DGUV
Deutsche Gesetzliche Unfallversicherung
Spitzenverband

IFA Report 1/2025

Funktionale Sicherheit von Maschinensteuerungen

– Anwendung der DIN EN ISO 13849 –

Impressum

Herausgegeben von: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)
Glinkastraße 40
10117 Berlin
Telefon: 030 13001-0 (Zentrale)
E-Mail: info@dguv.de
Internet: www.dguv.de

Verfasst von: Michael Hauke, Thomas Bömer, Christian Werner, Jan Zimmermann, Michael Dorra, Paul Rempel, Albert Bohlscheid, Torsten Borowski, Oliver Lohmaier, Andy Lunfiel, Jonas Stein, Jürgen Uppenkamp, Burkhard Köhler, Karl-Heinz Büllesbach, Stefan Otto, Martin Ulrich, Andre Steimers, Pascal Beckers, Martin Fechtner

Ausgabe: Mai 2025

Satz und Layout: Atelier Hauer + Dörfler; IFA

Bildnachweis: Titel: ©stock.adobe.com – Gorodenkoff; IFA
andere: IFA

ISBN (online) 978-3-948657-66-6
ISBN (print) 978-3-948657-64-2
ISSN: 0173-0387

Bezug: Bei Ihrem zuständigen Unfallversicherungsträger oder unter
www.dguv.de/publikationen › Webcode: p022734

Kurzfassung

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

Die Norm DIN EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ macht Vorgaben für die Gestaltung von sicherheitsbezogenen Teilen von Steuerungen. Das IFA begleitet die Weiterentwicklung dieser Norm und ihre Umsetzung in die Praxis bereits seit über 25 Jahren. Dieser Report ist eine Aktualisierung des gleichnamigen IFA Reports 2/2017 und seiner beiden Vorgänger aus den Jahren 1997 und 2008. Er stellt die wesentlichen Inhalte der Norm in ihrer nunmehr vierten Ausgabe von 2023 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. Zudem greift der Report neue Anforderungen aus der Maschinenverordnung auf, wenn diese Einfluss auf sicherheitsbezogene Teile von Steuerungen haben. Auf der Basis dieser Informationen erlaubt der Report die Auswahl des erforderlichen Performance Levels PL_r für steuerungstechnische Sicherheitsfunktionen. Die Bestimmung des tatsächlich erreichten Performance Levels PL wird detailliert erläutert. Auf die Anforderungen zum Erreichen des jeweiligen Performance Levels und seine zugehörigen Kategorien, auf die Bauteilzuverlässigkeit, Diagnosedeckungsgrade, Softwaresicherheit und Maßnahmen gegen systematische Ausfälle sowie Ausfälle 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. Die komplett neu überarbeitete und erweiterte Fassung dieses Reports zeigt, wie die Anforderungen der DIN EN ISO 13849-1 in die technische Praxis umgesetzt werden können, und leistet damit einen Beitrag zur einheitlichen Anwendung und Interpretation der Norm auf nationaler und internationaler Ebene.

Abstract

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

The DIN EN ISO 13849-1 standard, Safety of machinery – Safety-related parts of control systems, contains provisions governing the design of such parts. The Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) has monitored ongoing development of the standard and its implementation in practice for over 25 years. This report is an update of IFA Report 2/2017 with the same title, and its two predecessors, which were published in 2008 and 1997. It describes the essential subject-matter of the standard in its 2023 edition (now the fourth), 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 relationship between the standard and the essential safety requirements of the Machinery Directive is illustrated, and possible methods for risk assessment are presented. Where they have an impact on safety-related parts of control systems, the report addresses new requirements in the Machinery Directive. Based upon this information, the report can be used to select the required performance level (PL_r) for safety functions in control systems. Determining of the performance level (PL) actually attained is explained in detail. The requirements for attainment of the relevant PL and its associated categories, component reliability, levels of diagnostic coverage, software safety and measures for the prevention of systematic and common-cause failures are all discussed comprehensively. Background information is also provided on implementation of the requirements in real-case control systems. Numerous example circuits show, down to component level, how performance levels of 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 that are well-tried with respect to their safety functionality. A comprehensive bibliography is provided from which a more detailed understanding of the examples provided can be obtained. The completely revised and expanded edition of this report shows how the requirements of DIN EN ISO 13849-1 can be implemented in engineering practice, and thus makes a contribution to consistent application and interpretation of the standard at national and international level.

Résumé

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

La norme DIN EN ISO 13849-1 « Sécurité des machines – Parties des systèmes de commande relatives à la sécurité » fournit des directives quant à la conception des parties des systèmes de commande relatives à la sécurité. L'Institut de sécurité au travail de l'assurance sociale allemande contre les accidents (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, IFA) accompagne déjà le perfectionnement de la norme et sa mise en pratique depuis plus de 25 ans. Le présent rapport est une mise à jour du rapport éponyme de l'IFA datant de 02/2017 ainsi que des deux versions précédentes de 2008 et 1997. Il présente les points essentiels de la quatrième version de la norme, de 2023, et en illustre l'application à travers de nombreux exemples dans les domaines de l'électromécanique, de la technique des fluides, de l'électronique et de l'électronique programmable – ce qui inclut les systèmes de commande relevant de technologies mixtes. Il met en avant le lien existant entre la norme et les exigences essentielles de sécurité de la directive européenne relative aux machines. Par ailleurs, il cite différentes possibilités d'évaluation des risques. Le rapport reprend les nouvelles exigences de l'ordonnance sur les machines dès lors que celles-ci ont une influence sur les parties des systèmes de commande relatives à la sécurité. Sur la base de ces informations, le rapport permet de choisir le niveau de performance (PL_r) requis pour les fonctions de sécurité des systèmes de commande. Il détaille le processus de détermination du niveau de performance (PL) effectivement atteint. Il approfondit également les exigences à satisfaire pour atteindre le PL requis et ses catégories correspondantes, la fiabilité des composants, le taux de couverture de diagnostic, la sécurité des logiciels, les mesures de prévention des problèmes systématiques et les défaillances de cause commune. Des informations contextuelles sur la mise en œuvre des exigences dans le cadre de l'utilisation des systèmes complètent l'offre. De nombreux exemples de circuits montrent, jusqu'au niveau des éléments, comment réaliser la mise en œuvre technique des PL a à e avec les catégories B à 4 dans les technologies pertinentes. Ils fournissent également des indications sur les principes de sécurité appliqués et les éléments qui ont fait leurs preuves en termes de sécurité. Enfin, de nombreuses références permettent une compréhension plus approfondie des différents exemples. La version du présent rapport, entièrement remaniée et enrichie, montre comment satisfaire en pratique les exigences de la norme DIN EN ISO 13849-1. Ce faisant, elle contribue à garantir une application et une interprétation uniformes de la norme tant au niveau national qu'international.

Resumen

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

La norma DIN EN ISO 13849-1 „Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad.“ especifica cómo deben diseñarse las partes de los sistemas de mando relativas a la seguridad. El Instituto de protección laboral (IFA, por sus siglas en alemán) del Seguro de accidentes legal alemán lleva más de 25 años apoyando el desarrollo de la norma y su aplicación en la práctica. El presente informe es una actualización del informe homónimo del IFA del 2/2017 y de sus dos predecesores de los años 2008 y 1997. Presenta los contenidos esenciales de la norma en su cuarta edición del 2023 y explica su aplicación con numerosos ejemplos de los ámbitos de electromecánica, técnica de fluidos, electrónica y electrónica programable, entre los cuales se encuentran también sistemas de mando de diferentes tecnologías. Se señala la relación entre la norma y los requisitos básicos de seguridad de la directiva de máquinas. Asimismo, se presentan posibles procedimientos para la valoración del riesgo. El informe recopila los nuevos requisitos del reglamento de máquinas cuando estos influyen en las partes de los sistemas de mando relativas a la seguridad. Basándose en esta información, el informe permite elegir el Performance Level (PL_r) necesario para funciones de seguridad relativas a la técnica de mando. Se explica con detalle la determinación del Performance Level (PL) que realmente se alcanza. Se abordan con detalle los requisitos para alcanzar el PL pertinente 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 y errores con una causa común. La oferta se completa con información de fondo sobre la aplicación de los requisitos a la práctica de la técnica de mando. Numerosos ejemplos de circuitos muestran, hasta el nivel de los componentes, cómo pueden aplicarse técnicamente los PL de la a a la e con las categorías B a 4 en las diferentes tecnologías. En ellos, se hace alusión a los principios de seguridad empleados y a componentes cuya técnica de seguridad está acreditada. Numerosas referencias bibliográficas ayudan a comprender mejor los diferentes ejemplos. La nueva versión del informe, ampliada y completamente revisada, muestra cómo pueden aplicarse a la práctica técnica los requisitos de la norma DIN EN ISO 13849-1, con lo que contribuye a conseguir una aplicación e interpretación unitarias de la norma a nivel nacional e internacional.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Beschreibung
B_{10D}	Anzahl der Zyklen, bis 10 % der Bauteile gefahrbringend ausgefallen sind (für Bauteile mit mechanischem Verschleiß)
CCF	Ausfall infolge gemeinsamer Ursache, engl.: common cause failure
DC	Diagnosedeckungsgrad, engl.: diagnostic coverage
DC_{avg}	durchschnittlicher Diagnosedeckungsgrad
EMI	elektromagnetische Störung, engl.: electromagnetic interference
FMEA	Ausfalleffektanalyse, engl.: failure modes and effects analysis
MTTF	mittlere Dauer bis zum Ausfall, engl.: mean time to failure
$MTTF_D$	mittlere Dauer bis zum gefahrbringenden Ausfall, engl.: mean time to dangerous failure
MTBF	mittlere Zeit zwischen Ausfällen, engl.: mean time between failures
MV	Maschinenverordnung (EU) 2023/1230
M	Motor
n_{op}	mittlere Anzahl jährlicher Betätigungen, engl.: number of annual operations
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde, engl.: average frequency of a dangerous failure per hour
PL	Performance Level
PL_r	erforderlicher Performance Level, engl.: required performance level
RDF	Anteil gefahrbringender Ausfälle, engl.: ratio of dangerous failures
SB	Teilsystem, engl.: sub system
SPS	speicherprogrammierbare Steuerung
SRS	Spezifikation der Sicherheitsanforderungen, engl.: safety requirements specification
SRP/CS	sicherheitsbezogenes Teil einer Steuerung, engl.: safety-related part of a control system
SIL	Sicherheits-Integritätslevel, engl.: safety integrity level
SF	Sicherheitsfunktion, engl.: safety function
STO	sicher abgeschaltetes Drehmoment, engl.: safe torque off
TE	Testeinrichtung, engl.: test equipment
OTE	Ausgang der Testeinrichtung, engl.: output of test equipment
T_M	Gebrauchsdauer, engl.: mission time
T_{10D}	mittlere Zeit bis 10 % der Bauteile gefahrbringend ausfallen, engl.: mean Time until 10 % of the components fail dangerously
r_t	Testrate, engl.: test rate
r_d	Anforderungsrate, engl.: demand rate
LVL	Programmiersprache mit eingeschränktem Sprachumfang, engl.: limited variability language
FVL	Programmiersprache mit nicht eingeschränktem Sprachumfang, engl.: full variability language
SRASW	sicherheitsbezogene Anwendungssoftware, engl.: safety-related application software
SRESW	sicherheitsbezogene Embedded-Software, engl.: safety-related embedded software
V&V	Verifizierung und Validierung

1 Vorwort

2006 wurde die erste, grundlegende Revision der Steuerungsnorm DIN EN ISO 13849-1 veröffentlicht. Kurz darauf erschien der BGIA-Report 2/2008 „Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849“, der sich wie sein Vorläuferreport 6/97 erneut als Bestseller entwickelte. Mehr als 20 000 deutschsprachige gedruckte Exemplare wurden versendet, noch höher sind die Zahlen der Downloads auf den Internetseiten des Instituts für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA). Nach einer Normänderung 2015 gab es eine erfolgreiche Neuauflage als IFA Report 2/2017. Nun ist nach einer zweiten grundlegenden Revision 2023 die vierte Auflage der Steuerungsnorm erschienen. Mit ihr erscheint die vorliegende komplett überarbeitete und erweiterte Neuauflage unseres IFA Steuerungsreports.

Mit seinen Reports und weiteren Hilfsmitteln zur Anwendung der Norm – dem weitverbreiteten Software-Assistenten SISTEMA, den SISTEMA-Kochbüchern und der „Drehscheibe“ sowie dem neuen Software-Assistenten SOFTEMA – hat das IFA einen wichtigen Beitrag zur erfolgreichen Einführung von neuen Ansätzen zur Beurteilung und Auslegung der Zuverlässigkeit von pneumatischen, hydraulischen, elektronischen und programmierbaren Steuerungen geleistet. Die Kombination von strukturellen Anforderungen mit der Abschätzung von Ausfallhäufigkeiten ist in allen Normen der funktionalen Sicherheit, sowohl als ISO- wie als IEC-Normen, verankert und mittlerweile in fast allen Industriesektoren etabliert – so auch im Maschinenbau. Der Normensetzung ist es nicht zuletzt durch die intensive Mitwirkung erfahrener Fachleute des IFA gelungen, die DIN EN ISO 13849-1 so zu gestalten und weiterzuentwickeln, dass sie bei aller Komplexität der Materie praktisch anwendbar bleibt – einschließlich der Bewertung von sicherheitsbezogener Software. Die Vorgängernorm EN 954 mit ihren rein deterministischen Anforderungen wurde im Zuge der Normrevisionen endgültig abgelöst. Der Performance Level ist im Maschinenbau etabliert.

Prof. Dr. *Dietmar Reinert*

In den vergangenen Jahren hat die Norm ISO 13849-1 weltweit ihre Stellung als der Standard für Maschinensteuerungen ausgebaut und es konnten weitere Praxiserfahrungen gesammelt werden. Die Fachleute des IFA haben die wesentlichen Umsetzungsfragen in eigenen Veröffentlichungen kommentiert und ihre Meinungen mit den Anwendern und im Normungsgremium diskutiert.

Mit der Veröffentlichung der vierten Normausgabe 2023 war der richtige Zeitpunkt für eine weitere umfassende Überarbeitung des IFA Reports zu sicherheitsrelevanten Steuerungen von Maschinen gekommen. Das Autorenteam hat alle Inhalte und alle Beispiele überarbeitet und neue Themen ergänzt. Zusätzlich werden die Änderungen der Norm herausgestellt und interpretiert. Wiederum wird auch eine englische Sprachfassung erscheinen.

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

2 Einleitung

Seit dem 1. Januar 1995 müssen alle Maschinen, die innerhalb des europäischen Wirtschaftsraumes in Verkehr gebracht werden, den grundlegenden Anforderungen der Maschinenrichtlinie [1] genügen. Als Maschine gilt nach Artikel 2 dieser Richtlinie die Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eine/s beweglich ist, sowie gegebenenfalls von Betätigungsgeräten, Steuer- und Energiekreisen, die für eine bestimmte Anwendung zusammengefügt sind, z. B. Verarbeitung, Behandlung, Fortbewegung und Aufbereitung eines Werkstoffes. Seit der Novelle 2006/42/EG der Maschinenrichtlinie [2] werden auch Sicherheitsbauteile, die Hersteller mit dem Verwendungszweck der Gewährleistung einer Sicherheitsfunktion gesondert in Verkehr bringen und deren Ausfall und/oder Fehlfunktion die Sicherheit von Personen gefährdet und die für das Funktionieren der Maschine nicht erforderlich sind oder durch übliche Bauteile ersetzt werden können, unter den Begriff „Maschine“ im Sinne der Richtlinie gefasst. Als Maschinen im Sinne der Richtlinie bzw. zugehörige Produkte nach der neuen Verordnung über Maschinen, dazugehörige Produkte und unvollständige Maschinen (EU) 2023/1230 [3] gelten auch auswechselbare Ausrüstungen, Lastaufnahmemittel, Ketten, Seile, Gurte und abnehmbare Gelenkwellen. Detaillierte Ausführungen zu den einzelnen Punkten bietet der Leitfaden für die Anwendung der Maschinenrichtlinie 2006/42/EG [4]. Durch die neue Verordnung über Maschinen wird die Bedeutung sicherheitsrelevanter Software betont, sie kann jetzt auch ein Sicherheitsbauteil sein, wenn sie Sicherheitsfunktionen ausführt und separat in Verkehr gebracht wird.

Die grundlegenden Anforderungen an Konstruktion und Bau von Maschinen und Sicherheitsbauteilen finden sich im Anhang I der Richtlinie bzw. Anhang III der Verordnung. Neben den allgemeinen Grundsätzen für die Integration der Sicherheit gibt es in diesen Anhängen nach wie vor eigene Abschnitte zu Steuerungen und Befehlseinrichtungen von Maschinen und den Anforderungen an Schutzeinrichtungen. Die grundlegenden Sicherheitsanforderungen bei der Gestaltung von Maschinen und Sicherheitsbauteilen verpflichten Hersteller, eine Risikobeurteilung vorzunehmen, um alle mit der Maschine verbundenen Gefährdungen zu ermitteln. Drei Grundsätze werden genannt, um die mit den einzelnen Gefährdungen verbundenen Risiken auf ein akzeptables Maß zu reduzieren, die Anwendung muss in der nachfolgend angegebenen Reihenfolge erfolgen. Die Vorgehensweise wird auch 3-Stufen-Methode genannt:

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

Nach Artikel 7 der Maschinenrichtlinie bzw. Artikel 20 der Verordnung über Maschinen lässt die Einhaltung harmonisierter europäischer Normen, deren Fundstelle im Amtsblatt der Europäischen Union (EU) veröffentlicht worden ist („Listung“), die Übereinstimmung mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie vermuten. Mehrere Hundert harmonisierte europäische Normen vertiefen bzw. konkretisieren die im Anhang I der Maschinenrichtlinie bzw. Anhang III der Maschinenverordnung zugrunde formulierten Grundlagen zur Erreichung der Arbeitssicherheit an Maschinen.

Die neue Verordnung über Maschinen (EU) 2023/1230 ist im Juli 2023 offiziell im EU-Amtsblatt veröffentlicht worden. Die meisten Artikel gelten nach einer Übergangsfrist von 42 Monaten ab dem 20. Januar 2027 und die Verordnung löst die Maschinenrichtlinie 2006/42/EG ab. Bei der Überarbeitung wurde die komplette Struktur der Maschinenrichtlinie an die neuen technologischen Herausforderungen angepasst und um aktuelle Themen wie maschinelles Lernen und Datenverfälschung ergänzt. Somit erhebt die neue Maschinenverordnung beispielsweise den Anspruch, auch neue Technologien in der Verwendung im Arbeitsbereich sicher einzusetzen und Innovationen zu fördern. Durch die Verordnung sollen die Risiken zukünftiger Technologien abgedeckt werden und es wird eine klare Definition der Wirtschaftsakteure eingeführt.

Die Umsetzung der oben genannten 3-Stufen-Methode konkretisiert die Typ-A-Norm DIN EN ISO 12100 [5] und beschreibt den iterativen Prozess zur Risikominderung einschließlich des Verfahrens zur Identifizierung von Gefährdungen sowie deren Risikoeinschätzung und Risikobewertung. Der technische Report DIN ISO/TR 14121-2:2013 [6] ist ein praktischer Leitfaden für die Risikobeurteilung mit Verfahrensbeispielen.

Auf Basis dieser grundlegenden DIN EN ISO 12100 beschreiben die aktualisierte Norm DIN EN ISO 13849-1:2023 [7] und DIN EN ISO 13849-2:2013 [8], wie die erforderliche Risikominderung bei Gestaltung, Aufbau und Integration von sicherheitsbezogenen Teilen von Steuerungen und Schutzeinrichtungen unabhängig von der Technologie erreicht werden kann. Es werden demnach Ausführungen in Elektrik, Elektronik, Hydraulik, Pneumatik und auch Mechanik berücksichtigt. Im Sinne der 3-Stufen-Methode setzt die Anwendung der Normenreihe die Risikominderung durch Stufe 2 um, siehe **Abbildung 2.1**.

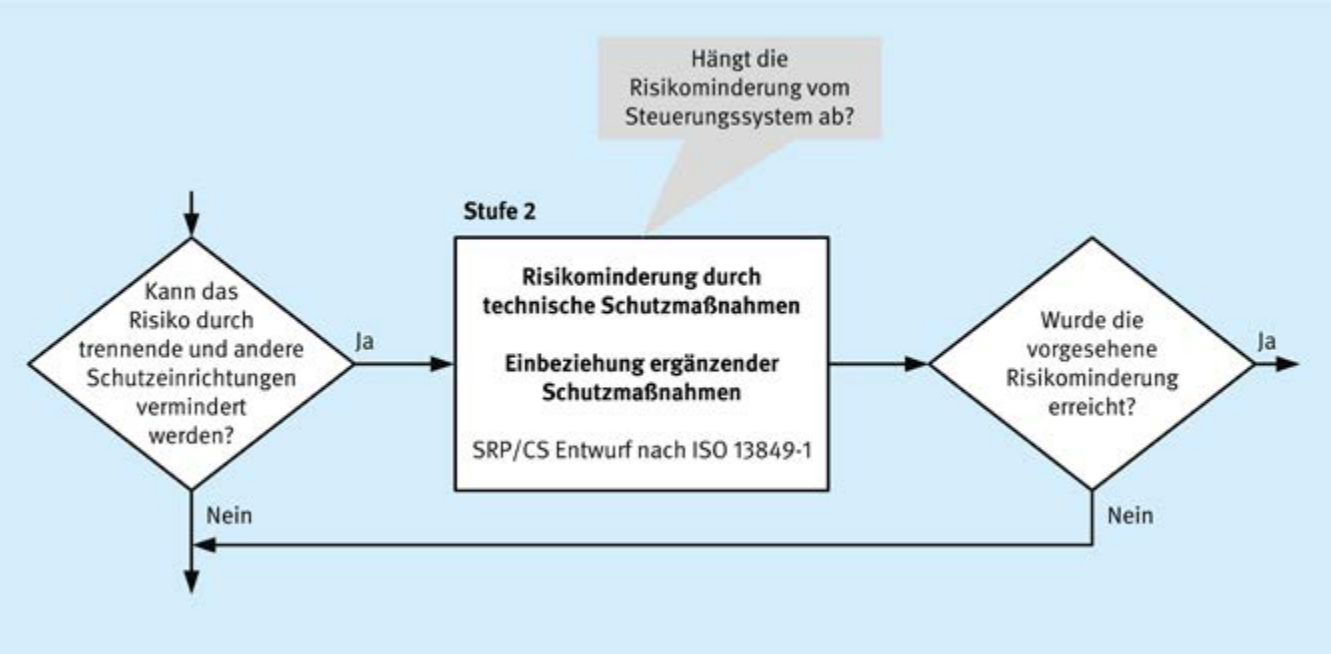


Abb. 2.1 Anwendung der Stufe 2 der DIN EN ISO 12100 zur Risikominderung (in Anlehnung an Bild 1 der DIN EN ISO 13849-1)

Mit DIN EN ISO 13849-1 wird eine allgemein anwendbare Systematik für Steuerungen von Maschinen und deren Schutzeinrichtungen vorgelegt. Die in der Norm beschriebenen Performance Level (PL) erweitern den aus DIN EN 954-1 bekannten Kategoriebegriff. Die sicherheitstechnischen Architekturen sind flexibel einsetzbar. Wesentlicher Pluspunkt der Norm ist die oben bereits skizzierte, technologieunabhängige Behandlung von sicherheitsbezogenen Teilen von Steuerungen (SRP/CS). Über den PL sind Kombinationen verschiedener Steuerungsstrukturen mit verschiedenen Technologien einfach realisierbar. Dabei bietet die Norm auf ca. 100 Seiten alles Notwendige aus einem Guss. Weitere 90 Seiten mit informativen Anhängen dienen als Hilfen zur praktischen Umsetzung. Die Methoden sind von der konkreten Anwendung oder Technologie unabhängig formuliert und werden deshalb von nahezu allen Produktnormen für die Sicherheit von Maschinen (in der Regel Typ-C-Normen) in Bezug genommen.

Die Norm erhielt als harmonisierte Norm nach Inkrafttreten der revidierten Maschinenrichtlinie 2006/42/EG im Dezember 2009 ein stärkeres Gewicht. Dies wird im Wesentlichen auf die Neuerung zurückgeführt, dass Logikeinheiten für Sicherheitsfunktionen in den Anhang IV der Richtlinie aufgenommen wurden, in der Verordnung über Maschinen ist dies nun Anhang I, Teil B. Für solche Produkte sind nach Richtlinie und Verordnung besondere Konformitätsbewertungsverfahren erforderlich, was sie verstärkt in den Mittelpunkt der Sicherheitsbetrachtung rückte [9; 10]. Anhang-IV-Produkte bzw. Anhang-I-Teil-B-Produkte sind nicht prinzipiell EG-baumusterprüfpflichtig – sie können auch unter einem von einer notifizierten Stelle bewerteten umfassenden Qualitätssicherungssystem des Herstellers in den Markt eingeführt werden oder nach harmonisierten Normen mit interner Fertigungskontrolle entwickelt und gefertigt sein. Bei Produkten, die im Anhang I, Teil A der Maschinenverordnung gelistet sind, wie Sicherheitsbauteile mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens oder Hebebühnen für Fahrzeuge, muss für die Konformitätsbewertung vor dem Inverkehrbringen eine notifizierte Stelle eingebunden werden. Durch die neue Maschinenverordnung ist für diese Produkte eine weitere Möglichkeit zur Konformitätsbewertung hinzugekommen. Demnach hat der Hersteller nun auch die Möglichkeit, im Rahmen einer Einzelprüfung (Modul G gemäß Anhang X) mithilfe einer notifizierten Stelle die Konformität nachzuweisen.

Der vorliegende, umfassend überarbeitete IFA Report hat zum Ziel, die Anwendung der DIN EN ISO 13849 zu erläutern und insbesondere anhand zahlreicher Lösungen die praktische Realisierung beispielhaft aufzuzeigen. Besonderes Augenmerk liegt auf der Darstellung und Interpretation der neuen oder überarbeiteten Anforderungen der vierten Ausgabe der DIN EN ISO 13849-1. Weder die Erläuterungen noch die Beispiele sind als offizieller nationaler oder europäischer Kommentar zu DIN EN ISO 13849-1 aufzufassen. Vielmehr sind in diesem Report die Erfahrungen des Instituts für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) aus 40 Jahren Praxis bei der Beurteilung von Schutz- und Steuereinrichtungen der unterschiedlichen Technologien und aus der langjährigen Mitwirkung in einschlägigen nationalen und internationalen Normungsgremien zusammengetragen.

Abb. 2.2
Die Seite www.dguv.de/ifa/13849 bietet den Einstieg und Links zu allen Praxishilfen zur Sicherheit von Maschinensteuerungen

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

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

Unter www.dguv.de/ifa/13849 bietet das IFA einen zentralen Zugang zu allen Informationen und Hilfen zur funktionalen Sicherheit von Maschinensteuerungen (**Abbildung 2.2**). Neben einer breiten Palette an weiteren Veröffentlichungen zu Spezialthemen und den freien Software-Tools „SISTEMA“ (Sicherheit von Steuerungen an Maschinen) und „SOFTEMA“ (Software von Steuerungen an Maschinen) können dort auch die SISTEMA-Projektdateien zu den Schaltungsbeispielen im Kapitel 11 heruntergeladen werden. Zukünftige Erweiterungen sollen stets aktuelle Hilfen zur Verfügung stellen.

Als Orientierung für die Leserinnen und Leser, die mit dem IFA Report 2/2017 bereits vertraut sind, sind am Anfang der Kapitel in diesem Report die wesentlichen Änderungen gegenüber der letzten Fassung kurz zusammengefasst.

3 Basisnormen zur funktionalen Sicherheit von Maschinensteuerungen

Änderung gegenüber dem IFA Report 2/2017

- Alle Angaben wurden an die aktuellen Ausgabestände der Normen angepasst.
- Die Verwendung von Teilsystemen, die nach generischen IEC-Normen zur funktionalen Sicherheit entwickelt worden sind, wurde ergänzt.

Neben der in diesem Report behandelten Norm DIN EN ISO 13849 gibt es alternative, aber relevante allgemeine Normen im Bereich der funktionalen Sicherheit[1]. Dies sind, wie in **Abbildung 3.1** dargestellt, die Normen der Reihe DIN EN 61508 [9] und ihre Sektornorm DIN EN IEC 62061 [10] für die Maschinenindustrie. Während DIN EN 61508 in ihrem Anwendungsbereich auf elektrische, elektronische und programmierbar elektronische Systeme beschränkt ist, wurde der Anwendungsbereich der Sektornorm mit der Ausgabe 2023-02 auf nicht-elektrische Technologien erweitert.

Als Klassifizierungsschema sind in DIN EN 61508 und DIN EN IEC 62061 sogenannte Sicherheits-Integritätslevel (SIL) festgelegt. Diese sind ein Gradmesser für die sicherheitsgerichtete Zuverlässigkeit. Es handelt sich einerseits um Ausfallgrenzwerte, die jeweils eine Dekade umfassen. Andererseits gibt es sogenannte Architektur-Einschränkungen und Anforderungen zur systematischen Eignung, die im jeweiligen Level erfüllt werden müssen. DIN EN 61508 unterscheidet zwei verschiedene Anwendungen von Sicherheitsfunktionen:

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

In der Betriebsart mit niedriger Anforderungsrate ist die Maßzahl für die Sicherheit die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls einer Sicherheitsfunktion bei Anforderung PFD_{avg} (Average Probability of Dangerous Failure on Demand). In der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung wird die mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde *PFH* (Average Frequency of a Dangerous Failure per Hour) bewertet. DIN EN ISO 13849-1 behandelt ausschließlich Sicherheitsfunktionen nach der zweiten Definition. Beide Normen aus dem Maschinensektor begrenzen den Anwendungsbereich, Systeme mit höchsten Risiken im Bereich von SIL 4 werden im Maschinenbereich nicht angenommen (**Abbildung 3.2**) und sie berücksichtigen ausschließlich eine Risikominderung im Sinne der DIN EN ISO 12100 durch sicherheitsbezogene Steuerungssysteme.

