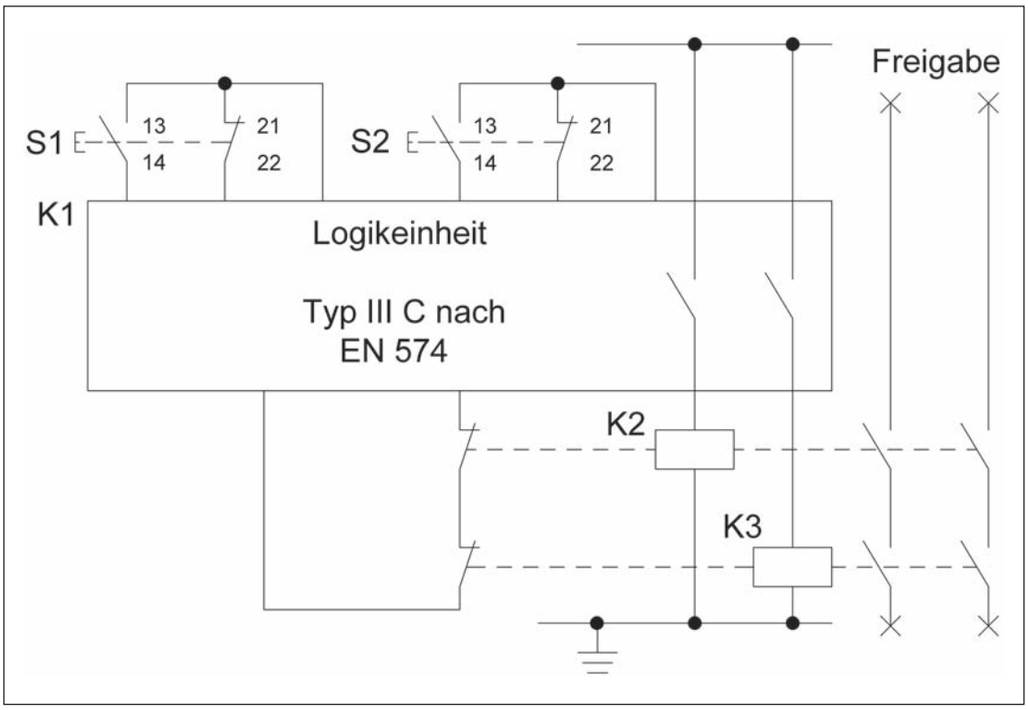


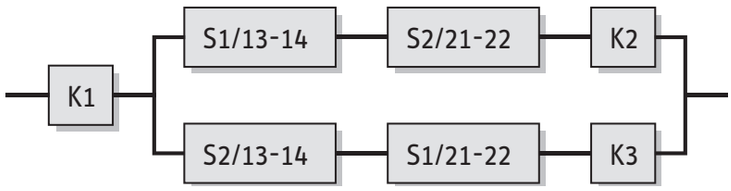
Abbildung 8.56: Zweihandschaltung, Signalverarbeitung durch eine Logikeinheit mit nachgeschalteten Hilfsschützen

Sicherheitsfunktion

- Ortsbindung der Hände des Bedieners 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) 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. Hinsichtlich mechanischer Fehler kann für diese Anwendung ein Fehlerausschluss bzgl. des Nichtöffnens des Öffnerkontakts erfolgen, wenn die Taster 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.
- 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, Abschnitt 8. Der Abstand 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.
- K2 und K3 besitzen zur Rücklesung zwangsgeführte Öffnerkontakte.

Bemerkung

- Anwendung z.B. an mechanischen Pressen (DIN EN 692)

Berechnung der Ausfallwahrscheinlichkeit

- K1 wird als Subsystem mit einer Ausfallwahrscheinlichkeit von $2{,}47 \cdot 10^{-8}$/Stunde [G] 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 20 000 000 Schaltspielen [H] angenommen. Da K2 und K3 ebenfalls Steuerströme schalten, gelten für K2 und K3 B_{10d}-Werte von je 20 000 000 Zyklen [N]. Bei 240 Arbeitstagen, 8 Arbeitsstunden und 20 Sekunden Zykluszeit ist für diese Komponenten n_{op} = 345 600 Zyklen/Jahr und $MTTF_d$ = 579 Jahre. 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 193 Jahren, gekürzt auf 100 Jahre („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 effektiven Testung. 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 (100 Jahre) und hohem DC_{avg} (99 %). Für die Kombination von S1, S2, K2 und K3 ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Wird ein Wert von $2{,}47 \cdot 10^{-8}$/Stunde [G] für K1 hinzuaddiert, so ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}94 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Unter Umständen ist zur Komplettierung der Sicherheitsfunktion zusätzlich die Ausfallwahrscheinlichkeit nachgeordneter Leistungselemente zu addieren.

Weiterführende Literatur

- DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte – Gestaltungsleitsätze (02.97). Beuth, Berlin 1997
- Recommendation for Use. Hrsg.: Vertikalgruppe 11 (VG 11) im europäischen Erfahrungsaustausch notifizierter Prüfstellen europa.eu.int/comm/enterprise/mechan_equipment/machinery/vertical_rfu.pdf. CNB/M/11.033/R/E Rev 05, S. 252, April 2006

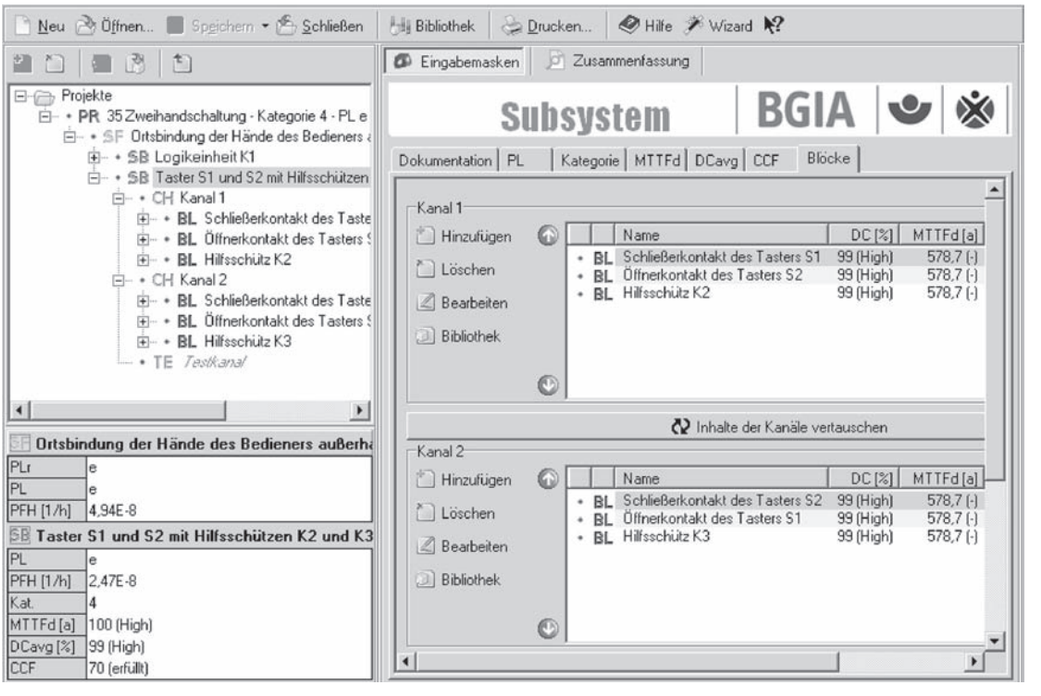


Abbildung 8.57: PL-Bestimmung mithilfe von SISTEMA

8.2.36 Verarbeitung von Signalen einer Lichtschranke – Kategorie 4 – PL e (Beispiel 36)

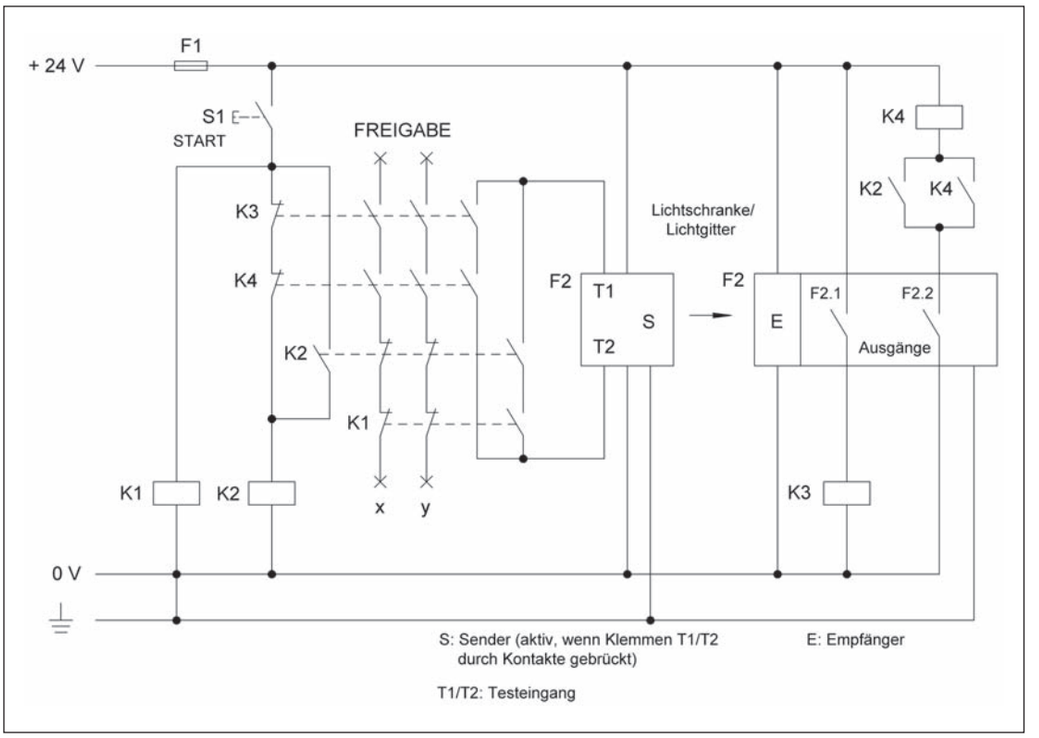


Abbildung 8.58: Elektromechanische Einbindung von sicherheitsrelevanten Signalen in die Maschinensteuerung am Beispiel einer Lichtschranke bzw. eines Lichtgitters

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Bleibende Stillsetzung einer gefahrbringenden Bewegung bei Zutritt zu einem Gefahrenbereich oder bei Eingriff in eine Gefahrenstelle sowie Anlauf- und Wiederanlaufsperre

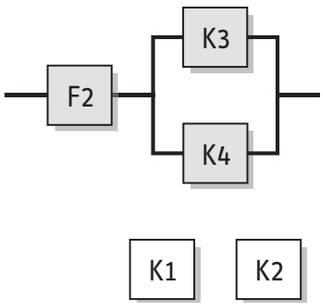
Funktionsbeschreibung

- Der Zutritt zu einem Gefahrenbereich oder Eingriff in eine Gefahrenstelle wird durch die Lichtschranke F2 detektiert. Die sicherheitsrelevanten Ausgangssignale der Lichtschranke (Schließer F2.1 und F2.2) entregen die in versetzter Spulenanordnung an die Spannungsversorgung angeschlossenen Hilfsschütze K3 und K4, die die Freigabesignale x und y sperren.

- Zur Aktivierung des Lichtschrankensenders werden bei betätigter Starttaste S1 die Testeingänge T1 und T2 zunächst über die dann angezogenen Hilfsschütze K1und K2 miteinander verbunden. K2 kann nur bei zunächst abgefallenen Hilfsschützen K3/K4 zum Anzug mit Selbsthaltung kommen. Bei geschlossener Lichtstrecke erfolgt dann auch der Anzug von K3 und K4. K4 gelangt nur über den Schließerkontakt von K2 zum Anzug mit Selbsthaltung. Mit dem Anzug von K3 und K4 ist bei noch betätigter Starttaste auch die Aktivierung des Lichtschrankensenders mit Selbsthaltung erfolgt, sodass die Starttaste losgelassen werden kann und mit dem Abfallen von K1 und K2 auch die Freigabepfade x und y geschlossen sind. Die Funktion der Anlaufsperre/Wiederanlaufsperre verhindert ein gültiges Freigabesignal nach einer Lichtstrahlunterbrechung oder nach einem Spannungsausfall mit darauf folgender Spannungswiederkehr so lange, bis nach einer erneuten Betätigung der Starttaste K3 und K4 wieder zum Anzug gelangen.

- Je ein Schließer von K3 und K4 ist sowohl in beiden Freigabepfaden als auch im Eingangskreis zur Aktivierung des Lichtschrankensenders (Testeingänge T1/T2) eingebunden. Mit dem Verbinden der Testeingänge erfolgt intern im Gerät eine Anlauftestung, z.B. durch eine definierte kurzzeitige Austastung des Lichtstrahls, die auf der Empfangsseite erwartungsgemäß nur innerhalb eines engen Zeitfensters als gültig bewertet wird. Bei erfolgreichem Anlauftest werden die Lichtschrankenausgänge frei geschaltet, im Störungs- bzw. Fehlerfall oder bei unterbrochener Lichtstrecke jedoch gesperrt.

- Fehler in den anderen Komponenten der Schaltung (Hilfsschütze, Ausgangskontakte der Lichtschranke, Starttaste), die in Kombination zum Verlust einer Sicherheitsfunktion führen könnten, werden nach einer Lichtstrahlunterbrechung während der Anlauf- bzw. Wiederanlauftestung aufgedeckt und verhindern eine erneute Freigabe.



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 K4 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Die Anzugsspannung der Hilfsschütze K3 und K4 muss größer als der halbe Wert der Spannungsversorgung gewählt werden, damit sich ein gleichzeitiger Anzug von K3 und K4 im Falle eines Kurzschlusses im Kabel (Reihenschaltung führt zur Spannungsaufteilung über den Schützspulen) auch in Kombination mit anderen Fehlern nicht gefahrbringend auswirken kann.
- Die Ausgangssignale der Lichtschranke F2 werden vom elektrischen Einbauraum des Empfängers gemeinsam in einem Kabel zusammen mit den Versorgungsleitungen zum elektrischen Einbauraum der Maschinensteuerung geführt. Durch Anwendung des Ruhestromprinzips und des Prinzips der versetzten Spulen (K3, K4) im geerdeten Steuerstromkreis werden alle im Kabel auftretenden Unterbrechungen, Erdschlüsse und Querschlüsse im aktivierten Zustand der Lichtschranke unmittelbar bemerkt (u.a. durch Ansprechen der Sicherung F1). Ein Kurzschluss, der die Überbrückung eines einzelnen Ausgangs bewirkt, wird spätestens nach dem Unterbrechen des Lichtstrahls der Lichtschranke beim erneuten Betätigen der Starttaste aufgedeckt. Daher ist gemeinsame Führung der Ausgangssignale innerhalb eines Kabels zulässig.
- Die Lichtschranke entspricht dem Typ 4 gemäß DIN EN 61496-1 und DIN CLC/TS 61496-2 sowie PL e.

Bemerkungen

- Wird die Schaltung in Anwendungen eingesetzt, bei denen die Lichtschranke sehr selten schaltet, so muss die Möglichkeit des Verlustes der Sicherheitsfunktion durch Fehlerhäufung (zwei einzeln unbemerkte Fehler) betrachtet werden. Periodische Prüfungen können einem solchen Verlust entgegenwirken.
- Angaben des Herstellers zur maximalen Schalthäufigkeit der Lichtschranke sind zu berücksichtigen.

Berechnung der Ausfallwahrscheinlichkeit

Es wird die Ausfallwahrscheinlichkeit der sicherheitsbezogenen Stoppfunktion, die auch im sicherheitsbezogenen Blockdiagramm dargestellt ist, berechnet. Werden die Kontakte der Freigabepfade x und y steuerungstechnisch weiterverarbeitet, so müssen diese zusätzlichen Steuerungsteile, z.B. Leistungsschütze, bei der Berechnung der Ausfallwahrscheinlichkeit berücksichtigt werden.

- Die Lichtschranke F2 liegt als handelsübliches Sicherheitsbauteil vor. Die Ausfallwahrscheinlichkeit $3{,}0 \cdot 10^{-8}$/Stunde [G] wird am Ende der Berechnung addiert.
- $MTTF_d$: Für K3 und K4 gilt wegen der unbekannten Lasten B_{10d} = 400 000 Zyklen [N]. Bei 220 Arbeitstagen, 8 Betriebsstunden/Tag und 120 Sekunden Zykluszeit beträgt n_{op} = 52 800 Schaltspiele/Jahr und damit die $MTTF_d$ 75 Jahre. Dies ist gleichzeitig die $MTTF_d$ pro Kanal („hoch“).
- DC_{avg}: DC = 99 % für K3 bis K4 ergibt sich aus der Einbindung der zwangsgeführten Öffnerkontakte in die Ansteuerung von K2. Dies entspricht gleichzeitig DC_{avg} („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte): Trennung (15), bewährte Bauteile (5), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Das Subsystem K3/K4 entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (75 Jahre) und hohem DC_{avg} (99 %). Dies ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $3{,}37 \cdot 10^{-8}$/Stunde. Die Gesamtausfallwahrscheinlichkeit wird durch Addition der Wahrscheinlichkeit gefährlicher Ausfälle von F2 ($3{,}0 \cdot 10^{-8}$/Stunde) ermittelt und beträgt $6{,}37 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Unter Umständen ist zur Komplettierung der Sicherheitsfunktion zusätzlich die Ausfallwahrscheinlichkeit nachgeordneter Leistungselemente zu addieren.

- Die verschleißbehafteten Elemente K3 und K4 sollten nach jeweils ca. sieben Jahren (T_{10d}) ausgetauscht werden.