Die augenscheinliche Überlappung des Regelungsanspruchs beider Normenwelten kann für Steuerungshersteller und andere Normennutzende auf den ersten Blick nur unbefriedigend sein. Sowohl EN ISO 13849-1 als auch EN IEC 62061 sind unter der Maschinenrichtlinie harmonisierte Normen. Die Teile 1 bis 4 der DIN EN 61508 haben zwar unter IEC-Aspekten den Status von Sicherheitsgrundnormen (Ausnahme: einfache Systeme, die z. B. nur aus elektromechanischen Bauteilen aufgebaut sind), 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 gleichwertige Ergebnisse?
- Sind die Klassifizierungsschemata (PL und SIL) kompatibel?
- Können Geräte, die unter Berücksichtigung einer der Normen entwickelt wurden, im Rahmen der Realisierung einer Sicherheitsfunktion nach einer anderen Norm eingesetzt werden?

Der grundlegende Ansatz der von der International Electrotechnical Commission (IEC) erarbeiteten Normen zur funktionalen Sicherheit (DIN EN 61508 und DIN EN IEC 62061), Ausfallhäufigkeiten und nicht speziell auch Architekturen als charakteristische Kenngröße zu definieren, erscheint zunächst universeller. DIN EN ISO 13849-1 vereint mit der Definition des PL den deterministischen Ansatz der Kategorien mit dem Aspekt der sicherheitstechnischen Zuverlässigkeit. Die vorgesehenen Architekturen im Sinne der Norm sind eher ein Angebot (vereinfachter Ansatz) als eine Verpflichtung. Sie

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

sind jedoch als zentrales Element der Vereinfachung des in DIN EN ISO 13849-1 implementierten probabilistischen Ansatzes zu verstehen und ihre Anwendung ist einer der Hauptaspekte dieses Reports. DIN EN ISO 13849-1 bietet Anwenderinnen und Anwendern die Möglichkeit, Sicherheitsfunktionen von einem Sensor (z. B. Laserscanner) bis hin zu einem Aktor (z. B. Ventil), auch wenn sie verschiedene Technologien umfassen, unter dem Dach einer Norm zu entwickeln und zu bewerten. Neben Teil 1 der DIN EN ISO 13849 existiert auch ein Teil 2 mit dem Titel „Validierung“, dessen normativer Teil in die vierte Ausgabe des Teils 1 integriert wurde und den Teil 2 in dieser Hinsicht ersetzt. Die Anhänge A bis D des Teils 2 enthalten umfangreiches Material zu den Themen „Grundlegende Sicherheitsprinzipien“, „Bewährte Sicherheitsprinzipien“, „Bewährte Bauteile“ und „Fehlerlisten“. Details hierzu sind im Anhang C dieses Reports dargestellt. Der Teil 2 befindet sich aktuell in der Überarbeitung, es sind aber neben der Streichung des bisherigen normativen Teils keine grundlegenden Änderungen zu erwarten. Zahlenmäßig gibt es zwischen PL und SIL korrespondierende *PFH*-Bereiche (**Abbildung 3.2**), die im praktischen Alltag schnell erste Abschätzungen erlauben.

Bisher gab es unzweifelhaft ein deutliches Übergewicht in der Anwendung der DIN EN ISO 13849-1. Das sich dies durch die Erweiterung des Anwendungsbereiches der DIN EN IEC 62061 grundlegend ändert, ist nicht zu erwarten. DIN EN ISO 13849-1 erlaubt eingeschränkt den Einsatz von sogenannten Standardkomponenten und kann auch auf Entwicklungen mit Embedded-Software als FVL (full variability language) angewendet werden – beides ist nicht im Anwendungsbereich der DIN EN IEC 62061 enthalten. Der Entwurf komplexer programmierbarer elektronischer Teilsysteme oder Teilsystemelemente fällt ebenfalls nicht in den Anwendungsbereich der DIN EN IEC 62061. Dies soll nach DIN EN 61508 oder damit verbundenen Normen erfolgen. Auch DIN EN ISO 13849-1 verweist für spezielle Fragestellungen wie die Auswirkungen von Abweichungen in Datenkommunikationsprozessen oder

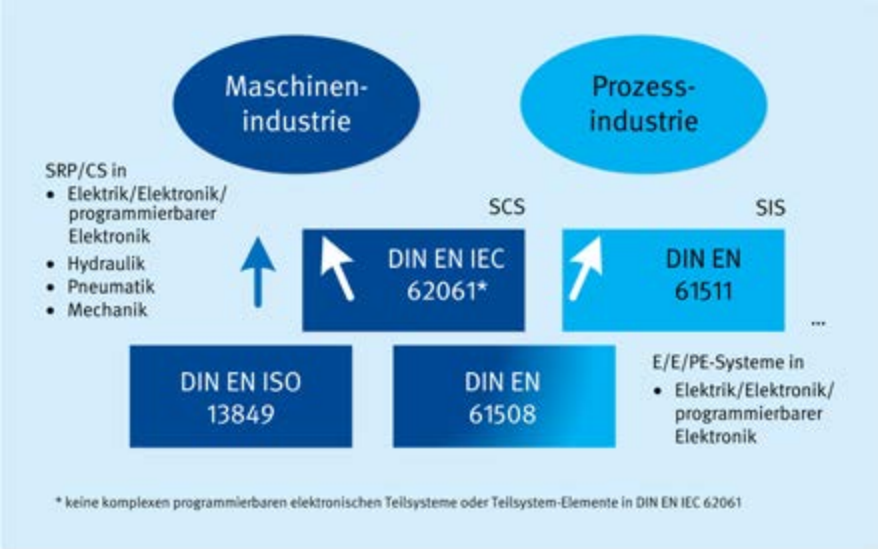


Abb. 3.1
Anwendungsbereiche verschiedener Basisnormen zur funktionalen Sicherheit; SRP/CS: sicherheitsbezogene Teile einer Steuerung; SCS: sicherheitsbezogenes Steuerungssystem; SIS: Prozessleittechnik-Sicherheitseinrichtung; E/E/PE-System: elektrisch/elektronisch/programmierbar elektronisches System

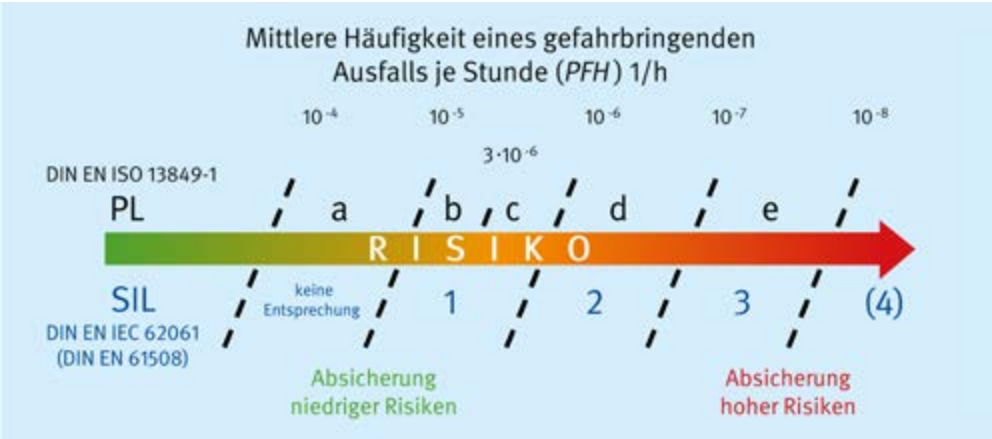


Abb. 3.2
PL und SIL als Häufigkeit eines gefahrbringenden Ausfalls je Stunde

Embedded-Software im PL e ohne Diversität für Spezifikation, Entwurf und Codierung in den beiden vorgesehenen Kanälen auf die DIN EN 61508.

Was die „Anerkennung“ untereinander angeht, können Teilsysteme, die nach DIN EN IEC 62061 entwickelt und validiert wurden, unter DIN EN ISO 13849-1 verwendet werden. Gleiches gilt für Teilsysteme nach DIN EN 61508, wenn sie für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung und nach Route 1_H dieser Norm entwickelt worden sind. Umgekehrt gilt dies nur eingeschränkt. Teilsysteme mit komplexen Komponenten, die nach DIN EN ISO 13849-1 entwickelt und validiert worden sind, hat der Normensetzer für die Verwendung in Sicherheitsfunktionen nach DIN EN IEC 62061 ausgeschlossen. Natürlich werden insbesondere Firmen, die Sicherheitskomponenten wie eine speicherprogrammierbare Steuerung (SPS) für Sicherheitsanwendungen in großer Zahl herstellen, weltweit auch andere Märkte als den Maschinenbereich bedienen wollen und daher z. B. neben DIN EN ISO 13849 auch DIN EN 61508 als Basis einer Entwicklung heranziehen.

Von Seiten der IEC wurde bereits 2011 der Vorschlag für eine Zusammenlegung beider Normen zu einer ISO/IEC-Norm gemacht (auch als „Merging“ bezeichnet) und 2012 mit dieser Arbeit begonnen. Das Ergebnis eines internationalen Fragebogens im Rahmen der Arbeiten zu ISO/IEC 17305 zeigt für die Bereiche Maschinenherstellung und Endanwendung eine klare Dominanz in der Anwendung der 13849-Normen. Unter Fachleuten wurde die Erstellung der geplanten ISO/IEC 17305 heftig diskutiert. Erklärte Ziele waren eine einfache Anwendung der neuen Norm und Beibehaltung bisheriger Methoden. Die Frage, ob eine neue Norm diesen Zielen gerecht geworden wäre und ob sie die bestehenden Normen hätte ablösen können, kann nicht beantwortet werden. Die Arbeiten wurden 2015 erfolglos eingestellt, was zu den nun abgeschlossenen Revisionen der vorhandenen Normen führte.

Mit den jeweiligen Überarbeitungen haben die Normensetzer von ISO und IEC die Anwendbarkeit und Eindeutigkeit der Formulierung von Anforderungen z. B. auch durch informative Anhänge zum Thema Software verbessert. Einzelne Anpassungen können auch als thematische Angleichung der beiden Normen gewertet werden, auch wenn die konkreten technischen Anforderungen sich nicht immer gleichen. Eine Zusammenlegung beider Normen wird in deutschen Normenkreisen aktuell nicht befürwortet.

Den zunehmend wichtiger werdenden und auch von der neuen Maschinenverordnung (EU) 2023/1230 thematisierten Aspekt „Security“ benennen beide Maschinennormen, ohne jedoch technisch konkret zu werden. Anhang O dieses Reports widmet sich dem Thema und gibt erste allgemeine Lösungsansätze.

4 Report und Norm im Überblick

Änderung gegenüber dem IFA Report 2/2017:

- Verweise aktualisiert
- Neuer Abschnitt 4.1 zum Management der funktionalen Sicherheit
- Abschnitt 4.5 (vorher 4.4) zu Änderungen durch die vierte Ausgabe der Norm 2023 neu verfasst
- Neuer Abschnitt 4.6 zu IFA Hilfen ausführlicher verfasst
- Abschnitt 4.7 (vorher 4.5) zur künftigen Entwicklung der Norm aktualisiert

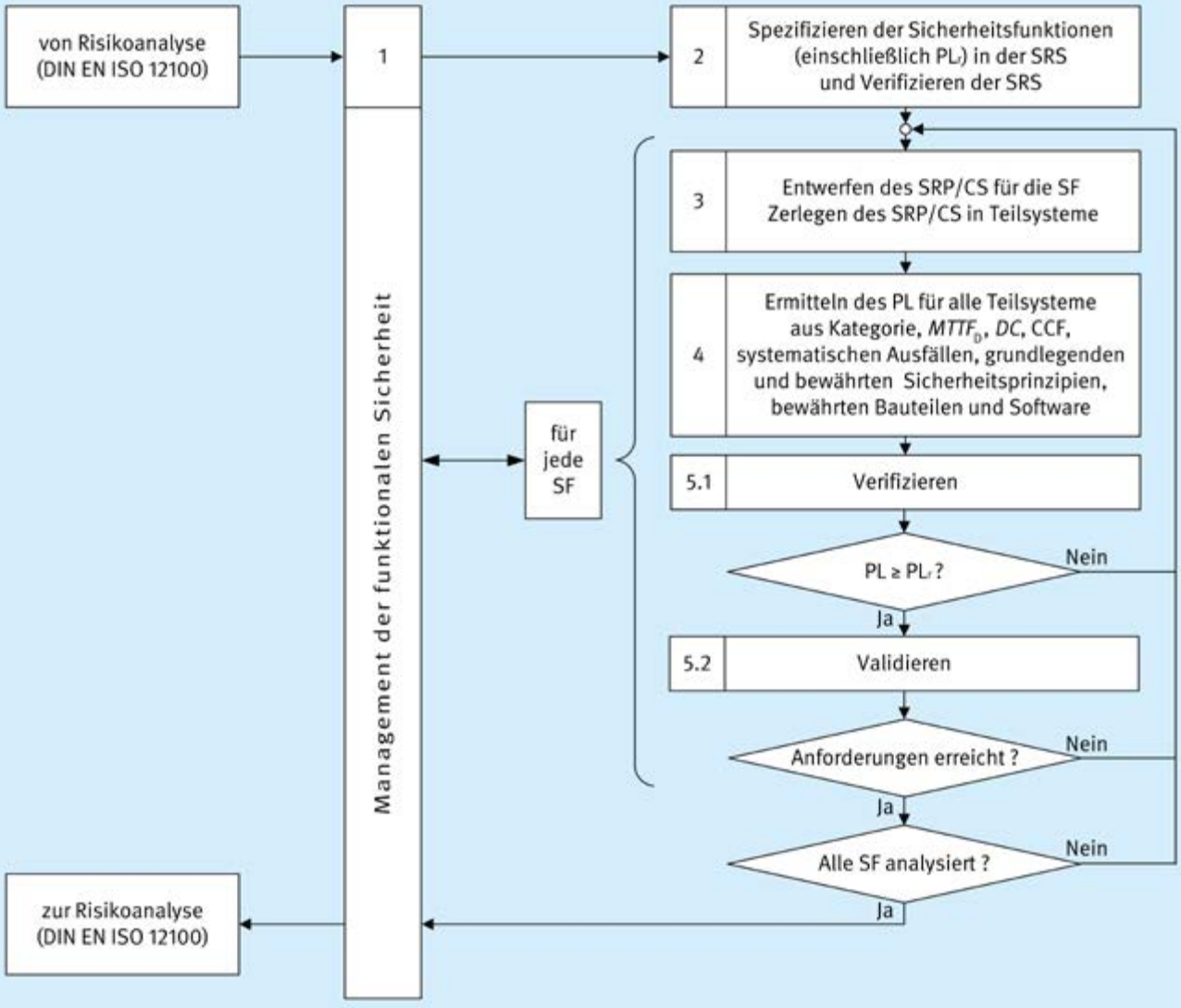


Abb. 4.1 Iterativer Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen: SF = Sicherheitsfunktion; PL = Performance Level; PL_r = erforderlicher Performance Level; SRP/CS = Safety-Related Part of a Control Systems (sicherheitsbezogener Teil einer Steuerung); SRS = Safety Requirements Specification (Spezifikation der Sicherheitsanforderungen); $MTTF_D$ = 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)

Dieses Kapitel stellt die Querbezüge zwischen der Norm und den weiteren Kapiteln und Anhängen dieses Reports her. Gleichzeitig gibt es einen Überblick über den iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen und orientiert sich dabei an **Abbildung 4.1**, die auf Bild 4 der Norm basiert. Am Ende des Kapitels werden die Änderungen von der dritten zur vierten Ausgabe der Norm und ihre zukünftige Entwicklung angesprochen sowie die begleitenden IFA Hilfen vorgestellt.

4.1 Management der funktionalen Sicherheit

Mit der vierten Ausgabe wurde in der Norm erstmals die Forderung nach einem Plan der funktionalen Sicherheit festgeschrieben. Bereits in den vorhergehenden Normausgaben gab es dazu verschiedene Ansätze, wie das V-Modell des Software-Sicherheitslebenszyklus oder den Validierungsplan. Strukturierte und systematische Entwicklung einschließlich Dokumentation gehört außerdem zum bewährten Fundament des Entwicklungsprozesses im Maschinenbau, besonders für sicherheitsbezogene Funktionen. Die nun auch explizit im Plan der funktionalen Sicherheit zu definierenden Maßnahmen für das Management der funktionalen Sicherheit sollen systematische Ausfälle bei der Spezifikation, Entwicklung und Umsetzung vermeiden. Daher beschreibt dieser Plan Aktivitäten, Aufgaben, Rollen und Verantwortlichkeiten, die bereits mit dem Spezifizieren der Sicherheitsfunktionen beginnen und den gesamten Entwicklungs- und Validierungsablauf einschließlich Modifikationen betreffen. In Abbildung 4.1 ist das Management der funktionalen Sicherheit daher mit Block 1 als durchgängige Aktivität vor und neben allen anderen Phasen des Entwicklungsablaufs dargestellt. Ausführliche Erläuterungen zu diesem Thema sind im folgenden Kapitel 5 zu finden. Zusätzlich werden in den weiteren Kapiteln jeweils spezifische Hinweise zu den Managementaktivitäten gegeben, die in den verschiedenen Entwicklungsphasen relevant sind.

4.2 Spezifizieren von Sicherheitsfunktionen und ihren Eigenschaften

Seit der ersten Normausgabe steht als bewährtes Konzept die Spezifikation der Sicherheitsfunktionen (SF) am Anfang des Entwicklungs- und Bewertungsprozesses für SRP/CS. Dieses Vorgehen ist in Abbildung 4.1 durch Block 2 dargestellt und wird im Kapitel 6 ausführlicher beschrieben. Die Frage lautet: Wie sieht der Beitrag der sicherheitsbezogenen Teile der Steuerung zur Reduzierung des Risikos einer Gefährdung an einer Maschine aus?

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

Die Sicherheitsfunktion kann von Teilen der Maschinensteuerung oder von zusätzlich notwendigen Komponenten übernommen werden. Beides sind in diesem Fall sicherheitsbezogene Teile von Steuerungen. Auch wenn durchaus dieselbe Hardware an verschiedenen Sicherheitsfunktionen beteiligt sein kann, kann die erforderliche Qualität der Risikominderung für jede Sicherheitsfunktion unterschiedlich sein. In der Norm wird die Qualität der Risikominderung durch den Begriff „Performance Level“ 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 auch durch trennende Schutzeinrichtungen, z. B. eine Schutztür, oder persönliche Schutzausrüstung, z. B. eine Schutzbrille, verringert werden. Hat man einmal festgelegt, was die steuerungstechnischen Schutzmaßnahmen anteilig leisten müssen, dann hilft ein einfacher Entscheidungsbaum – der „Risikograph“ – bei der schnellen und direkten Bestimmung des geforderten PL_r. Ist die Verletzung irreversibel (z. B. Tod, Verlust von Körperteilen) oder reversibel (z. B. Quetschungen, die verheilen können)? Hält sich die Bedienperson häufig und lange im Gefahrenbereich auf (z. B. öfter als einmal pro 15 Minuten) oder selten und kurz? Hat die Person eine Möglichkeit, den Unfall noch zu vermeiden (z. B. wegen langsamer Maschinenbewegung)? Diese drei Fragen entscheiden über den PL_r. Auch Normen für einzelne Maschinentypen enthalten typischerweise Angaben hinsichtlich des PL_r einzelner Sicherheitsfunktionen, sodass in solchen Fällen der Risikograph nicht zum Einsatz kommen muss oder bereits bei den vorgegebenen PL_r-Angaben berücksichtigt wurde. Details findet man in Abschnitt 6.4, Beispiele im Anhang A und Hinweise zum

Umgang mit überlagerten Gefährdungen in Anhang K. Den Besonderheiten der Betriebsartenwahl als eigene Sicherheitsfunktion widmet sich Anhang J.

4.3 Entwurf und technische Realisierung der Sicherheitsfunktionen

Stehen die Anforderungen an die sicherheitsbezogenen Teile von Steuerungen (SRP/CS) fest, die die jeweilige Sicherheitsfunktion ausführen, folgen zunächst deren Entwurf und danach deren Realisierung. Dies erfolgt typischerweise durch Nutzung bestehender Teilsysteme oder eine eigene Entwicklung solcher Teilsysteme. Daher richten sich die in der Norm aufgeführten Anforderungen sowohl an selbst entwickelte Teilsysteme als auch an die Kombination von Teilsystemen zu SRP/CS. Die Schritte der Blöcke 3 und 4 sind in den Kapiteln 7 bis 9 ausführlich beschrieben. Kapitel 7 widmet sich der Kombination eines SRP/CS aus Teilsystemen, die als bereits validierte Teilsysteme (durch einen PL oder SIL klassifiziert) in die sicherheitsbezogene Steuerung integriert werden können oder nach den in Kapitel 8 (Schwerpunkt Hardware) und Kapitel 9 (Software) beschriebenen Methoden neu entwickelt werden können. In der Tradition der bisherigen Steuerungsreports enthält auch dieser Report im Kapitel 11 viele ausgestaltete Schaltungsbeispiele für alle Steuerungstechnologien und jede Kategorie. Ein ausführlich beschriebenes Schaltungsbeispiel „Planschneidemaschine“ begleitet zusätzlich die allgemeinen Ausführungen in den Kapiteln 6 bis 10. Dadurch werden die nachfolgend beschriebenen Methoden für die Entwicklung und Einflussgrößen, die den PL bestimmen, anschaulich vermittelt.

Sicherheitsbezogene Teile von Steuerungen können ihre risikomindernde Wirkung nur entfalten, wenn am Anfang die Sicherheitsfunktion korrekt definiert wurde. Dieser wichtige Punkt wurde mit der vierten Ausgabe der Norm besonders betont. Bei der folgenden Realisierung fließen als Qualitätskriterien die Güte der verwendeten Bauteile (Lebensdauer), ihr Zusammenspiel (Dimensionierung), die Wirksamkeit der Diagnose (z. B. Selbsttests) und die Fehlertoleranz (Fehlersicherheit) der Struktur (in der Norm als sogenannte Kategorie klassifiziert) ein. Aus diesen Parametern bestimmt sich die mittlere Häufigkeit eines gefährlichen Ausfalls je Stunde (*PFH*) und somit der erreichte PL. DIN EN ISO 13849-1 lässt die zu verwendenden Berechnungsmethoden zur quantitativen Bestimmung des Ausfallhäufigkeit offen. So darf man durchaus die hoch komplexe Markov-Modellierung unter Berücksichtigung der oben genannten Parameter nutzen. Die Norm beschreibt jedoch ein im Sinne der praktischen Anwendbarkeit vereinfachtes Vorgehen, nämlich die Verwendung von vorgesehenen Architekturen mit Anwendung eines Säulendiagramms (Abbildung 8.7, Seite 82), in dem die Modellierung des PL schon vorweggenommen ist. Für Fachleute: Die Herleitung des Säulendiagramms findet sich in Anhang G.

Die Kategorien bleiben nach wie vor das Fundament bei der Bestimmung des PL. An ihrer Definition hat sich seit der ersten Ausgabe der Norm im Wesentlichen kaum etwas geändert (Ausnahme: die vierte Ausgabe bringt einen Paradigmenwechsel bei Kategorie 2), allerdings werden seit der zweiten Ausgabe zusätzliche quantitative 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 (**Tabelle 4.1**).

Einen detaillierten Überblick über die Kategorien liefert Tabelle 8.1 auf Seite 68. Ein wesentlicher Aspekt bei der Verwendung der vorgeschlagenen einfachen Rechenmethoden ist die Darstellung der Kategorien als logische Blockschaltbilder, den sogenannten vorgesehenen Architekturen (Designated Architectures).

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

Eine der meistgestellten Fragen zur Häufigkeit von Ausfällen betrifft die Beschaffung zuverlässiger Ausfalldaten, der $MTTF_D$-Werte ($MTTF_D$: Mean Time to Dangerous Failure), für die sicherheitsbezogenen Komponenten. Hier ist der Bauteil- oder Komponentenhersteller mit seinem technischen Datenblatt allen anderen Quellen vorzuziehen. Viele Komponentenhersteller stellen solche Daten bereits zur Verfügung. Aber auch wenn es keine Herstellerangabe gibt, lassen sich typische Beispielwerte aus etablierten Datensammlungen (z. B. SN 29500 oder IEC 61709) ermitteln. Die Norm und Anhang D dieses Reports listen ebenfalls einige realistische Werte aus der Praxis auf und geben Hinweise zur Modellierung im sicherheitsbezogenen Blockdiagramm.

Die Wirksamkeit der Diagnose, als Wert des mittleren Diagnosedeckungsgrades DC_{avg} (average Diagnostic Coverage), ermittelt sich nach folgendem einfachen Prinzip: Für jeden Block werden die Testmaßnahmen zusammengestellt, die den Block überwachen. Für jede dieser Testmaßnahmen wird einer von vier typischen *DC*-Werten aus einer Tabelle in der Norm ermittelt. Eine nur scheinbar komplexe, aber im Kern einfache Mittelungsformel hilft, daraus die Kenngröße DC_{avg} zu berechnen. Weitere Informationen liefern Abschnitt 8.2.14 sowie Anhang E.

Tabelle 4.1 Qualitative und quantifizierbare Aspekte der Kategorien; mit der zweiten Ausgabe der Norm vorgenommene Ergänzungen zu den quantifizierbaren Aspekten sind hellblau 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 ($MTTF_D$)	mindestens niedrig	hoch	mindestens niedrig	mindestens niedrig	hoch
Fehlererkennung (Tests)			X	X	X
Einfehlersicherheit				X	X
Berücksichtigung von Fehlerakkumulation					X
Mittlerer Diagnosedeckungsgrad – DC_{avg}	kein	kein	mindestens niedrig	mindestens niedrig	hoch
Maßnahmen gegen CCF			X	X	X
Hauptsächlich charakterisiert durch	Bauteilauswahl		Struktur		

Ähnlich einfach wird es schließlich bei der letzten Kenngröße CCF (Common Cause Failure) in Abschnitt 8.2.15: 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 Teilsysteme der Kategorien 2, 3 und 4 nachgewiesen werden, dass ausreichende Maßnahmen gegen CCF getroffen wurden. Dies geschieht anhand eines Punktesystems für acht typische, meist technische Gegenmaßnahmen, mit denen mindestens 65 von 100 möglichen Punkten erreicht werden müssen (Details im Anhang F).

Eine wichtige Ursache für potenzielle Ausfälle einschließlich CCF sind elektromagnetische Störeinflüsse. Den Störfestigkeitsanforderungen für sicherheitsbezogene Systeme widmet sich die Fachgrundnorm DIN EN 61000-6-7. Sie erlaubt neben Störfestigkeitsprüfungen als Nachweis auch andere Methoden, z. B. durch Konstruktion und Analyse. Diesen Ansatz hat die vierte Ausgabe der Norm mit einem Punkteschema für einen Maßnahmenkatalog aufgegriffen, Anhang L erläutert die Methodik.

Neben den zufälligen Hardware-Ausfällen, die durch gute Struktur und geringe Häufigkeit von Ausfällen beherrscht werden können, gibt es das weite Feld der sogenannten systematischen Ausfälle – verursacht durch dem System bereits seit der Konstruktion innewohnende Fehler wie Dimensionierungsfehler, Softwarefehler oder logische Fehler –, vor denen Maßnahmen zur Fehlervermeidung und -beherrschung schützen sollen. Hier haben vor allem die Softwarefehler einen großen Stellenwert. Anforderungen an sicherheitsbezogene Software sind seit der zweiten Ausgabe in der Norm enthalten und im Einzelnen schon länger aus einschlägigen Normen bekannt. Die konkreten Maßnahmen sind je nach gefordertem PL abgestuft. Weitere Informationen zu diesem komplexen Thema geben Abschnitt 8.1.1 für systematische Ausfälle sowie Kapitel 9 „Software“. Die Besonderheiten bei der Verwendung künstlicher Intelligenz im Rahmen von sicherheitsbezogenen Steuerungen beleuchtet Anhang M. DIN EN ISO 13849-1 weist zwar darauf hin, dass Securityaspekte einen Einfluss auf Sicherheitsfunktionen haben können. Sie enthält jedoch selbst keine Anforderungen zum Thema, sondern verweist auf ISO/TR 22100-4 und IEC/TR 63074 (in neuer Überarbeitung IEC/TS 63074). Mit der neuen Maschinenverordnung bekommt das Thema für Maschinenhersteller entsprechende Bedeutung. Der neue Anhang O des Reports gibt „Hinweise zu Security“. Einen Ausblick auf die Arbeiten zu einem neuen ISO/TR 13849-3, der Formeln zur *PFH*-Berechnung beschreiben wird, gibt Anhang N.