Weiterführende Literatur

- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (IEC 60204-1:2005, modifiziert). Abschnitt 9.4.3: „Schutz gegen fehlerhaften Betrieb durch Erdschlüsse, Spannungsunterbrechungen und Verlust der elektrischen Durchgängigkeit“. Beuth, Berlin 2007

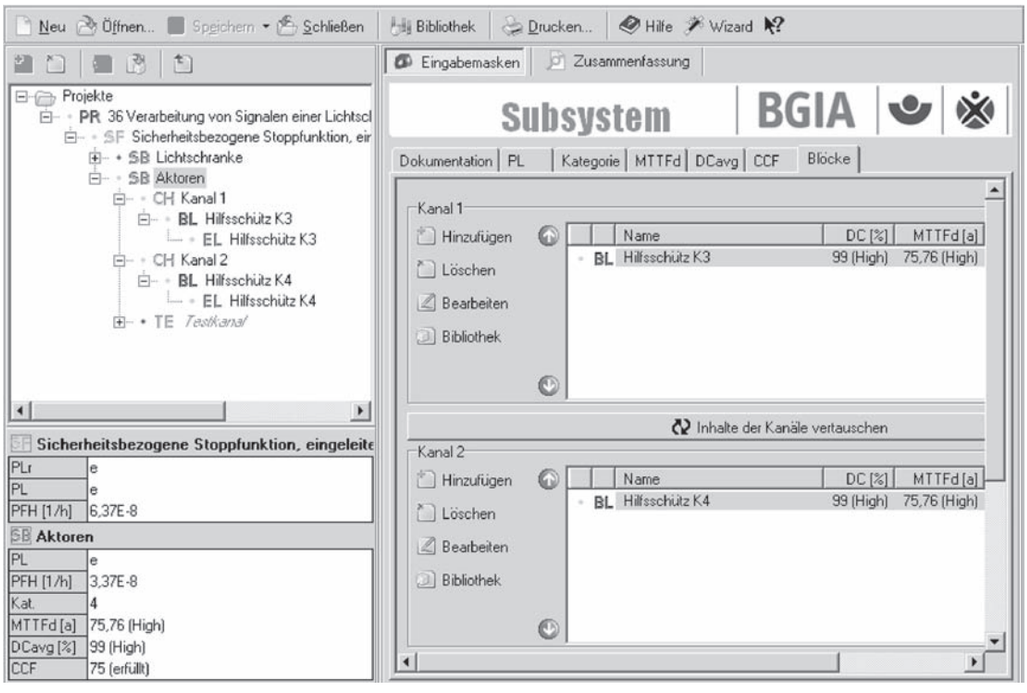


Abbildung 8.59: PL-Bestimmung mithilfe von SISTEMA

8.2.37 Planschneidemaschine mit programmierbar elektronischer Logiksteuerung – Kategorie 4 – PL e (Beispiel 37)

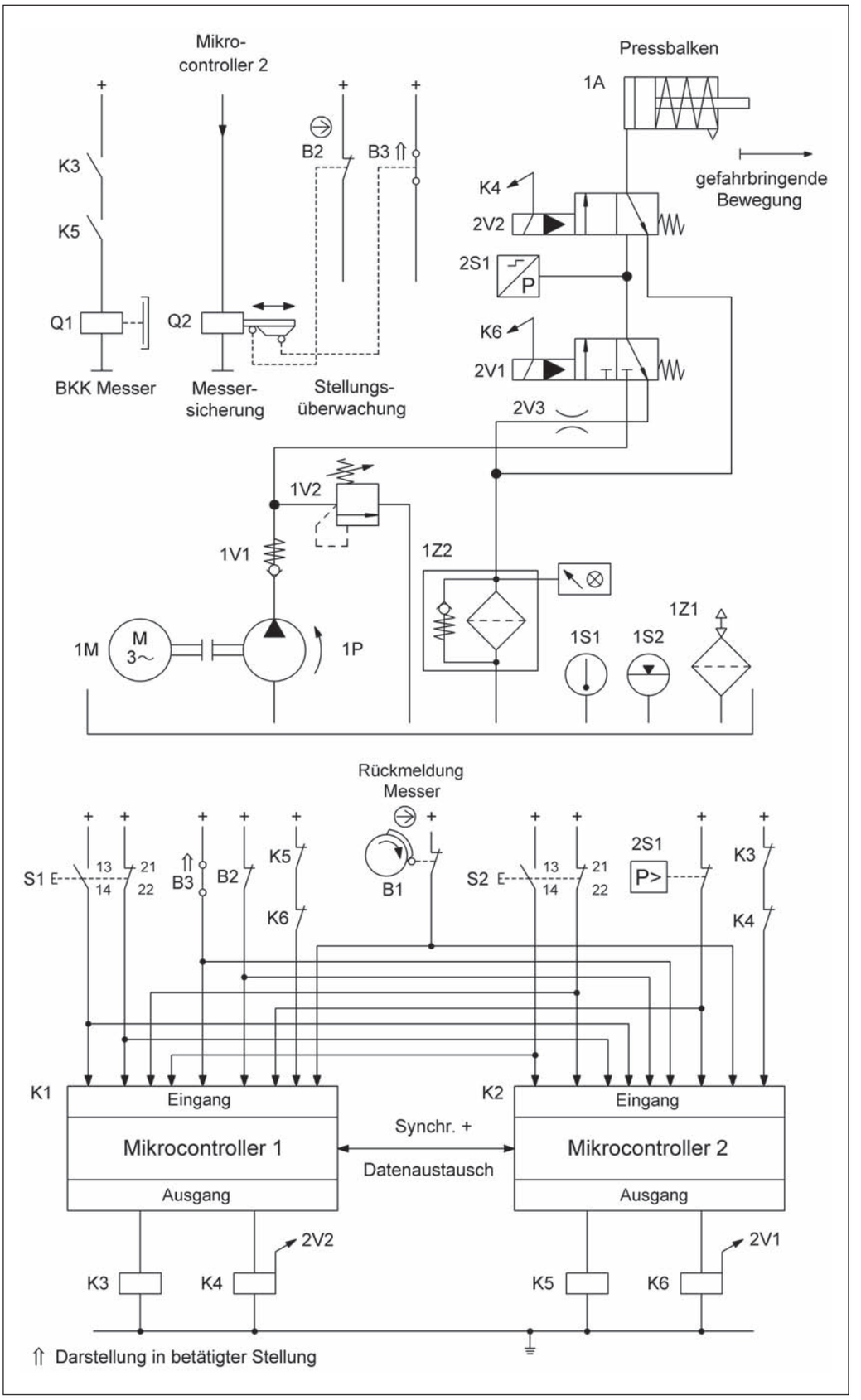
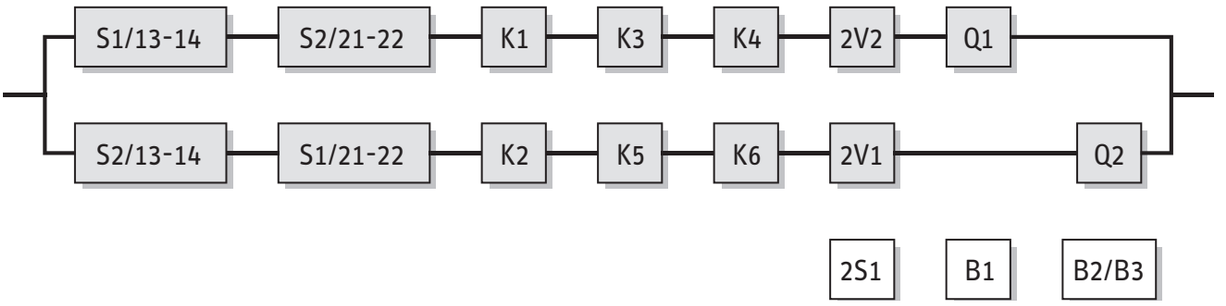


Abbildung 8.60: Ansteuerung eines elektrischen Messerantriebs und eines hydraulischen Pressbalkens



Sicherheitsfunktion

- Ortsbindung der Hände eines einzelnen Bedieners 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 wegen des definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) B_{10d}-Werte von je 2 000 000 Schaltspielen [H] 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 $MTTF_d$ = 1 736 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 die 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 den Überwachungselementen 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 $6{,}47 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

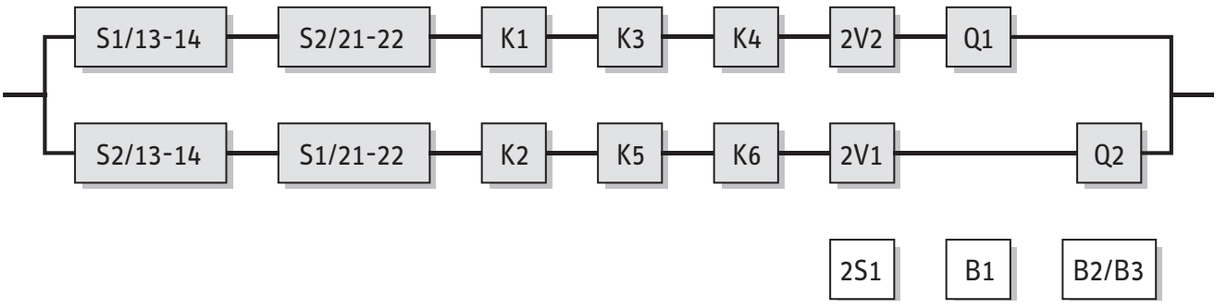
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für die verschleißbehafteten Elemente S1 und S2 ein Wert von über 17 Jahren (T_{10d}) für den vorgesehenen Austausch.

Weiterführende Literatur

- DIN EN 1010-3: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 3: Schneidemaschinen (12.02). Beuth, Berlin 2002

- DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze (02.97). Beuth, Berlin 1997

- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005



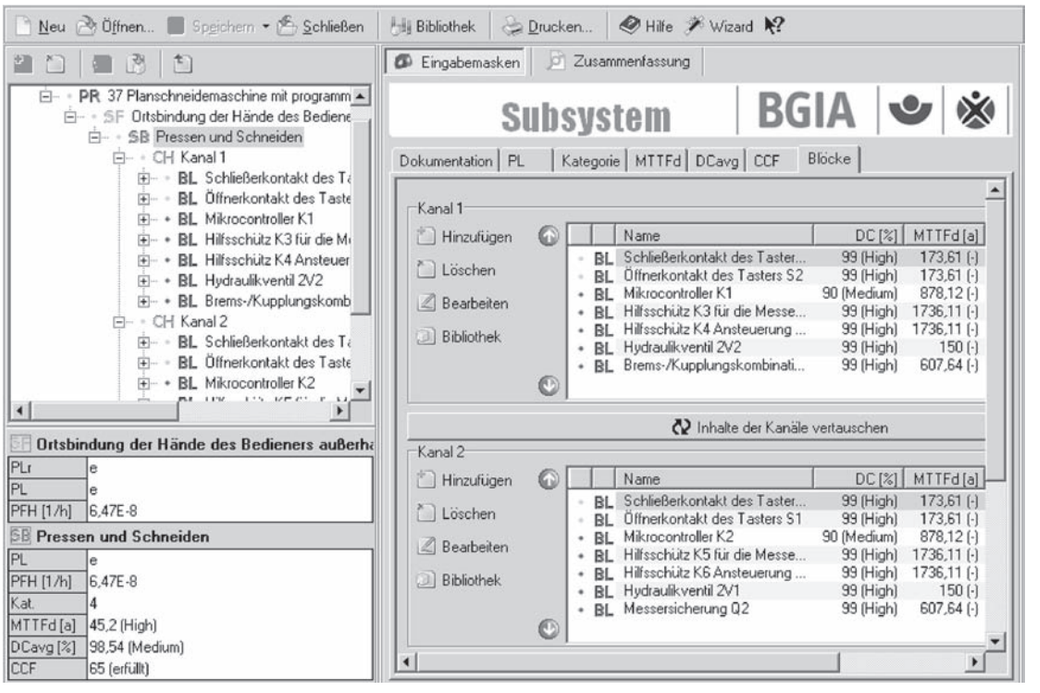


Abbildung 8.61:
PL-Bestimmung mithilfe von SISTEMA

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 Nr. L 207 (1998), S. 1; geänd. durch Richtlinie 98/79/EG - ABl. EG Nr. L 331 (1998), S. 1
http://eur-lex.europa.eu/

[2] DIN EN ISO 12100-1: Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 1: Grundsätzliche Terminologie, Methodologie (04.04). Beuth, Berlin 2004

[3] DIN EN ISO 12100-2: Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 2: Technische Leitsätze (04.04). Beuth, Berlin 2004

[4] DIN EN ISO 14121-1: Sicherheit von Maschinen – Risikobeurteilung – Teil 1: Leitsätze (12.07). Beuth, Berlin 2007

[5] ISO/TR 14121-2: Sicherheit von Maschinen – Risikobeurteilung – Teil 2: Praktische Anleitung und Verfahrensbeispiele (12.07). Beuth, Berlin 2007

[6] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (07.07). Beuth, Berlin 2007

[7] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (12.03). Beuth, Berlin 2003

[8] 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 Nr. L 157 (2006), S. 24; mit Berichtigung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG vom 9. Juni 2006. ABl. EU Nr. L 76 (2007), S. 35
http://eur-lex.europa.eu/

[9] *Ostermann, H.-J.; von Locquenghien, D.:* Wegweiser Maschinensicherheit. Bundesanzeiger Verlagsgesellschaft, Köln 2007

[10] *Reudenbach, R.:* Sichere Maschinen in Europa – Teil 1: Europäische und nationale Rechtsgrundlagen. 8. Aufl., Verlag Technik & Information, Bochum 2007

[11] DIN EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (03.97). Beuth, Berlin 1997

[12] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 0 bis Teil 7 (11.02 bis 10.05). Beuth, Berlin 2002 bis 2005

[13] DIN EN 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (10.05 und Berichtigung 1 06.06). Beuth, Berlin 2005

[14] *Bömer, T.:* Funktionale Sicherheit nach IEC 61508. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 219. 47. Lfg. XII/2005. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/330219

[15] *Hauke, M.; Schaefer, M.:* Sicherheitsnorm mit neuem Konzept. O + P Ölhydraulik und Pneumatik 50 (2006) Nr. 3, S. 142-147
www.dguv.de/bgia/de/pub/grl/pdf/2006_016.pdf

[16] *Schaefer, M.; Hauke, M.:* Performance Level Calculator – PLC. 3. Aufl. Hrsg.: BGIA – Institut für Arbeitsschutz 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 2008
www.dguv.de/bgia, Webcode d3508

[17] Summary list of titles and references of harmonised standards under Directive 98/37/EC on Machinery. Hrsg.: European Commission
http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist/machines.html

[18] *Reinert, D.:* Risikobezogene Auswahl von Steuerungen. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 320 100. 31. Lfg. I/98. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/320100

[19] DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

[20] DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

[21] Interpretationen zu Vorschriften: Wesentliche Veränderung von Maschinen. Hrsg.: Berufsgenossenschaft der chemischen Industrie (06/2005)
www.bgchemie.de/webcom/show_article.php/_c-781/_nr-2/i.html

[22] *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/bgia, Webcode d6303

[23] Berufsgenossenschaftliche Information BGI 5048-1 und -2: Ergonomische Maschinengestaltung, Checkliste, Auswertungsbogen und Merkheft (10.2006). Carl Heymanns, Köln 2006
www.dguv.de/bgia, Webcode d3443

[24] VDI/VDE 3850 Blatt 1: Nutzergerechte Gestaltung von Bediensystemen von Maschinen (5/2000). Blatt 2: Nutzergerechte Gestaltung von Bediensystemen von Maschinen – Interaktionsgeräte für Bildschirme (11/2002). Blatt 3: Nutzergerechte Gestaltung von Bediensystemen für Maschinen – Dialoggestaltung für Touchscreens (3/2004). Beuth, Berlin

[25] *Birolini, A.:* Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management. 3. Aufl., Springer, Berlin 1991

[26] 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

[27] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (06.03). Beuth, Berlin 2006

[28] Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Hrsg.: Fachausschuss Elektrotechnik, Köln 2002
www.dguv.de/bgia, Webcode d14884

[29] DIN EN 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2007) (11.08). Beuth, Berlin 2008

[30] *Reinert, D.; Schaefer, M.:* Sichere Bussysteme für die Automation. Hüthig, Heidelberg 2001

[31] *Huckle, T.:* Kleine BUGs, große GAUs. Vortrag zum Thema „Softwarefehler und ihre Folgen“.
http://www5.in.tum.de/~huckle/bugsn.pdf

[32] DIN EN 61508-3: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998 und Corrigendum 1999) (12.02). Beuth, Berlin 2002

[33] DIN EN 61131-3: Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (12.03). Beuth, Berlin 2003

[34] *Schaefer, M.; Gnedina, A.; Bömer, T.; Büllesbach, K.-H.; Grigulewitsch, W.; Reuß, G.; Reinert, D.:* Programmierregeln für die Erstellung von Software für Steuerungen mit Sicherheitsaufgaben. Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Dortmund, Fb 812. Wirtschaftsverlag NW, Bremerhaven 1998 (vergriffen, auszugsweise unter:
www.dguv.de/bgia, Webcode d3250

[35] MISRA Development Guidelines for Vehicle Based Software. Hrsg.: The Motor Industry Software Reliability Association
www.misra.org.uk

[36] SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Hrsg.: Siemens AG, Center for Quality Engineering, München 1994 bis 2005

[37] DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze (02.97). Beuth, Berlin 1997

[38] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005

[39] Norm-Entwurf DIN IEC 61508-2; VDE 0803-2:2006-07: Funktionale Sicherheit sicherheitsbezogener eletrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (07.06). Beuth, Berlin 2006

[40] *Kleinbreuer, W.; Kreutzkampf, F.; Meffert, K.; Reinert, D.:* Kategorien für sicherheitsbezogene Steuerungen nach EN 954-1. BGIA-Report 6/97. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 1997
www.dguv.de/bgia, Webcode d15190

[41] DIN EN 982: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Hydraulik (09.96). Beuth, Berlin 1996

[42] DIN EN 983: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Pneumatik (09.96). Beuth, Berlin 1996

[43] DIN EN 1037: Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf (04.96), Beuth, Berlin 1996

[44] DIN ISO 1219-1: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 1: Graphische Symbole für konventionelle und datentechnische Anwendungen (12/07). Beuth, Berlin 2007

[45] DIN ISO 1219-2: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 2: Schaltpläne (11.96). Beuth, Berlin 1996

[46] ISO 8573-1: Druckluft – Teil 1: Verunreinigungen und Reinheitsklassen (02.01). Beuth, Berlin 2001

[47] ISO 8573-1: Druckluft – Teil 1: Verunreinigungen und Reinheitsklassen; Korrektur 1 (04.02). Beuth, Berlin 2002

Anhang A:
Beispiele zur Risikobeurteilung

Beispiel 1: Schließkantensicherung

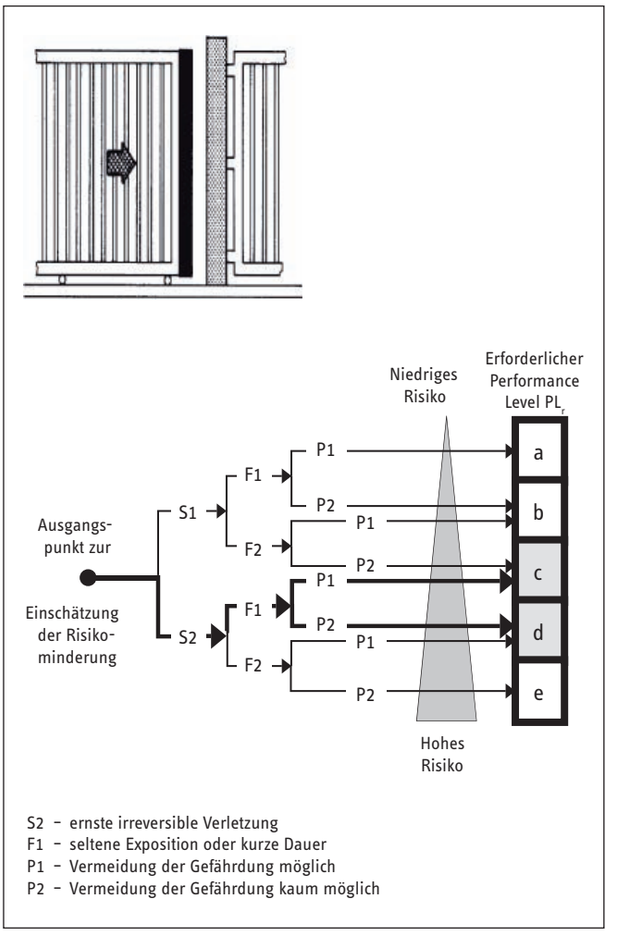
In Abbildung A.1 ist die Risikobeurteilung für die Sicherheitsfunktion

- SF1 Unterbrechung der Schließbewegung und Reversieren

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 und auch nur für kurze Zeit 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. Bei Schnelllauftoren ist diese Möglichkeit eingeschränkt (P2) und es ergibt sich ein erforderlicher Performance Level PL_r = d.