4.4 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 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 nötig (z. B. Verwendung anderer Bauteile mit besserer $MTTF_D$), bis der PL schließlich ausreichend gut ist. Ist diese Hürde genommen, so sind eine Reihe von Validierungsschritten notwendig, die bis zur dritten Ausgabe der Norm in Teil 2 der DIN EN ISO 13849 beschrieben waren, aber seit der vierten Normausgabe in Teil 1 der Norm enthalten sind. Diese teilweise auch schon entwicklungsbegleitend stattfindende Validierung stellt systematisch sicher, dass alle funktionalen und leistungsbezogenen Anforderungen an die sicherheitsbezogenen Teile der Steuerung erreicht wurden (siehe Block 5, Abbildung 4.1). Weitere Details dazu finden sich im Kapitel 10.

4.5 Änderungen durch die vierte Ausgabe der Norm aus dem Jahr 2023

Nach den Änderungen zur dritten Ausgabe der Norm– hier ging es in erster Linie darum, die Lesbarkeit und Anwendbarkeit zu verbessern – ist die nun vorliegende vierte Ausgabe der Norm das Ergebnis einer umfassenden Überarbeitung. Einen detaillierten Überblick, konzentriert auf die Änderungen zwischen dritter und vierter Normausgabe, hat das IFA bereits 2023 veröffentlicht [11]. Im Zuge der grundlegenden Überarbeitung wurden die seit 1997 immer weiter gewachsenen und ergänzten Kernabschnitte „Gestaltungsaspekte“, „Sicherheitsfunktionen“ und „Kategorien“ systematisch neu gegliedert, um nach einem „Überblick“ zunächst die „Spezifikation der Sicherheitsfunktionen“ und dann den Entwicklungsablauf abzubilden. Auch die Rolle der Teilsysteme innerhalb einer SRP/CS-Sicherheitskette wird nun präziser definiert – speziell im Hinblick auf die Integration von Teilsystemen, die nach IEC-Normen der funktionalen Sicherheit mit einem SIL versehen sind. Der bisher in den zweiten

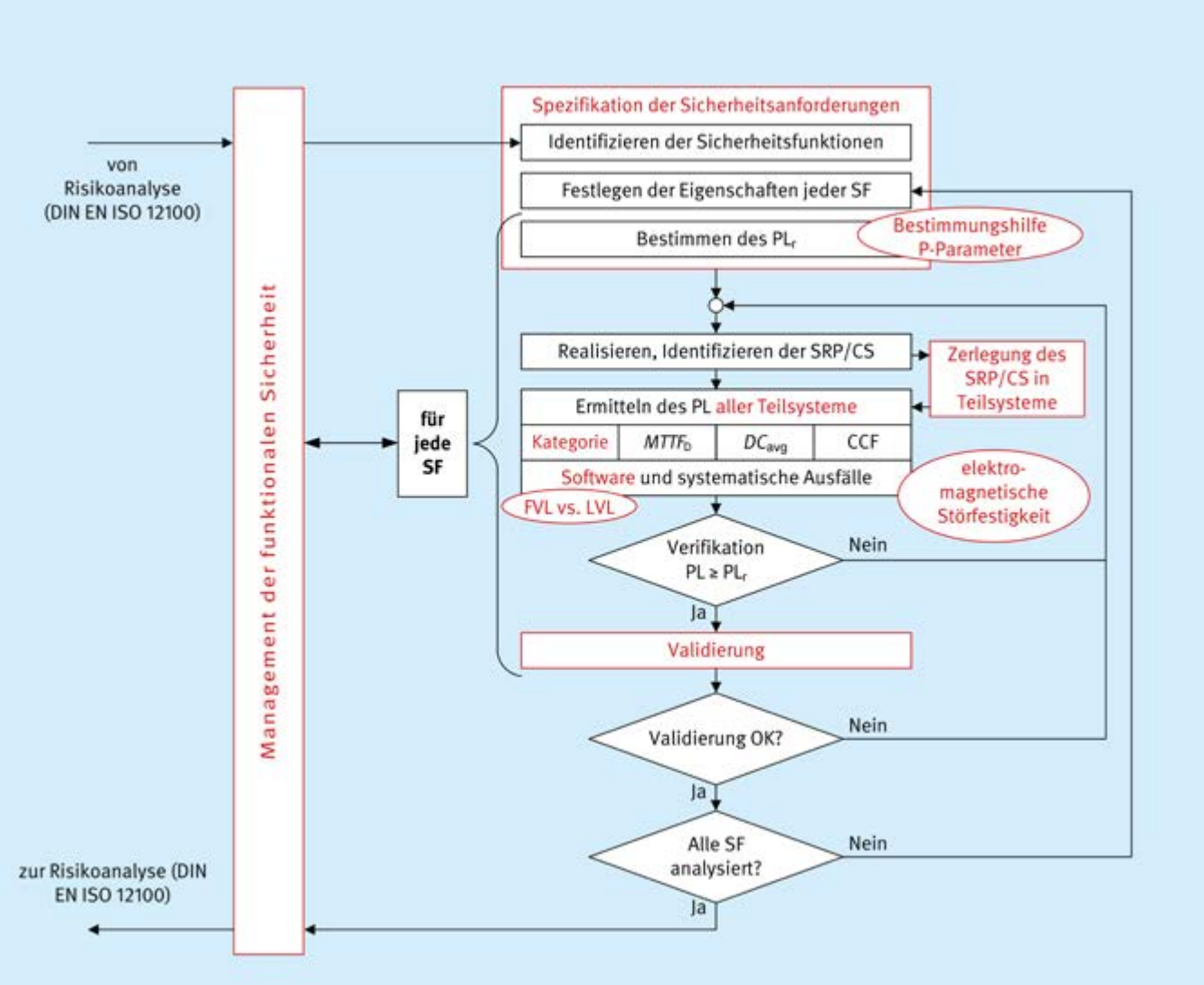


Abb. 4.2 Änderungen in der vierten Ausgabe der Norm in Bezug zum bisherigen Entwicklungsablauf (vgl. Abbildung 4.1): FS = Funktionale Sicherheit, FVL = Full Variability Language (Programmiersprache mit nicht eingeschränktem Sprachumfang), LVL = Limited Variability Language (Programmiersprache mit eingeschränktem Sprachumfang)

Tabelle 4.2 Wesentliche Änderungen in der vierten Ausgabe der Norm sowie die betroffenen Abschnitte von Norm und Report

Abschnitte der Norm	Änderung	Abschnitte des Reports
alle, speziell Überblick (4) bis Validierung (10)	Klarere Strukturierung der Normabschnitte orientiert am Entwicklungsprozess	alle, speziell Report und Norm im Überblick (4) bis Verifikation und Validierung (10)
Systematische Ausfälle (6.1.7), Management der funktionalen Sicherheit (G.5)	Verbindlichere Verankerung des Managements der funktionalen Sicherheit	Systematische Ausfälle (8.1.1), Management der funktionalen Sicherheit (5)
Spezifikation der Sicherheitsanforderungen (5.2)	Ausführlichere Spezifikation der Sicherheitsfunktionen in der SRS	Identifizierung der Sicherheitsanforderungen (6.3)
Möglichkeit zur Vermeidung oder Begrenzung eines Schadens (A.3.3)	Bestimmungshilfe für den P-Parameter (Möglichkeit zur Vermeidung oder Begrenzung eines Schadens) im Risikograph	Bestimmung des PL_r (6.4)
alle, speziell Zerlegung eines SRP/CS in Teilsysteme (5.5) und Kombination von Teilsystemen (6.2)	Klare Trennung zwischen SRP/CS und Teilsystemen	alle, speziell Kombination von Teilsystemen als SRP/CS (7)
Entwurfsaspekte (6), speziell Kategorien (6.1.3)	Kleinere Änderungen bei den Kategorien, insbesondere Paradigmenwechsel bei Kategorie 2	Gestaltung sicherer Steuerungen (8), speziell Ausfallhäufigkeit und Kategorien (8.2)
Elektromagnetische Störfestigkeit (Anhang L)	Leitlinien zur Umsetzung der Maßnahmen für die elektromagnetische Störfestigkeit	EMI und funktionale Sicherheit im Maschinenbereich (Anhang L)
Software-Sicherheitsanforderungen (7), Entwurf von Software (Anhang N)	Weitergehende Erläuterungen zu den Softwareanforderungen, u.a. vereinfachtes V-Modell für modulbasierte LVL, Entscheidungshilfe FVL/LVL, Abstufung der Anforderungen für Software im Testkanal oder bei Diversität	Entwicklung sicherheitsbezogener Software (9)
Validierung (10)	Übernahme der Validierungsanforderungen aus Teil 2 der Norm	Verifikation und Validierung (10)
Begriffe, Symbole und Abkürzungen (3)	Rückkehr zur Abkürzung *PFH* (ohne Index „D“) für die „mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde“	alle

Teil der Norm ausgelagerte Entwicklungsschritt der Validierung wurde nun als Abschnitt 10 inhaltlich weitgehend unverändert in den ersten Teil übernommen, um seine Bedeutung im Kontext eines sicherheitsgerichteten Designs klar herauszustellen. Die detailliertere Darstellung der Anforderungen an sicherheitsgerichtete Software, die neu aufgenommenen Strategien zur praktischen Umsetzung der elektromagnetischen Störfestigkeit und auch die neue Bestimmungshilfe zum P-Parameter des Risikographen stellen weitere wichtige Verbesserungen dar. **Tabelle 4.2** und **Abbildung 4.2** zeigen, welche Hauptänderungen in welche Abschnitte der Norm und des vorliegenden Reports eingeflossen sind.

Die Schaltungsbeispiele in Kapitel 11 des Reports wurden auf der Basis der obigen Normänderungen durchgängig aktualisiert.

Wegen der umfassenden Änderungen ersetzt die vierte Ausgabe der DIN EN ISO 13849-1 die vorherige Ausgabe erst mit einer Übergangsfrist von drei Jahren – beginnend mit der Listung im Amtsblatt der Europäischen Union im Mai 2024. Da die Änderungen – wie im vorherigen Abschnitt beschrieben – aber nur in wenigen Punkten die bestehenden Anforderungen berühren, erscheint der Übergang zwischen der dritten und vierten Ausgabe der Norm gut umsetzbar. Die deutlich gestiegene Seitenzahl der Norm ist hauptsächlich der Übernahme der Validierungsanforderungen und den zusätzlichen praktischen Hilfestellungen und Beispielen geschuldet.

Abb. 4.3
Überblick über die vom IFA zur Verfügung gestellten Hilfen zur praktischen Anwendung der DIN EN ISO 13849, www.dguv.de/ifa/13849

4.6 IFA Hilfen zur Anwendung der DIN EN ISO 13849

Den Entwicklungsprozess nach DIN EN ISO 13849-1 und den Übergang auf neue Norminhalte unterstützt das IFA, wie schon seit Längerem gewohnt, durch frei verfügbare Anwendungshilfen (**Abbildung 4.3**). Dies erfolgt einmal in Form erklärender und mit Beispielen versehener Literatur: Dazu gehören neben dieser Veröffentlichung weitere IFA Reports zu „Sicheren Antriebssteuerungen mit Frequenzumrichtern“ [12], „Sicherheitsbezogener Anwendungssoftware von Maschinen – Die Matrixmethode des IFA“ [13] und „Praxisgerechter Umsetzung der Anforderungen für sicherheitsbezogene Embedded- Software“ [14]. Weiterhin zählt dazu auch das etablierte Freeware-Programm „SISTEMA“ (Sicherheit von Steuerungen an Maschinen) [15], das die Berechnung und Dokumentation von PL_r und PL unterstützt (siehe Anhang H). Die fortlaufend ergänzte Reihe der SISTEMA-Kochbücher [16] widmet sich speziellen Themen, die bei der Anwendung der Norm eine Rolle spielen: Diese betreffen nicht nur SISTEMA selbst (SISTEMA-Bibliotheken, Verwendung von Netzwerkbibliotheken, Mehrere SISTEMA-Instanzen parallel ausführen), sondern auch den gesamten Entwurfsprozess nach der Norm (Definition von Sicherheitsfunktionen, Vom Schaltbild zum PL, Wenn die vorgesehenen Architekturen nicht passen). Die Palette der Unterstützungsangebote zur *PFH*-Bestimmung wird am niederschwelligen Ende abgerundet durch den vom IFA entworfenen „Performance Level Calculator“ [17], der das Säulendiagramm in Form einer Drehscheibe detailliert darstellt. Damit kann man den Einfluss von Kategorie, DC_{avg} und $MTTF_D$ auf *PFH* und PL einfach mit einem Handgriff abschätzen. Am anderen Ende stellt das IFA für erfahrene Personen einen Formelsatz in Anhang N zur Verfügung, mit dem die *PFH* flexibler und angepasster berechnet werden kann. Dahinter steht dasselbe Berechnungsmodell wie für das Säulendiagramm der Norm. Die Formeln unterstützen aber auch unsymmetrische Funktionskanäle und eine größere Bandbreite der Eingangsparameter (Details in Anhang N). Mit dem seit 2022 als Vollversion verfügbaren Freeware-Programm SOFTEMA (Software von Steuerungen an Maschinen) [18] steht ein weiteres mächtiges Werkzeug bereit. SOFTEMA unterstützt durch automatisierte Anwendung von Tabellen die IFA Matrixmethode zur Spezifikation, Validierung und Prüfung sicherheitsgerichteter Anwendungsprogramme, die auf zuvor beurteilte Funktionsbausteine zurückgreifen (siehe Anhang I). Zur weiteren Unterstützung gibt es hier die Reihe der SOFTEMA-Kochbücher [19]. Alle weiterführenden Hilfen und Literatur – darunter z. B. Hinweise auf die Prüfgrundlagen und Prüfgrundsätze [20] des DGUV Test, des Prüf- und Zertifizierungssystems der Deutschen Gesetzlichen Unfallversicherung (DGUV), finden sich auf den Internetseiten des IFA unter www.dguv.de/ifa/13849.

4.7 Künftige Entwicklung von DIN EN ISO 13849

Im direkten Anschluss an die Revision von Teil 1 der Norm hat das zuständige Normungsgremium mit den Vorarbeiten zur Überarbeitung von Teil 2 begonnen. Durch die Übernahme der Validierungsanforderungen in Teil 1 beschränkt sich Teil 2 folglich auf die informativen Anhänge mit grundlegenden und bewährten Sicherheitsprinzipien sowie bewährten Bauteilen, Fehlerlisten und Fehlerausschlüssen für die verschiedenen Steuerungstechnologien. Zusätzlich wird dort ein Validierungsbeispiel mit Schwerpunkt FMEA und *DC*-Bestimmung gezeigt. Bis zum Abschluss der Überarbeitung von Teil 2 sind die Validierungsanforderungen sowohl dort als auch in der vierten Ausgabe von Teil 1 enthalten. Diese vorübergehende Doppelung ist aber unproblematisch, da sich die Anforderungen inhaltlich gleichen. Der oben genannte formelbasierte Ansatz zur *PFH*-Berechnung soll im Format eines Technischen Reports (ISO/TR 13849-3) als dritter Teil der Normenreihe veröffentlicht werden, siehe dazu auch Anhang N.

5 Management der funktionalen Sicherheit und Entwicklungsablauf

Änderung gegenüber dem IFA Report 2/2017:

- Dieses Kapitel 5 ist neu und basiert auf dem bisherigen Abschnitt 6.1.1 Entwicklungsablauf, ergänzt um neue Inhalte zum Management der funktionalen Sicherheit.
- Der Kasten 5.1 wurde angepasst, besonders um den Unterschied zwischen der Neuentwicklung von Teilsystemen und dem Einsatz bereits qualifizierter Teilsysteme zu verdeutlichen.

Während IEC-Normen für funktionale Sicherheit (IEC 61508 und IEC 62061) schon länger explizite Anforderungen an das Management der funktionalen Sicherheit stellen, hat die DIN EN ISO 13849-1 dieses Thema bisher mit Blick auf eher einfach realisierte Sicherheitsfunktionen im Maschinenbau weniger ausführlich behandelt. Trotzdem gab es bis zur dritten Ausgabe der Norm schon verschiedene – mehr oder weniger offensichtliche – Anforderungen an einen Prozess für das Management der funktionalen Sicherheit, meist mit dem Ziel der Vermeidung und Beherrschung systematischer Fehler in der Entwicklung: Schon die für alle Technologien geltenden grundlegenden Sicherheitsprinzipien „Anwendung geeigneter Werkstoffe und Herstellungsverfahren“ und „Geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems“ erfordern Planungs- und Ma-

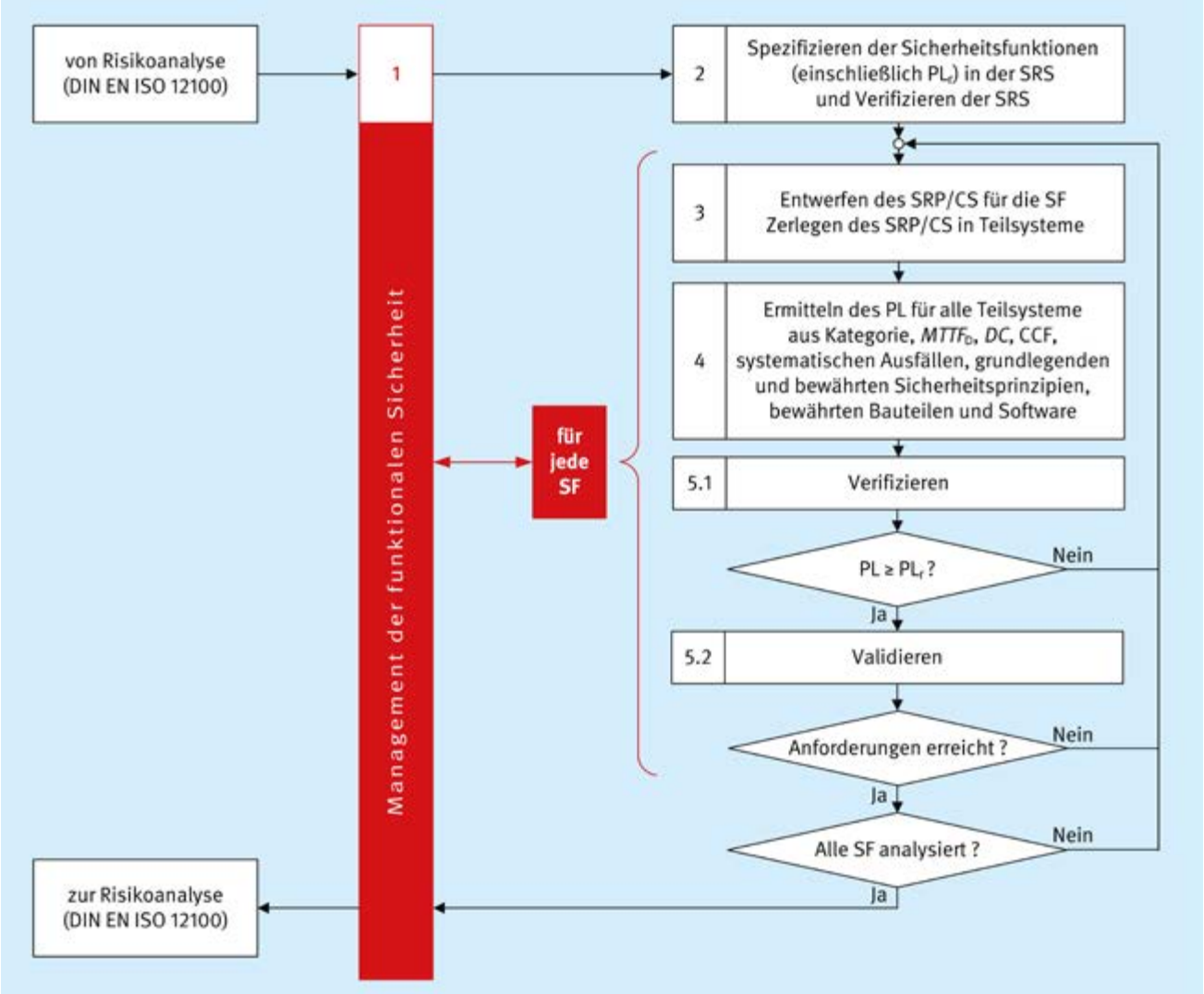


Abb. 5.1 Das Management der funktionalen Sicherheit begleitet den gesamten SRP/CS-Entwicklungsprozess schon ab der Spezifikationsphase

nagementaktivitäten, die sich bei den bewährten Sicherheitsprinzipien „Verringerung von Fehlermöglichkeiten (Trennung sicherheitsbezogener von anderen Funktionen)“ und „Gleichgewicht zwischen Komplexität/Vereinfachung“ fortsetzen. Auch bei den Maßnahmen zur Vermeidung und Beherrschung systematischer Ausfälle sowie den Maßnahmen gegen Ausfälle gemeinsamer Ursache spielen Reviews und werkzeugunterstütze Entwicklung eine wichtige Rolle. Explizit wird mit dem phasenorientierten V-Model des Software-Sicherheitslebenszyklus bereits eine strukturierte Softwareentwicklung gefordert. Auch der im Validierungsplan zu dokumentierende Validierungsprozess setzt ein geplantes Vorgehen mit festen Vorgaben voraus.

Daher ist es nur konsequent, dass die DIN EN ISO 13849-1 mit ihrer vierten Ausgabe das Management der funktionalen Sicherheit unter der Überschrift „Systematische Ausfälle“ (Unterabschnitt 6.1.7 der Norm) nun ausdrücklich fordert: Die Entwicklung und Umsetzung der Sicherheitsfunktionen in Hardware und Software sollen systematisch erfolgen und in einem Plan der funktionalen Sicherheit dokumentiert werden. Dadurch sollen Fehler in der Spezifikation, Entwicklung und Umsetzung von vorneherein vermieden oder verbliebene Fehler erkannt und beseitigt werden. Im neuen Unterabschnitt G.5 nennt die Norm im Detail, wie ein geeignetes Management der funktionalen Sicherheit aussehen sollte. Die an anderen Stellen der Norm gestellten Managementanforderungen, z. B. zum Projektmanagement im Rahmen des Software-Sicherheitslebenszyklus oder im Rahmen der Validierung, können hier integriert werden. Wie in **Abbildung 5.1** skizziert, steht das Management der Funktionalen Sicherheit daher an erster Stelle, da bereits vor Beginn des SRP/CS-Entwicklungsprozesses Aktivitäten und Aufgaben festgelegt sein sollten, z. B. wer für das Spezifizieren der Sicherheitsfunktionen zuständig ist. Darüber hinaus regeln die Managementvorgaben alle Phasen des SRP/CS-Entwicklungsprozesses bis hin zu dessen Abschluss.

Im folgenden Abschnitt 5.1 wird zunächst auf den Plan der Funktionalen Sicherheit eingegangen, der mit der vierten Normauflage neu eingeführt wurde. Abschnitt 5.2 beschreibt anschließend fehlervermeidende Maßnahmen im Entwicklungsablauf, die auch vorher schon in der Norm gefordert waren.

5.1 Plan der Funktionalen Sicherheit

Da der Plan der funktionalen Sicherheit den Entwicklungsablauf von der Spezifikations- und Konzeptphase bis zur Modifikation beschreibt, sollte er in der Regel ein eigenständiges Dokument sein, das bereits zum Projektbeginn einer SRP/CS-Entwicklung vorliegt und auch projektspezifische Belange berücksichtigt. Dabei kann der Umfang und Detaillierungsgrad durchaus individuell an das Entwicklungsprojekt angepasst sein: Einflussgrößen dafür sind die Größe des Projekts, seine Komplexität, die Neuartigkeit des Produkts und der dafür erforderlichen Technologie. Darüber hinaus geht ein,

- in welchem Maße standardisierte Entwicklungsmethoden (z. B. Verwendung von qualifizierten Sicherheitsbauteilen und -modulen) verwendet werden können und
- wie mögliche Folgen bei einem Fehler im Entwicklungsprozess aussehen.

Hier macht es auch einen Unterschied, ob ein komplettes SRP/CS entwickelt wird oder nur ein Teilsystem. Im Einzelnen sollte der Plan der funktionalen Sicherheit mindestens die folgenden Punkte beschreiben:

a) Alle relevanten Aktivitäten und Aufgaben im Verlauf der Entwicklung und Umsetzung des SRP/CS
   - Folgende Aktivitäten sind mindestens zu berücksichtigen: Spezifikation, Entwicklung, Integration, Analyse, (Funktions-)Tests, Verifikation und Validierung.
   - Bei der Planung sind alle relevanten Entwicklungsinhalte und Anforderungen an das SRP/CS zu berücksichtigen. Diese reichen beispielsweise ausgehend von den Sicherheitsfunktionen über die Hardware und Software aller Teilsysteme, deren Kombination, softwarebasierte manuelle Parametrierung, die Kategorien und PL mit qualitativen (z. B. Sicherheitsprinzipien, systematische Ausfälle) und quantifizierbaren Aspekten (*PFH*-Bestimmung) bis hin zur Bedienoberfläche und der Benutzerinformation. Im Plan der funktionalen Sicherheit soll identifiziert werden, wie die Umsetzung aller in der Spezifikation der Sicherheitsanforderungen (SRS) und Entwurfsdokumenten festgelegten Sicherheitsanforderungen nachverfolgt wird (Anforderungsverfolgung bzw. Requirements-Tracing).
   - Die Position jeder Aktivität im Gesamtablauf sollte ersichtlich sein und wann sie stattfinden soll. Beispielsweise wird im Plan der funktionalen Sicherheit festgelegt, wer wann die SRS verfasst und wer sie wann überprüft (z. B. per Review) und freigibt. Hier ist auch die Integration in die Risikobewertung zu beschreiben.

  - Da die DIN EN ISO 13849-1 sich mit der Gestaltung von SRP/CS befasst, bezieht sich der dort geforderte Plan der funktionalen Sicherheit in erster Linie auf den Entwicklungsprozess (einschließlich Modifikation) und nicht direkt auf Fertigung, Betrieb usw. (im Gegensatz zu vgl. DIN EN IEC 62061, Anhang I, speziell Abbildung I.2). Mit Umsetzung ist in diesem Zusammenhang daher die Umsetzung des Designs in Hardware und Software und nicht das Einbauen in die Maschine gemeint.
  - Im Sinne der Reduzierung systematischer Ausfälle ist es trotzdem ratsam, neben dem Einbauen in die Maschine auch sicherheitsbezogene Aspekte bei Fertigung, Betrieb usw. in das Management der funktionalen Sicherheit einzubeziehen (z. B. Rückläufermonitoring und „Incident Reporting“, siehe DIN EN 61508), besonders bei hoher Komplexität des SRP/CS.
  - Als Nachweis können unterschiedliche Maßnahmen, z. B. Reviews, Analysen, Prüfungen, Verifikationen oder Validierungen, angewendet werden.

b) Die Rollen und Hilfsmittel, die nötig sind, um die Aktivitäten durchzuführen und zu überprüfen (z. B. in Form eines Reviews)
  - Der Hinweis z. B. auf ein QS-Handbuch allein ist nicht ausreichend. Bezogen auf das konkrete SRP/CS-Projekt sind die Rollen und Hilfsmittel konkret zu benennen.
  - Ein Managementkonzept nach ISO 9001 ist eine gute Basis, aber das Management der funktionalen Sicherheit geht darüber hinaus, z. B. hinsichtlich des Software-Sicherheitslebenszyklus oder des Validierungsplans.
  - Explizite Anforderungen an die Unabhängigkeit von Personen nennt die DIN EN ISO 13849 nur für die Validierungsaktivitäten.

c) Ablauf und Verfahrensbeschreibung für Konfiguration, Dokumentation, Freigaben und Modifikation von Hardware- und Software-Entwicklung einschließlich der erforderlichen Aktivitäten, bevor eine Modifikation durchgeführt wird
  - Versionsmanagement und Konfigurationsmanagement fallen ebenso unter diesen Punkt wie das Verfolgen/Tracken der Entwicklungsaktivitäten. Zudem muss beschrieben werden, wie geeignete Reaktionen auf Abweichungen von Anforderungen aussehen, wenn diese während des Entwicklungsprozesses, beispielsweise bei der Validierung, festgestellt werden.
  - Nach Abschnitt 10.8 der Norm muss auch die Validierung durch Analyse und Prüfung in geeigneter Weise aufgezeichnet werden, um den Validierungsprozess für jede Sicherheitsanforderung zu belegen.

d) Das Erstellen eines Validierungsplans

e) Identifikation relevanter Aktivitäten vor Ausführung jeder Änderung
  - Identifikation der Ursache der Änderung
  - Einflussanalyse
  - zu wiederholende Aktivitäten
  - zu überarbeitende Dokumente

Tabelle 5.1 zeigt ein Beispiel, wie ein Plan der funktionalen Sicherheit für eine einfache Realisierung aussehen könnte. Dieses Muster kann als Vorlage zur Anpassung an eigene Entwicklungen genutzt werden. Für komplexere Realisierungen ist in der Regel eine umfangreichere Dokumentation erforderlich. Die Aktivitäten im Entwicklungsprozess sind als Zeilen in Tabelle 5.1 aufgeführt. Zu jeder Aktivität sind die zugehörigen Dokumente, die in der Norm genannt werden, angegeben, einschließlich der Referenz auf den entsprechenden Abschnitt der Norm, um die dort niedergelegten Anforderungen nachschlagen zu können. Die Rollen beim Erstellen, Prüfen und Freigeben jedes Dokuments sind durch die Spalten abgebildet. Diese Spalten können zur Verfolgung und Dokumentation der Managementaktivität genutzt werden. Wenn Aktivitäten wiederholt werden müssen, z. B. weil Analyse, Prüfung, Verifikation oder Validierung eine Abweichung von der SRS gezeigt hat, können die resultierenden neuen Dokumentenversionen als zusätzliche Zeilen in der Tabelle hinzugefügt werden. Dies ist beispielhaft für die Aktivität „Spezifikation (sowie ihre Validierung)“ in **Tabelle 5.2** dargestellt.