Abbildung A.1:
Risikobeurteilung für die Schließkantensicherungen an kraftbetätigten Fenstern, Türen und Toren



[1] *Schließkantensicherungen fielen bisher unter die Bauproduktrichtlinie. Da die eingesetzten Schaltleisten jedoch Sicherheitsbauteile nach der Maschinenrichtlinie sind, werden auch Schließkantensicherungen nach dieser Richtlinie bewertet.*

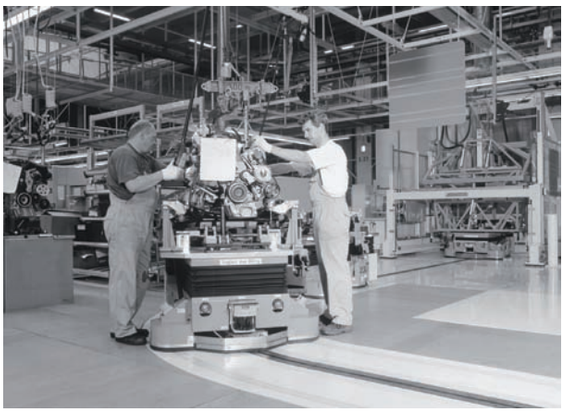
Beispiel 2: Fahrerloses Transportfahrzeug

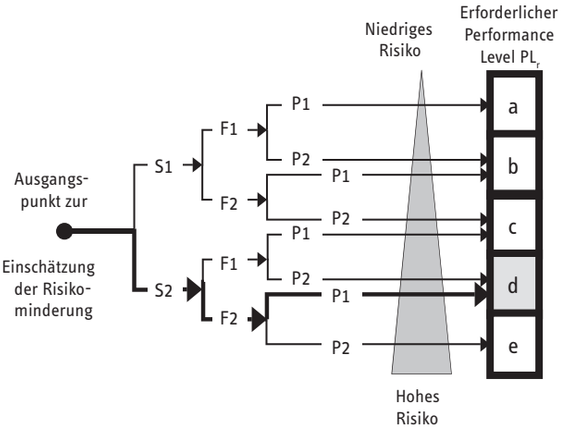
An fahrerlosen Transportfahrzeugen wird für den Auffahrschutz die Sicherheitsfunktion

- SF1 Stillsetzen des Transportfahrzeugs

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 gerechnet werden (F2). Da das Fahrzeug mit recht niedriger Geschwindigkeit fährt (in der Regel 3 bis 5 km/h), hat ein Fußgänger 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)

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

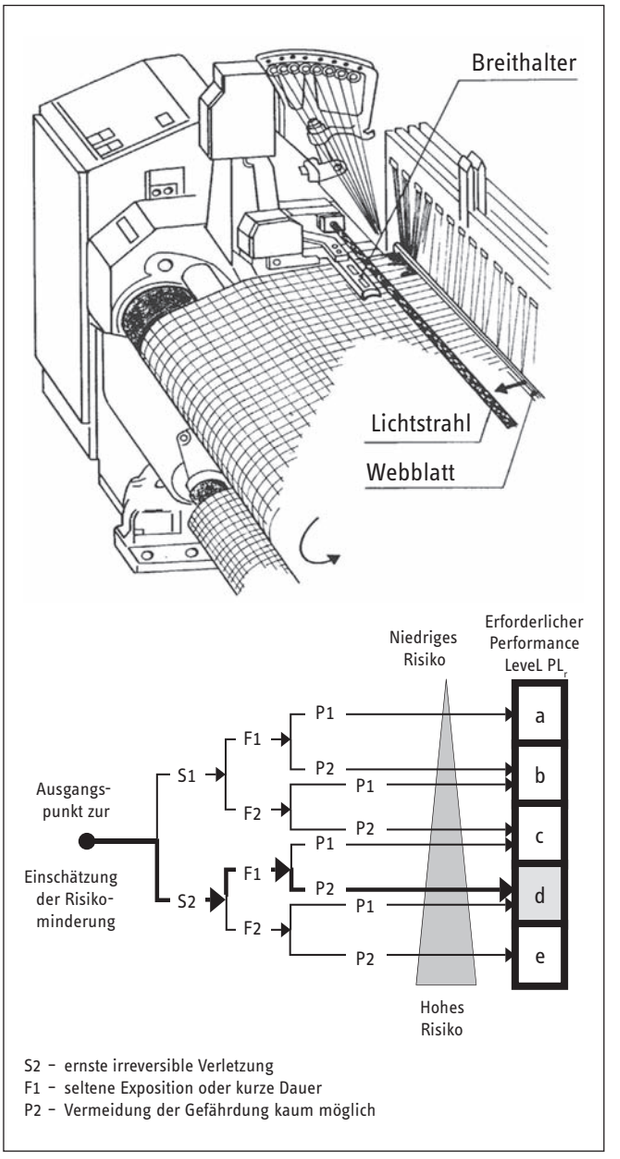
Beispiel 3: Webmaschine

Webmaschinen werden zum vollautomatischen Weben von Stoffen eingesetzt. Die wesentliche Gefährdung besteht in der Quetschung zwischen Webblatt und Breithalter. Bei Kettfadenbrüchen muss der Weber bei stehender Maschine in die Gefahrenstelle eingreifen, um die Kettfadenenden wieder zu verbinden. Zur Verhinderung des unerwarteten Anlaufs wird die Sicherheitsfunktion

- SF1 Sicher abgeschaltetes Moment

eingesetzt. Bei einem Maschinenanlauf kann der Weber Fingerquetschungen und -brüche davontragen (S2). Die Häufigkeit bzw. Dauer der Gefährdungsexposition kann mit selten bezeichnet werden (F1). Befindet sich der Weber mit den Händen 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).

Abbildung A.3:
Risikobeurteilung für eine Webmaschine



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.

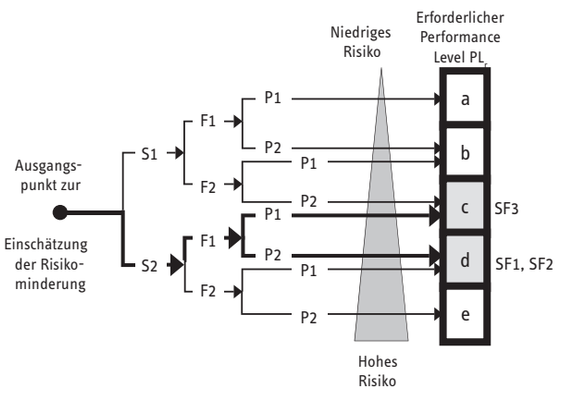
Ein Einzug zwischen die Zylinder führt zu schweren Verletzungen (S2). Da Tätigkeiten im Gefahrenbereich nur zu Wartungsarbeiten anfallen, kann die Häufigkeit bzw. Dauer der Gefährdungsexposition mit selten bezeichnet werden (F1). Die Möglichkeit, der gefahrbringenden Bewegung auszuweichen, ist bei Produktionsgeschwindigkeiten 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 nur dann verwendet werden, wenn die Druckmaschine zuvor stillgesetzt (SF1) und die zulässige Zylinderdrehzahl begrenzt wurde (SF2). Damit sind die möglichen Maschinenbewegungen für den Bediener überschaubar und er kann den gefahrbringenden Bewegungen ausweichen (P1). Für SF3 ist daher ein erforderlicher Performance Level PL_r = c ausreichend (siehe Abbildung A.4). Wie man diese Sicherheitsfunktionen realisieren kann, ist in Kapitel 8 im Beispiel 24 auf Seite 160 ff. beschrieben.

Die Beispiele 1 bis 3 sind dem BGIA-Handbuch [1] entnommen, in dem sich zahlreiche weitere Anwendungen aus dem Maschinenschutz finden.

Literatur

[1] BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de

Abbildung A.4:
Risikobeurteilung an einer Rotationsdruckmaschine



S2 – ernste irreversible Verletzung
F1 – seltene Exposition oder kurze Dauer
P1 – Vermeidung der Gefährdung möglich
P2 – Vermeidung der Gefährdung kaum möglich

Anhang B:
Sicherheitsbezogenes Blockdiagramm und FMEA

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* (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).

B1 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: Shut-Down-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.

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 sinnigerweise 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 noch 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, und 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, (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) 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].

B2 Zweck und Eigenart einer FMEA für die Quantifizierung

Für den quantitativen Nachweis des PL muss die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (*PFH*) 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].

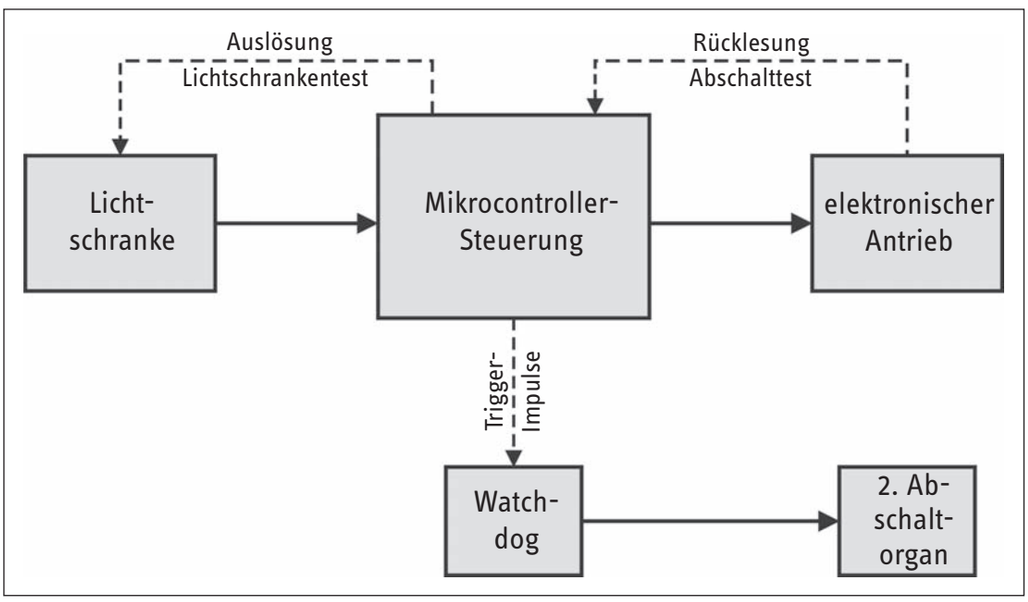


Abbildung B.1: Beispiel für das sicherheitsbezogene Blockdiagramm einer einkanaligen Maschinensteuerung in Kategorie 2

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* bzw. des PL einfließen.

B2.1 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 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.

B2.2 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 weniger weitere Ausfälle ausreichen, 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 dann, 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

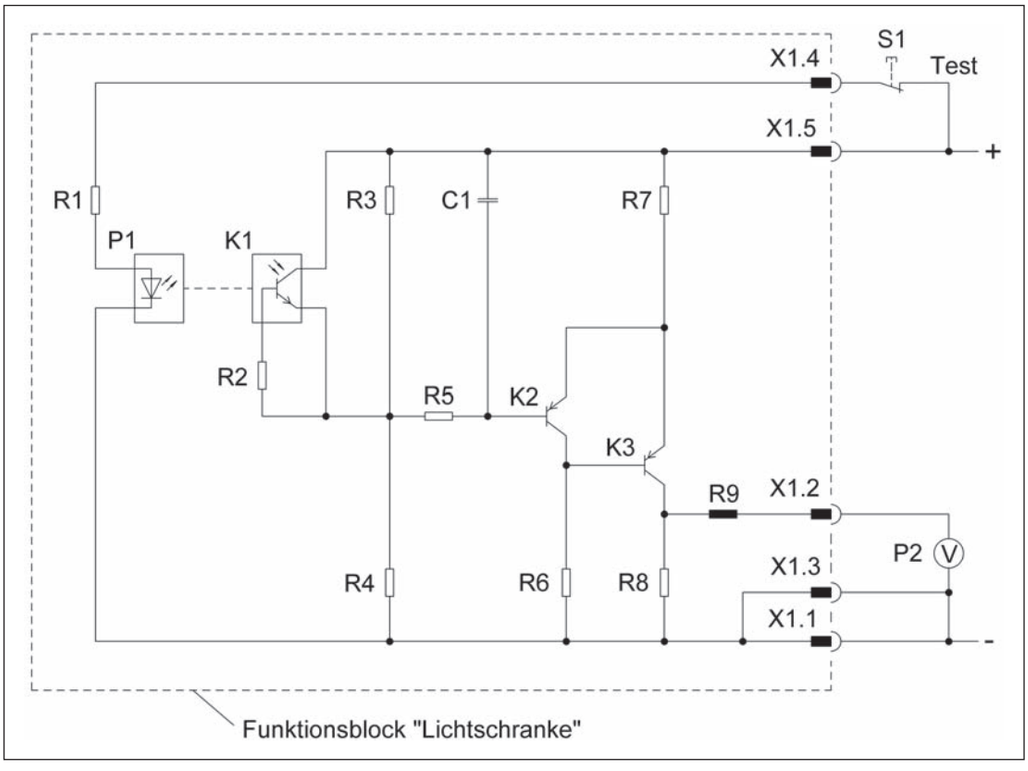


Abbildung B.2: Angenommene Schaltung (einfaches Beispiel) des Funktionsblocks „Lichtschranke“ aus dem sicherheitsbezogenen Blockdiagramm nach Abbildung B.1

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“.

B2.3 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_{10}-Werten abgeleitet werden können (siehe Tabelle D.2 dieses Reports).

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].

B2.4 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 und 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 FIT = 10^{-9}/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 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 (s.o.). Nach der „reinen Lehre“ müsste dies in zwei Schritten geschehen: Die Gesamtausfallrate wird zuerst auf die verschiedenen Ausfallarten (z.B. Unterbrechung, Kurzschluss, Drift, Funktionsänderung) verteilt. 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 der Praxis liegen oft keine oder nur widersprüchliche Angaben zur Ausfallartenverteilung von Bauelementen vor. Daher bietet sich der in Abbildung B.3 beschrittene pragmatische Weg an, nur zu prüfen, 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).

Abbildung B.3:

Sinnvolle Ausführungsform einer FMEA-Tabelle für den Funktionsblock „Lichtschranke“ aus Abbildung B.2

Bezeichnung des Funktionsblocks:	Lichtschranke
Gefährliche Ausfallrichtung des Funktionsblocks:	Anliegen 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): 9 905,9 *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.*

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 hohe 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.

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 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 ergibt 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.

B3 „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 (vgl. [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. 2nd ed. Hrsg.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina 1998

[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, Center for Quality Engineering, München 1994-2005

[4] IEC/TR 62380 (ehemals UTE C 80-810): 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 2: Reliability Prediction Procedure for Electronic Equipment. Hrsg.: Telcordia Technologies Inc., Piscataway, New Jersey

[6] 217Plus (Nachfolgeprodukt für das „MIL-Handbook 217F“) Hrsg.: Reliability Information Analysis Center (RIAC), Utica, New York, 2006

[7] DIN EN IEC 61709: Bauelemente der Elektronik, Zuverlässigkeit, Referenzbedingungen für Ausfallraten und Beanspruchungsmodelle zur Umrechnung (1/1999). Beuth, Berlin 1999

[8] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für DIN EN 61508-2 und DIN EN 61508-3; Anhang C. (6/2003). Beuth, Berlin 2003

Anhang C:
Fehlerlisten, Fehlerausschlüsse und Sicherheitsprinzipien

C1 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 61496-1 [2], Anhang B, oder DIN EN 60947-5-3 [3], Anhang A, sind ebenfalls Fehlerlisten (hier jeweils für elektrische Bauelemente) mit teilweise geringfügigen Abweichungen zur DIN EN ISO 13849-2 vorhanden.
Der Beitrag 340 220 [4] erläutert Hintergründe und das Zustandekommen der Fehlerlisten (Nachdruck am Ende dieses Anhangs).

C2 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 neue 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. Diese Aspekte werden bei der anstehenden Überarbeitung der Norm als Änderungsvorschläge eingebracht.

C2.1 Beispiele für Fehlerausschlüsse an Bauteilen

C2.1.1 Bauteile der Fluidtechnik

Für pneumatische und hydraulische Bauteile sind häufig vergleichbare Fehlerausschlüsse formuliert. Es sind jedoch 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.

C2.1.2 Elektrische Bauteile

- Optokoppler

  DIN EN ISO 13849-2, Tabelle D.20, gibt an, dass die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs“ unter folgenden Voraussetzungen ausgeschlossen werden: *„Das verwendete Basismaterial sollte nach IEC 60249 und die Kriech- und Luftstrecken sollten mindestens nach IEC 60664:1992, Verschmutzungsgrad 2/Einsatzklasse III bemessen sein.“*

  Hier handelt es sich offensichtlich um eine fehlerhafte Zuordnung von Anforderungen im Rahmen der Normerstellung. Daher verwendet das BGIA als notifizierte Prüfstelle in der Praxis die beiden folgenden Anforderungen für die Formulierung eines Fehlerausschlusses, die auch in IEC 61800-5-2 [5] übernommen wurden:

  - Der Optokoppler ist aufgebaut in Übereinstimmung mit Überspannungskategorie III gemäß IEC 60664-1:1992, Tabelle 1. Wird eine SELV/PELV-Spannungsversorgung verwendet, genügt Verschmutzungsgrad 2/Überspannungskategorie II.

  - Es müssen Maßnahmen vorhanden sein, die sicherstellen, dass ein interner Ausfall des Optokopplers nicht zu einer erhöhten Temperatur seines Isoliermaterials führen kann.

- Leiterplatte/bestückte Leiterplatte

  Die Fehlerannahme „Kurzschluss zwischen benachbarten Leiterbahnen/Kontaktstellen“ kann nach Norm ausgeschlossen werden, sofern folgende Voraussetzungen zutreffen:

  - Als Leiterplatte wird Basismaterial nach IEC 60249 verwendet.

  - Kriech- und Luftstrecken werden bemessen nach IEC 60664-1:1992 nach Verschmutzungsgrad 2/Überspannungskategorie III.

  - In der Praxis auch akzeptiert: Entspricht die Spannungsversorgung den Anforderungen an SELV/PELV, genügt zur Dimensionierung der Kriech- und Luftstrecken Verschmutzungsgrad 2/Überspannungskategorie II. Ein Minimalabstand von 0,1 mm darf jedoch nicht unterschritten werden.

  - 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.

- Zu dem Fehlerausschluss „Kurzschluss“ ist aus heutiger Sicht anzumerken, dass beim Einsatz bleifreier Lötprozesse und Bauteile das mögliche Entstehen nadelförmiger Zinn-Whisker berücksichtigt werden muss. Zinn-Whisker sind leitfähig, bis zu mehrere 100 µm lang und können zu einem Kurzschluss zwischen Leiterbahnen bzw. Anschlüssen führen. Daher muss das Risiko des Wachstums solcher Whisker bewertet werden. Bei zu hohem Risiko darf der Fehlerausschluss nicht erfolgen. Die Quellen [6] und [7] können bei der Bewertung hilfreich sein.

- Leitungen/Kabel

  Die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Leitern“ kann unter folgenden Voraussetzungen ausgeschlossen werden: Die Leiter sind

  - dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt (z.B. durch Kabelkanal, Panzerrohr) oder

  - in unterschiedlichen Mantelleitungen verlegt oder innerhalb eines elektrischen Einbauraumes verlegt unter der Voraussetzung, dass sowohl die Leitungen als auch der Einbauraum den jeweiligen Anforderungen entsprechen, siehe EN 60204-1 oder

  - einzeln durch eine Erdverbindung geschützt.

- 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: Dieser Fehlerausschluss gilt nur für den elektrischen Teil des Schalters (es handelt sich um einen Fehlerausschluss aus der Fehlerliste zur Elektrik). Der mechanische Teil des Schalters – z.B. der an der Schutztür montierte getrennte Betätiger für einen Bauart-2-Schalter, das Anfahrlineal für einen Bauart-1-Schalter oder die Mechanik innerhalb des Schalters – muss zusätzlich betrachtet werden. Daher sind im Teil 1 der DIN EN ISO 13849 in Tabelle C.1 auch trotz dieses „elektrischen“ Fehlerausschlusses B_{10d}-Werte angegeben.

C3 Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien werden in den Tabellen A.1, B.1, C.1 und D.1 (einschließlich D.2) der informativen Anhänge der DIN EN ISO 13849-2 behandelt.

C3.1 Allgemein für alle Technologien

- Anwendung geeigneter Werkstoffe und 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.

C3.2 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.

C3.3 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.

C3.4 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 die SRP/CS bei fehlerhaftem Programmablauf in einen definierten sicheren Zustand bringen können muss.

C4 Bewährte Sicherheitsprinzipien

Die Tabellen A.2, B.2, C.2 und D.3 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.

C4.1 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.

C4.2 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.

C4.3 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. Der 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.

C4.4 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 sogenannte 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 entsprechender BGIA-Report [8]. Abhängig von der Anwendung können auch „Fehlererkennung durch den Prozess“ und „Fehlererkennung durch Vergleich zwischen Kanälen“ als bewährte Sicherheitsprinzipien gelten.

C5 Bewährte Bauteile

Bewährte Bauteile für Mechanik und Elektrik werden in den Tabellen A.3 und D.4 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.

C5.1 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 [9] berücksichtigt werden.

C5.2 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 982 [10] und DIN EN 983 [11] ab.

Sicherheitstechnisch bewährte Bauteile können z.B. sein:

- Wegeventile, Sperrventile und Druckventile

C5.3 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 [12; 13]. 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 [14]. Den Geräten gemeinsam ist die Ausrüstung mit zwangsöffnenden Hilfsstromschaltern zur Energieunterbrechung nach Anhang K in DIN EN 60947-5-1 [15]. 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.

- 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, Anhang K, [15] entsprechen.

- Weitere nicht komplexe und nicht programmierbare Bauteile, deren Ausfallarten vorhersehbar sind. Beispiele sind passive Bauteile, Widerstände, Dioden, Transistoren, Thyristoren, Operationsverstärker und Spannungsregler.

Literatur

[1] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (12.03). Beuth, Berlin 2003

[2] DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (01.05). Beuth, Berlin 2005

[3] DIN EN 60947-5-3: Niederspannungsschaltgeräte – Teil 5-3: Steuergeräte und Schaltelemente – Anforderungen für Näherungsschalter mit definiertem Verhalten unter Fehlerbedingungen (PDF) (11.05). Beuth, Berlin 2005

[4] *Bömer, T.; Grigulewitsch, W.; Kühlem, W.; Meffert, K.; Reuß, G.:* Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Kennzahl 340 220. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 48. Lfg. V/06. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitsschutz - BGIA, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/340220

[5] DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

[6] Test method for measuring whisker growth on tin and tin alloy surface finishes, JESD22A121.01. Hrsg.: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2005 www.jedec.org/download/search/22a121-01.pdf

[7] Environmental acceptance requirements for tin whisker susceptibility of tin and tin alloy surface finishes, JESD201. Hrsg.: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2006 www.jedec.org/download/search/JESD201.pdf

[8] *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/bgia, Webcode d6163

[9] ISO 4960: Kaltband aus unlegierten Stählen mit Kohlenstoffgehalten über 0,25 % (07.99). Beuth, Berlin 1999 (in Überarbeitung)

[10] DIN EN 982: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Hydraulik (09.96). Beuth, Berlin 1996

[11] DIN EN 983: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Pneumatik (09.96). Beuth, Berlin 1996

[12] DIN EN 60269-1: Niederspannungssicherungen – Teil 1: Allgemeine Anforderungen (11.05). Beuth, Berlin 2005

[13] DIN EN 60127-1: Geräteschutzsicherungen – Teil 1: Begriffe für Geräteschutzsicherungen und allgemeine Anforderungen an G-Sicherungseinsätze (02.07). Beuth, Berlin 2007

[14] DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (03.07). Beuth, Berlin 2007

[15] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005

BGIA

Sicherheitstechnisches Informations- und Arbeitsblatt

Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten –

1 Einleitung

Für technische Einrichtungen, an denen beim Versagen einer Steuerung oder Schutzeinrichtung Personen zu Schaden kommen können, gelten besondere Sicherheitsanforderungen bezüglich des Verhaltens im Fehlerfall. Beispiele hierfür sind aus technischen Regeln und Normen unterschiedlicher technischer Bereiche bekannt, zum Beispiel aus der Maschinen- und Anlagentechnik, der Verkehrs- und Transporttechnik, der Medizintechnik und der Energietechnik. Auch die Maschinenrichtlinie [1] fordert, dass Steuerungen insbesondere so konzipiert und gebaut sein müssen, dass Fehler in der Logik zu keiner gefährlichen Situation führen.

Welche Auswirkungen Fehler in sicherheitsrelevanten Steuerungen haben können, zeigt das sicherheitstechnische Informations- und Arbeitsblatt 330 250 dieses Handbuches [2].

Die in den technischen Regeln, Unfallverhütungsvorschriften und Normen formulierten Sicherheitsanforderungen hängen sehr stark von der jeweiligen Anwendung ab. Sie reichen im einfachsten Fall von organisatorischen Maßnahmen, wie regelmäßige, willensabhängige Funktionsprüfungen, über automatische Testschaltungen bis hin zu so genannten selbstüberwachten Steuerungen, bei denen sich Fehler selbsttätig bemerkbar machen. Der Begriff Fehlerbetrachtung bezeichnet die Gesamtheit der Überlegungen, die notwendig sind, um das sicherheitstechnische Verhalten einer Einrichtung im Fehlerfall zu beschreiben und auch praktisch zu überprüfen. Eine der wichtigsten Fragen im Rahmen der Fehlerbetrachtung ist, welche Fehler an Bauelementen unterstellt werden müssen. Eine solche Fehlervereinbarung ist notwendig, um dem Entwickler verbindliche Kriterien für den Entwurf seines steuerungstechnischen Sicherheitskonzepts zu liefern. Andererseits soll mit dieser Fehlervereinbarung gewährleistet werden, dass verschiedene Prüfstellen und Prüfer beim gleichen Prüfobjekt nicht zu unterschiedlichen Ergebnissen gelangen.

Welche Fehler sind nun in eine solche Fehlerliste aufzunehmen? Würde man alle theoretisch denkbaren Fehler eines Bauelementes bei der Fehlerbetrachtung unterstellen, so gäbe dies nicht nur einen extrem hohen Prüfaufwand, teilweise wäre die Prüfung überhaupt nicht mehr durchführbar. Hinweise auf unterstellte Fehler und Fehlerausschlüsse hat es in der Vergangenheit in vielen Anwendungsbereichen gegeben, z. B. in der Eisenbahnsignaltechnik. Diese Fehlerlisten waren jedoch nur bedingt auf allgemeine industrielle Anwendungen übertragbar und widersprachen sich sogar teilweise in Detailfestlegungen. In den meisten Normen und Sicherheitsregeln waren jedoch keine Aussagen enthalten, welche Fehler bei der Fehlerbetrachtung konkret zu unterstellen sind.

2 Anforderungen an eine Fehlerliste

Um für steuerungstechnische Sicherheitsprüfungen immer gleiche Voraussetzungen zu schaffen, hat das *Berufsgenossenschaftliche Institut für Arbeitsschutz – BGIA* die bei Prüfungen zugrunde gelegten Fehlerarten elektrischer, hydraulischer und pneumatischer Bauelemente zusammengestellt und in diesem Handbuch in den Jahren 1987 und 1990 veröffentlicht. Diese Zusammenstellungen für den industriellen Maschinen- und Anlagenbau wurden im Laufe der Zeit mehrfach überarbeitet und um Hinweise aus der einschlägigen Literatur und den Technischen Regeln ergänzt. Die Listen – auch schon vor ihrem Erscheinen seit vielen Jahren in der Prüfpraxis erprobt – stellen einen Kompromiss verschiedener, teilweise widersprüchlicher Anforderungen dar, die nachstehend erläutert werden:

Hoher Fehlerabdeckungsgrad

Die bei der Fehlerfallprüfung unterstellten Fehler sollten möglichst viele aller möglichen Fehler abdecken. Je höher der Fehlerabdeckungsgrad, desto geringer ist das Risiko, unter Umständen gefährliche Fehlerarten zu übersehen.

Durchführbarkeit

Je komplexer ein Bauelement, desto größer ist die Vielfalt der möglichen Fehler. So enthielt beispielsweise der Entwurf allgemeiner Richtlinien für signaltechnisch sichere Schaltungen und Einrichtungen der Elektronik allein für einen Transistor bereits 51 Fehlerarten; bei einfachen integrierten Schaltkreisen ergibt sich schon eine astronomisch hohe Zahl unterschiedlicher Fehlermöglichkeiten. Zur Durchführung der Fehlerfallprüfung müssen deshalb die theoretisch möglichen Fehlerarten eingeschränkt werden. Gleichzeitig muss gewährleistet sein, dass trotzdem ein hoher Fehlerabdeckungsgrad hinsichtlich der Fehlerauswirkung erreicht wird. Dies erreicht man zum Beispiel durch die Annahme eines worst-case-Fehlers bei einem Bauteil oder auch bei einer ganzen Baugruppe. Worst-case-Fehler bedeutet, dass an den Ausgängen des Bauelementes oder der Baugruppe der sicherheitstechnisch ungünstigste Fehler unterstellt wird.

Möglichkeit des Fehlereinbaus

Nach Möglichkeit sollten Fehler unterstellt werden, die in die zu prüfende Originalschaltung auch eingebaut werden können. Dies ist nicht immer möglich, denkt man beispielsweise an bestimmte interne Driftvorgänge in Halbleiter-Bauelementen oder an die Miniaturisierung elektronischer Bauelemente. Je nach Schaltungsprinzip bleibt hier unter Umständen nichts anderes übrig, als die Auswirkung solcher Fehler mit Hilfe von Analyse und Simulation zu ermitteln. In der Fluidtechnik lässt sich eine Fehlerursache häufig nicht mit vertretbarem Aufwand realistisch simulieren, z. B. eine Feststoffverschmutzung des Druckmediums. Die Auswirkungen der Fehlerursache, z. B. Hängenbleiben des bewegten Bauteils, können aber in der Regel als Fehler eingebaut werden.

Reproduzierbarkeit

Die eingebauten Fehler sollten, soweit möglich, so ausgewählt sein, dass sich ein reproduzierbares Prüfergebnis ergibt.

Wirtschaftlichkeit

Die unterstellten Fehler sollen einen rationellen Fehlereinbau erlauben. Ein Einbau der Fehler in das betrachtete Bauelement bzw. in die Originalschaltung erfordert aber immer einen deutlich höheren Zeitaufwand als eine theoretische Fehlerbetrachtung. Deshalb sollte man es bei einfach zu übersehenden Bauelementen und Schaltungen bei einer theoretischen Fehlerbetrachtung belassen.

Herstellerunabhängigkeit

Die Art der eingebauten Fehler sollte weitgehend unabhängig vom Hersteller der Bauelemente sein. Fehlerausschlüsse können aber meistens nur konstruktionsspezifisch formuliert werden und sind damit manchmal indirekt herstellerabhängig.

Realistische Fehlerausschlüsse

Ohne die Annahme konkreter Fehlerausschlüsse sind sichere Steuerungen nicht realisierbar. Diese Fehlerausschlüsse sind, abgesehen von wenigen physikalisch begründeten Einzelfällen, jeweils ein Kompromiss zwischen den sicherheitstechnischen Erfordernissen einerseits und den technischen und wirtschaftlichen Möglichkeiten andererseits. Gründe für Fehlerausschlüsse sind insbesondere

- die physikalische Unmöglichkeit einer bestimmten Fehlerart (Beispiel: starke Zunahme der Kondensatorkapazität oder Vergrößerung des Volumenstroms einer Konstantpumpe ohne Änderung der Betriebs- und Antriebsparameter)
- allgemein anerkannte, anwendungsunabhängige technische Regeln oder Erfahrungen (Beispiel: Zwangsführung bei Relais oder plötzlicher Bruch eines Ventil-Schieberkolbens in viele Einzelstücke)
- technische und wirtschaftliche Aspekte, die anwendungsabhängig und damit abhängig vom konkreten Risiko der Anwendung sind (Beispiel: Leitungsschluss bei extern verlegten Kabeln oder selbstständiges Schalten eines Ventils ohne Ansteuerung bei Anwendungen mit relativ geringem Risiko)

Die beiden erstgenannten Gründe für einen Fehlerausschluss stellen den Regelfall dar. Dennoch sind in bestimmten Anwendungen weitergehende Fehlerausschlüsse möglich. Diese zusätzlichen Fehlerausschlüsse richten sich insbesondere nach der Auftrittswahrscheinlichkeit dieser Fehler. Sie lässt sich durch konkrete Ausfallraten belegen oder von entsprechenden betrieblichen Erfahrungen ableiten.

3 Normung von Fehlerlisten

Die vormals in den sicherheitstechnischen Informations- und Arbeitsblättern 340 220 und 340 225 aufgeführten Fehlerlisten für elektri-

sche, hydraulische und pneumatische Bauelemente hat die europäische Normung mit geringen Anpassungen in die europäische/internationale Norm EN ISO 13849-2 [3] übernommen. In den Anhängen A bis D finden sich im Hinblick auf die Validierung von sicherheitsbezogenen Steuerungsteilen allgemeine Fehlerlisten zu mechanischen, pneumatischen, hydraulischen und elektrischen Bauteilen. Diese bilden heute die Grundlage für Prüfungen nach DIN EN 954-1 [4].

Auch in Produktnormen des Maschinenbereiches finden sich vereinzelt Fehlerlisten, z. B. im Anhang B der DIN EN 61496-1 [5] und in der DIN EN 60947-5-3 [6] (hier jeweils für elektrische Bauelemente); diese Listen weichen kaum von der Fehlerliste für elektrische Bauelemente in [3] ab. Teil 2 der DIN EN 61508 [7] enthält in Tabelle A.1 eine sehr knappe und allgemein gehaltene Liste von Fehlern oder Ausfällen, die während des Betriebs erkannt werden müssen oder zur Bestimmung des Anteils ungefährlicher Ausfälle zu analysieren sind. Interessant ist diese Liste in Bezug auf die einzelnen Elemente eines Rechnersystems, z. B. Hauptprozessor (CPU), Takt und Speicher.

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 Nr. L 207 (1998)

[2] *Börner, F.; Kreutzkampf, F.*: Unfälle und Störfälle, verursacht durch das Versagen von Steuerungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 250. In: BGIA-Handbuch 22. Lfg. VI/94. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitsschutz – BGIA. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.

[3] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung. Beuth, Berlin (Dezember 2003)

[4] DIN EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze. Beuth, Berlin (März 1997)

[5] DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen. Beuth, Berlin (Januar 2005)

[6] DIN EN 60947-5-3: Niederspannungsschaltgeräte; Teil 5-3: Steuergeräte und Schaltelemente; Anforderungen für Näherungsschalter mit definiertem Verhalten und Fehlerbedingungen (PDF). Beuth, Berlin (Februar 2000)

[7] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme. Beuth, Berlin (Dezember 2002)

Bearbeiter:

Dipl.-Ing. T. Bömer, Dipl.-Ing. W. Grigulewitsch,
Dipl.-Ing. W. Kühlem, Dr.-Ing. K. Meffert,
Dipl.-Ing. G. Reuß
Fachbereich Unfallverhütung – Produktsicherheit

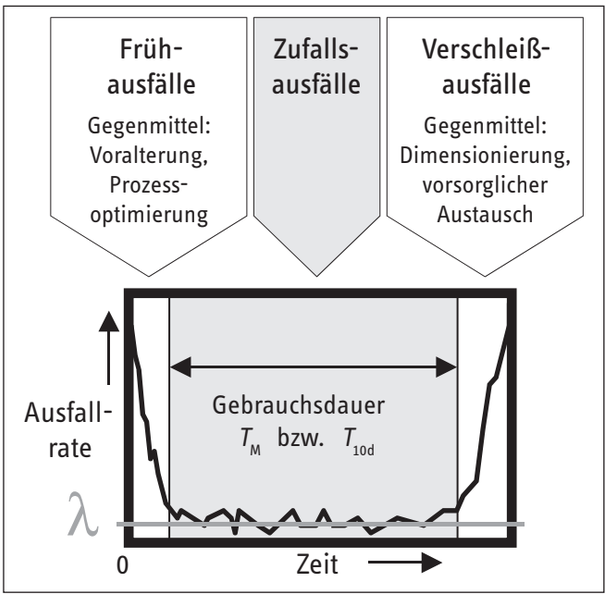
Anhang D:
Mean Time to Dangerous Failure ($MTTF_d$)

D1 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.

Abbildung D.1:
„Badewannenkurve“ der Ausfallrate



D1.1 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. elektromechanische 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.

$$MTTF_d = \frac{1}{\lambda_d} \qquad (1)$$

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 (siehe Seite 222) 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.

D1.2 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

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

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. 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 unakzeptabel erscheint. Am anderen Ende des Spektrums erscheint ein statistisch abgesicherter Nachweis von Zuverlässigkeiten > 100 Jahre $MTTF_d$ sehr fragwürdig. 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 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 Jahren findet erst auf Kanalebene statt, d.h. für einzelne Bauteile können deutlich höhere $MTTF_d$-Werte in die Berechnung einfließen.

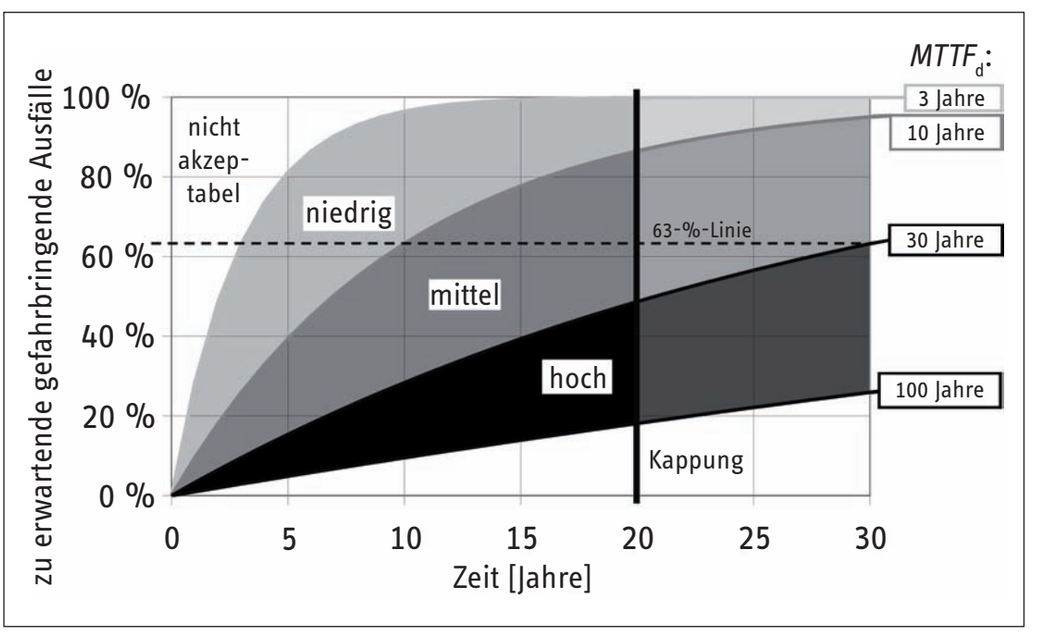


Abbildung D.2:
Illustration der $MTTF_d$

D1.3 Woher kommen die Daten?