Weitere Managementaspekte, die sich in dieser Tabelle nicht angemessen abbilden lassen, sollten zusätzlich in geeigneter Form dokumentiert werden. Dies betrifft beispielsweise

- zu verwendende bzw. verwendete Ressourcen, z. B. Entwicklungstools,
- das Verfahren zum Versionsmanagement.

Die in der Norm genannten Dokumente müssen nicht unbedingt als einzelne Dokumente vorliegen. Vielmehr geht es darum, dass die erforderlichen Informationen in geeigneter Form dokumentiert sind, was z. B. auch durch entsprechende Abschnitte in einem Gesamtdokument erfüllt werden kann.

Tabelle 5.1 Beispielhafte Vorlage eines Plans der funktionalen Sicherheit für Aktivitäten und Dokumente im Entwicklungsprozess

Aktivität im Entwicklungsprozess ▸ Dokument (Referenz auf den Normenabschnitt)	Version	erstellt durch, Datum	geprüft durch, Datum	Prüf-Ergebnis	Freigabe durch, Datum
Spezifikation (sowie ihre Validierung) ▸ SRS (**5.2.1.3**) ▸ Validierungsaufzeichnung **(10.8, 5.4, 10.2**)					
Entwicklung Hardware (**10.1.5**) ▸ Funktionsbeschreibung inkl. sicherheitsbezogenem Blockdiagramm ▸ Bestimmung *PFH* und PL ▸ Schaltplan ▸ Zeichnung/Montageplan ▸ Ablaufdiagramm ▸ Bauteilliste ▸ ggf. Fehlerlisten/Fehlerausschlüsse (**10.1.3**, **10.1.4**) ▸ Prüfplan (**10.4.1a**) ▸ Prüfaufzeichnungen (**10.4.1b**), Berichte über Reviews, Validierungsaufzeichnung (**10.8**) ▸ ggf. weitere Dokumente					
Entwicklung Software (**7.1**, **7.3.1**, **7.4**) ▸ SW-Design-Spezifikation ▸ SW-System-Design-Spezifikation ▸ Modul-Design-Spezifikation ▸ Quellcode ▸ Testplan (z. B. Modul-, SW-Integrations-Testplan) ▸ Berichte über Reviews, Prüfungen, Validierung (ab PL c) ▸ ggf. weitere Dokumente					
Softwarebasierende manuelle Parametrierung (**6.3**) ▸ Hersteller/Integrator: Verifikation des Parametrierungstools (**6.3.4**) ▸ Benutzer: Dokumentation der Parametrierung (**6.3.5**)					
Validierungsplanung ▸ Validierungsplan (**10.1.2**)					
Analyse (**10.1.5i**) ▸ Dokumentation HW-Analyse ▸ Dokumentation SW-Analyse ▸ Validierungsaufzeichnung (**10.8**)					
Prüfung/Tests (**10.4.5**, **10.5**) ▸ Dokumentation HW-Tests (**10.4.1b**) ▸ Dokumentation SW-Tests (**10.4.1b**) ▸ Dokumentation Funktionstests aller SF (**10.4.1b**) ▸ Validierungsaufzeichnung (**10.8**)					
Benutzerinformation ▸ für die Integration (**13.2**) ▸ für den Benutzer (**13.3**)					

Aktivität im Entwicklungsprozess ▸ Dokument (Referenz auf den Normenabschnitt)	Version	erstellt durch, Datum	geprüft durch, Datum	Prüf-Ergebnis	Freigabe durch, Datum
Validierung der Sicherheitsfunktionen (**10.5**), sowie Validierung und Verifizierung der Sicherheitsintegrität des SRP/CS und aller Teilsysteme (**10.6**) ▸ Validierungsaufzeichnung (**10.8**)					
Änderungsmanagement mit Auswirkungsanalyse ▸ Dokumentation der zu wiederholenden Phasen, zu überarbeitenden Dokumente usw. (**7.3.1g**, **7.4j**, **G.5e**)					

Tabelle 5.2 Beispielhaft ausgefüllte Vorlage eines Plans der funktionalen Sicherheit für Aktivitäten und Dokumente im Entwicklungsprozess, auszugsweise für die Aktivität „Spezifikation (sowie ihre Validierung)“

Aktivität im Entwicklungsprozess ▸ Dokument (Normreferenz)	Version	erstellt durch, Datum	geprüft durch, Datum	Prüf-Ergebnis	Freigabe durch, Datum
Spezifikation (sowie ihre Validierung) ▸ SRS (**5.2.1.3**) ▸ Validierungsaufzeichnung (**10.8**)	V1.13	Meier, 13.04.23	Müller, 20.04.2023	Mängel, Überarbeitung erforderlich	keine Freigabe
▸ SRS (**5.2.1.3**) ▸ Validierungsaufzeichnung (**10.8**)	V1.16	Meier, 25.04.23	Müller, 27.04.2023	**OK**	**Schulze, 30.04.2023**
Entwicklung Hardware (**10.1.5**) ▸ ...	...	...	...	...	...

5.2 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 muss, wie in **Abbildung 5.2** dargestellt, auf den gesamten Lebenszyklus einer Maschine ausgerichtet sein. Wie die in der vierten Ausgabe der DIN EN ISO 13849-1 aufgenommenen Anforderungen zum Management der funktionalen Sicherheit belegen, 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 in Abschnitt 4 der Norm deutlich. Die Phase der Validierung ist durch eigene strukturierte Abläufe gekennzeichnet und wird in Kapitel 10 genauer beschrieben (siehe Abbildung 5.2). Sehr ausführlich wird die Strukturierung in Lebensphasen durch das bei der Erstellung sicherheitsrelevanter Software verwendete V-Modell gekennzeichnet; Kapitel 9 erläutert dies. Auch wenn der Gestaltungsprozess für SRP/CS zwar auf Modifikationen während des Entwicklungsprozesses eingeht, aber z. B. nicht explizit auf die Phase der Instandhaltung, so wird diese Phase dennoch über erforderliche Inhalte in der Benutzerinformation berücksichtigt.

Da SRP/CS Teile einer Maschine sind, können Anforderungen aus jeder Phase des Lebenszyklus der Maschine auch Einfluss auf ein SRP/CS haben. Daher müssen auch alle Phasen im Lebenszyklus der Maschine bei der Identifikation und Festlegung der Eigenschaften von Sicherheitsfunktionen berücksichtigt werden. Um dies möglichst umfassend und nachprüfbar zu gestalten, müssen Sicherheitsfunktionen vor der Herstellung der Maschine spezifiziert werden. Abschnitt 6.3 dieses Reports und das SISTEMA-Kochbuch 6 [21] widmen sich ausführlich dem Thema, wie eine Sicherheitsfunktion definiert wird und was dabei zu beachten ist. Teilsysteme, die nicht speziell für eine Anwendung entwickelt werden, z. B. ein Lichtgitter oder eine Sicherheits-SPS, bedürfen einer besonders genauen Beschreibung ihrer Kenndaten und ihrer Schnittstellen, um eine korrekte Verwendung sicherzustellen.

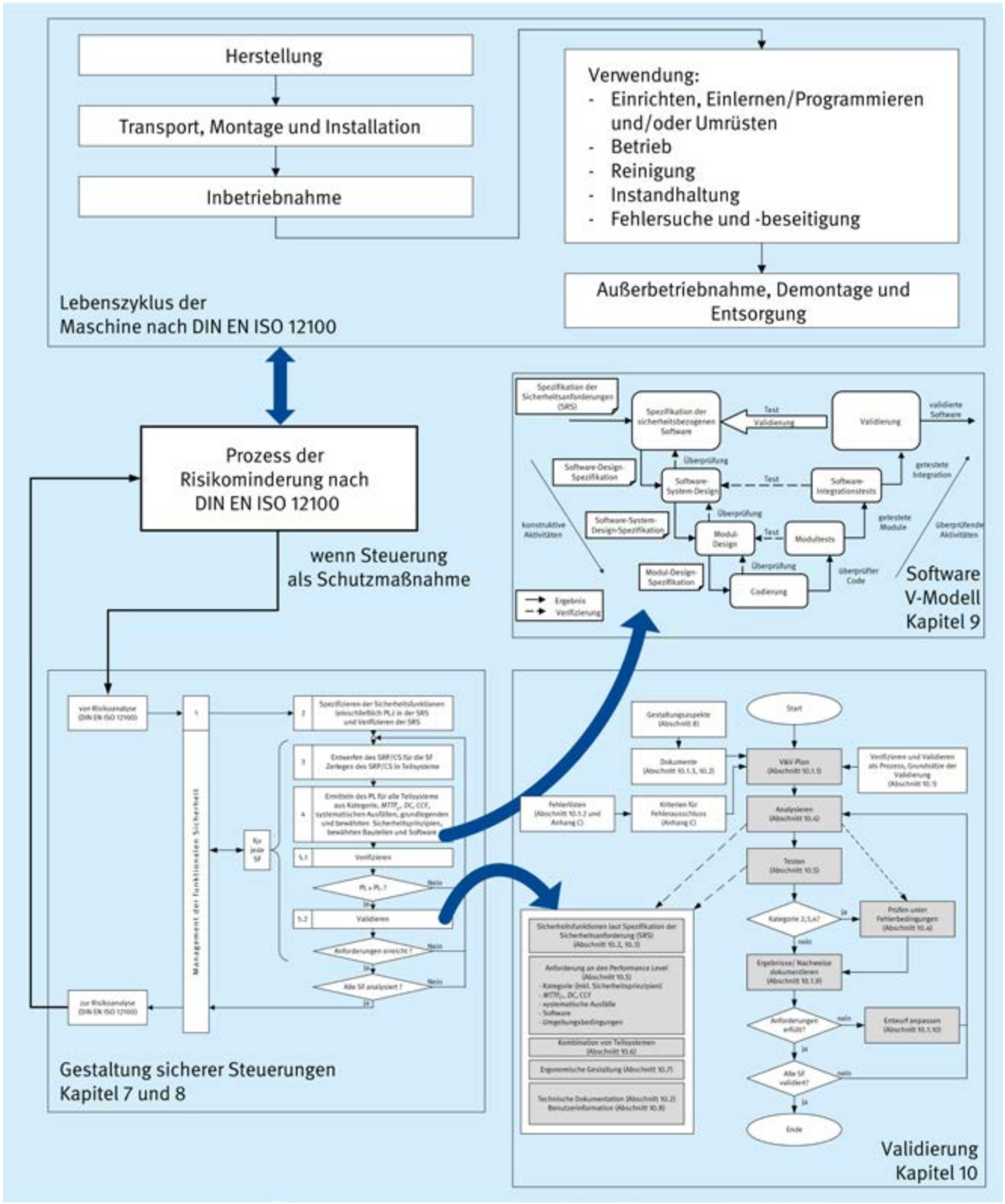


Abb. 5.2 Lebenszyklus der Maschine und SRP/CS-Entwicklung

Mit der Spezifikation der Sicherheitsfunktionen beginnt die SRP/CS-Entwicklung. 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 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 5.1** ein allgemeines Gliederungsschema für eine Spezifikation der Sicherheitsanforderungen aufgezeigt, dass die Spezifikation der Sicherheitsfunktionen einschließt. Dieses Gliederungsschema bezieht sich auf SRP/CS, die die gesamte Sicherheitsfunktion ausführen. Für Teilsysteme, die Teilfunktionen ausführen, ist die Spezifikation entsprechend anzupassen.

Kasten 5.1 Allgemeines Gliederungsschema für eine Spezifikation der Sicherheitsanforderungen

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

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

3. Erforderliche(r) Performance Level (PL_r)
   - 3.1 Referenz auf vorhandene Dokumentation zur Risikobeurteilung der Maschine
   - 3.2 Ergebnisse der Risikobeurteilung für jede ermittelte Gefährdung oder Gefährdungssituation und Festlegung der zur Risikominderung jeweils erforderlichen Sicherheitsfunktion(en)

4. Sicherheitsfunktionen (Angaben gelten für jede Sicherheitsfunktion, siehe auch Tabelle 4 in [21])
   - Funktionsbeschreibung („Erfassen – Verarbeiten – Ausgeben“) einschließlich aller funktionalen Eigenschaften (siehe auch Tabellen 6.1 und 6.2)
   - Aktivierungs-/Deaktivierungsbedingungen oder -ereignisse (z. B. Betriebsarten der Maschine)
   - Verhalten der Maschine beim Auslösen der Sicherheitsfunktion
   - zu berücksichtigende Wiederanlaufbedingungen
   - Leistungskriterien/Leistungsdaten
   - Ablauf (zeitliches Verhalten) der Sicherheitsfunktion mit Reaktionszeit
   - Häufigkeit der Betätigung (d. h. Anforderungsrate), Erholungszeiten nach Anforderung
   - sonstige Daten
   - einstellbare Parameter (soweit vorgesehen)
   - Einordnung und Zuordnung von Prioritäten bei gleichzeitiger Anforderung und Bearbeitung mehrerer Sicherheitsfunktionen
   - Verhalten bei Energieausfall
   - funktionales Konzept zur Trennung bzw. Unabhängigkeit/Rückwirkungsfreiheit zu Nicht-Sicherheitsfunktionen und weiteren Sicherheitsfunktionen

5. Vorgaben für den SRP/CS-Entwurf
   - 5.1 Zuweisung, durch welche SRP/CS und in welcher Technologie die Sicherheitsfunktion realisiert werden soll; welche Teilsysteme sollen neu entwickelt werden und welche bereits qualifizierten Teilsysteme sollen zum Einsatz kommen
   - 5.2 Auswahl der Kategorie, vorgesehene Architektur (Struktur) als sicherheitsbezogenes Blockdiagramm mit Beschreibung bei Neuentwicklung von Teilsystemen
   - 5.3 Schnittstellenbeschreibung (Prozessschnittstellen, interne Schnittstellen, Bedienschnittstellen, Bedien- und Anzeigeelemente usw.)

5.4 Einschaltverhalten, Umsetzung des erforderlichen Anlaufverhaltens und Wiederanlaufverhaltens
5.5 Leistungsdaten: Zykluszeiten, Reaktionszeiten usw.
5.6 Verhalten des SRP/CS bei Bauteilausfällen und -fehlern (Erreichen und Aufrechterhalten des sicheren Zustandes) einschließlich Zeitverhalten bei Neuentwicklung von Teilsystemen
5.7 Zu berücksichtigende Ausfallarten von Bauteilen, Baugruppen oder Blöcken und ggf. Begründung für Fehlerausschlüsse bei Neuentwicklung von Teilsystemen
5.8 Konzept zur Umsetzung der Erkennung und Beherrschung von zufälligen und systematischen Ausfällen (Selbsttests, Testschaltungen, Überwachungen, Vergleiche, Plausibilitätsprüfungen, Fehlererkennung durch den Prozess usw.) bei Neuentwicklung von Teilsystemen
5.9 Bei Implementierung von Sicherheitsfunktionen durch Software relevante Angaben und Vorgaben für Entwicklung und Validierung
5.10 Vorzusehende CCF-Maßnahmen bei Neuentwicklung von Teilsystemen
5.11 Quantitative Aspekte
5.11.1 Zielwerte für $MTTF_D$ und DC_{avg} bei Neuentwicklung von Teilsystemen oder *PFH* beim Einsatz bereits qualifizierter Teilsysteme
5.11.2 Schalthäufigkeit verschleißbehafteter Bauteile
5.11.3 Häufigkeit von Maßnahmen zur Fehleraufdeckung
5.11.4 Gebrauchsdauer, falls abweichend von der Berechnungsgrundlage der vorgesehenen Architekturen (20 Jahre)
5.12 Betriebs- und Grenzdaten (Betriebs- und Lagertemperaturbereich, Feuchteklasse, IP-Schutzart, Schock-/Vibrations-/EMI-Störfestigkeitswerte, Versorgungsdaten mit Toleranzen usw.)
(IP = International Protection, EMI = elektromagnetische Störung, electromagnetic interference)
5.13 Konzept zur Trennung bzw. Unabhängigkeit/Rückwirkungsfreiheit zu Nicht-Sicherheitsfunktionen und weiteren Sicherheitsfunktionen
5.14 Anzuwendende Grundnormen für die Konstruktion (zur Ausrüstung, zum Schutz gegen elektrischen Schlag/gefährliche Körperströme, zur Störfestigkeit gegen Umgebungsbedingungen usw.)
5.15 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
5.16 Allgemeine technische Voraussetzungen und organisatorische Rahmenbedingungen für die Inbetriebnahme, Prüfung und Abnahme sowie Wartung und Instandhaltung

Eine solche Spezifikation muss, um Gültigkeit zu erlangen, vor dem nächsten Entwicklungsschritt verifiziert werden. Dabei geht es in erster Linie um Vollständigkeit, Korrektheit, Verständlichkeit und Widerspruchsfreiheit. Dass es vorteilhaft ist, eine solche Verifikation, z. B. in Form einer Inspektion, durch an einem Projekt Unbeteiligte durchführen zu lassen, liegt auf der Hand. Wird sicherheitsrelevante Software eingesetzt, so muss aus einer solchen Spezifikation der Sicherheitsanforderungen eine eigenständige Softwarespezifikation abgeleitet werden (siehe Abschnitt 9.2).

Mit der Spezifikation ist das erste Dokument im Ablauf der Gestaltung von SRP/CS entstanden. Grundsätzlich hat die Dokumentation einen hohen Stellenwert im Sinne einer nachvollziehbaren Entwicklung. Man sollte beachten, dass ein Produkt unter Umständen von einer anderen Person als der, die es entwickelt hat, weiter gepflegt wird. Auch in dieser Situation ist eine gut geschriebene Spezifikation sehr wertvoll. Details zur erforderlichen Dokumentation im Rahmen des iterativen Gestaltungsprozesses von SRP/CS finden sich im Abschnitt 9.8 zur Software und in den Abschnitten 10.1.4 ff. Dokumente müssen eindeutig identifizierbar sein und eine Versionsverwaltung, die Änderungen nachvollziehbar darstellt, enthalten.
Für die korrekte Umsetzung von Sicherheitsfunktionen ist der Inhalt der Benutzerinformationen entscheidend. DIN EN ISO 13849-1 enthält in Abschnitt 13 eine Liste der Informationen, die in der Benutzerinformation mindestens enthalten sein müssen. Der Inhalt der herstellerinternen technischen Dokumentation von SRP/CS wird in Abschnitt 12 der Norm aufgelistet. Ergänzend dazu hat der Gesetzgeber in der Maschinenrichtlinie 2006/42/EG und der zukünftig geltenden europäischen Maschinenverordnung Anhang IV Auflagen zur Dokumentation aufgeführt, die sich teilweise mit den normativen Anforderungen überschneiden. **Kasten 5.2** zeigt den Inhalt der erforderlichen technischen Unterlagen für Maschinen nach europäischer Maschinenrichtlinie Anhang VII, A für Maschinen und zugehörige Produkte.

Kasten 5.2 Technische Unterlagen für Maschinen: Auszug aus der Maschinenrichtlinie (2006/42/EG), Anhang VII, A

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 Sicherheitsfunktionen und ihr Beitrag zur Risikominderung

Änderung gegenüber dem IFA Report 2/2017:

- Erweiterung der erforderlichen Informationen zur Spezifikation einer Sicherheitsfunktion
- Tabellarische Bestimmungshilfe für den P-Parameter und ergänzende Hinweise zum S-Parameter hinzugefügt
- Normenreferenzen (einschließlich Maschinenverordnung) aktualisiert

Der vorliegende IFA 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 6.7 wird anschließend die Umsetzung am praktischen Beispiel einer Planschneidemaschinensteuerung gezeigt.

6.1 Anforderungen der EG-Maschinenrichtlinie

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

Sofern für die zu konstruierende Maschine eine harmonisierte produktspezifische Norm (Typ-C-Norm) vorliegt [22], die im Amtsblatt der EU veröffentlicht wurde, kann von einer Berücksichtigung der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen bereits ausgegangen werden. Im Anhang ZA der harmonisierten Norm wird der Zusammenhang zwischen Anhang I der EG-Maschinenrichtlinie und der Norm beschrieben. Für alle betrachteten grundlegenden Anforderungen der EG-Maschinenrichtlinie spricht man in diesen Fällen von einer Vermutungswirkung, denn bei Anwendung der Norm darf man die Übereinstimmung mit den betrachteten Anforderungen der EG-Maschinenrichtlinie vermuten. Werden Anforderungen aus dem Anhang I der EG-Maschinenrichtlinie in der harmonisierten Norm nicht betrachtet, müssen diese Anforderungen in der Risikobeurteilung des Herstellers berücksichtigt werden. Die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen sind leicht verändert in den Anhang III Teil B der Maschinenverordnung übernommen worden. Hinzugekommen ist zum Beispiel die Anforderung des Schutzes gegen Korrumpierung (1.1.9). Zudem wurde der Abschnitt 1.2.1 „Sicherheit und Zuverlässigkeit von Steuerungen“ um Anforderungen hinsichtlich der industriellen Security ergänzt. Diese Änderungen bilden die Grundlage für das neue Kapitel 8.2.19 (Fernzugriff) dieses Reports.

Die Strategie zur Risikominderung ist aber immer dann anzuwenden, wenn keine Norm mit Vermutungswirkung existiert, wenn davon abgewichen wurde oder wenn zusätzliche Aspekte vorliegen, die von der Produktnorm nicht abgedeckt sind. Zur Feststellung der von einer Produktnorm nicht berücksichtigten Sachverhalte sind die ersten beiden Schritte der im Folgenden beschriebenen Strategie zur Risikominderung immer durchzuführen, also die Grenzen der Maschine festzulegen und die Gefährdungen zu identifizieren.

[1] Eine Sicherheitsfunktion wird 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.

6.2 Strategie zur Risikominderung

Das in DIN EN ISO 12100 vorgestellte Verfahren zur Risikominderung wurde in Bild 1 der DIN EN ISO 13849-1 übernommen und um die in dieser Norm konkretisierten Aspekte ergänzt (**Abbildung 6.1**). 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 gehörten die bestimmungsgemäße Verwendung (z. B. zulässige Materialien, die verarbeitet werden dürfen) der Maschine einschließlich aller Betriebsarten und der unterschiedlichen Eingriffsmöglichkeiten. Außerdem muss die vernünftigerweise vorhersehbare Fehlanwendung der Maschine berücksichtigt werden. Damit wird unter anderem die Manipulation von Schutzeinrichtungen berücksichtigt.

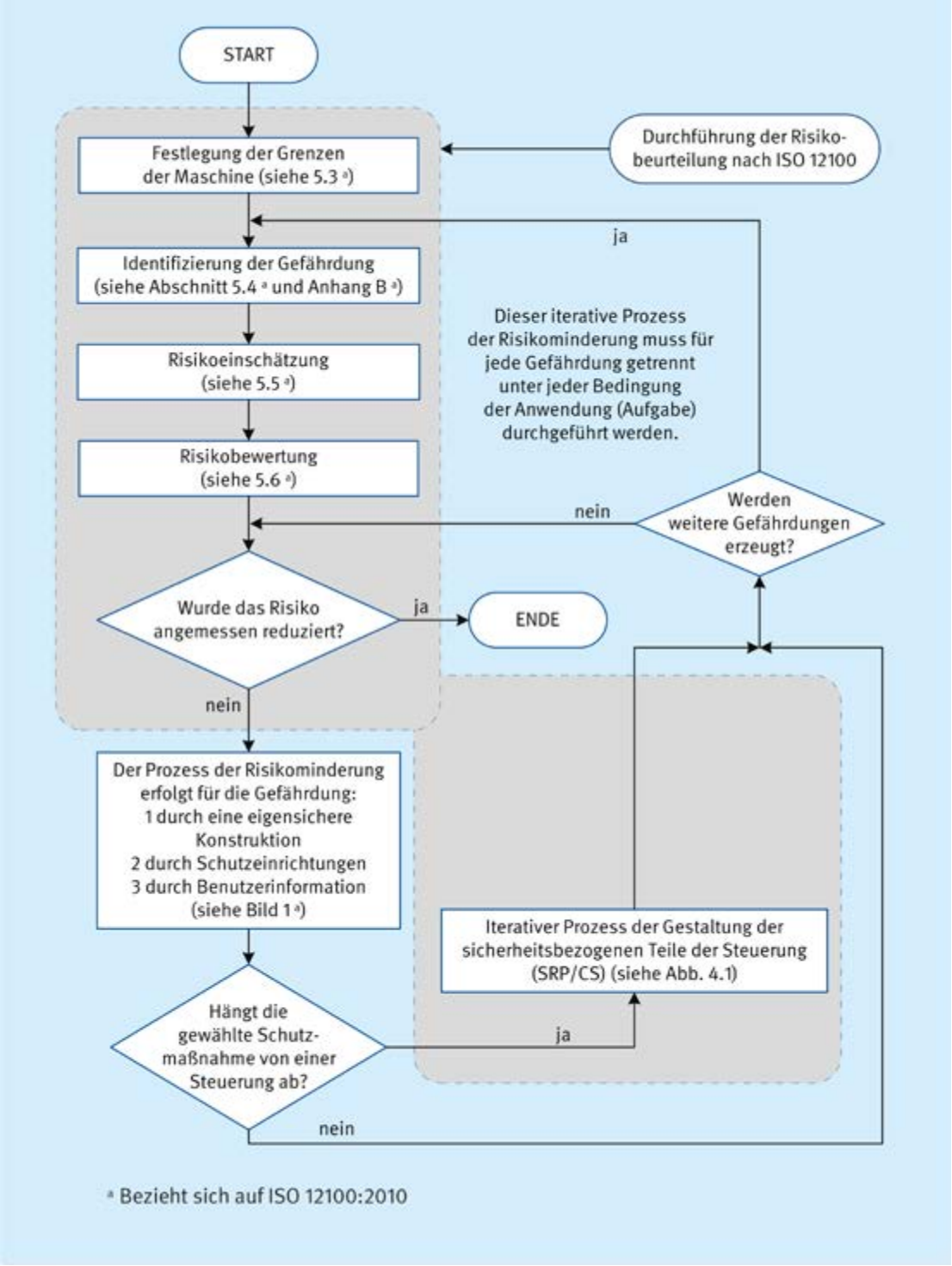


Abb. 6.1
Iterativer Prozess zur Risikominderung

Abb. 6.2
Beispiele für Gefährdungen (Quelle: DIN EN ISO 7010)

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

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

Weitere Details zu diesem Prozessschritt sind in DIN EN ISO 12100 zu finden. Für die systematische Identifizierung der Gefährdungen gibt es verschiedene Verfahren, Beispiele finden sich in DIN ISO/TR 14121-2. Darüber hinaus sind mögliche Gefährdungen ausführlich in Anhang B von DIN EN ISO 12100 aufgelistet, einen Auszug zeigt **Abbildung 6.2**.

6.2.1 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:

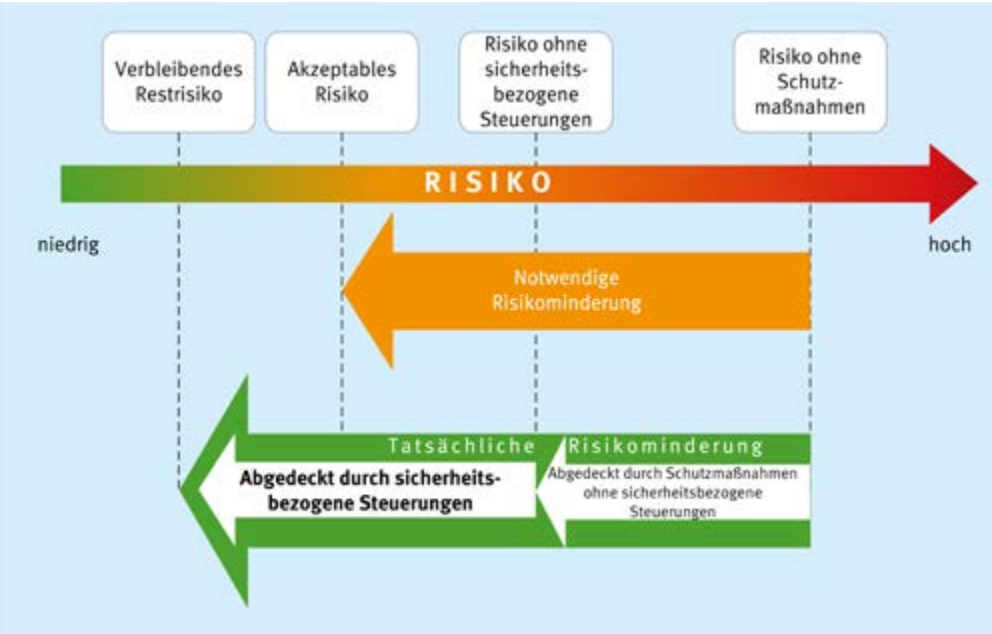


Abb. 6.3
Risikoeinschätzung und Risikominderung

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 6.3** zeigt hierzu die Anteile der Risikominderung mit und ohne sicherheitsrelevante Teile einer Steuerung. Weitere Informationen zum Thema Risiko enthält das IFA-Handbuch [23].

6.2.2 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 ISO 12100 vor:

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

6.3 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 (**Abbildung 6.4**).