Ein mögliches Problem für den Normanwender, besonders zum Zeitpunkt der ersten Veröffentlichung der revidierten DIN EN ISO 13849-1, sind fehlende $MTTF_d$-Angaben für Sicherheitsbauteile [2]. Grundsätzlich schlägt die Norm eine Hierarchie von Datenquellen vor, die an erster Stelle Herstellerangaben nennt, dann typische Zahlenwerte, die in der Norm selbst gelistet sind, 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, sind die in der Norm selbst gelisteten $MTTF_d$-Werte von besonderer Bedeutung – zumindest so lange, bis die Angabe von $MTTF_d$-Werten vonseiten der Hersteller zur Selbstverständlichkeit wird.

D2 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 kaum eine Rolle. Bei den meisten elektronischen Komponenten hingegen ist das Ausfallverhalten, innerhalb der typischen Einsatzdauer vergleichsweise „billiger“ Einwegkomponenten, 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, weshalb DIN EN ISO 13849-1 hier unterschiedliche Herangehensweisen vorschlägt.

D2.1 $MTTF_d$ mechanischer Steuerungskomponenten

Der Ansatz konstanter Ausfallrate 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 kann von der gewählten Applikation abhängen. 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.

D2.2 BGIA-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, wurde im BGIA eine Diplomarbeit zu diesem Thema initiiert, deren Ergebnisse als BGIA-Report 6/2004 „Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen“ [3] veröffentlicht wurden. Da es sich in der Regel bei Ventilen, die Steuerungsaufgaben übernehmen, um Wegeventile in Schieberbauweise handelt, wurden die $MTTF_d$-Wert 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 bzw. 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, wurde eine zustandsorientierte Instandhaltung durchgeführt.

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 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 hat seine Instandhaltungsmaßnahmen und Einsatzbedingungen im Laufe der Jahre kontinuierlich verbessert. Des Weiteren wurden gegenüber Anwender A die Einsatzbedingungen durch zusätzliche Maßnahmen verbessert, z.B. Über-

wachung der Öltemperatur, größere Öltanks, meist außerhalb der Maschine untergebracht, feinere Rücklauffilter, 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.

D2.3 $MTTF_d$ 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 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 vom Anwender 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).

Auch wenn DIN EN ISO 13849-1 unter diesen Voraussetzungen einen $MTTF_d$-Wert für hydraulische Ventile angibt, sollte dennoch jeder Hersteller von Ventilen für seine Bauteile möglichst eigene Ausfallzahlen ermitteln und eine eigene $MTTF_d$ angeben.

D2.4 $MTTF_d$ 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. 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, kann die Lebensdauer auch von den betrieblichen Umgebungsbedingungen stark beeinflusst werden. 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.

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 von grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003, 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 13849-2:2003, 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 den Anwender fest. Der Anwender ist über seine Verantwortung zu informieren, die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003, Tabellen B.1 oder D.1, für die Implementierung und den Betrieb des Bauteils zu erfüllen. Für Kategorie 1, 2, 3 oder 4 ist der Anwender über seine Verantwortung zu informieren, die bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003, Tabellen B.2 oder D.2, für die Implementierung und den Betrieb des Bauteils zu erfüllen.

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.

D2.4.1 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. Als Methode zur Bestimmung der Weibull-Parameter kann die „Lineare Regression XY" angewendet werden. Bei unvollständigen Daten, d.h., wenn z.B. nicht schadhafte Teile berücksichtigt werden sollen, sind auch andere Methoden anwendbar. Als Ergebnis können aus den Diagrammen die Kennwerte für die Parameter b und T abgelesen werden. Daraus lässt sich dann die nominale Lebensdauer B_{10} bestimmen, bei der 10 % der betrachteten Bauteile ausgefallen sind. Der $MTTF_d$-Wert wird mit der nominalen Lebensdauer B_{10} ermittelt. Für eine Zuverlässigkeitsanalyse mithilfe der Weibull-Statistik ist entsprechende 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 vier Teilen:

- Teil 1: Allgemeine Verfahren
- Teil 2: Ventile
- Teil 3: Zylinder mit Kolbenstange
- Teil 4: Druckregler

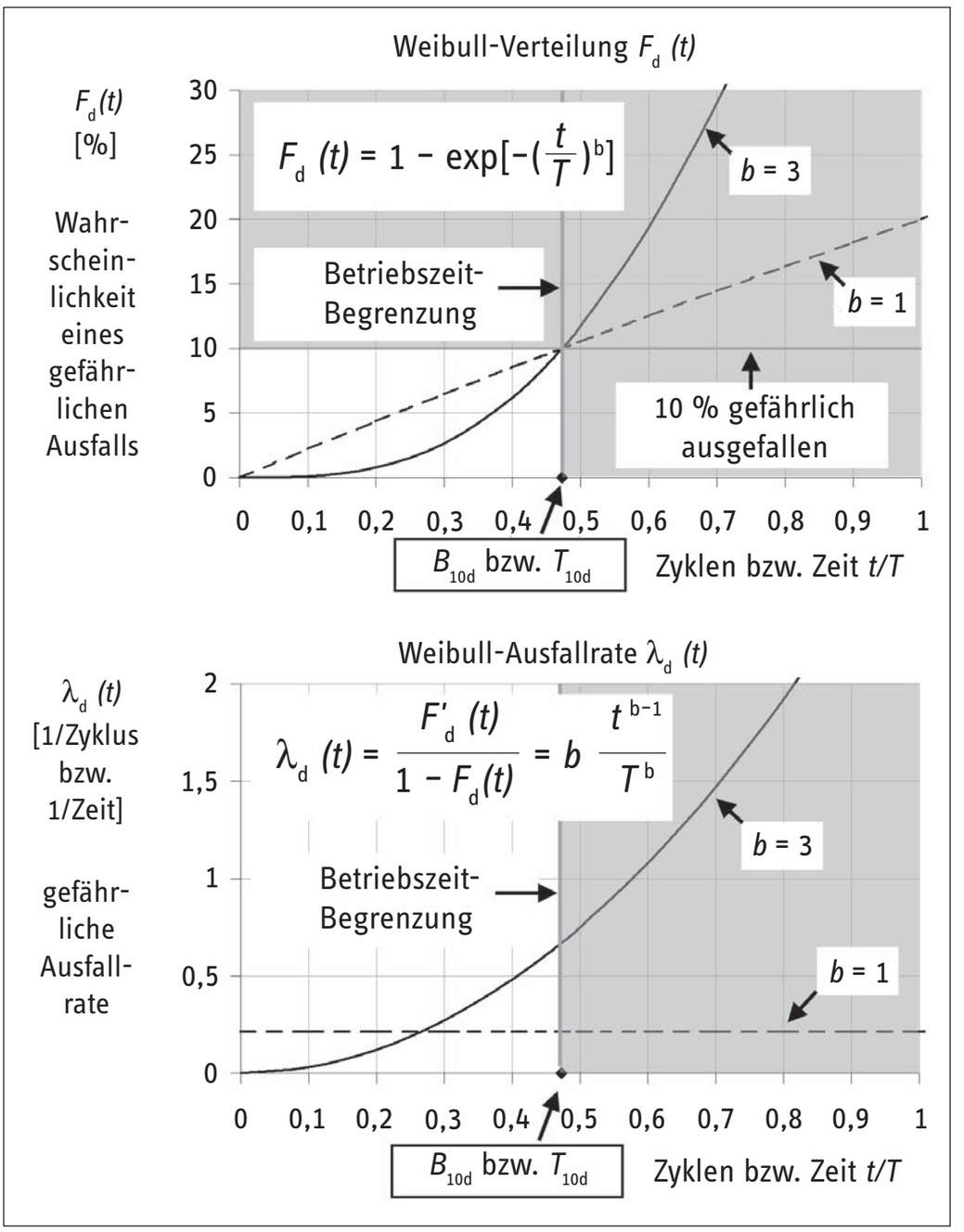


Abbildung D.3: Illustration der Umrechnung von B_{10d} in $MTTF_d$

Bei der Ermittlung der Zuverlässigkeit von Pneumatikventilen wird die Lebensdauer (B_{10}-Wert bzw. B-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 bis 10 % der betrachteten Menge ausgefallen sind. Da das Ausfallkriterium „Verfügbarkeit" bei Ventilen auch nicht sicherheitsrelevante Ausfälle beinhaltet (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:

$$B_{10d} = 2 \cdot B_{10} \tag{2}$$

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.

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.

D2.4.2 Umrechnung von B_{10d} in $MTTF_d$

Da der $MTTF_d$-Wert in Jahren angegeben wird, muss der als Anzahl von Zyklen angegebene B_{10d}-Wert entsprechend umgeformt werden. Folgende Parameter sind für die Bestimmung des $MTTF_d$-Wertes notwendig

- h_{op} → mittlere Betriebszeit in Stunden (h) je Tag
- d_{op} → mittlere Betriebszeit in Tagen je Jahr
- t_{Zyklus} → mittlere Zeit zwischen dem Beginn zweier aufeinanderfolgender Zyklen des Bauteils (z.B. Schalten eines Ventils) in Sekunden (s) je Zyklus

Aus diesen Parametern kann die mittlere Anzahl jährlicher Betätigungen n_{op} (in Zyklen pro Jahr) ermittelt werden:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{Zyklus}} \cdot 3\,600\ \frac{s}{h} \tag{3}$$

Setzt man den n_{op}-Wert in Gleichung (4) ein, ergibt sich die $MTTF_d$ für das betrachtete Bauteil in Jahren:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}} \tag{4}$$

Dabei wird die Betriebszeit des Bauteils auf den sogenannten T_{10d}-Wert (Zeit, bei der 10 % der betrachteten Bauteile gefährlich ausgefallen sind) begrenzt. Dieser T_{10d}-Wert kann wie folgt ermittelt werden:

$$T_{10d} = \frac{B_{10d}}{n_{op}} \tag{5}$$

Dies bedeutet, dass die betrachteten Bauteile vor Erreichen des T_{10d}-Wertes ausgewechselt werden sollten.

Die Umrechnung des B_{10d}-Wertes in einen $MTTF_d$-Wert unter Zuhilfenahme von n_{op} und der Begrenzung durch T_{10d} beruht auf einer Näherung. Das reale, von Verschleißeffekten geprägte Ausfallverhalten, das gut durch eine Weibull-Funktion beschrieben wird, wird durch eine Exponentialverteilung mit konstanter Ausfallrate (deren Kehrwert den $MTTF_d$-Wert darstellt) genähert. Dieses Verfahren wird in Abbildung D.3 illustriert. Die durchgezogene Linie stellt eine Weibull-Verteilung mit $b = 3$ dar. Die gestrichelte Linie entspricht dann einer Exponentialverteilung mit $b = 1$, welche die ursprüngliche Weibull-Verteilung im Punkt ($t = B_{10d}$; $F_d = 10$ %) schneidet. Wird der Zusammenhang $MTTF_d = 1/\lambda_d$ für Exponentialverteilungen und die Umrechnung von Zyklen in Zeiten durch n_{op} berücksichtigt, so leitet sich aus dieser Schnittbedingung die Näherungsformel für die Umrechnung von B_{10d} in $MTTF_d$ ab. Dabei wird ausgenutzt, dass die Ausfallrate vor Erreichen der Verschleißphase sehr gering ist und erst ab einem gewissen Zeitpunkt deutlich ansteigt. Dieser Zeitpunkt wird näherungsweise durch B_{10d} (in Zyklen) bzw. T_{10d} (als Zeit in Jahren) festgelegt. Indem nun die Einsatzdauer auf T_{10d} beschränkt wird, kann die leicht ansteigende Ausfallrate durch einen konstanten Wert in der Nähe von T_{10d} zur sicheren Seite hin abgeschätzt werden. In Abbildung D.3 lässt sich erkennen, dass diese Begrenzung der Einsatzdauer auf T_{10d} sehr wichtig ist: Oberhalb steigt der real zu erwartende Anteil gefährlicher Ausfälle mit der Zeit gegenüber der exponentiellen Näherung deutlich an. Auch die gewählte „Ersatz-Ausfallrate" $\lambda_d = 1/MTTF_d$ der exponentiellen Näherung entspricht ungefähr dem arithmetischen Mittelwert der real zu erwartenden Ausfallrate bis zum Zeitpunkt T_{10d}. Jenseits von T_{10d} ergeben sich jedoch durch das Eintreten in die Verschleißphase starke Abweichungen.

D2.5 Verfahren guter ingenieurmäßiger Praxis

Sind keine Herstellerangaben für die Zuverlässigkeit von Bauteilen verfügbar, schlägt die Norm als erste Alternative vor, Datenbankwerte 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, B_{10d}-Werte oder Fehlerausschlüsse in Tabelle D.2 aufgeführt. Dieser 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 der Tabelle D.2 ist allerdings an verschiedene Voraussetzungen gebunden:

- Der Hersteller des Bauteils bestätigt die Verwendung von grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 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 13849-2:2003 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 Anwender fest und informiert ihn über seine Verantwortung, die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 für die Implementierung und den Betrieb des Bauteils zu erfüllen.
- Der Anwender erfüllt die grundlegenden und/oder bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 für die Implementierung und den Betrieb des Bauteils.

Tabelle D.2:
Typische Zuverlässigkeitskennwerte, die bei guter ingenieurmäßiger Praxis als erreicht angenommen werden können

	Grundlegende und bewährte Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003	Andere relevante Normen	Typische Werte: $MTTF_d$ (Jahre) B_{10d} (Zyklen) bzw. Fehlerausschluss
Mechanische Bauteile	Tabellen A.1 und A.2	–	$MTTF_d$ = 150
Hydraulische Bauteile	Tabellen C.1 und C.2	EN 982	$MTTF_d$ = 150
Pneumatische Bauteile	Tabellen B.1 und B.2	EN 983	B_{10d} = 20 000 000
Relais und Hilfsschütze mit vernachlässigbarer Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20 000 000
Relais und Hilfsschütze mit maximaler Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400 000
Näherungsschalter mit vernachlässigbarer Last	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Näherungsschalter mit maximaler Last	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 400 000
Schütze mit vernachlässigbarer Last	Tabellen D.1 und D.2	IEC 60947	B_{10d} = 20 000 000
Schütze mit nominaler Last	Tabellen D.1 und D.2	IEC 60947	B_{10d} = 2 000 000
Positionsschalter unabhängig von der Last[a)]	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Positionsschalter (mit separatem Betätiger, Zuhaltung) unabhängig von der Last[a)]	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 2 000 000
Positionsschalter und Taster[b)] bei ohmscher Last und Überdimensionierung (≤ 10 % der maximalen Last) bezogen auf die elektrischen Kontakte	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 1 000 000
Positionsschalter und Taster[b)] bei Überdimensionierung nach Tabelle D.2, DIN EN ISO 13849-2:2003, bezogen auf die elektrischen Kontakte	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 100 000
Not-Halt-Geräte bei Einsatz unter geringer umwelttechnischer Belastung, z.B. in Laboren[a)]	Tabellen D.1 und D.2	IEC 60947 ISO 13850	Fehlerausschluss bis 100 000 Zyklen, sofern Herstellerbestätigung vorliegt
Not-Halt-Geräte bei Einsatz unter normaler umwelttechnischer Belastung, z.B an Maschinen[a)]	Tabellen D.1 und D.2	IEC 60947 ISO 13850	Fehlerausschluss bis 6 050 Zyklen
Zustimmungsschalter (3-stufig) unabhängig von der Last[a)]	Tabellen D.1 und D.2	IEC 60947	Fehlerausschluss bis 100 000 Zyklen

a) falls Fehlerausschluss für Zwangsöffnung möglich ist

b) für Schließerkontakte und für Öffnerkontakte, falls Fehlerauschluss für Zwangsöffnung nicht möglich ist

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 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 Anwender bzw. Betreiber der Maschine seinerseits ist für die Einhaltung aller Sicherheitsprinzipien verantwortlich, die Implementierung und Betrieb des Bauteils betreffen. Unter diesen Voraussetzungen kann bei der Berechnung der $MTTF_d$ oder bei der Annahme eines Fehlerausschlusses 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. Einen Sonderfall stellen Not-Halt-Geräte und Zustimmungsschalter dar, für die unter bestimmten Bedingungen ein Fehlerausschluss angenommen werden kann.

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. Insofern können diese Werte 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. 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. Damit kann für den elektrischen Teil unabhängig von der Last von einem Fehlerausschluss ausgegangen werden und die zitierten B_{10d}-Werte begründen sich hauptsächlich durch Ausfälle in der Betätigungsmechanik. Aus dieser Sichtweise ergeben sich z.B. auch die deutlichen Unterschiede zwischen Positionsschaltern ohne bzw. mit separatem Betätiger oder Zuhaltungen. Für Schließerkontakte und Öffnerkontakte ohne zwangsöffnende Eigenschaften kann allerdings kein Fehlerausschluss herangezogen werden. Dies äußert sich in deutlich geringeren typischen B_{10d}-Werten. Da Not-Halt-Geräte und Zustimmungsschalter eine garantierte fehlerfreie Mindestbetätigungsanzahl (siehe Tabelle D.2) aufweisen müssen, kann bis zu dieser Betätigungsanzahl ein Fehlerausschluss auch für die Mechanik angenommen werden. Hierbei müssen wegen der manuellen Betätigung im Gegensatz zu Positionsschaltern auch keine Fehler in der Anfahrmechanik oder Dejustage berücksichtigt werden. Bei Not-Halt-Geräten wird zwischen geringer und normaler Beanspruchung unterschieden. Die in der Typprüfung nachzuweisende fehlerfreie Mindestbetätigungsanzahl von 6 050 Zyklen gilt dabei für normale umwelttechnische Beanspruchung. Einige Hersteller bestätigen zusätzlich 100 000 Zyklen für den Einsatz bei geringer umwelttechnischer Beanspruchung. Um den Fehlerausschluss für Zwangsöffnung für den elektrischen Teil von elektromechanischen Sicherheitsbauteilen anwenden zu können, ist es erforderlich, dass diese Komponenten zusätzlich zu den obigen Voraussetzungen die Bedingungen für „bewährte Bauteile“ erfüllen.

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 Angepasstheit der mechanischen wie der elektrischen Bauteileigenschaften an die zu erwartende Belastung gehören.

D2.6 $MTTF_d$ 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 noch in $MTTF_d$-Werte umgerechnet werden, z.B. mithilfe der vereinfachenden Annahme, dass nur 50 % aller Ausfälle gefahrbringend sind. Sind trotzdem 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 für Bauteile, Siemens AG (wird unregelmäßig aktualisiert) www.pruefinstitut.de
- IEC/TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment, identisch zu RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l’Electricité et de la Communication www.ute-fr.com
- Reliability Prediction of Electronic Equipment, MIL-HDBK-217F, Department of Défense, Washington DC, 1982; mittlerweile fortgeführt als 217Plus System Reliability Assessment Tool, Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York 13502-1348 (theRIAC.org)
- Reliability Prediction Procedure for Electronic Equipment, Telcordia SR-332, Issue 01, May 2001 (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06)
- EPRD, Electronic Parts Reliability Data (RAC-STD-6100), Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York 13502-1348 (theRIAC.org)
- NPRD-95, Nonelectronic Parts Reliability Data (RAC-STD-6200), Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York 13502-1348 (theRIAC.org)
- British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)
- Chinese Military Standard, GJB/z 299B

Neben diesen Datensammlungen gibt es auf dem Markt eine Reihe von Hilfsprogrammen, die diese oder andere Datenbanken per Software zugänglich machen. 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 DIN EN ISO 13849-1 sind sogar für einige typische elektronische Komponenten Werte aufgelistet, die der Datensammlung SN 29500 entnommen und mit einem Sicherheitsfaktor von 10 versehen sind. Da diese Werte eher beispielhaften Charakter haben, sind sie hier nicht wiedergegeben. Der Sicherheitsfaktor 10 in Anhang C.5 der Norm soll den Worst Case abdecken, wenn ein sehr pauschaler Richtwert gesucht wird. Bei korrekter Verwendung der Datenquellen ist ein zusätzlicher Sicherheitsfaktor in der Regel nicht erforderlich. Die Anpassung an Beanspruchungen außerhalb der Referenzbedingungen wird in DIN EN ISO 13849-1 nicht explizit gefordert und sollte im Sinne der Einfachheit mit Augenmaß angewendet werden.

D3 Integration bereits zertifizierter Komponenten und Geräte

In noch seltenen, aber in Zukunft wohl häufigeren Fällen können Hersteller ihre Komponenten bereits mit der Angabe einer $MTTF_d$ im Datenblatt versehen. Ein ähnlicher Fall ergibt sich, falls für die Komponenten bereits in den Herstellerinformationen ein SIL nach DIN EN 61508 oder ein PL nach DIN EN ISO 13849-1, verbunden mit der Angabe einer „durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde“ (bzw. PFH-Wert nach DIN EN 61508), genannt wird. Falls solche Komponenten nur in einem Kanal des SRP/CS verwendet werden, kann die angegebene Ausfallwahrscheinlichkeit pro Stunde (*PFH*) als Ersatzwert für die Ausfallrate in die gefährliche Richtung betrachtet werden, wobei komponenteninterne Merkmale wie Redundanz und Eigendiagnose bereits berücksichtigt sind:

$$MTTF_d = \frac{1}{\lambda_d} \approx \frac{1}{PFH} \quad \text{(„Black-Box“-Komponenten mit PFH innerhalb eines Kanals)} \tag{6}$$

D4 „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 auf viel schlechtere Werte führt, bietet DIN EN ISO 13849-1 das sogenannte „Parts Count“-Verfahren an. Im Wesentlichen handelt es sich dabei um eine Summation mit drei 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):

$$\lambda_d = \frac{1}{2}\sum_{i=1}^{N}\lambda_i \text{ bzw. } \lambda_d = \sum_{i=1}^{N}\lambda_{di} \tag{7}$$

Da DIN EN ISO 13849-1 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.

D5 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. (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 DIN EN ISO 13849-1: Jeder $MTTF_d$-Wert eines Kanals, der rechnerisch > 100 Jahre ist, wird regelgemäß auf den Höchstwert von 100 Jahren reduziert. 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.

D6 Symmetrisierung bei mehreren Kanälen

Sobald zwei Kanäle in einer Steuerung vorhanden sind (dies ist in der Regel bei Kategorie 3 und 4 der Fall), 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:

$$MTTF_d = \frac{2}{3}\left(MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right) \tag{8}$$

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 [5]). 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. Während $MTTF_d$ bereits für jeden beteiligten Kanal auf 100 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
http://www.dguv.de/bgia/de/pub/grl/pdf/2007_016.pdf

[3] *Schuster, U.:* Untersuchung des Alterungsprozesses von hydraulischen Ventilen. BGIA-Report 6/04. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2004
www.dguv.de/bgia, Webcode d6362

[4] *Weibull, W.:* A statistical distribution function of wide applicability. J. Appl. Mech. 18 (1951), S. 292-297

[5] *Goble, W.M.:* Control systems safety evaluation and reliability. 2nd ed. Hrsg.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina 1998

Anhang E:
Bestimmung des Diagnosedeckungsgrades *(DC)*

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 die ganze Steuerung (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 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, geht DIN EN ISO 13849-1 einen anderen Weg und schlägt für typische Diagnosemaßnahmen DC-Eckwerte vor, von deren Erreichung ausgegangen werden kann. Auf diese Weise wird eine mühsame FMEA durch eine tabellarische Bewertung der umgesetzten Diagnosemaßnahmen ersetzt. Dies ist in ähnlicher Weise oft gängige und ökonomisch sinnvolle Praxis von Prüfstellen.

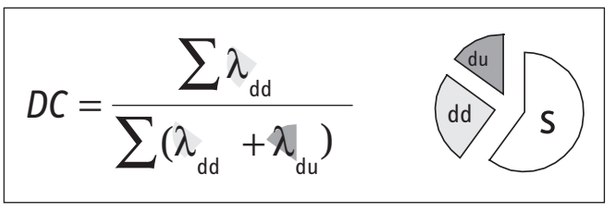
Da der Anteil der unerkennbar gefahrbringenden Ausfälle (also 1 – *DC*) die für die Ausfallwahrscheinlichkeit relevante Größe zur Bewertung der realisierten Test- und Überwachungsmaßnahmen ist, erklärt sich die Wahl der Eckwerte (60, 90 und 99 %), mit deren Hilfe vier DC-Qualitätsstufen gebildet werden (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 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

Es muss grundsätzlich unterschieden werden zwischen dem *DC* eines einzelnen Tests für eine bestimmte Komponente bzw. einen Block und dem durchschnittlichen Diagnosedeckungsgrad DC_{avg} (average) für die gesamte betrachtete Steuerung. Die Gruppenbildung mithilfe der Eckwerte wird dabei sowohl zur Qualifizierung der einzelnen Tests herangezogen als auch bei der Benennung von DC_{avg}. Da der DC_{avg} eine der Eingangsgrößen für die vereinfachte Quantifizierung der Ausfallwahrscheinlichkeit mithilfe des Säulendiagramms ist, wird der berechnete DC_{avg}-Wert auf einen der vier Eckwerte (0 %, 60 %, 90 % und 99 %) in Einklang mit Tabelle E.1 abgerundet bzw. in eine der vier DC-Klassen (kein, niedrig, mittel und hoch) eingeordnet. Ein DC_{avg}-Wert von 80 % wird im vereinfachten Ansatz daher auf einen Wert von 60 % herabgestuft (anders als im BGIA-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.

Abbildung E.1:
Illustration des Diagnosedeckungsgrades



In Tabelle E.2 sind typische Test- und Überwachungsmaßnahmen bezogen auf Komponenten bzw. Blöcke und ihre DC-Bewertung nach DIN EN ISO 13849-1 dargestellt. Je nach Funktion (I, L, O bzw. Eingabe, Logik, Ausgabe), Kategorie und Technologie sind unterschiedliche Maßnahmen üblich. Ihre Bewertung kann je nach Ausführung oder äußeren Umständen schwanken, z.B. je nach Anwendung, in der die Steuerung betrieben wird. Die indirekte Überwachung durch Wegaufnehmer oder Entschalter an den Aktoren statt an den Steuerungselementen lässt je nach Anwendung z.B. keinen Rückschluss zu, ob jeder von zwei

Tabelle E.2:
DC-Eckwerte für typische Test- und Überwachungsmaßnahmen 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					Der erreichte DC-Wert ist abhängig von der Häufigkeit eines Signalwechsels in der Anwendung.
● ohne Dynamisierung	X		X	0-99	
● 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 [2] zu erreichen.
Überwachung von Eigenschaften	X			60	
Programmlaufüberwachung					zeitliche Überwachung
● einfache zeitliche		X		60	
● 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

redundanten Steuerungskanälen die Sicherheitsfunktion noch unabhängig ausführen kann. Generell wird bei der Bewertung nicht unterschieden zwischen automatischen (z.B. regelmäßig ablaufenden Programmroutinen) oder willensabhängigen Tests (z.B. manuell durch den Bediener in regelmäßigen Abständen eingeleitete Tests). Auch welche Einheit einen Test durchführt, ist unerheblich, z.B. bei Selbsttests. Wichtig ist aber, dass ein Test nur dann überhaupt wirksam ist, wenn 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.

<table>
<tr><th colspan="5">typische Realisierung in verschiedenen Technologien</th></tr>
<tr><th>Mechanik</th><th>Pneumatik</th><th>Hydraulik</th><th>Elektrik</th><th>(Programmierbare) Elektronik</th></tr>
<tr><td colspan="5">siehe Maßnahmenbeschreibung</td></tr>
<tr><td rowspan="2"></td><td colspan="4">manuelle Initiierung der Prüffunktion</td></tr>
<tr><td colspan="2" rowspan="2">Positionserfassung des Ventilschiebers,
Höhe des DC abhängig von der
konkreten Ausführung</td><td colspan="2">Vergleich von Eingängen oder Ausgängen ohne Kurzschlusserkennung</td></tr>
<tr><td>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 colspan="2">Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen;
Ventilüberwachung durch Druckschalter</td><td colspan="2">Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen</td></tr>
<tr><td>Stellungsüberwachung direkt am überwachten Steuerungselement</td><td colspan="2">Stellungsüberwachung direkt am Ventilschieber über den gesamten Hub</td><td>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>
<tr><td colspan="3">Überwachung von Antwortzeiten, Signalstärke analoger Signale</td><td colspan="2">Überwachung von Antwortzeiten, Signalstärke analoger Signale
(z.B. Widerstand, Kapazität)</td></tr>
<tr><td colspan="3">nicht relevant

nicht relevant</td><td>Zeitglied als Watchdog, mit Triggersignalen im Programm der Logik

durch einen Watchdog, wobei die Testeinrichtung Plausibilitätstests des Verhaltens der Logik durchführt</td></tr>
<tr><td></td><td></td><td></td><td>Erkennung z.B. verschweißter Kontakte durch Ansteuerung und Rücklesung</td><td>Erkennung verborgener Fehler in Programm- und Datenspeicher, Eingangs-/Ausgangsanschlüssen, Schnittstellen</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Testung der Reaktionsmöglichkeit des Watchdogs</td></tr>
</table>

Tabelle E.2:
(Fortsetzung)

Maßnahme	hauptsächlich relevant für			DC [%]	Maßnahmen-Beschreibung
	I	L	O		
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					
● ohne Überwachung des Aktors			X	0	
● mit Überwachung eines der Aktoren entweder durch die Logik oder durch eine Testeinrichtung			X	90	
● mit Überwachung der Aktoren 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*

[2] *PL e erfordert in der Regel zwei Kanäle. Daher sollte mindestens der komplemantäre Block des redundanten Kanals eine andere DC-Maßnahme umsetzen, deren DC mindestens so groß sein sollte wie der angenommene DC durch den Prozess.*

typische Realisierung in verschiedenen Technologien				
Mechanik	Pneumatik	Hydraulik	Elektrik	(Programmierbare) Elektronik
	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 Folgendes: 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.15 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.

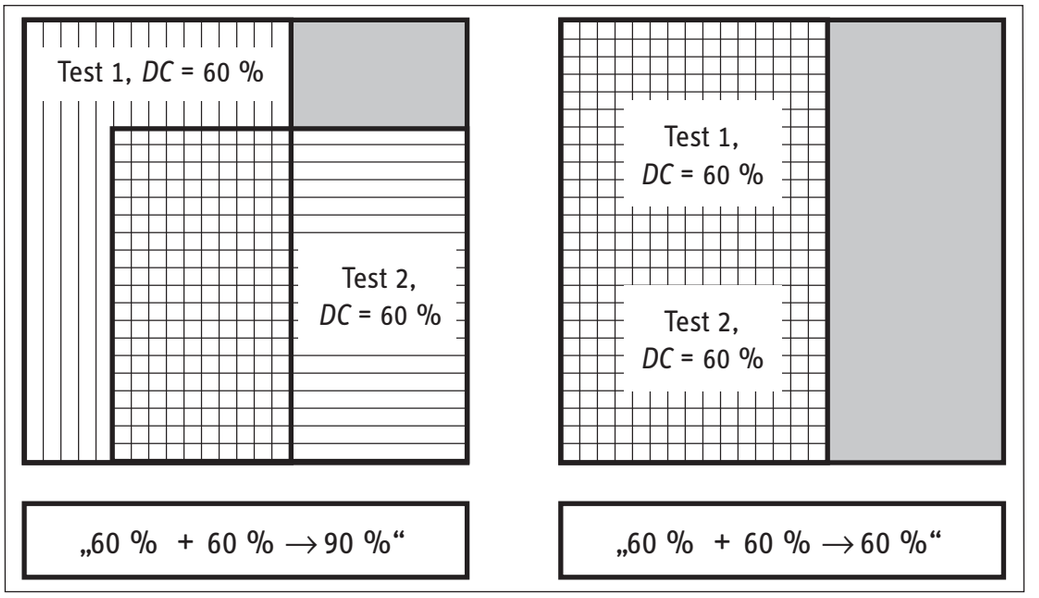


Abbildung E.2: Wirken auf einen Block mehrere Tests, so kann deren Überlappung zu einem höheren Gesamt-DC führen (links) oder auch nicht (rechts); die schraffierten Flächen repräsentieren den Anteil der erkannten gefahrbringenden Ausfälle; die quadratische Gesamtfläche repräsentiert alle gefahrbringenden Ausfälle (100 %)

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 (ist dieser 0 %, d.h., gibt es Einheiten, die gar nicht getestet werden, so wäre nach dieser groben Abschätzung auch der Block-DC 0 %). Ein besserer und genauerer Wert für den Block-DC lässt sich durch Gewichtung der Einzel-DC mit der zugehörigen Ausfallrate λ_d (=1/$MTTF_d$) erreichen. Die gewichtete Mittelungsformel entspricht dabei Gl. (1) für DC_{avg}. Je nach Genauigkeit gipfelt eine solche Analyse allerdings ebenfalls in einer FMEA.

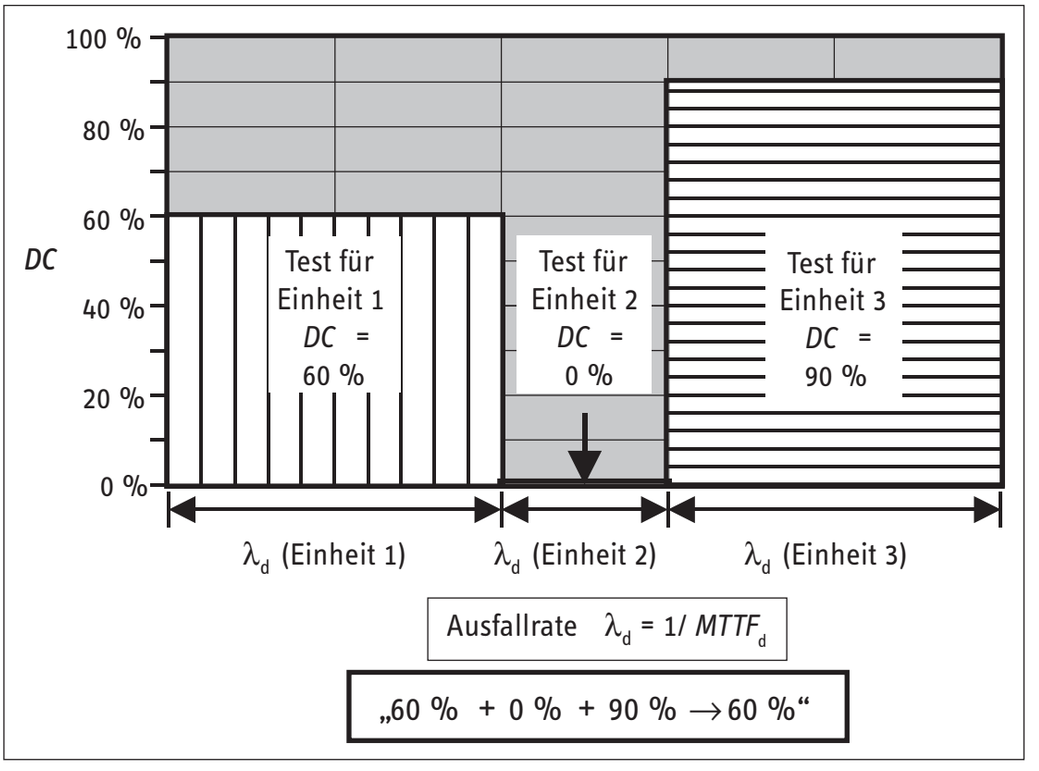


Abbildung E.3: Bei der DC-Mittelung für mehrere Einheiten eines Blocks führt die Gewichtung der Einzel-DC 60 %, 0 % und 90 % mit λ_d auf einen anderen Wert (60 %) als z.B. das ungewichtete arithmetische Mittel (50 %)

Der durchschnittliche *DC* für die gesamte betrachtete Steuerung wird mit DC_{avg} bezeichnet und errechnet sich aus den DC-Werten aller ihrer Blöcke. Im Gegensatz zur $MTTF_d$ pro Kanal wird nicht zwischen den Steuerungskanälen unterschieden, sondern direkt ein Gesamtwert ermittelt. Die Mittelungsformel gewichtet die Einzel-DCs 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:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}} \quad (1)$$

Die Summation läuft über alle relevanten Blöcke mit folgender Festlegung:

- Für Blöcke ohne *DC* wird eine *DC* = 0 % eingesetzt. Diese tragen damit nur zum Nenner des Bruchs bei.
- Für Blöcke mit Fehlerausschluss bezüglich der gefahrbringenden Ausfallrichtung (verschwindender 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 Steuerungskanälen ausführen, werden berücksichtigt. Blöcke, die nur allein der Testung dienen, werden nicht berücksichtigt. Für Kategorie-2-Strukturen bedeutet dies, dass Blöcke des Überwachungskanals („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 nur geringe 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. Grundsätzlich anders sieht dies in Kategorie-2-Strukturen aus. Der Ausfall der Testeinrichtung macht hier aus einem einkanalig getesteten System ein einkanalig ungetestetes System, das beim nächsten Ausfall die Sicherheitsfunktion nicht mehr ausführen 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 größer sein als die Anforderungsrate der Sicherheitsfunktion. Damit soll gewährleistet werden, dass ein Ausfall von einem Test bemerkt werden kann, bevor eine Anforderung der Sicherheitsfunktion nicht bedient werden kann (siehe auch Anhang G).
- Die $MTTF_d$ der testenden Einheit (TE) sollte mindestens halb so groß sein wie die $MTTF_d$ der zu testenden Einheit (L). Durch diese Annahme wird sichergestellt, dass die Ausfallwahrscheinlichkeit der Testeinrichtung nicht unangemessen hoch ist.

Lässt sich der Funktionskanal nicht auf die Blöcke I, L und O (bzw. der Testkanal auf die Blöcke TE und OTE) abbilden, kann die obige Bedingung so interpretiert werden, dass die $MTTF_d$ des gesamten Testkanals mindestens halb so groß sein soll wie die $MTTF_d$ des Funktionskanals. 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

Anhang F:
Ausfälle infolge gemeinsamer Ursache (CCF)

Der Begriff des Ausfalls infolge gemeinsamer Ursache CCF (Common Cause Failure) beschreibt die Tatsache, dass in einem redundanten System oder einem einkanaligen System mit externer Testeinrichtung 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).

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] 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 Experten 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 %.