Für die Gestaltung der sicherheitsbezogenen Teile von Steuerungen ist nach DIN EN ISO 13849-1 ein iterativer Prozess vorgesehen (siehe Abbildung 4.1), der mit der Spezifikation der Sicherheitsfunktionen beginnt. **Abbildung 6.5** zeigt den für diesen Abschnitt des Reports relevanten Teil. Um Fehler beim Spezifizieren der Sicherheitsfunktion auszuschließen, gilt es vorher im Rahmen des Managements der funktionalen Sicherheit (siehe Kapitel 5) festzulegen, wer wann wie die Spezifikation erstellt. Auf das Identifizieren der Sicherheitsfunktionen im Rahmen des oben beschriebenen Prozesses der Risiko-

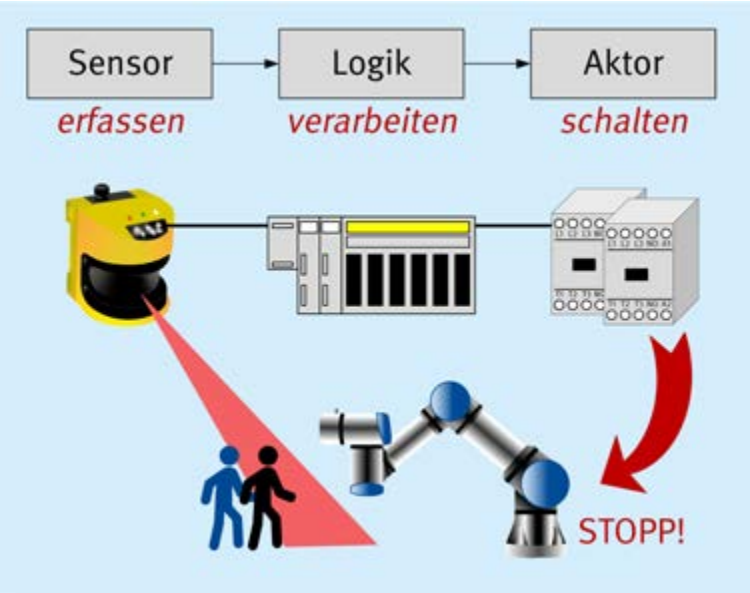


Abb. 6.4
Sicherheitsfunktionen werden von SRP/CS ausgeführt

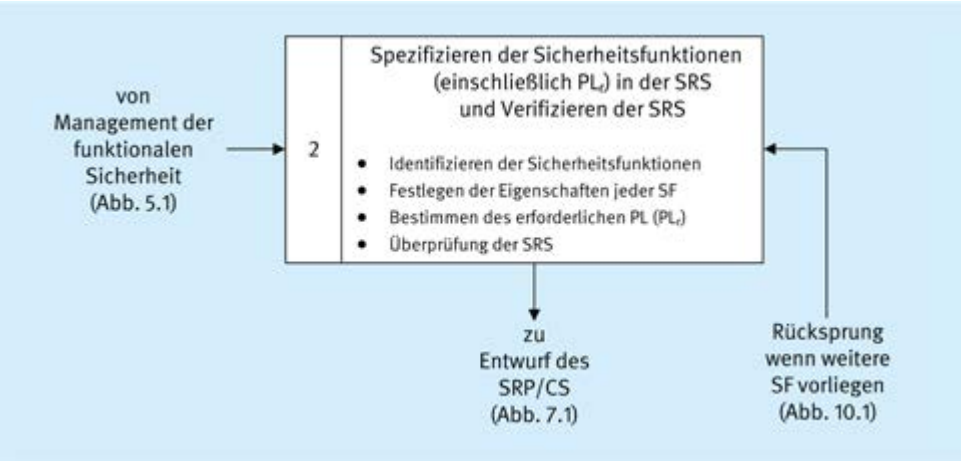


Abb. 6.5
Ausschnitt aus dem iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP/CS)

minderung folgt die detaillierte Festlegung ihrer Eigenschaften, von denen der erforderliche PL_r [2] eine wichtige Kenngröße darstellt.

6.3.1 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) Stillsetzen aller gefahrbringenden Bewegungen eines Roboters, wenn eine Person seinen Arbeitsbereich betritt (siehe Abbildung 6.4),
b) gesteuertes Stillsetzen der Bewegung und Einfallen der Haltebremse im Stillstand,
c) Verhindern einer Quetschstelle infolge der Absenkung von Maschinenteilen,
d) Leistung des Schneidlasers bei direkter Exposition am Auge absenken,
e) Absturz der Achse im Einrichtbetrieb verhindern,
f) Ausweichbewegungen des Roboters bei Betreten seines Gefahrenbereiches,
g) Einzug von Personen verhindern,
h) 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 in Abschnitt 6.7 beschrieben. In diesem Beispiel wird durch die elektronische Ansteuerung die Bewegung zunächst bis zum Stillstand abgebremst, anschließend fällt eine mechanische Haltebremse ein.

Hinweise zu möglichen Sicherheitsfunktionen geben die folgenden Tabellen. In **Tabelle 6.1** sind die Sicherheitsfunktionen nach Anhang M 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 6.5). **Tabelle 6.2** zeigt weitere Sicherheits-Teilfunktionen für sichere Antriebssteuergeräte nach DIN EN 61800-5-2 – PDS(SR), Power Drive Systems(Safety Related) [24]. Diese Norm enthält unter anderem die häufig angewendeten Sicherheits-Teilfunktionen zur Verhinderung eines unerwarteten Anlaufs STO (STO, Safe Torque Off), zum sicheren Stillsetzen SS1 und SS2 und zur sicheren Begrenzung einer Geschwindigkeit SLS (SLS, Safely-Limited Speed).

Tabelle 6.3 zeigt weitere Sicherheits- Teilfunktionen aus der Fluidtechnik nach dem VDMA Einheitsblatt 24584 [25].

Als weitere Hilfestellung enthält die DIN EN ISO 13949-1 zusätzliche Anforderungen an häufig verwendete spezifische Sicherheitsfunktionen, die im Folgenden aufgelistet sind:

- Sicherheitsbezogene Stopp-Funktion,
- Manuelle Rückstellfunktion,
- Wiederanlauffunktion,
- Lokale Steuerungsfunktion,
- Überbrückungsfunktion,
- Sicherheitsbezogene Parameter,
- Schwankungen, Verlust und Wiederkehr der Spannungsversorgung,
- Anforderungen an die Betriebsartenwahl,
- Sicherheitsfunktion(en) für die Instandhaltungsaufgaben.

[2] 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

Tabelle 6.1 Sicherheitsfunktionen aus DIN EN ISO 13849-1

Sicherheitsfunktion	Beispiel für mögliche Anwendung
Sicherheitsbezogene Stoppfunktion	Auslösen einer Schutzeinrichtung führt zu STO, SS1 oder SS2 (Tabelle 6.2)
Manuelle Rückstellfunktion	Quittierung beim Verlassen von hintertretbaren Bereichen
Start-/Wiederanlauffunktion	Nur zulässig bei steuernden trennenden Schutzeinrichtungen nach DIN EN ISO 12100
Lokale Steuerungsfunktion	Steuern von Maschinenbewegungen von einem Standort innerhalb des Gefahrenbereichs
Überbrückungsfunktion (Muting)	Zeitweises Deaktivieren von Schutzeinrichtungen durch die sicherheitsbezogene Steuerung, 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
Abtrenn- und Energieableitungsfunktion	Öffnung eines Hydraulikventils zum Druckabbau
Betriebsartenwahl	Aktivierung von Sicherheitsfunktionen durch Betriebsartenwahlschalter
Interaktion zwischen verschiedenen SRP/CS	Sichere Steuerung und Koordinierung von unabhängig voneinander betriebenen Elementen innerhalb einer Maschine (zum Beispiel, System zur Verhinderung von Zusammenstößen)
Überwachung der Parametrierung der sicherheitsbezogenen Eingangswerte	Zyklische Überprüfung der parametrierbaren sicherheitsbezogenen Grenzwerte
Funktion zum Stillsetzen im Notfall	Reaktion auf die Betätigung eines Not-Halt-Geräts durch STO oder SS1 (Tabelle 6.2)
Überwachung oder Begrenzung der Geschwindigkeit des Drehmoments, der Leistung, der Position (z. B. Positionbegrenzungseinrichtung), der Bewegung, des Moments, des Drucks, der Anhaltezeit, des Anhaltewegs	Sicher begrenzte Geschwindigkeit (SLS, Safely-Limited Speed)
Sichere Bremsenansteuerung	Abbremsen oder Abschalten eines Elektromotors zum Stoppen der gefahrbringenden Bewegung

Tabelle 6.2 Sicherheits-Teilfunktionen 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-r SS1-t	Safe Stop 1	Sicherer Stopp 1	Motor verzögert; Überwachung Bremsrampe und STO nach Stillstand (SS1-r) oder STO nach Ablauf einer Verzögerungszeit (SS1-t); Stopp-Kategorie 1 nach DIN EN 60204-1
SS2-r SS2-t	Safe Stop 2	Sicherer Stopp 2	Motor verzögert; Überwachung Bremsrampe und SOS nach Stillstand (SS2-r) oder SOS nach Ablauf einer Verzögerungszeit (SS2-t); Stopp-Kategorie 2 nach DIN EN 60204-1
SOS	Safe Operating Stop	Sicherer Betriebshalt	Motor steht still und widersteht externen Kräften
SLA	Safely-Limited Acceleration	Sicher begrenzte Beschleunigung	Das Überschreiten eines Beschleunigungsgrenzwerts wird verhindert.
SLS	Safely-Limited Speed	Sicher begrenzte Geschwindigkeit	Das Überschreiten eines Geschwindigkeitsgrenzwerts wird verhindert.
SLT	Safely-Limited Torque	Sicher begrenztes Moment	Das Überschreiten eines Drehmoment-/Kraftgrenzwerts wird verhindert.
SLP	Safely-Limited Position	Sicher begrenzte Position	Das Überschreiten eines Positionsgrenzwerts wird verhindert.
SLI	Safely-Limited Increment	Sicher begrenztes Schrittmaß	Der Motor wird um ein spezifiziertes Schrittmaß verfahren und stoppt anschließend.
SDI	Safe Direction	Sichere Bewegungsrichtung	Die nicht beabsichtigte Bewegungsrichtung des Motors wird verhindert.
SMT	Safe Motor Temperature	Sichere Motortemperatur	Das Überschreiten eines Motortemperaturgrenzwerts wird verhindert.
SBC	Safe Brake Control	Sichere Bremsenansteuerung	Sichere Ansteuerung einer externen Bremse
SCA	Safe Cam	Sicherer Nocken	Während sich die Motorposition in einem spezifizierten Bereich befindet, wird ein sicheres Ausgangssignal erzeugt.
SSM	Safe Speed Monitor	Sichere Geschwindigkeitsüberwachung	Während die Motordrehzahl niedriger als ein spezifizierter Wert ist, wird ein sicheres Ausgangssignal erzeugt.
SAR	Safe Acceleration Range	Sicherer Beschleunigungsbereich	Die Beschleunigung des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
SSR	Safe Speed Range	Sicherer Geschwindigkeitsbereich	Die Geschwindigkeit des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
STR	Safe Torque Range	Sicherer Momentenbereich	Das Drehmoment des Motors (die Kraft bei Linearmotoren) wird innerhalb spezifizierter Grenzwerte gehalten.

Tabelle 6.3 Sicherheits-Teilfunktionen nach dem VDMA Einheitsblatt 24584

Abkürzung	Bezeichnung englisch	Bezeichnung deutsch	Funktion
STO	Safe Torque Off	Sicher abgeschaltetes Moment	Dem Antrieb wird keine Energie zugeführt, die eine Bewegung oder Kraft (Moment) verursachen kann. In den Kolbenräumen gespeicherte Energie wird abgeleitet, so dass keine Arbeit verrichtet werden kann.
SSC	Safe Stopping and Closing	Sicheres Anhalten und Absperren	Der Antrieb wird stillgesetzt. Die Energiezu- oder -abfuhr zu mindestens einem Kolbenraum des Antriebs wird gesperrt und damit gespeicherte Energie verwendet, um das Stillsetzen zu erzielen.
SDI	Safe Direction	Sichere Bewegungsrichtung	Die SDI-Funktion verhindert, dass sich der Antrieb in die unzulässige Richtung bewegt.
SDE	Safe De-energization	Sicheres Energiefreischalten	Die Funktion SDE ermöglicht das sichere Energiefreischalten. Dies erfolgt in der Pneumatik durch Entlüften und in der Hydraulik durch Druckentlastung
THC	Two-hand Control	Zweihandsteuerung	Die beiden Eingangssignale müssen zusammen das Ausgangssignal der Zweihandschaltung erzeugen und aufrechterhalten, und zwar nur so lange, wie beide Eingangssignale anliegen.
PUS	Prevention of unexpected start-up	Vermeidung von unerwartetem Anlauf	Die Anforderungen zur Vermeidung eines unerwarteten Anlaufs sind in DIN EN ISO 14118 beschrieben. Eine Kombination von Sicherheits-Teilfunktionen des Einheitspapieres kann für die Umsetzung geeignet sein.

Bei der Ausführung einer Sicherheitsfunktion entscheiden eine Vielzahl von Randbedingungen darüber, ob die erforderliche Risikominderung tatsächlich erreicht wird. Daher sind zusammen mit der Auswahl eine Reihe von Eigenschaften zu berücksichtigen und für jede Anwendung individuell festzulegen. Fehler und Ungenauigkeiten in der Spezifikation einer Sicherheitsfunktion (z. B. hinsichtlich der erforderlichen Reaktionszeit) können zu unbedachten Gefährdungen führen. Je später im Entwicklungsprozess solche Fehler erkannt werden, umso größer kann der Aufwand für daraus resultierende Modifikationen werden. Diesem wichtigen Aspekt wurde mit der vierten Ausgabe der Norm daher auch deutlich mehr Gewicht gegeben. Zu den in der Norm genannten Informationen, die für jede Sicherheitsfunktion in der Spezifikation der Sicherheitsanforderungen dokumentiert werden müssen, zählen:

- die eindeutige Bezeichnung der Sicherheitsfunktion im Sinne der Referenzierbarkeit,
- die genaue Beschreibung des auslösenden Ereignisses,
- die genaue Beschreibung der erforderlichen Reaktion, um einen sicheren Zustand zu erreichen,
- der erforderliche PL_r,
- die Ansprechzeit der Maschine (Reaktionszeit plus Anhaltezeit) bis zum Erreichen des sicheren Zustands (der Nachlauf des gesamten Systems, also die Reaktionszeit der Schutzeinrichtung plus die Anhaltezeit des gefahrbringenden Maschinenteils, steht dabei in wechselseitiger Abhängigkeit mit dem Sicherheitsabstand zum Gefährdungsbereich)
- die unterschiedlichen Betriebsarten (z. B. Automatikbetrieb, Einrichtbetrieb, Störungsbeseitigung), in denen die Sicherheitsfunktion aktiv sein muss,
- Schnittstellen der Sicherheitsfunktion mit der Maschinensteuerung und anderen Sicherheitsfunktionen,
- Reaktionen beim Erkennen eines Fehlers der Sicherheitsfunktion, um einen sicheren Zustand einzuleiten und aufrechtzuerhalten, bis der Fehler behoben ist,
- Verwendung unterschiedlicher Sicherheitsfunktionen bei vorhandener bzw. ausgefallener Energieversorgung (siehe auch Kapitel 5.2.3.1 der Norm),
- Häufigkeit der Betätigung (Anforderungsrate der Sicherheitsfunktion),
- ggf. eine Priorität, falls mehrere Sicherheitsfunktionen gleichzeitig aktiv sein können,
- Sicherheitsanforderungen in Typ-C-Normen, beispielsweise Festlegung sicherheitsbezogener Parameter wie der maximal zulässigen Geschwindigkeit,
- die Bedingungen, um den Wiederanlauf der Maschine nach einer Auslösung der Sicherheitsfunktion zu erlauben.

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

Die festgelegten Sicherheitsfunktionen müssen in der Spezifikation der Sicherheitsanforderungen (SRS) inklusive aller dazugehörigen Anforderungen vollständig beschrieben werden. Es empfiehlt sich, das Requirement Tracking toolunterstützt zu realisieren, um eine Vorwärts- und Rückwärtsverfolgbarkeit sicher zu stellen.

6.3.2 Beispiele, bei denen die Definition der Sicherheitsfunktion Einfluss auf die spätere Berechnung der *PFH* hat

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

Beispiel 1

Sicherheitsfunktion „Stillsetzen beim Öffnen der Schutztür“

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

Bei der späteren Berechnung der *PFH* der Sicherheitsfunktion werden daher die *PFH*-Werte der folgenden Blöcke[3] addiert:

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

Das Resultat der Berechnung kann eine *PFH* sein, die für die Anwendung nicht mehr ausreichend ist, obwohl vielleicht nur die Antriebe 1 und 3 am momentanen Standort der Bedienperson gefahrbringende Bewegungen auslösen und die restlichen Antriebe rein „funktional“ stillgesetzt werden. In diesem Fall empfiehlt es sich, für die Sicherheitsfunktion nur die Bewegungen zu berücksichtigen, die tatsächlich eine Gefährdung darstellen, und die Sicherheitsfunktion in Hinblick auf die für die Sicherheit der Bedienperson kritischen Antriebe umzuformulieren. Das zugehörige funktionale Schaltbild ist in **Abbildung 6.6** dargestellt.

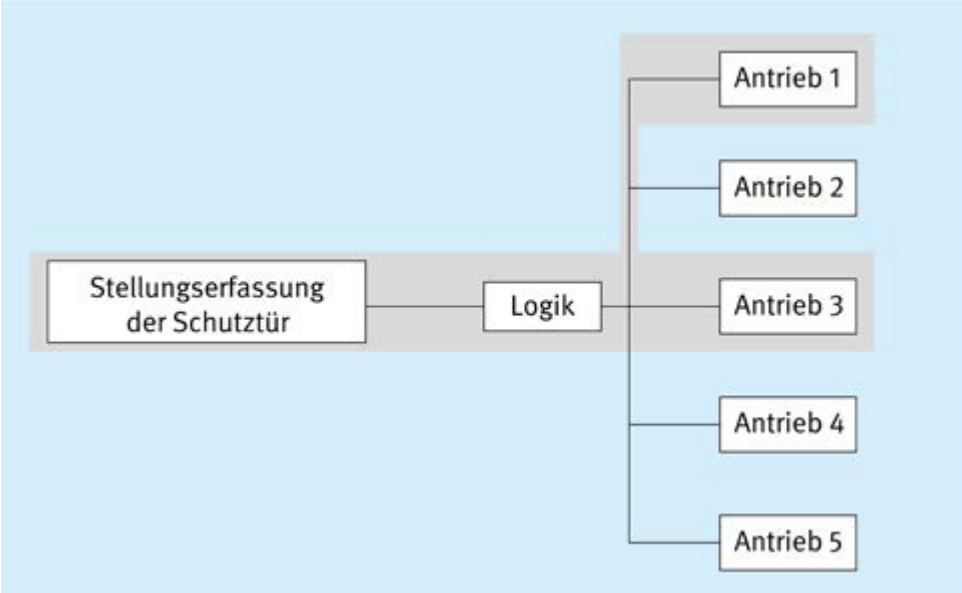


Abb. 6.6
Stillsetzen der Antriebe 1 und 3 beim Öffnen der Schutztür

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

Sind an den gefahrbringenden Bewegungen in dem betrachteten Gefährdungsbereich mehrere Antriebe beteiligt, so spricht man von überlagerten Gefährdungen. Ist die Anzahl der zu berücksichtigenden Antriebe zu hoch, können sich auch hier die *PFH*-Werte der einzelnen Antriebe zu einer Gesamt-*PFH* summieren, die für den erforderlichen PL der Sicherheitsfunktion zu hoch ist. Die DIN EN ISO 13849-1 sieht eine Berücksichtigung überlagerter Gefährdungen vor und beschreibt diese im informativen Anhang A, Kapitel A.4. Demnach können unter Umständen die in der jeweiligen Sicherheitsfunktion betrachteten Gefährdungen auf Einzelgefährdungen bzw. die gefahrbringenden Maschinenbewegungen auf die Bewegungen einzelner Maschinenteile reduziert werden. Ob dies im Einzelfall möglich ist, muss während der Risikobeurteilung bestimmt werden. Eine Hilfestellung hierzu bieten SISTEMA-Kochbuch 6 und die Information zu Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen [26].

Beispiel 2

Sicherheitsfunktion „Stillsetzen des Antriebs beim Öffnen einer Schutztür“

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

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

Abbildung 6.7 zeigt das funktionale Schaltbild und die Blöcke der Sicherheitsfunktion SF3.

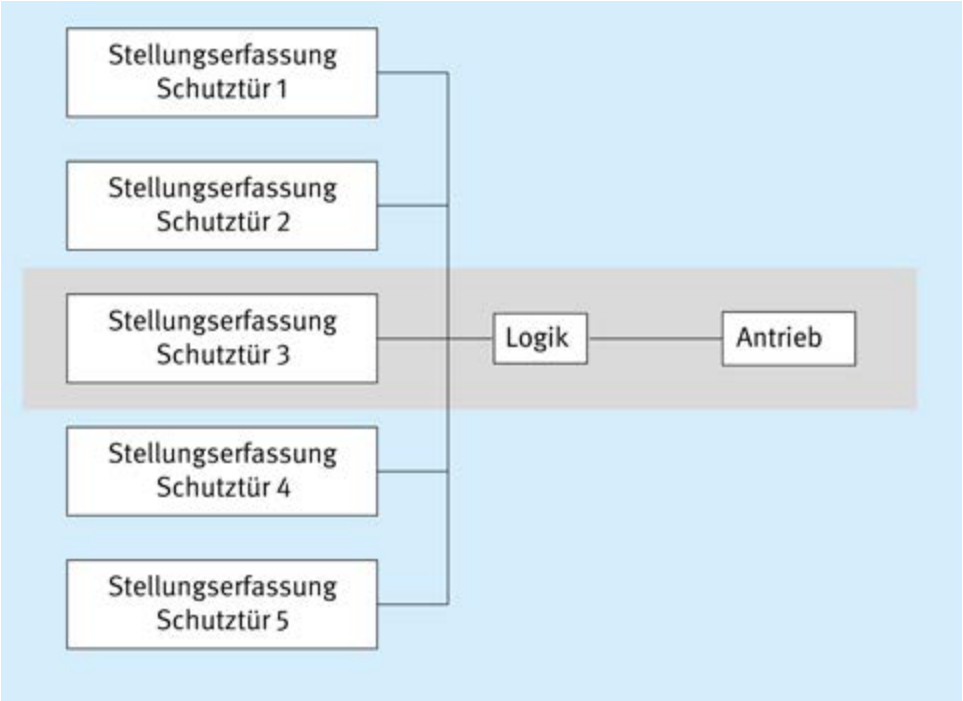


Abb. 6.7
Stillsetzen des Antriebs beim Öffnen der Schutztür 3

Beispiel 3

Not-Halt-Funktion „Stillsetzen aller Antriebe bei Betätigung eines Not-Halt-Gerätes“ (siehe Abschnitt 6.5)

An einer größeren Maschine sind 20 Not-Halt-Geräte installiert, deren Betätigung alle 50 Antriebe schnellstmöglich stillsetzt. Welche Komponenten sind in diesem Fall bei der Realisierung der Not-Halt-Funktion zu berücksichtigen? Es ist nicht vorhersehbar, welches Not-Halt-Gerät zum Auslösen der Not-Halt-Funktion betätigt wird. Da der Bediener immer nur ein Not-Halt-Gerät betätigt, werden die 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 die schlechteste *PFH*, ist also unter anderem abhängig von der Anzahl der Antriebe in der Sicherheitskette, die am ungünstigsten Standort gefahrbringende Bewegungen erzeugen, sowie den jeweiligen einzelnen *PFH*-Werten. Das zugehörige Blockschaltbild ist in **Abbildung 6.8** dargestellt.

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

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

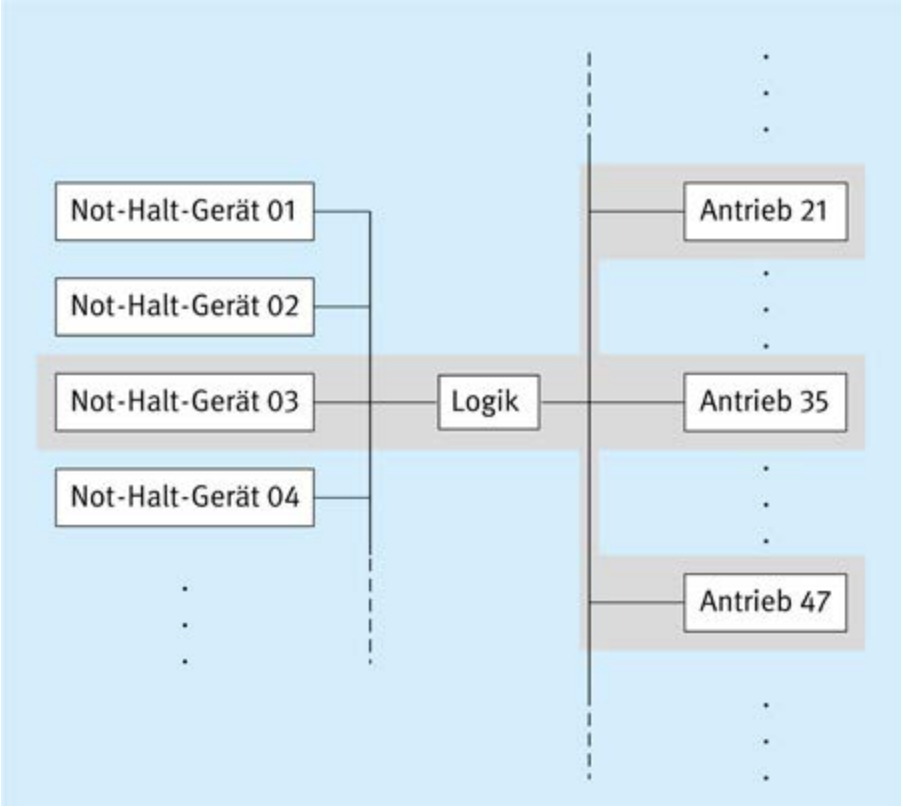


Abb. 6.8
Not-Halt der Gesamtmaschine, ungünstigster Fall

Die Beispiele zeigen, dass sich bei der Definition einer Sicherheitsfunktion eine „lokale Sichtweise“ empfiehlt, die folgende Fragestellungen berücksichtigen sollte:

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

6.4 Bestimmung des erforderlichen PL_r

Für jede vorgesehene Sicherheitsfunktion muss ein erforderlicher Performance Level PL_r festgelegt werden – im technischen Sinne der Sollwert. Die Anforderungen ergeben sich aus der notwendigen Risikominderung, bei deren Festlegung unter anderem ein ggf. unbekanntes Unfallgeschehen zu berücksichtigen ist. DIN ISO/TR 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.

6.4.1 Risikograph

Der Entscheidungsbaum im Anhang A der Norm führt direkt zum erforderlichen Performance Level PL_r und wird im Folgenden erläutert (**Abbildung 6.9**). Weitere Beispiele zur Bestimmung des PL_r finden sich in Anhang A.

Beginnend am Ausgangspunkt werden die Risikoparameter[4] bewertet:

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

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.

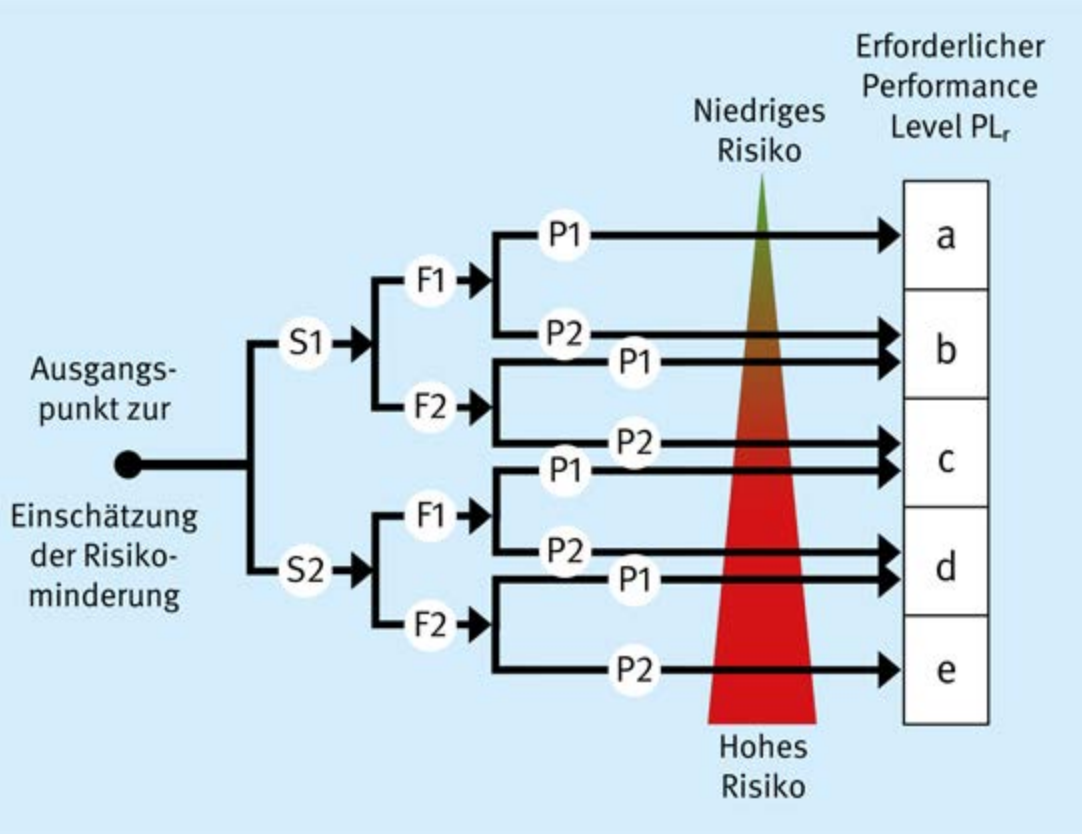


Abb. 6.9
Risikograph zur Bestimmung des PL_r für jede Sicherheitsfunktion

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. Zudem gibt ISO/TR 14121-2 zur Bestimmung des S-Parameters weitere Hilfestellungen, wie beide Parameter voneinander abgegrenzt werden können. Hiernach kann S1 gewählt werden, wenn die Ausfallzeit einer verunfallten Person nicht länger als zwei Tage andauert, dementsprechend wird S2 bei einer Ausfallzeit von mehr als zwei Tagen empfohlen.

Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2

Häufigkeit und Dauer der Gefährdungsexposition werden bewertet mit:

[4] Die Wahrscheinlichkeit für den Eintritt eines Gefährdungsereignisses wird unabhängig von den anderen Risikoparametern betrachtet.

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

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

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

Möglichkeit zur Vermeidung der Gefährdung P1 und P2

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

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

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

Um den P-Parameter besser abschätzen zu können, gibt die DIN EN ISO 13849-1 in Anhang A eine zusätzliche Hilfestellung. In Tabelle A.1 sind verschiedene Auswahlmöglichkeiten gegeben, die verkürzt in **Tabelle 6.4** wiedergegeben sind.

Tabelle 6.4 Einflussfaktoren für den P-Parameter

Faktor	C	B	A
Benutzung der Maschine durch		Laie (unausgebildete Person, keine ausreichende Praxiserfahrung)	Fachkraft (Person, die eine Ausbildung und Schulung, sowie jahrelange Praxis vorweist)
Zeitliche Möglichkeit sich der Gefährdung zu entziehen (Geschwindigkeit des Bauteils, welches die Gefährdung erzeugt)	Zu wenig Zeit zum Entkommen: Hohe Geschwindigkeit, z. B. > 1 000 mm/s oder Zeit bis zur Gefährdung < 1 s	Begrenzte Zeit zum Entkommen: Mittlere Geschwindigkeit, z. B. 251mm/s bis 1 000mm/s oder Zeit bis zur Gefährdung 1 bis 3 s	Ausreichend Zeit zum Entkommen: Niedrige Geschwindigkeit, z. B. < 250mm/s oder Zeit bis zur Gefährdung ≥ 3 s
Räumliche Möglichkeit sich der Gefährdung zu entziehen	Nicht möglich	Gelegentlich/selten möglich (möglich in < 50 % der Fälle)	Leicht möglich (möglich in ≥ 50 % der Fälle)
Wahrnehmung der Gefährdung	Nicht möglich	Möglich in < 50 % der Fälle	Möglich in ≥ 50 % der Fälle
Komplexität der Tätigkeiten (Umfang und Anzahl der notwendigen Interaktionen)		Mittlere bis hohe Komplexität (Fehlersuche, mehrere Tätigkeiten/Bewegungen gleichzeitig)	Geringe Komplexität (sehr einfache Tätigkeiten, Einzeltätigkeit)

Wird bei den Einflussfaktoren mindestens einmal „C“ oder mindestens dreimal „B“ gewählt, sollte P2 für die Risikoeinschätzung verwendet werden. Sollte keinmal „C“ und nur höchstens einmal „B“ ermittelt werden, P1. Bei allen anderen Kombinationen ist eine individuelle Einschätzung der Gefährdungssituation notwendig.

Wahrscheinlichkeit des Eintritts eines Gefahrenereignisses

Ein weiterer Einflussfaktor auf die Festlegung des PL_r ist die Wahrscheinlichkeit für den Eintritt eines Gefährdungsereignisses (siehe DIN EN ISO 12100, 5.5.2.3.2). Hierbei können menschliches Verhalten und technisches Versagen eine Rolle spielen. Beides lässt sich zahlenmäßig schwer abschätzen, die Norm nennt aber hierzu beispielhaft die Kriterien

- Zuverlässigkeitsdaten,
- Unfallgeschichte an vergleichbaren Maschinen.

Sofern Fakten vorliegen, mit denen die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses als „niedrig“ bewertet kann, darf der PL_r um einen Level verringert werden, jedoch PL a nicht unterschreiten. Eine Einschätzung als „niedrig“ sollte aber in jedem Fall begründet und dokumentiert werden.

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

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

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

6.5 Ergänzende Schutzmaßnahmen

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

- Stillsetzen im Notfall,
- Umkehrung von Bewegungen,
- Energietrennung und Energieableitung.

Definitionsgemäß handelt es sich hierbei nicht um technische Schutzmaßnahmen oder Sicherheitsfunktionen im Sinne der DIN EN ISO 13849. Allerdings sollen diese ergänzenden Schutzmaßnahmen auch dann greifen, wenn technische Schutzmaßnahmen (trennende und/oder nicht trennende Schutzeinrichtungen) versagt haben bzw. durch Manipulation unwirksam gemacht wurden. Generell sind für ergänzende Schutzmaßnahmen zunächst die Anforderungen der DIN EN 60204-1 [27] an Steuerstromkreise und Steuerfunktionen von Maschinen zu berücksichtigen. Im Abschnitt 9.4 „Steuerfunktionen im Fehlerfall“ wird ein angemessenes Niveau der sicherheitstechnischen Leistungsfähigkeit verlangt, das durch die Risikobewertung der Maschine festzulegen ist. Insbesondere für die Not-Halt-Funktion gelten aber auch die Anforderungen der DIN EN ISO 13849-1. Dies schließt die Bestimmung eines PL mit ein. Dieser sollte für Not-Halt-Funktionen, wie in DIN EN ISO 13850 [28] festgelegt, mindestens PL c betragen. In jedem Falle dürfen ergänzende Schutzmaßnahmen nicht die Funktion und das Niveau von Schutzeinrichtungen beeinflussen.

6.6 Überprüfung der Spezifikation der Sicherheitsanforderungen

Bevor nun mit der Gestaltung der Sicherheitsfunktionen begonnen werden kann (siehe Kapitel 7) ist die Spezifikation der Sicherheitsanforderungen, einschließlich aller Sicherheitsfunktionen, mit Blick auf die vorgesehene Risikominderung an der Maschine zu validieren. Nur so kann eine verlässliche Entwicklungsgrundlage bereitgestellt werden. Weitere Erläuterungen dazu gibt Abschnitt 9.2 dieses Reports.

6.7 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 oder modernisiert, 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 für „alte“ Maschinen ebenso wie für neue. Dazu gehört unter anderem die Anwendung der DIN EN ISO 13849. Bei der Entscheidung, ob eine „wesentliche Veränderung“ vorliegt, hilft ein Interpretationspapier des Bundesministeriums für Arbeit und Soziales (https://www.bmas.de/DE/Arbeit/Arbeitsschutz/Produktsicherheit/interpretationspapier-wesentliche-veraenderung-von-maschinen.html). Im Allgemeinen liegt keine wesentliche Änderung vor, wenn Änderungen vorgenommen werden, die das Sicherheitsniveau einer Maschine erhöhen. Werden steuerungstechnische Maßnahmen umgesetzt, muss diese Veränderung aber individuell bewertet werden.

6.8 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 (**Abbildung 6.10**) 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.

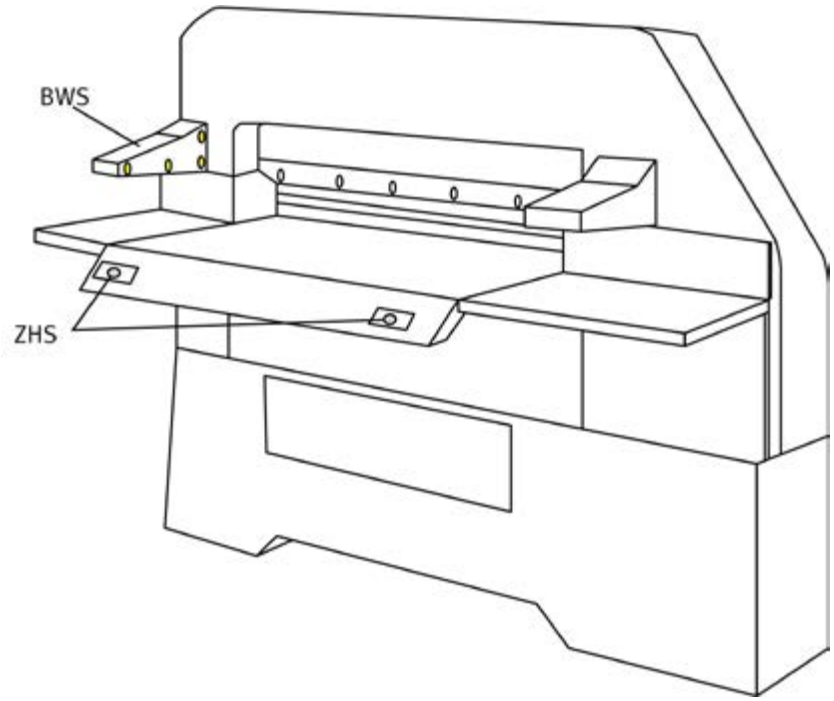


Abb. 6.10
Planschneidemaschine mit Zweihandschaltung (ZHS) und berührungslos wirkender Schutzeinrichtung (BWS)

6.8.1 Festlegung der Grenzen der Maschine

Räumliche Grenzen

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

Zeitliche Grenzen

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

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

6.8.2 Identifizierung der Gefährdungen

Folgende mechanische Gefährdungen sind für eine Planschneidemaschine signifikant:

G1 – Quetschen durch den Pressbalken,

G2 – Schneiden durch das Schneidmesser während des Schnittvorgangs,

G3 – Schneiden durch das Schneidmesser im Ruhezustand.

Risikoeinschätzung

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

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

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

Die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses aufgrund technischen Versagens ist nicht bekannt. Das Unfallgeschehen an vergleichbaren Maschinen ist jedoch gering, sodass die hier vorgesehenen Schutzeinrichtungen offensichtlich ausreichend sind. Sollte die Risikoanalyse für eine Sicherheitsfunktion einen höheren PL_r ergeben als an den vergleichbaren Maschinen tatsächlich realisiert, so darf prinzipiell eine Reduzierung des PL_r um einen Level erfolgen. Da die Sicherheitsfunktionen vergleichbarer Planschneidemaschinen jedoch mit dem höchsten PL realisiert werden, wird in diesem Fall eine Reduzierung des PL_r nicht möglich sein (siehe Abschnitt 6.7.4).

Risikobewertung

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

Inhärent sichere Konstruktion

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

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

6.8.3 Notwendige Sicherheitsfunktionen

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

SF1 – STO (Safe Torque Off), Sicher abgeschaltetes Moment zur Vermeidung eines unerwarteten Anlaufs,

SF2 – Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung,

SF3 – Erkennung eines Eingriffs weiterer Personen in den Gefahrenbereich durch eine BWS (berührungslos wirkende Schutzeinrichtung, z. B. ein Lichtgitter) und sofortige Schnittunterbrechung,

SF4 – Selbsttätiger Stopp aller Bewegungen nach jedem Einzelschnitt bzw. nach Beendigung der automatischen Schnittfolge,

SF5 – Reduzierung der dynamischen Presskraft für den Pressbalken bei der Funktion „Schnitt andeuten“,

SF6 – Selbsttätige Rückkehr von Pressbalken und Messer in ihre Ausgangslage bei Schnittunterbrechung.

Anmerkung: Es wäre möglich, auf die Maschinenteile Schneidmesser und Pressbalken das Prinzip der überlagerten Gefährdungen anzuwenden (siehe Abschnitt 6.3.2). In diesem Fall würden SF1, SF3, SF4 und SF6 aufgeteilt werden, sodass für Schneidmesser und Pressbalken jeweils eigene Sicherheitsfunktionen definiert wären. Im vorliegenden Fall wird darauf jedoch verzichtet, da aufgrund der geringen Anzahl der Bauteile in SF1 bis SF6 die erforderliche PFH auch für diese zusammengefassten Sicherheitsfunktionen erreicht werden kann.

Eigenschaften der Sicherheitsfunktionen

Bei Eingriff in das Lichtgitter ist der Schnitt sofort zu unterbrechen. Die Sicherheitsfunktion SF3 hat daher Priorität gegenüber SF2. Für SF5 ist die maximal zulässige Kraft für den Pressbalken bei „Schnittlinie andeuten“ anzugeben (siehe DIN EN 1010-3 [29]).

6.8.4 Bestimmung des erforderlichen PL_r

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

S2 – ernste, üblicherweise irreversible Verletzung,

F2 – dauernder Aufenthalt im Gefahrenbereich, die Häufigkeit ist also höher als einmal alle 15 Minuten,

P2 – Vermeidung einer Gefährdungssituation kaum möglich; keine Möglichkeit der Wahrnehmung der Gefährdung; sehr geringer Abstand zwischen Messer/Pressbalken und Hand; begrenzte Räumlichkeiten, um sich der Gefährdung zu entziehen.

Entsprechend dem Risikographen in Abbildung 6.9 ergibt sich aus dieser Bewertung ein erforderlicher Performance Level PL_r e. An vergleichbaren Maschinen ist das Unfallgeschehen gering. Die hier betrachteten Sicherheitsfunktionen dieser Maschinen sind bereits mit PL e realisiert worden, wie es in DIN EN 1010-3 vorgegeben ist. Das Ergebnis der Risikoanalyse wird also durch die Praxis bestätigt; eine mögliche Reduzierung des PL_r ergibt sich hieraus nicht. **Abbildung 6.11** zeigt Dokumentation und Risikograph in der Software SISTEMA für die Sicherheitsfunktion SF1.

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

6.8.5 Ausführliche Spezifikation am Beispiel der Sicherheitsfunktion SF2 „Ortsbindung“

Exemplarisch wird die Sicherheitsfunktion SF2 folgendermaßen ausführlich spezifiziert:

- Kurzbezeichnung: Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches während einer gefahrbringenden Press- und Schneidbewegung,
- auslösendes Ereignis: mindestens ein Stellteil der Zweihandschaltung wird losgelassen,
- erforderliche Reaktion und sicherer Zustand: die gefahrbringende Bewegung von Pressbalken und Messer wird unterbrochen, sowohl Messer als auch Pressbalken kehren durch Federkraft in ihre obere Ausgangslage zurück,
- PL_r = e,
- Ansprechzeit der Maschine (Reaktionszeit plus Anhaltezeit): 250 ms (passend zum Abstand der Stellteile zu Pressbalken und Messer),
- Betriebsart in denen die Sicherheitsfunktion aktiv sein muss: Einzelschnitt,
- Schnittstellen der Sicherheitsfunktion mit der Maschinensteuerung und anderen Sicherheitsfunktionen: es werden nicht sichere Signale ausgetauscht, dies muss ohne Rückwirkungen auf die Sicherheitsfunktion erfolgen,
- Reaktionen beim Erkennen eines Fehlers der Sicherheitsfunktion: Pressbalken und Messer verbleiben so lange in der oberen Ausgangslage, bis der Fehler behoben und quittiert wurde,
- Ausfall der Energieversorgung: Pressbalken und Messer kehren durch Federkraft in ihre obere Ausgangslage zurück,
- Häufigkeit der Betätigung: ein Loslassen eines Stellteils innerhalb des Arbeitszyklus erfolgt höchstens einmal je Stunde,
- Priorität: SF3 hat Vorrang vor SF2,
- Sicherheitsanforderungen in Typ-C-Normen: siehe DIN EN 1010-3 (Schneidemaschinen) und DIN EN 13851 (Zweihandschaltungen),
- Bedingungen für den Wiederanlauf: Pressbalken und Messer müssen in die obere Ausgangslage zurückgekehrt sein, beide Stellteile wurden losgelassen und synchron erneut betätigt.

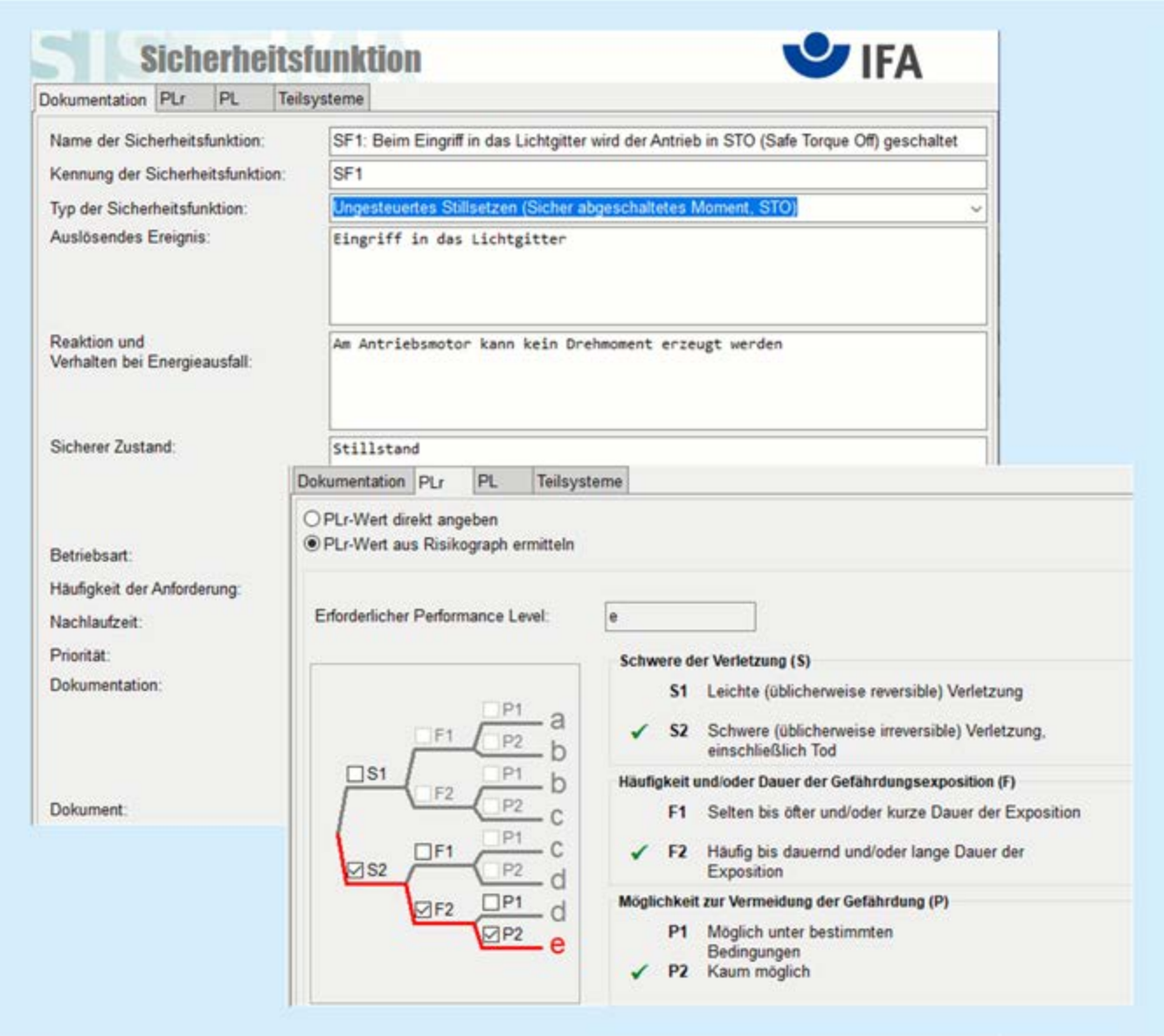


Abb. 6.11 Dokumentation und Risikograph für SF1

6.8.6 Ergänzende Schutzmaßnahmen

Folgende Maßnahmen sind erforderlich:

1. Stillsetzen im Notfall:
   In der Maschinensteuerung stehen bereits geeignete Sicherheitsfunktionen mit PL = e zur Verfügung, die für den Not-Halt verwendet werden. Bei zweikanaliger Verdrahtung des Not-Halt-Gerätes entspricht dann auch das Stillsetzen im Notfall einem PL = e.
2. Die Befreiung einer eingeklemmten Person erfordert eine rückläufige Bewegung von Messer und Pressbalken, die durch Federkraft ausgeführt wird.

7 Gestaltung sicherer Steuerungen durch Kombination von Teilsystemen

Änderung gegenüber dem IFA Report 2/2017:

In Anlehnung an die neue Struktur der Norm wurde das bisherige Kapitel 6 (Gestaltung sicherer Steuerungen) auf die vier Kapitel 5, 7, 8 und 9 aufgeteilt. Das neue Kapitel 7 basiert auf den bisherigen Abschnitten 6.1 „Einleitung“ und 6.4 „Kombination von SRP/CS als Subsysteme“. Die restlichen Abschnitte des bisherigen Kapitels 6 befinden sich nun im Kapitel 5 „Entwicklungsablauf“, Kapitel 7 „Gestaltung von Teilsystemen auf Basis von Kategorien“ und im Kapitel 8 „Entwicklung sicherheitsbezogener Software.

7.1 Bestimmung des erreichten Performance Levels (PL)

Wenn die genaue Sicherheitsfunktion und ihr geforderter Beitrag zur Risikominderung in Form des Performance Levels PL_r feststehen, schließt sich der konkrete Entwurf der sicherheitsbezogenen Teile der Steuerung (SRP/CS) an, die die Sicherheitsfunktionen ausführen. Den entsprechenden Ausschnitt aus dem iterativen Gestaltungsprozess der DIN EN ISO 13849-1 zeigt **Abbildung 7.1**.

Die sicherheitstechnische Qualität der SRP/CS wird als einer von fünf PL angegeben. Jedem dieser PL ist ein Bereich der mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde, abgekürzt durch *PFH* (nach der früheren Definition als Probability of a Dangerous Failure per Hour), zugeordnet (**Tabelle 7.1**). Neben der Bestimmung der *PFH* sind weitere Maßnahmen notwendig, z. B. zur Ertüchtigung von Software oder gegen systematische Ausfälle, um den entsprechenden PL zu erreichen.

Tabelle 7.1 Zuordnung der Ausfallhäufigkeit zu den PL

Performance Level (PL)	Mittlere Häufigkeit eines gefahrbringenden 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 $< 10^{-7}$

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

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

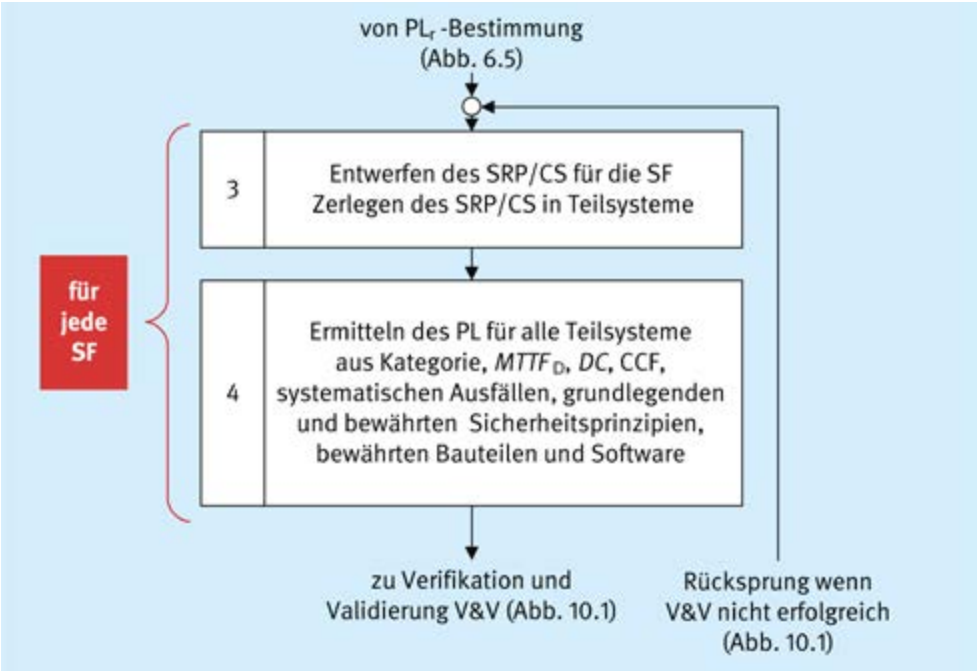


Abb. 7.1
Ermittlung des erreichten PL in der Realisierungsphase der SRP/CS als Ausschnitt aus dem iterativen Gestaltungsprozess, siehe Abbildung 4.1

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

Für beide Aspekte 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.

Die gesamte Maschinensteuerung (Control System, CS) teilt sich in sicherheitsbezogene Teile (SRP/CS), die Sicherheitsfunktionen ausführen, und in die meistens deutlich umfangreicheren, nicht sicherheitsbezogenen Teile auf, die alleine den normalen Betriebsfunktionen dienen (**Abbildung 7.2**). Jedes SRP/CS ist dabei in der Regel als Verkettung mehrerer Teilsysteme realisiert, wobei die Anzahl von einem bis zu vielen Teilsystemen variieren kann.

Im weiteren Verlauf dieses Kapitels wird zunächst in den Abschnitten 7.2 bis 7.4 die Kombination und Integration von Teilsystemen beschrieben, aus denen sich ein SRP/CS zusammensetzt. Da für eine Vielzahl von sicherheitsgerichteten Steueraufgaben auf Sensor-, Logik- und Aktorebene bereits bewertete bzw. zertifizierte Teilsysteme wie sogenannte Sicherheitslichtgitter oder Sicherheits-SPS einsetzbar sind, lassen sich Sicherheitsfunktionen oft durch Integration und Kombination solcher Teilsysteme aufbauen. Falls es beabsichtigt ist, Teilsysteme selbst nach DIN EN ISO 13849 zu entwickeln, so finden sich dazu in Kapitel 8 ausführliche Erläuterungen. In dem in Abschnitt 6.8 beschriebenen praktischen Beispiel der Steuerung einer Planschneidemaschine erfolgt keine Verwendung bereits bewerteter bzw. zertifizierter Teilsysteme und die Sicherheitsfunktion wird durchgängig von einen einzigen Teilsystem ausgeführt. Das Beispiel der Planschneidemaschine wird daher erst in Kapitel 8.4 fortgeführt.

7.2 Kombination von SRP/CS aus Teilsystemen

Ein SRP/CS als Kombination sicherheitsbezogener Teile einer Steuerung beginnt an dem Punkt, an dem sicherheitsbezogene Signale erzeugt werden (einschließlich z. B. Betätiger und Rolle eines Positionsschalters oder Lichtstrahlen eines Lichtgitters) und endet an den Ausgängen der Leistungssteuerungselemente (einschließlich z. B. Hauptkontakte eines Schützes oder zum Zylinder abgehende Anschlüsse an einem Ventil). Treten im energielosen Zustand keine Gefährdungen auf (Ruhestromprinzip), gelten Leistungselemente wie Motoren oder Zylinder nicht als SRP/CS. Wirken jedoch externe oder interne Fremdkräfte (z. B. an Vertikalachsen), so müssen die Leistungselemente zusätzlich sicherheitstechnisch ertüchtigt sein (z. B. Rückschlagventil an Zylindern, zusätzliche mechanische Bremse).