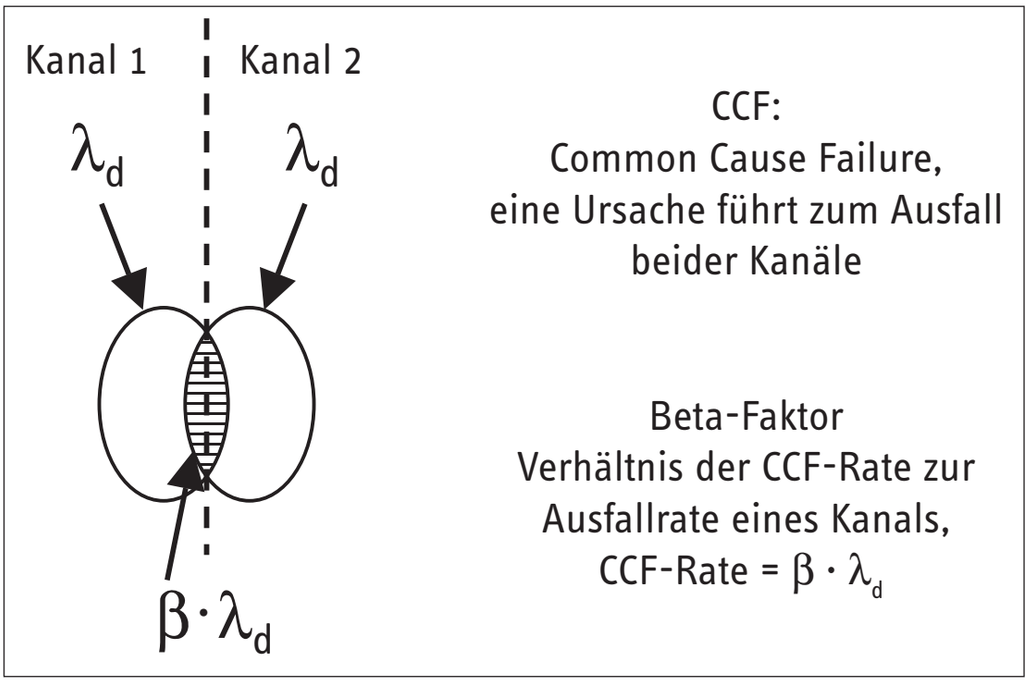


Abbildung F.1: Illustration des Ausfalls infolge gemeinsamer Ursache (CCF) anhand des Beta-Faktor-Modells

- 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 Sicherheits- 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 oder 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

  - Art der Initiierung, z.B. Druck und Temperatur

  - Messung von Entfernung und Druck

  - digital und analog

  - Bauteile von unterschiedlichen Herstellern

- Entwurf/Anwendung/Erfahrung: Schutz gegen Überspannung, Überdruck, Überstrom usw. (15 Punkte) und Verwendung bewährter Bauteile (5 Punkte)

- Beurteilung/Analyse (5 Punkte): Wurden die Ergebnisse einer Ausfalleffektanalyse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache in der Entwicklung zu vermeiden?

- Kompetenz/Ausbildung (5 Punkte): Wurden Konstrukteure/Monteure geschult, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu erkennen?

- Umgebungsbedingungen hinsichtlich Schutz vor Verunreinigung und elektromagnetischer Beeinflussung gegen CCF in Übereinstimmung mit den angemessenen Normen (25 Punkte):

  - 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

  - Elektrische Systeme: Wurde das System hinsichtlich elektromagnetischer Immunität gegen CCF geprüft, z.B. wie in zutreffenden Normen festgelegt?

  Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.

- Umgebungsbedingungen hinsichtlich anderer Einflüsse (10 Punkte): Wurden alle Anforderungen der Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchtigkeit (z.B. wie in den relevanten Normen festgelegt) berücksichtigt?

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 (06.03). Beuth, Berlin 2003

Anhang G:
Was steckt hinter dem Säulendiagramm in Bild 5 der DIN EN ISO 13849-1?

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* (Probability of a Dangerous Failure per Hour) 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* liefern (Mittelwert während der Gebrauchsdauer). Eigentlich müsste vom Anwender der Norm für jedes zu untersuchende System ein maßgeschneidertes Modell erstellt werden. Für einige gebräuchliche Strukturvarianten, die sogenannten „vorgesehenen Architekturen" aus DIN EN ISO 13849-1, Abschnitt 6.2 (vgl. Abschnitte 6.2.1 bis 6.2.7 dieses Reports), wurden im BGIA Markov-Modelle entwickelt, deren numerische Ergebnisse als sogenanntes „Säulendiagramm" in der Norm in Abschnitt 4.5.4, Bild 5 (Abbildung 6.10 bzw. G.3 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 Teilsysteme 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 $MTTF_d$ der Testeinrichtung muss mindestens den halben Wert der $MTTF_d$ für die getestete Logik 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 vom Anwender 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.3 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 i.d.R. kurz darauf (spätestens nach einigen Stunden) manuell abgeschaltet werden,
- 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*, die durchschnittliche Anzahl der ausfallbedingt nicht bedienten Anforderungen der Sicherheitsfunktion pro Stunde dar. Bei ständig vorliegender Anforderung (Continuous Mode of Operation) gibt sie die Anzahl der gefährlichen Systemausfälle pro Stunde an (Ausnahme: Kategorie 2, deren *PFH* nur für zeitdiskrete Anforderungen berechnet wurde). Da die so ermittelte *PFH* 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* ist die mathematische Größe, die auf der vertikalen Achse des Säulendiagramms aufgetragen ist (vgl. Abbildung G.3 dieses Anhangs).

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* aus. Lediglich bei der für Kategorie 2 vorgesehenen Architektur muss gefordert werden, dass die Testung sehr viel häufiger erfolgt als die Anforderung der Sicherheitsfunktion (vgl. DIN EN ISO 13849-1, Abschnitt 4.5.4; Ausnahme: Testintervall und die Zeit für die sicherheitsgerichtete Reaktion sind zusammen kürzer als die spezifizierte Systemreaktionszeit). Die Norm schlägt dazu 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* lediglich um ca. 10 %. Aus ähnlichem Grund gelten die per Diagramm ermittelten PFH-Werte – mit der Einschränkung bei der Kategorie-2-Architektur – für beliebige Anforderungsraten und beliebige (mittlere) Reparaturzeiten. (Bei weniger als einer Anforderung pro Jahr liefert das Säulendiagramm eine Abschätzung zur sicheren Seite.)

Die Säulen für Kategorie B und 1 in Abbildung G.3 wurden mithilfe eines Modells berechnet, das die Anforderung der Sicherheitsfunktion und die Reparatur berücksichtigt. Die PFH-Werte bei diesen Kategorien lassen sich aber auch sehr gut durch die einfache Beziehung $PFH \approx \lambda_d = 1/MTTF_d$ annähern. Dies bedeutet nichts anderes, als dass die *PFH* des einkanaligen ungetesteten Systems (*DC* = 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.1 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 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 wirken kann.

Aus dem sicherheitsbezogenen Blockdiagramm in Abbildung G.1 kann der Zustandsgraph in Abbildung G.2 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.2 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.2 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 gekennzeichnet 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 den Übergangspfeilen um. Die Summe der Zustandswahrscheinlichkeiten bleibt konstant Eins. Dabei ergibt sich auch ein zeitabhängiger Zufluss in den Zustand „Gefährliche Situation/Schaden“, dessen zeitlicher Mittelwert während der 20-jährigen Gebrauchsdauer die *PFH* darstellt, d.h. die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Systems je Stunde.

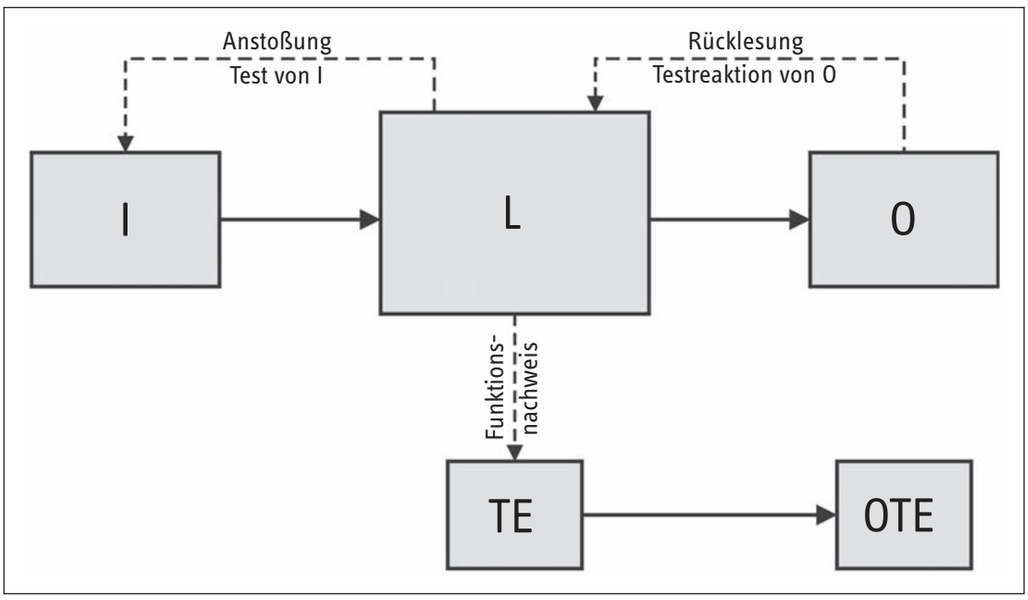
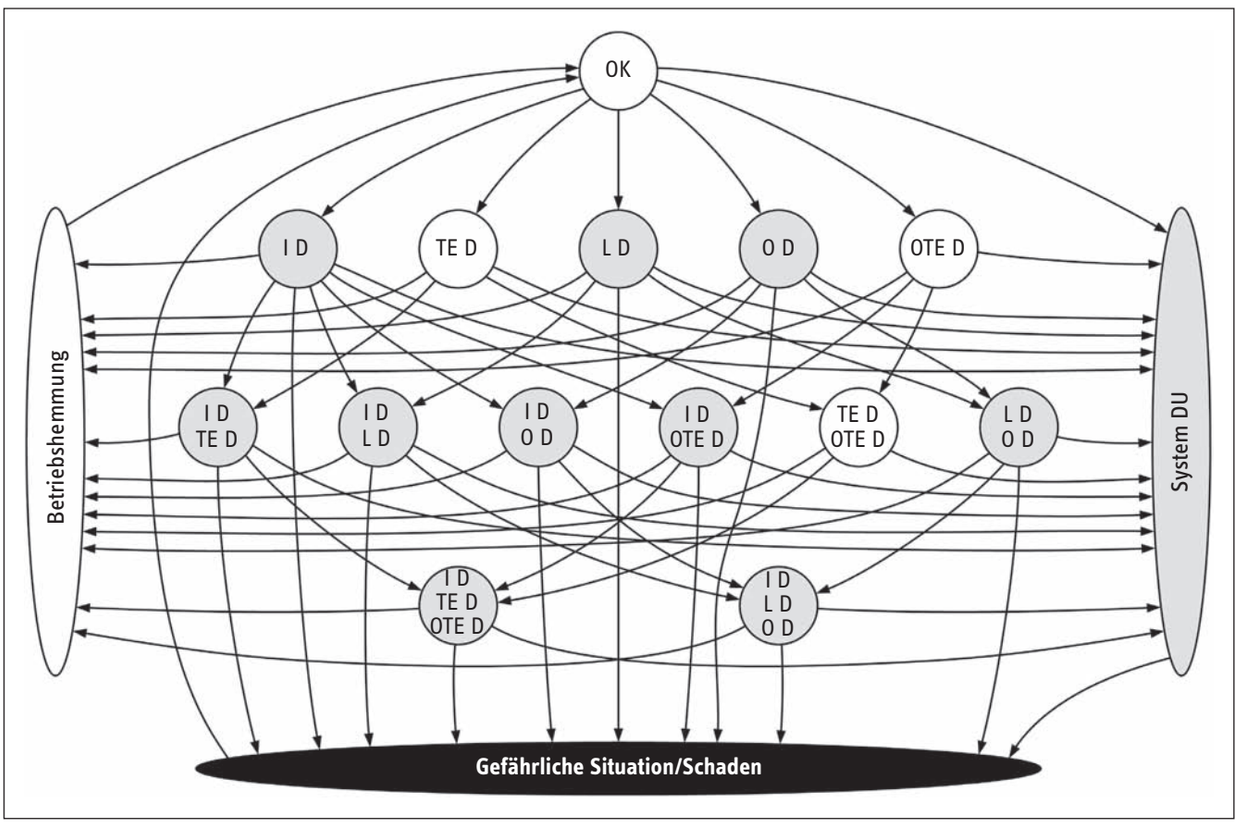


Abbildung G.1:
Vorgesehene Architektur für Kategorie 2 nach DIN EN ISO 13849-1, Abschnitt 6.2.5

Abbildung G.2:
Zustandsgraph des Markov-Modells zur vorgesehenen Architektur für Kategorie 2 für die Ermittlung der PFH



Diese *PFH* 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 könnten beispielsweise mit dem Markov-Modell in Abbildung G.2 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.1 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-Intervallen auf der logarithmisch geteilten PFH-Skala die Performance Levels a bis e zugewiesen. Dies ist in Abbildung G.3 gezeigt, in der Bild 5 der Norm DIN EN ISO 13849-1 um eine zusätzliche PFH-Skala ergänzt wurde.

Eine Besonderheit gibt es beim PFH-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 $\sqrt{10 \cdot 10^{-6}}\text{/h} \approx 3 \cdot 10^{-6}$/h. Die Zuordnung von PFH-Intervallen und Performance Level deckt sich im Wesentlichen mit Tabelle 6.1 und DIN EN 61508-5, Abbildung D.2, siehe [3; 4].

In Anhang K der Norm ist der Inhalt von Abbildung G.3 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-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 einem sogenannten „Performance Level Calculator“ (PLC) enthalten, einer handlichen Drehscheibe aus Karton zur PL-Bestimmung, die u.a. beim BGIA erhältlich ist [5].

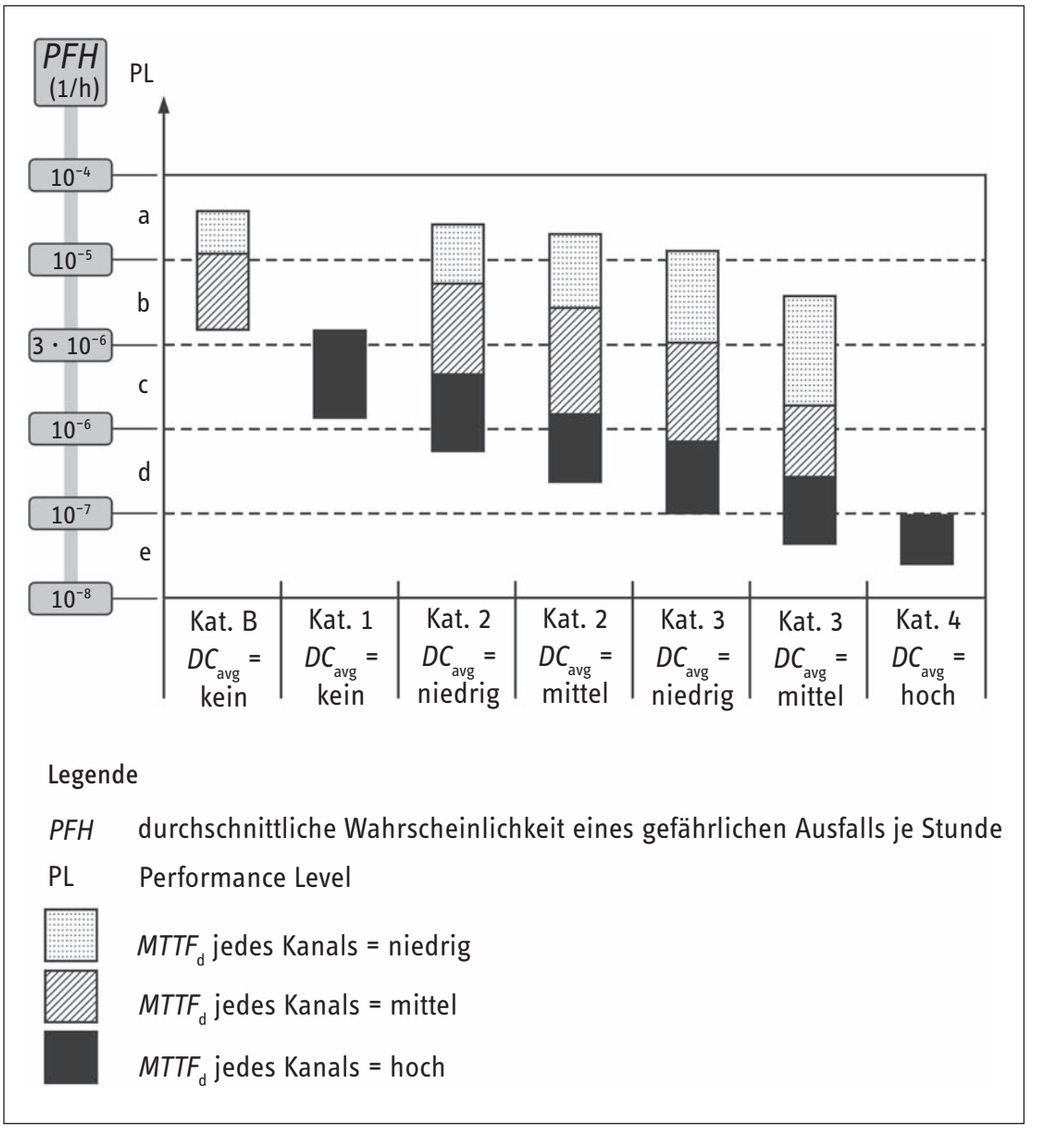


Abbildung G.3: PFH und Performance Level in Abhängigkeit von Kategorie, DC und $MTTF_d$

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 nächst kleineren DC_{avg}-Stufe, also mit „kein“, „niedrig“ bzw. „mittel“ weitergearbeitet werden. Diese Vorgehensweise schätzt das System zur sicheren Seite ab. Wegen der wenigen Stufen der DC_{avg}-Skala kann jedoch manchmal eine nur kleine Systemänderung, die den Wert DC_{avg} eine der Schwellen gerade unterschreiten lässt, zu einer 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 den nächst kleineren Wert überkompensiert, wodurch die ermittelte *PFH* schlechter (größer) wird. Dieser paradox erscheinende Effekt ist eine Folge der Grobstufigkeit der DC_{avg}-Skala, also letztlich eine Konsequenz der Einfachheit von Bild 5 (bzw. Tabelle K.1) der Norm, vgl. Abbildung G.3 dieses Reports.

Der beschriebene Effekt kann verhindert oder gemildert werden, indem anstelle von Abbildung G.3 eine Grafik mit feinerer Abstufung der DC_{avg}-Werte benutzt wird (Abbildung G.4). Mit Rücksicht auf die begrenzte Genauigkeit von DC_{avg}-Werten (vgl. DIN EN ISO 13849-1, Tabelle 6, Anmerkung 2) wurden für alle Kategorien auch die minimal möglichen DC_{avg}-Werte berücksichtigt. Zur PFH-Bestimmung bietet sich der BGIA-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-Wert ermittelt werden.