Die Sicherheitsfunktion wird von einem solchen SRP/CS, beginnend bei einem auslösenden Ereignis bis zum Erreichen des sicheren Zustands, vollständig allein ausgeführt. In der Realität ist es aber oft notwendig, verschiedene Teilsysteme hintereinander zu schalten, die jeweils in Teilen die Sicherheitsfunktion ausführen. Solche Teilsysteme können in unterschiedlichen Technologien aufgebaut sein oder verschiedene innere Strukturen (Kategorien, siehe Kapitel 8) oder Performance Level realisieren. Häufig werden etwa unterschiedliche Technologien in der Sensor-

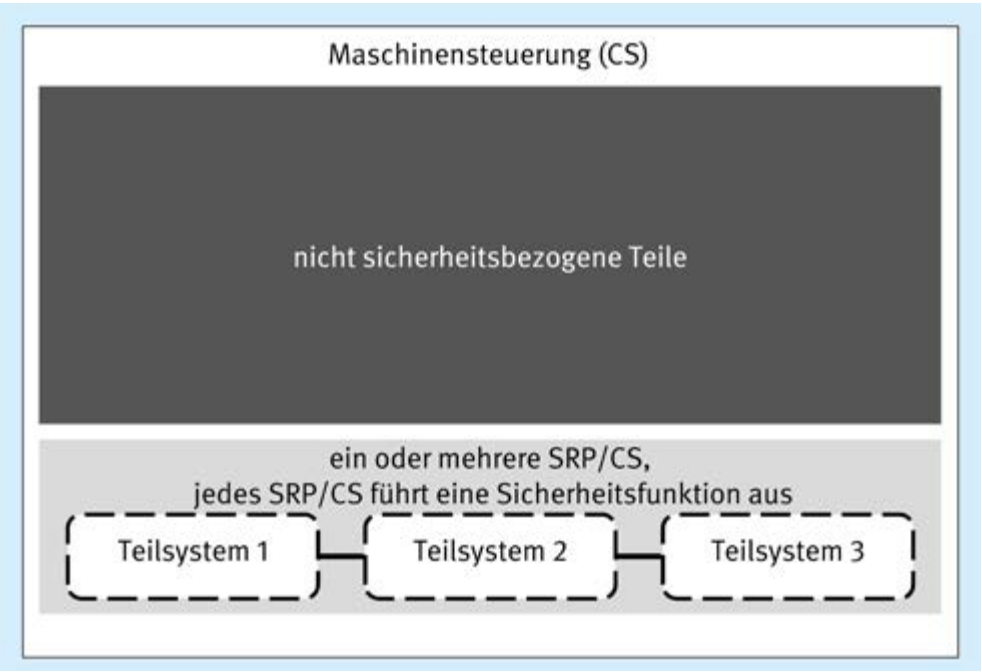


Abb. 7.2
SRP/CS und Teilsysteme innerhalb der Maschinensteuerung

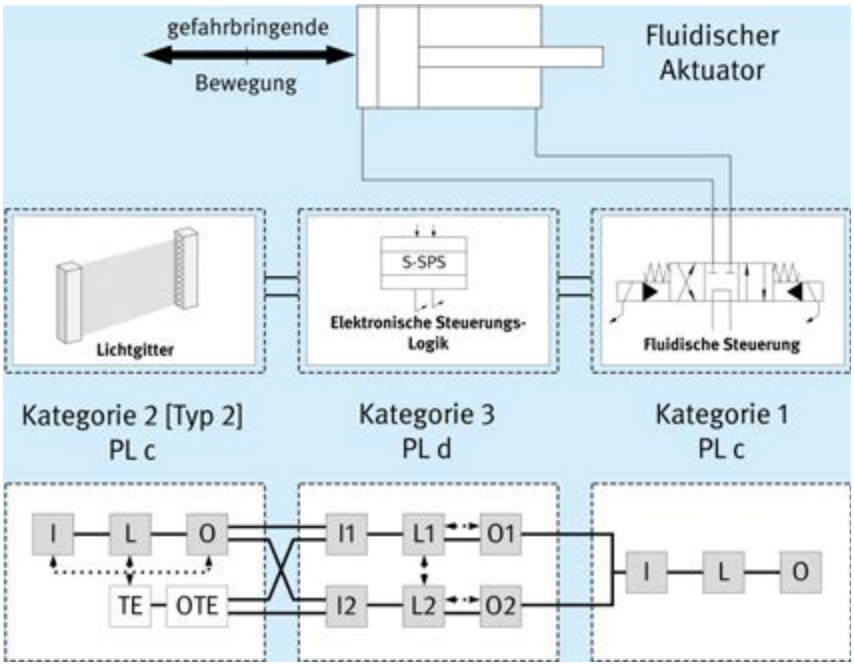


Abb. 7.3
SRP/CS als Reihenschaltung von Teilsystemen zur Realisierung einer Sicherheitsfunktion „Unterbrechung des Lichtgitters führt zum Stillstand der gefahrbringenden Bewegung des fluidischen Aktuators“

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 7.3** dargestellt.

An einer Maschine sind oft mehrere Sicherheitsfunktionen erforderlich, die durch unterschiedliche Kombinationen von Teilsystemen umgesetzt werden (**Abbildung 7.4**). Typisch ist die Trennung in drei Ebenen, dargestellt als Sicherheitsfunktion 1, die von einem SRP/CS 1 technisch ausgeführt wird: Ein Sensor-Teilsystem „Eingang 1“ erfasst das Eintreten des auslösenden Ereignisses. Ein Logik-Teilsystem „Logik 1“ bewertet diese Information und signalisiert dem Aktor-Teilsystem „Ausgang 1“, dass der Maschinenaktuator so angesteuert werden muss, dass ein sicherer Zustand erreicht wird. Die Anzahl der Teilsysteme, die zu einem SRP/CS verkettet werden, ist dabei variabel. SRP/CS 2 und SRP/CS 3 in Abbildung 7.4 benutzen z. B. getrennte Eingangs-Teilsysteme 4 und 6, aber ein gemeinsames Teilsystem 5, das sowohl die Logik- wie die Ausgangs-Funktionalität in sich vereinigt. Weiterhin kann es Schnittstellen zum nicht-sicherheitsbezogenen Teil der Steuerung geben, wenn z. B. für Sicherheitsfunktionen genutzte Sensor-Teilsysteme in die Steuerung des Produktionsprozesses eingebunden sind.

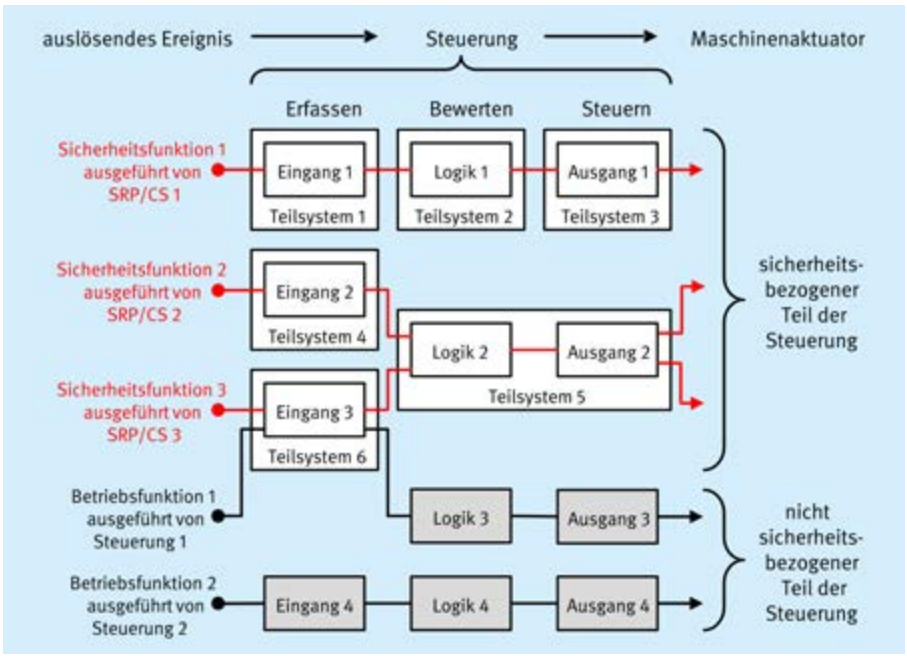


Abb. 7.4
Kombinationsmöglichkeiten von SRP/CS aus Teilsystemen

In ähnlicher Weise, in der für jedes SRP/CS die von ihm auszuführende Sicherheitsfunktion spezifiziert wird, kann für Teilsysteme eine Teilfunktion definiert werden. Beispielsweise reagiert ein Lichtgitter auf die Unterbrechung seiner Lichtstrahlen mit einem festgelegten Signal an seiner Schnittstelle zur nachfolgenden Steuerung.

Jedes nach DIN EN ISO 13849-1 entwickelte Teilsystem lässt sich als Ganzes auf eine Kategorie mit einem entsprechenden Performance Level abbilden (siehe Kapitel 8). In der vom Hersteller eines Teilsystems zu liefernden Information für die Integration des SRP/CS ist daher die Angabe einer Kategorie zusätzlich zu PL und *PFH* für ein nach DIN EN ISO 13849-1 entwickeltes Teilsystem zwingend erforderlich. Für Sicherheitsfunktionen gilt diese Pflicht nur für die Angabe von PL und *PFH*, da die zugehörigen SRP/CS zuvor validierte Teilsysteme enthalten können, die nach anderen Normen für funktionale Sicherheit mit SIL und *PFH* bewertet sind. Außerdem können verschiedene nach DIN EN ISO 13849-1 entwickelte Teilsysteme mit unterschiedlichen Kategorien im SRP/CS integriert sein.

7.3 Arten von Teilsystemen

Bei der Maschinenkonstruktion gibt es grundsätzlich zwei verschiedene Arten von Teilsystemen, aus denen sich SRP/CS aufbauen lassen:

- Bereits zertifizierte Teilsysteme zeichnen sich dadurch aus, dass für sie eine Bewertung der sicherheitstechnischen Leistungsfähigkeit schon vorliegt. Diese Bewertung kann nach DIN EN ISO 13849-1 in Form von PL, *PFH* und Kategorie erfolgen (siehe Kapitel 8) oder nach IEC-Normen für funktionale Sicherheit in Form von SIL und *PFH* (siehe Kapitel 3). Funktional sichere Teilsysteme mit entsprechender Bescheinigung der Kenndaten und ausführlichen Anwendungshinweisen gibt es in großer Bandbreite als zukaufbare Komponenten. Eine andere Möglichkeit ist die Modularisierung der Entwicklung von SRP/CS, indem variabel einsetzbare (Sensor-/Logik-/Aktor-)Baugruppen zusammengestellt und vorab als Teilsysteme bewertet werden. Im sicherheitsbezogenen Blockdiagramm (siehe 8.2.9) werden bereits bewertete bzw. zertifizierte Teilsysteme als sogenannte „gekapselte Teilsysteme“ dargestellt.
- Nach DIN EN ISO 13849 bei der Maschinenkonstruktion selbst entwickelte Teilsysteme können flexibel an die gewünschte Applikation angepasst werden. Sie werden nach den im Kapitel 8 dargestellten Prinzipien entworfen und mit PL, *PFH* und Kategorie bewertet. Da nicht für alle Anwendungen im Maschinenbereich bereits zertifizierte Teilsysteme erhältlich sind, die beispielsweise für die speziellen Einsatzbedingungen geeignet sind oder besondere Leistungsanforderungen erfüllen, ist diese Alternative im Maschinenbau unverzichtbar. Manche Sicherheitsfunktionen lassen sich nur unter Verwendung von Standardbauteilen, die nicht ursprünglich für den Einsatz im Bereich funktionaler Sicherheit entwickelt wurden, realisieren. Die erforderliche Zuverlässigkeit wird dann auf Ebene des Teilsystems unter anderem durch die Steuerungsarchitektur (Kategorie), Tests und andere zusätzliche Maßnahmen zur Fehlervermeidung und -beherrschung erreicht.

Die in Kapitel 8 ausführlich beschriebene Zuordnung einer Kategorie erfolgt auf der Ebene eines Teilsystems. Einer der großen Vorteile des mit der zweiten Normenausgabe eingeführten PL-Konzepts ist die einfache Kombinationsmöglichkeit: Teilsysteme verschiedener Kategorien, aber ähnlicher Performance Level können zu einem Gesamtsystem gemischter Kategorien, aber mit definiertem Gesamt-PL kombinieren werden. Die Möglichkeit, ein SRP/CS mit einer durchgängigen Kategorie aus nur einem einzelnen Teilsystem vom Sensor bis zum Aktor aufzubauen, ist davon unbenommen und wird in der Praxis ebenfalls oft umgesetzt.

7.4 Bestimmung von PL und *PFH* bei der Kombination von Teilsystemen

Die Reihenschaltung mehrerer Teilsysteme auch unterschiedlicher Technologie sieht typischerweise aus wie in Abbildung 7.3 skizziert: Lichtgitter, elektronische und fluidische Steuerung werden hintereinander geschaltet, um insgesamt die Sicherheitsfunktion (Stillsetzung der gefahrbringenden Bewegung bei Unterbrechung eines Lichtstrahls) auszuführen. Der Zylinder 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 auch für die Verknüpfung von Steuerungsteilen sowohl unterschiedlicher Kategorien als auch unterschiedlicher Performance Level. Wie die Praxis schon oft gezeigt hat, kann ein hydraulisches Teilsystem der Kategorie 1 wegen der hohen Zuverlässigkeit der Komponenten unter Umständen vergleichbar sicher sein wie ein elektronisches Teilsystem der Kategorie 3 mit mittlerem Niveau der Fehlererkennung und niedriger Bauteil-Zuverlässigkeit. Daher orientiert sich der PL für die Zusammenschaltung am niedrigsten PL in der Serienschaltung und nicht an der niedrigsten Einzelkategorie. Mit der Anzahl der Steuerungselemente und ihrem jeweiligen *PFH*-Beitrag steigt allerdings die Gesamt-Ausfallhäufigkeit des vollständigen SRP/CS. Daher kann der PL der Reihenschaltung gegenüber dem niedrigsten Teilsystem-PL noch um eine Stufe verringert sein, wenn z. B. durch die *PFH*-Addition die *PFH*-Grenze zum nächstkleineren PL überschritten wird.

In der Regel liegen die *PFH*-Werte für alle Teilsysteme vor (geeignet sind auch *PFH*-Werte in Kombination mit einem SIL nach DIN EN 61508 oder DIN EN 62061). Dann kann daraus durch Aufaddieren der für den Gesamt-PL relevante *PFH*-Wert gebildet werden:

$$PFH = \sum_{i=1}^{N} PFH_i = PFH_1 + PFH_2 + \ldots + PFH_N \quad (7.1)$$

mit

- N = Zahl der an der Sicherheitsfunktion beteiligten Teilsysteme,
- *PFH* = mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde des Gesamtsystems (SRP/CS),
- PFH_i = mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde des i-ten Teilsystems.

Der Gesamt-PL wird dann begrenzt durch

- den niedrigsten PL aller an der Sicherheitsfunktion beteiligten Teilsysteme (Begrenzung durch nicht quantifizierbare Aspekte wie Software und systematische Eignung) und
- den PL, der sich durch die Addition der *PFH* einzelner Teilsysteme ergibt, siehe Gleichung (7.1) (Begrenzung durch quantifizierbare Aspekte).

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

- Zunächst wird der niedrigste PL aller in Reihe geschalteter Teilsysteme ermittelt, dies ist $PL_{niedrig}$.
- Anschließend wird die Häufigkeit des Auftretens von $PL_{niedrig}$ in der Reihenschaltung der Teilsysteme abgezählt, dies ist $N_{niedrig}$.
- Aus $PL_{niedrig}$ und $N_{niedrig}$ lässt sich dann nach **Tabelle 7.2** der Gesamt-PL bestimmen.

Beim Verfahren nach Tabelle 7.2 wird als Näherung für die Teilsysteme eine Ausfallhäufigkeit genau in der Mitte (auf einem logarithmischen Maßstab) des für den jeweiligen $PL_{niedrig}$ gültigen Bereichs angenommen.

Tabelle 7.2 Vereinfachte PL-Bestimmung für in Reihe geschaltete Teilsysteme ohne *PFH*-Angabe

$PL_{niedrig}$	$N_{niedrig}$	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

Da bei beiden Methoden alle Teilsystem-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. Dabei wird unterstellt, dass sicherheitsbezogene Anwendungssoftware (SRASW) nach den in Kapitel 9 beschriebenen Anforderungen entwickelt wurde. Zusätzlich ist bei der Kombination von Teilsystemen besonderes Augenmerk auf die Schnittstellen zwischen den Teilsystemen zu richten:

- Alle Verbindungen (z. B. Leitungen oder Datenkommunikation durch Bussysteme) müssen im PL eines der beteiligten Teilsysteme bereits berücksichtigt sein oder Fehler in den Verbindungen müssen ausgeschlossen oder vernachlässigt werden können.
- Die hintereinander geschalteten Teilsysteme müssen an den Schnittstellen technisch und funktional zueinander passen. Das heißt, jeder Ausgangsstatus eines ansteuernden Teilsystems, der die Anforderung der Sicherheitsfunktion signalisiert, muss als auslösendes Ereignis für die Einleitung des sicheren Zustandes des nachgeordneten Teilsystems geeignet sein. Anders ausgedrückt müssen die verketteten Teilfunktionen aller Teilsysteme lückenlos und passgenau die gesamte Sicherheitsfunktion abbilden.

Durch die von der Norm vorgesehene Addition der Teilsystem-*PFH*-Werte können bei hintereinander geschalteten zweikanaligen Teilsystemen geringe Rechenfehler zur unsicheren Seite auftreten. Streng genommen müssten die beiden Ausgänge des ersten Teilsystems zusätzlich über Kreuz in die Eingänge des zweiten Teilsystems eingelesen und verglichen werden. Oft erfolgt die kreuzweise Verdoppelung der Eingangsinformationen allerdings bereits intern auf der Eingangsebene des zweiten Teilsystems. Um den Aufwand nicht unnötig in die Höhe zu treiben, ist die geringfügige *PFH*-Unterschätzung bei der Addition in der Ausgestaltung der Norm vernachlässigt worden.

Mit den bisher beschriebenen Regeln lassen sich Teilsysteme viel flexibler kombinieren, als dies in der ersten Ausgabe der Norm als DIN EN 954-1 auf der Basis der Kategorien möglich war. Diese Teilsysteme 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 Teilsystemen kann es vorkommen, dass sich zweikanalige und (getestete) einkanalige Teile abwechseln. **Abbildung 7.5** zeigt beispielhaft ein gekapseltes Logik-Teilsystem (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 Teilsysteme prinzipiell austauschbar. Es empfiehlt sich

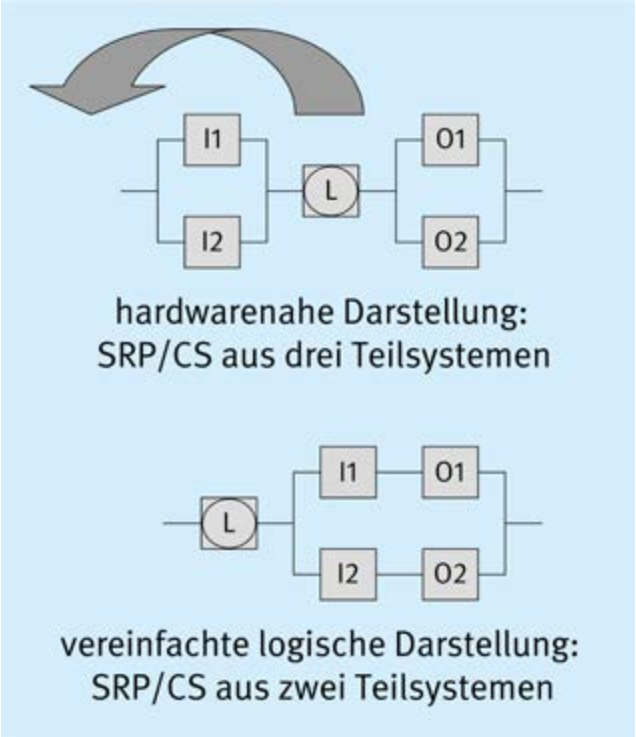


Abb. 7.5
Gemischte Teilsysteme lassen sich im sicherheitsbezogenen Blockschaltbild umsortieren, z. B. indem gekapselte Teilsysteme (hier „L“) vorgezogen werden

daher, wie in Abbildung 7.5 gezeigt, Teilsysteme gleicher Struktur zusammenzufassen. Dadurch wird die PL-Bestimmung einfacher und unnötige Abschneideeffekte, z. B. die mehrfache Begrenzung der $MTTF_D$ des Kanals auf 100 Jahre (siehe Kapitel 8.2.11), werden vermieden.

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

Einen weiteren Spezialfall stellt die Integration von bereits mit einem PL (oder SIL) oder einer *PFH* versehenen Teilsystemen als Block in einem mehrkanaligen Teilsystem dar. Hier kann als grobe Regel ohne Ansehen der inneren Struktur des Teilsystems der Kehrwert der *PFH* als Block-$MTTF_D$ angesetzt werden. Da alle unter Umständen intern realisierten Diagnosemaßnahmen des Teilsystems bereits in der Ausfallhäufigkeit berücksichtigt sind, können für die *DC* des Blocks nur zusätzliche, von außen auf das Teilsystem wirkende Diagnosemaßnahmen herangezogen werden. Ausführlichere Hinweise finden sich in Abschnitt 2 von SISTEMA Kochbuch 4 [30]. Dort wird in Abschnitt 3 auch der Fall angesprochen, dass mehr als zwei Funktionskanäle parallel geschaltet werden.

In dem Fall, dass für ein SRP/CS nur bereits bewertete bzw. zertifizierte Teilsysteme kombiniert werden, die keine Software enthalten, ist eine Bewertung insbesondere der quantifizierbaren Aspekte des Gesamt-PLs bereits mit den in diesem Kapitel beschriebenen Methoden möglich. Die in Kapitel 10 beschriebenen Anforderungen an Verifikation und Validierung bezogen auf die Integration sind natürlich trotzdem anzuwenden und schließen auch einen Funktionstest der Sicherheitsfunktion ein.

Werden Teilsysteme vollständig nach DIN EN ISO 13849-1 entwickelt, gelten die im Kapitel 8 beschriebenen Anforderungen und Erläuterungen. Der in Abschnitt 8.3 beschriebene Aspekt der softwarebasierten Parametrierung kann allerdings auch bei der Integration zertifizierter Teilsysteme relevant sein.

Kapitel 9 beschreibt die Anforderungen an die Entwicklung sicherheitsbezogener Software. Dies betrifft sowohl sicherheitsbezogene Embedded-Software (SRESW) selbst entwickelter Teilsysteme als auch sicherheitsbezogene Anwendungs-Software (SRASW). Da SRASW nicht nur in selbst entwickelten Teilsystemen genutzt werden kann, können die Anforderungen an SRASW auch bei der reinen Integration zertifizierter Teilsysteme relevant werden.

8 Gestaltung von Teilsystemen auf Basis von Kategorien

Änderung gegenüber dem IFA Report 2/2017

- In Anlehnung an die neue Struktur der Norm wurde das bisherige Kapitel 6 (Gestaltung sicherer Steuerungen) in vier Kapitel (5, 7, 8 und 9) aufgeteilt. Das neue Kapitel 8 basiert auf den bisherigen Abschnitten 6.1.2 „Systematische Ausfälle“, 6.1.3 „Ergonomie“, 6.2 „Quantifizierung der Ausfallwahrscheinlichkeit“ und 6.5 „PL-Bestimmung am Beispiel einer Planschneidemaschine“. Die restlichen Abschnitte des bisherigen Kapitels 6 befinden sich nun im Kapitel 5 „Entwicklungsablauf“, Kapitel 7 „Gestaltung sicherer Steuerungen durch Kombination von Teilsystemen“ und im Kapitel 9 „Entwicklung sicherheitsbezogener Software“.
- In Abschnitt 8.1.2 wurden Literaturverweise ergänzt und angepasst sowie Teile des Textes entsprechend der neuen Maschinenverordnung überarbeitet.
- Abschnitt 8.2.4 wurde an die Änderungen bei bewährten Bauteilen angepasst.
- In Abschnitt 8.2.5 wurde die geänderte Definition der Kategorie 2 ergänzt.
- In Abschnitt 8.2.7 wurde ein Hinweis zur Fehlerakkumulation in Kategorie 4 hinzugefügt.
- In Abschnitt 8.2.10 wurde für Teilsysteme ein Hinweis ergänzt, dass ein PL e nicht allein auf Fehlerausschlüssen beruhen darf.
- In Abschnitt 8.2.12 wurden Felddaten als optionale Datenquelle für $MTTF_D$-Werte hinzugefügt.
- Abschnitt 8.2.17 beschreibt nun auch die Erweiterung des alternativen Verfahrens zur Bestimmung von PL und *PFH* ohne $MTTF_D$ auf Eingangs- und Logik-Teilsysteme.
- Ein neuer Abschnitt 8.2.19 zum Remote-Zugang und mit Security-Hinweisen wurde eingefügt.
- Ein neuer Abschnitt 8.3 beschreibt die softwarebasierte Parametrierung.
- In Abschnitt 8.4 wurde das Beispiel der Planschneidemaschine aktualisiert.

In vielen Fällen lässt sich eine Sicherheitssteuerung (SRP/CS) nicht allein aus bereits zertifizierten Teilsystemen kombinieren. Vielmehr werden ein oder mehrere Teilsysteme gezielt für eine konkrete Anwendung aus einzelnen Bauteilen aufgebaut (siehe Kapitel 7). Dieses Kapitel beschäftigt sich daher ausführlich mit allen Anforderungen, die bei der Entwicklung von Teilsystemen nach DIN EN ISO 13849-1 [7] zu beachten sind. Wie in Abbildung 7.1 auf Seite 56 in Block 4 gezeigt, geht es dabei in erster Linie um hardwarebezogene Anforderungen. Die Anforderungen an sicherheitsbezogene Software befinden sich im nächsten Kapitel. Den Einstieg in diesem Kapitel bilden die in Abschnitt 8.1 beschriebenen qualitativen Aspekte, zu denen die notwendigen Maßnahmen zur Beherrschung systematischer Ausfälle und ergonomische Gestaltungsaspekte zählen. In Abschnitt 8.2 werden zunächst die Kategorien und dann weitere Einflussfaktoren vorgestellt, um schließlich die darauf basierende vereinfachte Methode zur Bewertung der quantifizierbaren Aspekte zu erläutern. Abschnitt 8.3 stellt im Anschluss Anforderungen an softwarebasierte Parametrierung vor. Abschließend zeigt Abschnitt 8.4 die beispielhafte Umsetzung der Anforderungen dieses Kapitels und führt damit das in Kapitel 5 begonnene Steuerungsbeispiel einer Planschneidemaschine fort.

8.1 Qualitative Anforderungen

Die in der Norm enthaltenen qualitativen Anforderungen tragen zur Zuverlässigkeit eines SRP/CS bei, indem Ausfälle vermieden werden, deren Ursachen im Entwicklungsablauf liegen. Es handelt sich dabei nicht um Zufallsausfälle, deren Wahrscheinlichkeit abgeschätzt werden kann, sondern um systematische Ausfälle wie Planungs- und Spezifikationsfehler. Auch wenn die Vermeidung solcher Ausfälle das erste Ziel ist, können sie nie ganz ausgeschlossen werden. Aus diesem Grund müssen Maßnahmen zur Beherrschung der von ihnen hervorgerufenen Auswirkungen getroffen werden. Strategien zur Beherrschung von zufälligen Hardwareausfällen wie Redundanz oder Tests können auch gegen systematische Ausfälle helfen. Ein besonderes Augenmerk liegt in diesem Zusammenhang auf einer ergonomischen Gestaltung der Maschine und ihres Steuerungssystems, da unbedachte oder benutzerunfreundliche Realisierungen erfahrungsgemäß zu gefährlichen Fehlanwendungen oder zu einer Umgehung der Sicherheitseinrichtungen führen.

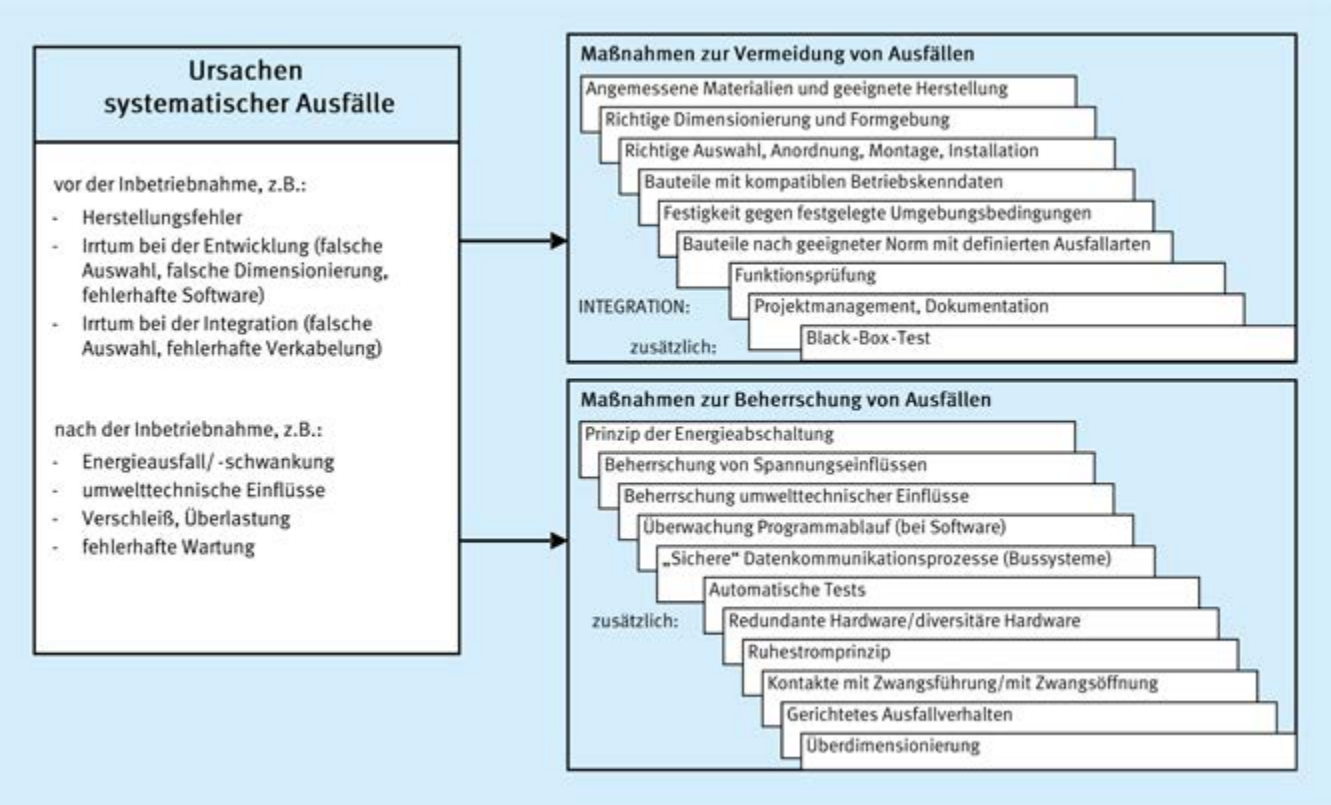


Abb. 8.1 Maßnahmen gegen systematische Ausfälle nach Anhang G der Norm

8.1.1 Systematische Ausfälle

Systematische Ausfälle haben im Gegensatz zu zufälligen Bauteilausfällen Ursachen, die nur durch Änderungen der Gestaltung, des Herstellungsprozesses oder der Betriebsverfahren beseitigt werden können. Sie entstehen irgendwann im Laufe des Entwicklungszyklus eines Produktes, z. B. durch Fehler in der Spezifikation, im Entwurf oder bei einer Änderung. Zu den Gründen für systematische Ausfälle zählen im Sinne der Norm auch Produktionsausfälle, Auswirkungen durch Umweltbelastungen oder Betriebsausfälle. Auch fehlerhafte Entwicklungswerkzeuge können zu systematischen Ausfällen führen. Die Realisierung mehrkanaliger Strukturen und auch die Betrachtung der Häufigkeit von Bauteilausfällen sind wichtige Elemente der sicherheitstechnischen Gestaltung. Was helfen die schönsten Zahlen zur Ausfallhäufigkeit, 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).