Literatur

[1] DIN EN 954-1: Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (03.1997). Beuth, Berlin 1997

[2] *Goble, W.M.:* Control systems safety evaluation and reliability. 2nd ed. Hrsg.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina 1998

[3] DIN EN 61508-1: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 und Corrigendum 1999) (11.02). Beuth, Berlin 2002

[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 61508-5:1998 und Corrigendum 1999) (11.02). Beuth, Berlin 2002

[5] *Schaefer, M.; Hauke, M.:* Performance Level Calculator – PLC. 3. Aufl. Hrsg.: BGIA – Institut für Arbeitsschutz 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 im März 2008
www.dguv.de/bgia, Webcode d3508

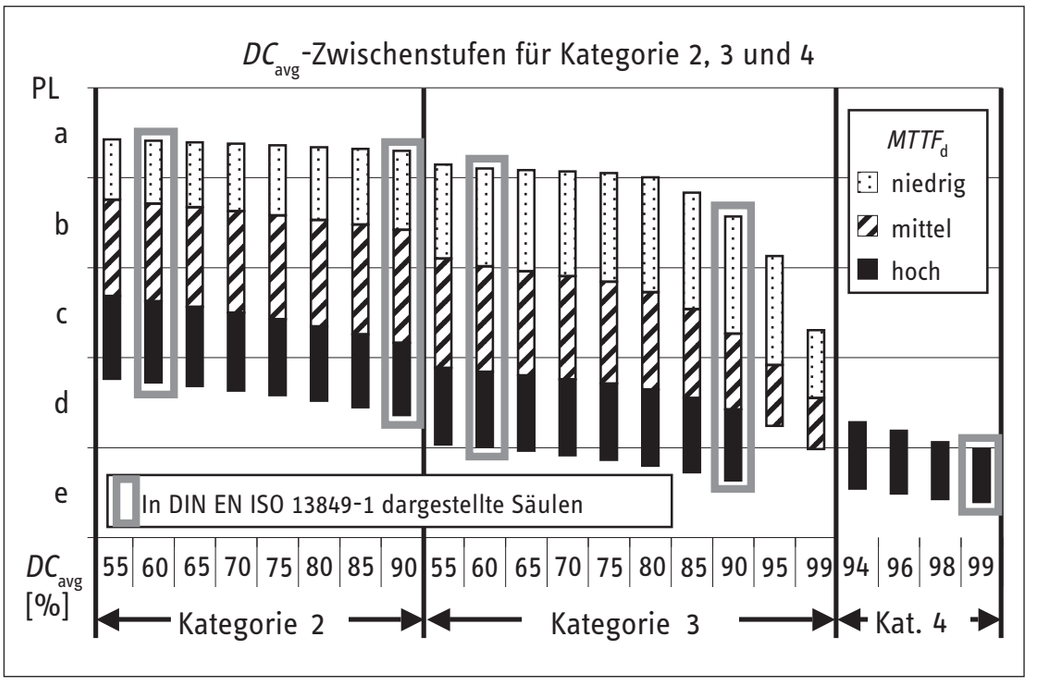


Abbildung G.4: Performance Level bei feinstufigerer Auflösung der DC_{avg}-Skala (Erweiterung von Bild 5 aus DIN EN ISO 13849-1)

Anhang H:
SISTEMA – Der Softwareassistent zur Bewertung von SRP/CS

H1 Was kann SISTEMA?

Mit dem Software-Assistenten SISTEMA (**Si**cherheit von **Ste**uerungen an **Ma**schinen) steht Entwicklern und Prüfern von sicherheitsbezogenen Maschinensteuerungen eine umfassende Hilfestellung bei der Bewertung der Sicherheit im Rahmen der DIN EN ISO 13849-1 zur Verfügung. Das Windows-Tool bietet dem Nutzer 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).

Über Eingabemasken werden relevante Parameter wie Risikoparameter zur Bestimmung des erforderlichen Performance Levels (PL_r), Kategorie des SRP/CS, Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) bei mehrkanaligen Systemen, mittlere Bauteilgüte ($MTTF_d$) und die mittlere Testqualität (DC_{avg}) von Bauelementen bzw. Blöcken Schritt für Schritt erfasst. Nachdem die geforderten Daten in SISTEMA eingetragen wurden, sind die berechneten Ergebnisse sogleich sichtbar. Praktisch für den Benutzer: Jede Parameteränderung wird in ihrer Auswirkung auf das Gesamtsystem über die Programmoberfläche direkt angezeigt. Das umständliche Nachschlagen in Tabellen und Ausrechnen von Formeln (Bestimmung der $MTTF_d$ nach dem „Parts Count"-Verfahren, Symmetrisierung der $MTTF_d$ für jeden Kanal, Abschätzung des DC_{avg}, Ermittlung von *PFH* und PL etc.) wird durch die Software übernommen und entfällt daher weitestgehend. Dies ermöglicht es dem Benutzer, Parameterwerte zu variieren, um so die Auswirkungen von Änderungen zu beurteilen, ohne dabei großen Aufwand zu treiben. Die Resultate können schließlich in einem Übersichtsdokument ausgedruckt werden.

H2 Wie wird SISTEMA verwendet?

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

Der Benutzer eröffnet zunächst ein Projekt und kann darin die Maschine bzw. die Gefahrenstelle, die weiter betrachtet werden soll, definieren. Dem Projekt werden schließlich alle erforderlichen Sicherheitsfunktionen zugewiesen. Diese können durch den Benutzer festgelegt und dokumentiert sowie mit einem PL_r belegt werden. Der tatsächlich erreichte 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 der Benutzer entweder direkt einen $MTTF_d$-Wert und einen DC-Wert einträgt, oder aber auf der niedrigsten Hierarchieebene die Werte für die einzelnen Elemente einträgt, aus denen sich der Block zusammensetzt.

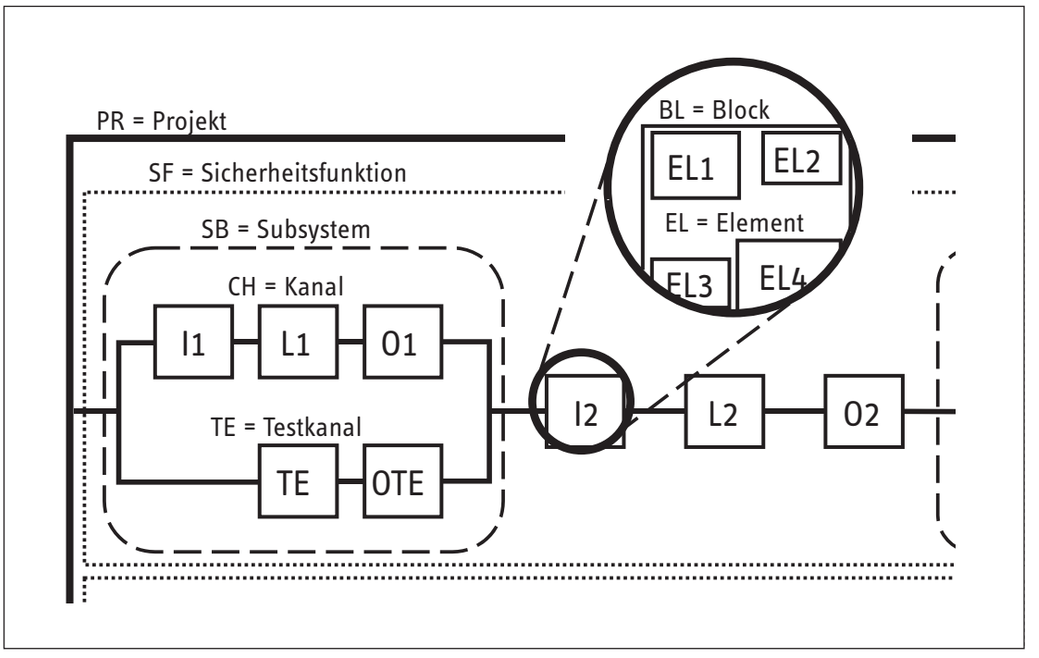


Abbildung H.1: In SISTEMA betrachtete Hierarchieebenen

Komfortable Bibliotheksfunktionen runden den Leistungsumfang von SISTEMA ab. Die mitgelieferten Bibliotheken enthalten einige Standardelemente; Blöcke und komplette Subsysteme lassen sich jedoch durch den Benutzer beliebig erweitern. Optional können weitere Bibliotheksmodule nachinstalliert werden, falls diese von Herstellern für ihre Komponenten verfügbar sind.

H3 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. Hat der Benutzer beispielsweise einen Block in der Baumansicht markiert, so zeigt diese Tabelle alle darin enthaltenen Elemente mit ihren $MTTF_d$- und DC-Werten an.

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

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

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

H4 Wo ist SISTEMA zu erhalten?

Die Software SISTEMA wird auf den Internetseiten des BGIA zum Download bereitgestellt. Zunächst wird SISTEMA nur in deutscher Sprache erhältlich sein, Versionen für weitere Sprachen werden folgen. Das Tool wird im Übrigen nach Registrierung als Freeware zur kostenlosen Benutzung angeboten. Aktuelle Informationen sowie den Link zum Download erhalten Sie unter der Internetadresse www.dguv.de/bgia über den Webcode 2447262.

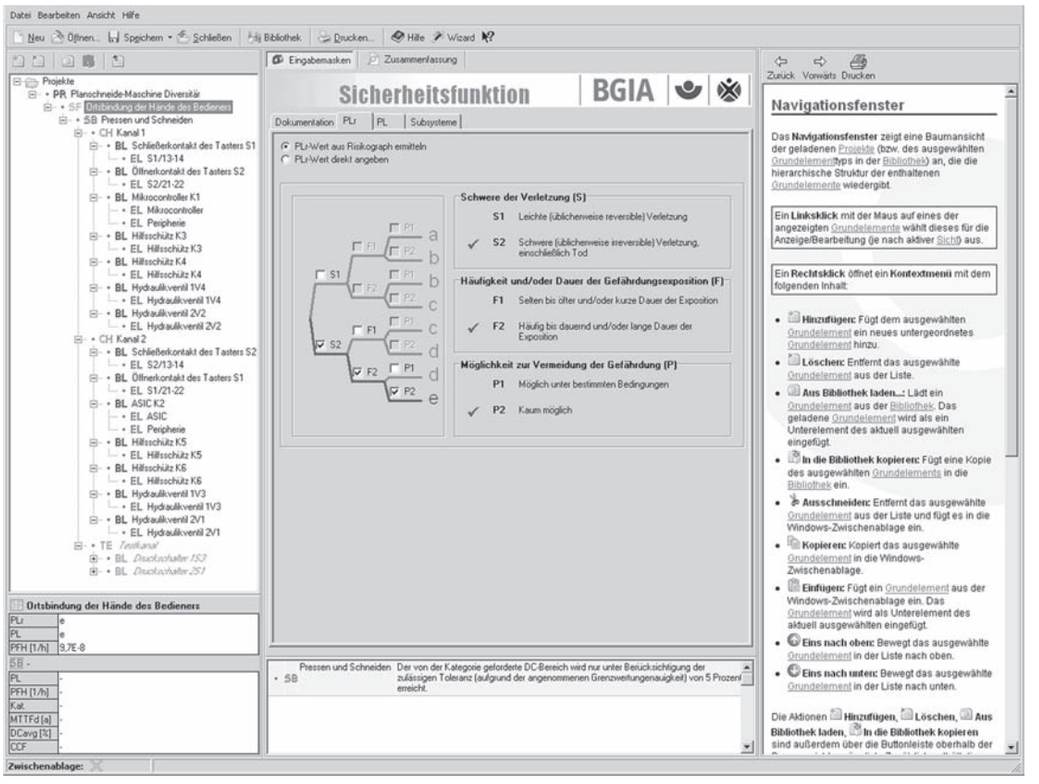


Abbildung H.2: Programmoberfläche von SISTEMA

Anhang I:
Positionspapier des VDMA

VDMA-Positionspapier

Funktionale Sicherheit: Sicherheitsbezogene Teile von Steuerungen nach EN ISO 13849-1

1. Einleitung

Der VDMA (Verband Deutscher Maschinen- und Anlagenbau) ist der größte europäische Verband der Investitionsgüterindustrie. Er ist Interessenvertreter, Dienstleister und Ansprechpartner für rund 3.000 deutsche und europäische Unternehmen des Maschinen- und Anlagenbaus. In Deutschland beschäftigt der Maschinen- und Anlagenbau rund 865.000 Menschen, mit einem Umsatz von € 151 Milliarden und einem Exportanteil von rund 75%. VDMA-Mitgliedsunternehmen sind global aktiv und haben allein in der EU insgesamt 1.649 Tochterunternehmen gegründet, wovon 327 produzierende Tätigkeiten ausführen. Das hohe technische Niveau der mehr als 20.000 unterschiedlichen Produkte der Investitionsgüterindustrie begründet ihren weltweiten Ruf als „Innovationsbranche".

2. Situation: Funktionale Sicherheit

Nach einer Übergangszeit von 3 Jahren wird Ende 2009 die über viele Jahre im Maschinen- und Anlagenbau verwendete Norm EN 954-1:1996 "*Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen – Teil 1*" durch die im November letzten Jahres erschienene EN ISO 13849-1:2006-11 (ISO 13849-1:2006-11) ersetzt werden. Dies wird für den Anwender einen Betrachtungswechsel weg von der Deterministik[1], hin zur Probabilistik[2] mit sich bringen und bei nicht wenigen Anwendern im Maschinen- und Anlagenbau aber auch bei Komponentenlieferanten Fragen zur praktischen Umsetzung nach sich ziehen.
Ebenso wie die EN ISO 13849-1 bemüht sich die bereits Ende 2005 abgeschlossene Norm EN 62061 "*Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*" (IEC 62061:2005) um die Vormachtstellung auf diesem Themengebiet. Die EN 62061 gilt als ein sektorspezifischer Ableger der aus 8 Teilen bestehenden IEC Horizontalnorm EN 61508:2001 "Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme" mit Ausrichtung auf den Maschinenbau.

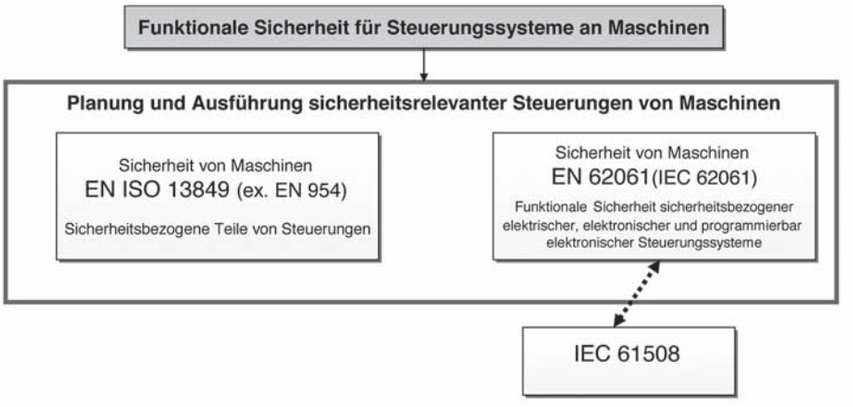
[1] Vorbestimmtheit, kausaler Zusammenhang
[2] Wahrscheinlichkeit, nicht streng kausal zusammenhängend

Während sich die IEC-Normen sehr stark auf das Thema Probabilistik mit Hilfe wahrscheinlichkeits-theoretischer Mathematik und Modellierung konzentrieren, wurde bei der Erarbeitung der ISO Norm 13849-1, ausgehend von der deterministisch orientierten EN 954-1, ein für den Anwender überschaubarer und begrenzter Anteil an probabilistischen Elementen zu den bekannten Elementen der EN 954-1 hinzugefügt, um Aufwand und Nutzen in einem ausgewogenen Verhältnis zu halten, und auch um den Bedürfnissen des mittelständischen Maschinen- und Steuerungsbauers zu entsprechen. Damit wird dem Willen der EG-Kommission entsprochen, dass Normen, die gesetzliche Anforderungen konkretisieren, von klein- und mittelständischen Unternehmen in der Praxis angewendet werden können.
In Bezug auf die Entwicklung sicherheitsbezogener Embedded-Software (Firmware, Systemsoftware) ab dem höchsten Anforderungslevel verweist auch die EN ISO 13849-1 auf die entsprechenden Teile der Normenreihe EN 61508.

3. Ausblick

Die EN ISO 13849-1 wird nach einem Übergangszeitraum von 3 Jahren nach Veröffentlichung die EN 954-1 zum 30.11.2009 ablösen. Mit dem im Mai 2007 neu erschienenen Amtsblatt zur Maschinenrichtlinie ist die EN ISO 13849-1 als harmonisierte Norm unter der EG-Maschinenrichtlinie gelistet und löst damit bei Anwendung die Vermutungswirkung zur Einhaltung der Richtlinie aus.
Die EN 62061:1995 ist bereits seit August 2006 als harmonisierte Norm unter der EG-Maschinenrichtlinie gelistet.
Bereits im Vorfeld der Fertigstellung der Normen, wurde in gemeinsamen Sitzungen beider verantwortlichen Normungskomitees der Versuch unternommen, mit einer gemeinsamen Tabelle in der Einleitung eine Empfehlung hinsichtlich der bevorzugten Anwendung beider Normen zu geben.
Nach der Fertigstellung der ISO 13849-1 im November 2006 haben sich beide Normungskomitees dahingehend geeinigt, einen gemeinsamen Anhang für beide Normen zu erstellen, der das Verständnis und die Anwendung der beiden Standards erleichtern soll.
Als weiterer Schritt ist geplant, in naher Zukunft beide Normen zu einer gemeinsamen Norm oder einer mehrteiligen Norm verschmelzen zu lassen, die das Thema "Funktionale Sicherheit für Steuerungssysteme an Maschinen" abdeckt.

4. Normen im Blickfeld



5. Fazit

Der VDMA begrüßt die Bemühungen der verantwortlichen Normungskomitees und erwartet, dass die beiderseits angestrebten Zielvorstellungen erfolgreich umgesetzt werden, die für eine verbesserte Kohärenz der Normen und für mehr Transparenz für die Anwender sorgen.

Der VDMA vertritt die folgende Auffassung:

- Als praktikabler Weg, um das für die Anwendung erforderliche Schutzniveau zu bestimmen, erweist sich in den meisten Anwendungsfällen des Maschinen- und Anlagenbaus die Ermittlung des Performance Levels (PL) nach der EN ISO 13849-1. Die EN 62061 ist insbesondere für klein- und mittelständische Unternehmen im Maschinen- und Anlagenbau, die eine Vielzahl von Projekten im Sondermaschinenbau bearbeiten und Einzelfertigung von Maschinen realisieren, zu komplex und zu umfangreich.

- Um die Auswahl von Komponenten sowie die Integration von Maschinen in Anlagen und Netzwerkumgebungen, die nach dem SIL (Safety Integrity Level) der EN 62061 klassifiziert wurden, zu ermöglichen, ist eine klare, verbindliche und leicht verständliche Zuordnungstabelle zwischen PL und SIL notwendig.

- Zur Unterstützung der Anwender und deren Konstrukteure sind Hilfsmittel , die den Umgang mit der Norm erleichtern, bereits zu Beginn der Übergangsphase zur Verfügung zu stellen, um Erfahrungswerte und Erkenntnisse zu sammeln. Die entsprechenden Bemühungen des BGIA (Berufsgenossenschaftliches Institut für Arbeitsschutz), in Kürze einen Leitfaden mit Musterberechnungen zu gängigen Konstruktionen und eine Software zur Verfügung zu stellen, mit deren Hilfe man die "Sicherheitsbezogenen Teile von Steuerungen" rechnerisch auf Basis der EN ISO 13849-1 ermitteln kann, werden vom VDMA begrüßt und entsprechend unterstützt.

- Da die probabilistische Betrachtungsweise der neuen Normenansätze auf geeigneten Zuverlässigkeitskennwerten von Bauteilen aufbaut, ist es wichtig, dass diese Werte zumindest für die Standardkomponenten in zentralen und zugänglichen Bibliotheken zur Verfügung stehen. Im Hinblick auf eine praxistaugliche Lösung unterstützt der VDMA ein konzertiertes Vorgehen der Hersteller entsprechender Bauteile.

Kontakt:
Dieter Gödicke
Telefon: +49 69 66 03-14 92
E-Mail: dieter.goedicke@vdma.org

Frankfurt, 30.05.2007 - DG

Anhang J:
Stichwortverzeichnis

Eine Übersicht der in den Schaltungsbeispielen verwendeten Abkürzungen findet sich in Tabelle 8.2 auf Seite 90.

Seite

C

D

E

F

Seite

F (Fortsetzung)

G

H

I

K

L

Seite

L (Fortsetzung)

M

N

O

P

Seite

P (Fortsetzung)

Q

R

S

T