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 zur Beherrschung (G.2). Abbildung 8.1 gibt eine Übersicht von Maßnahmen gegen systematische Ausfälle. Die Maßnahmen zur Vermeidung von Ausfällen müssen sich dabei durch alle Lebensphasen eines Produktes ziehen und werden demnach in diesem Report teilweise auch in anderen Kapiteln, insbesondere im Kapitel 10 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 8.1** als „zusätzlich" gekennzeichnet).

Für ein besseres Verständnis werden die Maßnahmen in der Norm größtenteils kurz erläutert. Es sei darauf hingewiesen, dass Diversität im Allgemeinen, also nicht nur wie in Abbildung 8.1 für Hardware aufgeführt, in der täglichen Praxis des IFA ein großer Nutzen unterstellt wird – vergleiche dazu auch die Ausführungen zu Anforderungen an Software im Abschnitt 9.10.

Worin besteht nun der Unterschied zu den Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (Common Cause Failure, CCF; siehe Abschnitt 8.2.15)? 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 Ansatz, 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 CCF zu erfüllen.

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

Beispiel 1

Maßnahmen zur Beherrschung von Auswirkungen eines Energieausfalls

Bei der Gestaltung von Teilsystemen und sicherheitsbezogenen Teilen von Steuerungen sind auch Störungen der Energieversorgung (elektrische Spannung, Luftdruck in der Pneumatik, Hydraulikdruck) zu berücksichtigen (siehe Abschnitt 5.2.2.8 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. Ist dies der Fall, werden ihre Auswirkungen auf den PL 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. Sie können nur als systematische Ausfälle – teilweise sogar als Betriebszustand – betrachtet werden, die vom Teilsystem bzw. SRP/CS beherrscht werden müssen, sodass der sichere Zustand erreicht und/oder aufrechterhalten wird. Seit der dritten Ausgabe der Norm sollen hierfür jeweils unterschiedliche Sicherheitsfunktionen vorgesehen werden:

a) mit verfügbarer Energie,
b) ohne verfügbare Energie.

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

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“ legen u. a. fest, dass bei der Konstruktion und Herstellung von pneumatischen Bauteilen auf die „Anwendung geeigneter Werkstoffe und Herstellungsverfahren“ und „geeignetes Vermeiden einer Verunreinigung der Druckluft“ geachtet werden muss. Diese Anforderungen beziehen sich vor allem auf die Auswahl der Werkstoffe, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Reibung, Verschleiß, Korrosion und Temperatur bzw. auf die Berücksichtigung von hoch wirksamer Filtration der Druckluft/Abscheidung von Feststoffen und Wasser. Weiterhin sind in den Tabellen C.1 und C.2 in ähnlicher Weise die Anforderungen an hydraulische Bauteile festgelegt. Auch hier müssen „ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Druckmediums“ getroffen und auf die „richtige Dimensionierung und Formgebung“ geachtet werden.

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

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

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

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

Beispiel 3

Trennung sicherheitsbezogener von anderen Funktionen

Normen funktionaler Sicherheit thematisieren generell die Trennung sicherheitsbezogener Funktionen von anderen Funktionen (Nicht-Sicherheitsfunktionen) – so auch DIN EN ISO 13849-2 und zwar z. B. als grundlegendes oder bewährtes Sicherheitsprinzip „Trennung“ bzw. „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. Eine oft verwendete Art der Trennung von Standard-Anwendungssoftware und sicherheitsrelevanter Anwendungssoftware (SRASW, siehe Kapitel 9) ist natürlich, diese mit getrennten Programmiersystemen (sogenannte Engineering-Suiten) zu erstellen und auf verschiedenen Speicherprogrammierbaren Steuerungen (SPS) ablaufen zu lassen. Insbesondere aus wirtschaftlichen Gründen wird man jedoch versuchen, die gesamte Anwendungssoftware mit nur einem Programmiersystem und ggf. in einem gemeinsamen Engineering-Ablauf zu erstellen. Dabei ist allerdings eine Vielzahl von Aspekten zu berücksichtigen, z. B. die Anforderung, dass sicherheitsrelevante Variablen, Ergebnisse oder Ausgänge nicht von nicht sicherheitsrelevanten Softwareteilen (Programm, Funktionsbaustein, Funktion/Anweisung u. ä.) überschrieben werden dürfen. Verknüpfungen beider Welten sind zwar zulässig, jedoch nur unter Einhaltung festgelegter Konventionen erlaubt. Dabei müssen sicherheitsrelevante Signale und Funktionen immer Priorität behalten: So ist eine „ODER“-Verknüpfung für die Freigabe gefahrbringender Bewegungen 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 – ist bei der Konstruktion also unerlässlich. Doch ist die Analyse, wo (technisch) und wie (funktional) solche Einflüsse möglich sind, durch den Einsatz oben geannanter 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.

Neben den oben beschriebenen Einzelmaßnahmen sieht die Norm vor, alle Aktivitäten, Ressourcen, Rollen und Verfahren systematisch zu planen und durchzuführen bzw. zu dokumentieren. Dies muss in einem Plan der funktionalen Sicherheit erfolgen, dessen Ziel das Management der funktionalen Sicherheit ist. Die Abschnitte 4.1 und 5.1 beschreiben hierzu Details. Besonders hinzuweisen ist in diesem Zusammenhang auch auf die Fehleranfälligkeit von Änderungen. Eine Einflussanalyse dient dazu, die notwendigen Aktivtäten bis hin zu einer erneuten (Teil-)Validierung festzulegen.

8.1.2 Ergonomie

Die europäische Maschinenverordnung (EU) 2023/1230 (MV) fordert in Anhang III Abschnitt 1.1.6 vom Maschinenhersteller, dass Belästigung, Ermüdung sowie körperliche und psychische Fehlbeanspruchung des Bedienpersonals unter Berücksichtigung der in der MV als Mindestanforderung genannten ergonomischen Prinzipien bereits bei der Konzeption der Maschine auf das mögliche Mindestmaß zu reduzieren sind. Dies gilt daher auch für die Schnittstellen zwischen dem Bedienpersonal einer Maschine und den SRP/CS, die an die körperlichen Voraussetzungen des Bedienpersonals anpassbar sein müssen. Darunter fallen sowohl konkrete Schutzeinrichtungen wie eine Schutztür mit Positionsschalter als auch die Bedienung einer Sicherheitsfunktion z. B. über Taster. Des Weiteren wird in der MV die Anpassung der Mensch-Maschinen-Schnittstelle (Human-Machine Interface, HMI) an die Eigenschaften des Bedienpersonals auch bei selbst weiterentwickelndem Verhalten der Maschine bzw. der zugehörigen Produkte, die mit unterschiedlichen Autonomiegraden realisiert werden, gefordert. Es muss bei der Beabsichtigung des oben beschriebenen Verhaltens angemessen und ausreichend auf das Bedienpersonal (z. B. verbal durch Worte, Gesten, Gesichtsausdrücke oder Körperbewegungen) reagiert werden. Geplante Aktionen der Maschine und die Gründe dafür (was die Maschine tun wird und warum) müssen dem Bedienpersonal verständlich mitgeteilt werden.

Weiterhin sind ein von der Maschine vorgegebener Arbeitsrhythmus und Überwachungstätigkeiten, die dauernde Aufmerksamkeit erfordern, zu vermeiden.

Welche Bedeutung ergonomische Prinzipien für SRP/CS haben und dass nicht immer jede bestimmungsgemäße Verwendung oder vorhersehbare Fehlanwendung von SRP/CS bei der Konstruktion einer Maschine berücksichtigt wird, zeigt der HVBG-Report „Manipulation von Schutzeinrichtungen an Maschinen“ [31]. Auf der Internetseite https://stop-defeating.org sind Hilfsmittel und weitere Informationen zum Thema „Manipulation verhindern“ verfügbar.

Aus den oben genannten Gründen fordert die Norm die Verwendung ergonomischer Prinzipien und verweist dazu in Kapitel 9 auf Abschnitt 6.2.8 der EN ISO 12100:2010 und in einer Anmerkung auf den zugehörigen technischen Report DIN ISO/TR 22100-3. Des Weiteren wird auf die EN ISO 9241 „Ergonomie der Mensch-System-Interaktion“, Teil 210 „Prozess zur Gestaltung gebrauchstauglicher interaktiver Systeme“ verwiesen. Damit Maschinenkonstrukteure die Gestaltung der Mensch-Maschine-Schnittstelle der SRP/CS überprüfen können, wurde im IFA die Checkliste „Ergonomische Maschinengestaltung von Werkzeugmaschinen der Metallbearbeitung“ entwickelt und als DGUV Information 209-068/069 veröffentlicht [32]. Konkreter behandelt werden u. a. handbediente Stellteile (Tastaturen, Tasten und Eingabegeräte, Displays und Anzeigen), optische Gefahrensignale und die Softwareergonomie von Bedienoberflächen. Eine gute Ergonomie der eingesetzten Software ist für die Güte der Arbeitsergebnisse, die Zufriedenheit und Motivation der Beschäftigten entscheidend. Weitere Informationen zum Thema Softwareergonomie liefert z. B. die DGUV Information 215-450 [33]. Eine Konstruktionshilfe bei der nutzergerechten Gestaltung von Bediensystemen für Maschinen bietet z. B. die VDI/VDE-Richtlinie 3850 [34].

8.2 Quantifizierung der Ausfallhäufigkeit

Die von der Norm zur Ermittlung des PL geforderte zahlenmäßige Bestimmung der Ausfallhäufigkeit, 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, die bei dieser „Bestimmung“ berücksichtigt werden sollen, genannt, die Wahl der Methode zur Ermittlung der Ausfallhäufigkeit aus diesen Einflussgrößen bleibt aber frei. Hier ist grundsätzlich jede abgesicherte und anerkannte Methode erlaubt, z. B. Zuverlässigkeits-Blockdiagramme, Fehlerbaum-Methode, Markov-Modellierung oder Petri-Netze. Je nachdem, wer die Ausfallhäufigkeit 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 Ausfallhäufigkeit unerfahren sind, sicherlich Bedarf nach Hilfestellung seitens DIN EN ISO 13849-1. Dieser Tatsache wird Rechnung getragen, indem ein vereinfachter Ansatz angeboten wird, der trotz wissenschaftlich fundierter Grundlagen (Markov-Modellierung) Schritt für Schritt eine einfache Möglichkeit der Quantifizierung beschreibt. Zwar werden dort an einigen Stellen konservative Abschätzungen zur sicheren Seite getroffen, die den geschätzten Zahlenwert der Ausfallhäufigkeit gegenüber exakteren Methoden verschlechtern können, dafür ist die Methode aber auch für nicht mathematisch versierte Personen praktikabel. Zudem ist das Verfahren weitgehend eindeutig und damit nachvollziehbar. Im Folgenden wird dieses vereinfachte Verfahren ausführlich im Allgemeinen und anhand eines durchgerechneten praktischen Beispiels (siehe Abschnitt 8.4) vorgestellt. Weitere Details zu einzelnen Spezialthemen können in den Anhängen nachgelesen werden.

8.2.1 Vorgesehene Architekturen ...

Die Struktur oder Architektur eines Teilsystems bestimmt die Toleranz gegenüber Fehlern (Fehlertoleranz) und stellt das Gerüst dar, auf dem alle anderen quantifizierbaren Aspekte aufbauen, um schließlich den PL des Teilsystems zu bilden. Die Erfahrungen bei der praktischen Umsetzung 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 Kapitel 7). Dies sind das einkanalige ungetestete System mit unterschiedlich zuverlässigen Bauteilen am einen Ende des Spektrums, das im Mittelfeld durch Tests aufgewertet werden kann, und schließlich das zweikanalige hochwertig getestete System am anderen Ende. Systeme mit mehr als zwei Kanälen oder andere „exotische“ Strukturen sind im Maschinenbau extrem selten vertreten und können mit dem vereinfachten Verfahren nur bedingt bewertet werden. Meist reicht es aber selbst bei mehr als zwei Kanälen aus, die beiden zuverlässigsten zu berücksichtigen, um den PL mit dem vereinfachten Verfahren der vorgesehenen Architekturen hinreichend genau abzuschätzen. Daher werden Systeme mit mehr als zwei Kanälen in DIN EN ISO 13849-1 nicht betrachtet. Das SISTEMA-Kochbuch 4 [30] hilft in einigen dieser Fälle: „Wenn die vorgesehenen Architekturen nicht passen“. Neben der „horizontalen“ Einteilung in verschiedene funktionale oder testende Kanäle ist meist auch eine „vertikale“ Einteilung des Teilsystems 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}: durchschnittlicher Diagnosedeckungsgrad) 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 (typischerweise drei, nämlich 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 einen der fünf Grundtypen abbilden lässt. Dann hilft meist eine Zerlegung der Sicherheitskette in mehrere Abschnitte, sogenannte Teilsysteme, von denen sich jedes einzeln auf eine vorgesehene Architektur abbilden lässt. Wie diese Teilsysteme wieder zusammengesetzt und aus den einzelnen Performance Leveln wieder ein Gesamtwert ermittelt werden kann, wird in Kapitel 7 näher erläutert. Die folgenden Ausführungen beziehen sich auf Teilsysteme, die einer Kategorie nach DIN EN ISO 13849-1 zugeordnet werden können. Manchmal wird ein SRP/CS durchgehend von einem einzigen Teilsystem mit durchgehender Kategorie gebildet. In diesem Fall ist eine Unterscheidung zwischen SRP/CS und Teilsystem nicht erforderlich.

8.2.2 ... und Kategorien

Die Kategorien klassifizieren Teilsysteme in Bezug auf ihre Widerstandsfähigkeit gegen Fehler und das Verhalten der von ihnen ausgeführten Teilfunktion im Fehlerfall, basierend auf der Zuverlässigkeit und/oder der strukturellen Anordnung (**Tabelle 8.1**). Eine höhere Widerstandsfähigkeit gegenüber Fehlern bedeutet eine höhere mögliche Risikominderung. Für die Bestimmung der Ausfallhäufigkeit und des PL bilden die Kategorien deshalb das Rückgrat, das durch die Bauteilzuverlässigkeit ($MTTF_D$), die Tests (DC_{avg}) und die Widerstandsfähigkeit gegenüber 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 Teilfunktion 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 Teilfunktion überwiegend durch strukturelle Maßnahmen erreicht. In Kategorie 2 wird der Funktionskanal, der die Teilfunktion ausführt, in regelmäßigen Abständen durch einen Testkanal (Testeinrichtung TE mit Ausgang OTE) selbsttätig überprüft. Zwischen den Testphasen kann die Teilfunktion 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 Ausfall der Teilfunktion. 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 8.1 Zusammenfassung der Anforderungen für Kategorien

Kategorie	Zusammenfassung der Anforderungen	Verhalten der Teilfunktion	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Kanals	DC_{avg}	CCF
B	Teilsysteme 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 Teilfunktion führen.	überwiegend durch die Auswahl von Bauteilen charakterisiert	mindestens niedrig*	kein	nicht relevant
1	Die Anforderungen von Kategorie B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Teilfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	überwiegend durch die Auswahl von Bauteilen charakterisiert	hoch	kein	nicht relevant
2	Die Anforderungen von Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Das Teilsystem muss in geeigneten Zeitabständen getestet werden.	Das Auftreten eines Fehlers kann zum Verlust der Teilfunktion zwischen den Tests führen. Der Verlust der Teilfunktion wird durch den Test erkannt.	überwiegend durch die Struktur charakterisiert	mindestens niedrig*	mindestens niedrig	Maßnahmen erforderlich, siehe Anhang F
3	Die Anforderungen von Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Das Teilsystem muss so gestaltet werden, dass: • ein einzelner Fehler in irgendeinem seiner Teile nicht zum Verlust der Teilfunktion führt, und • wenn immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	Wenn ein einzelner Fehler auftritt, bleibt die Teilfunktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Teilfunktion führen.	überwiegend durch die Struktur charakterisiert	mindestens niedrig*	mindestens niedrig	Maßnahmen erforderlich, siehe Anhang F
4	Die Anforderung von Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Das Teilsystem muss so gestaltet werden, dass: • ein einzelner Fehler in irgendeinem seiner Teile nicht zum Verlust der Teilfunktion führt, und • der einzelne Fehler bei oder vor der nächsten Anforderung der Teilfunktion erkannt wird. Wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Teilfunktion führen.	Wenn ein einzelner Fehler auftritt, bleibt die Teilfunktion immer erhalten. Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Teilfunktion (hoher DC_{avg}). Die Fehler werden rechtzeitig erkannt, um einen Verlust der Teilfunktion zu verhindern.	überwiegend durch die Struktur charakterisiert	hoch	hoch einschließlich der Fehleranhäufung	Maßnahmen erforderlich, siehe Anhang F

* Abweichungen zu Tabelle 5 der Norm ergeben sich aus den in 8.2.3 bis 8.2.6 beschriebenen Anforderungen.

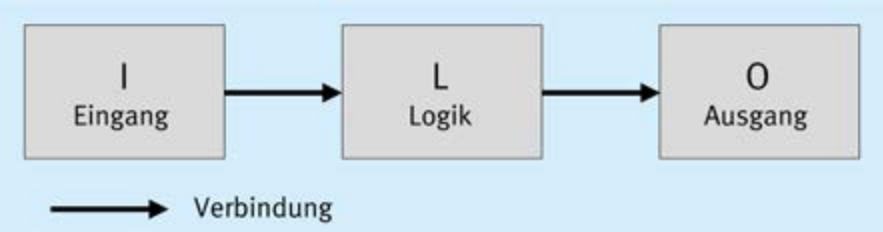


Abb. 8.2
Vorgesehene Architektur für Kategorie B und Kategorie 1

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

In den Kategorien 3 und 4 müssen auch Ausfälle infolge gemeinsamer Ursache, die ein gleichzeitiges Versagen mehrerer Kanäle hervorrufen können, in ausreichendem Maße beherrscht werden. Das gilt ebenso für die Kategorie 2, da die Testeinrichtung mit ihrem eigenen Abschaltpfad ebenfalls einen zweiten Kanal (Testkanal für den Funktionskanal) 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.

8.2.3 Kategorie B

Die Teilsysteme müssen nach den zutreffenden Normen unter Verwendung der grundlegenden Sicherheitsprinzipien für die bestimmte Anwendung so gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert werden, dass sie folgendem standhalten können:

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

Bezüglich elektromagnetischer Störfestigkeit verweist die Norm auf besondere Anforderungen in den entsprechenden Produktnormen, z. B. DIN EN 61800-3 für Antriebssysteme. Sie betont die Wichtigkeit der Anforderungen an die Störfestigkeit besonders für die funktionale Sicherheit der Teilsysteme. Wenn keine Produktnorm vorhanden ist, bietet die Norm seit ihrer vierten Ausgabe drei alternative sogenannte Pfade an, mit denen die erforderliche elektromagnetische Störfestigkeit für funktionale Sicherheit erreicht werden kann. Anhang L geht ausführlich auf dieses Thema ein.

Die für alle Kategorien verbindlichen 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 8.1), 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 reicht für die $MTTF_D$ jedes Kanals ein niedriger Wert (zur Definition von „niedrig“ bis „hoch“ siehe Tabelle 8.2 auf Seite 77). Tritt ein Bauteilausfall auf, kann es zum Ausfall des Teilsystems führen. Es sind keine Überwachungsmaßnahmen gefordert, d. h. auch kein DC_{avg}. Auch Ausfälle infolge gemeinsamer Ursache sind bei einkanaligen Steuerungen nicht relevant, daher werden keine Anforderungen hinsichtlich CCF gestellt.

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

Die vorgesehene Architektur für Kategorie B in **Abbildung 8.2** entspricht einem einkanaligen Teilsystem mit Eingabe- (Input I), Verarbeitungs- (Logik L) und Ausgabeebene (Output O).

8.2.4 Kategorie 1

Zusätzlich zu den Anforderungen für Kategorie B, z. B. Verwendung grundlegender Sicherheitsprinzipien, müssen Teilsysteme 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 dokumentierten erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet wurde (hier gibt die Norm einen Hinweis auf das in DIN EN 61508-2 benutzte Konzept der „Betriebsbewährung“, das im Maschinenbau schwer erfüllbare dokumentarische Anforderungen an eine

Eignungsanalyse und Tests für die vorgesehene Anwendung, eine Demonstration der Gleichwertigkeit zwischen dem vorgesehenen Betrieb und der vorherigen Betriebserfahrung, einschließlich einer Einflussanalyse zu den Unterschieden und einen statistischen Nachweis auf Basis eines effektiven Systems für die Erfassung von Ausfällen beinhaltet) oder
- in Anhang A bis D der DIN EN ISO 13849-2 als bewährtes Bauteil unter den dort genannten Bedingungen aufgelistet ist oder
- unter Anwendung von Prinzipien, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen entsprechend den zutreffenden Produkt- und Anwendungsnormen 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 dritte oben genannte Bedingung erfüllen. Die Entscheidung, ein bestimmtes Bauteil als bewährt zu akzeptieren, hängt von der Anwendung ab. Komplexe elektronische Bauteile, z. B. speicherprogrammierbare Steuerungen (SPS), Mikroprozessoren oder anwendungsspezifische integrierte Schaltungen (ASIC), dürfen generell nicht als gleichwertig zu „bewährt" betrachtet werden. Dieser Ausschluss ist dadurch begründet, dass diese Bauteile ein vielfältiges, teilweise unvorhersehbares Ausfallverhalten, z. B. ausgelöst durch elektromagnetische Störungen, zeigen. Software-Fehler oder Soft-Errors sind praktisch nicht mehr vollständig beherrschbar. Folgerichtig dürfen sie grundsätzlich nicht als „Black Box" mit einfachem, definiertem Ausfallverhalten betrachtet werden. Auch ihre hohe Änderungsrate (verursacht durch Modifikation von Hardware und Software) erhöht die Wahrscheinlichkeit für systematische Ausfälle durch Fehler im Entwicklungs- und Fertigungsprozess. DGUV Test Information 06 [35] erläutert diese Einschätzung näher.

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 8.2.10) eine „unendlich 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 Ausfall des Teilsystems führen. Jedoch ist die $MTTF_D$ des Kanals in Kategorie 1 größer als in Kategorie B. Folglich ist der Ausfall des Teilsystems 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 8.2), da die Unterschiede in der Bauteilzuverlässigkeit und nicht in der Struktur liegen.

8.2.5 Kategorie 2

Zusätzlich zu den Anforderungen für Kategorie B (z. B. Verwendung grundlegender Sicherheitsprinzipien) müssen Teilsysteme der Kategorie 2 bewährte Sicherheitsprinzipien verwenden und so gestaltet sein, dass ihr Funktionskanal, der die Teilfunktion ausführt, in angemessenen Zeitabständen getestet wird. Hier gilt die zusätzliche Bedingung, dass alle Teile des Funktionskanals (Eingang I, Logik L und Ausgang O, **Abbildung 8.3)** ein Mindestmaß an Fehleraufdeckung besitzen (siehe *DC*-Anforderungen weiter unten). Die Teilfunktion muss vor oder bei ihrer Anforderung getestet werden, bevor eine Gefährdungssituation eintritt, beispielsweise
- vor dem Start eines neuen Zyklus,
- vor dem Start anderer Bewegungen,
- unmittelbar bei Anforderung der Teilfunktion oder
- periodisch während des Betriebs, wenn die Risikobeurteilung und die Betriebsweise zeigen, dass dies notwendig ist.

Die Testung erfolgt in der Regel automatisch durch den Testkanal, bestehend aus der Testeinrichtung TE und ihrem separaten Ausgang OTE (siehe Abbildung 8.3). Sie kann abhängig von der Risikobeurteilung aber auch manuell eingeleitet werden. Jeder Test der Teilfunktion muss entweder
- den Betrieb zulassen, wenn keine Fehler erkannt wurden, oder
- eine Ausgabe für die Einleitung geeigneter Steuerungsmaßnahmen erzeugen (OTE), wenn ein Fehler erkannt wurde.

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

Für die vorgesehene Architektur der Kategorie 2 (Abbildung 8.3) berücksichtigt die Berechnung der $MTTF_D$ und DC_{avg} nur die Blöcke des Funktionskanals (d. h. I, L und O). Die $MTTF_D$ der Blöcke des Testkanals (d. h. TE und OTE) geht nur indirekt ein, da dort vorausgesetzt wird, dass die $MTTF_D$ des Testkanals mindestens halb so groß wie die $MTTF_D$ des Funktionskanals ist. Für die $MTTF_D$ des Funktionskanals sind Werte von niedrig bis hoch erlaubt. Der

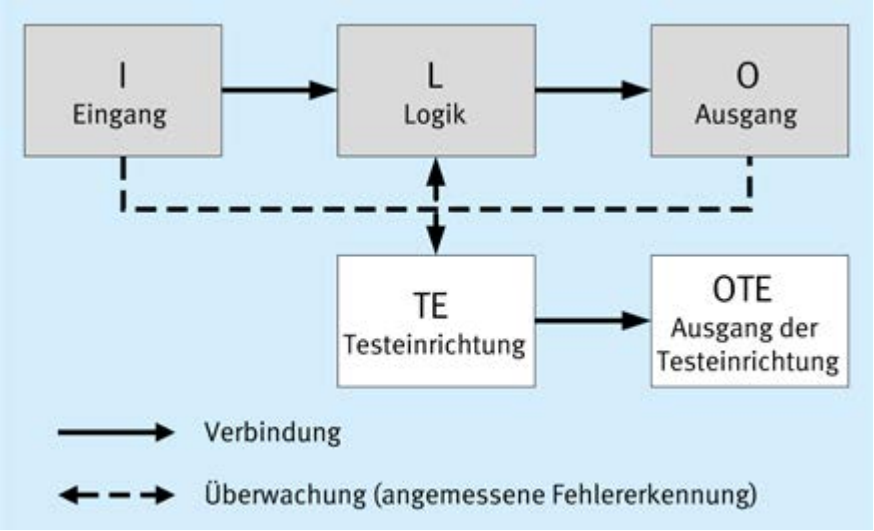


Abb. 8.3
Vorgesehene Architektur für Kategorie 2; gestrichelte Linien kennzeichnen vernünftigerweise durchführbare Fehlererkennung

DC aller Teile des Funktionskanals (I, L und O) und somit auch der DC_{avg} müssen mindestens niedrig sein. Ausreichende Maßnahmen gegen CCF müssen ebenfalls angewendet werden (siehe Abschnitt 8.2.15 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 werden (weitere Hinweise unten). In einigen Fällen ist die Kategorie 2 nicht anwendbar, da sich der Test der Teilfunktionen nicht bei allen Bauteilen durchführen lässt. Da das Teilsystem zwischen den Tests unbemerkt ausfallen kann, ist die Testhäufigkeit ein kritischer Parameter. Außerdem könnte die Testung selbst früher als der Funktionskanal unbemerkt ausfallen. In der zweiten Ausgabe der Norm wurden im Rahmen des vereinfachten Verfahrens für die Abschätzung des PL mithilfe der vorgesehenen Architektur und des Säulendiagramms (Abbildung 8.7, Seite 82) daher Bedingungen an die Testhäufigkeit und die $MTTF_D$ des Testkanals geknüpft. Diese Bedingungen wurden mit der vierten Normausgabe generell für Teilsysteme der Kategorie 2 verpflichtend und lauten:

- Der $MTTF_D$-Wert des Testkanals ist nicht kleiner als der halbe $MTTF_D$-Wert des Funktionskanals und
- die Testrate ist mindestens 100-mal höher als die mittlere Anforderungsrate der Sicherheitsfunktion (ausnahmsweise mindestens 25-mal höher, siehe Abschnitt 8.2.14) oder
- die Testung erfolgt unmittelbar bei Anforderung der Sicherheitsfunktion und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand (in der Regel wird die Maschine angehalten) ist kürzer als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855).

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

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

- Die Norm forderte bis zur dritten Ausgabe pauschal die Testung der Sicherheitsfunktion (bezogen auf ein Teilsystem entspricht dies der Teilfunktion). Da diese deterministische Forderung genaugenommen einer perfekten Fehlererkennung, also einem *DC* von 100 % entspricht (alle gefährlichen Fehler, die zum Ausfall der Sicherheitsfunktion führen, werden erkannt), passt dies nicht zur quantitativen Sichtweise, die für Kategorie 2 nur einen Mindestwert für DC_{avg} von „niedrig“, also 60 %, fordert. Außerdem würde eine strenge Auslegung erfordern, dass die Sicherheitsfunktion testweise ausgelöst wird (z. B. durch das kurzzeitige Ausschalten der Sendedioden eines Lichtgitters) und das provozierte Abschalten der Ausgangselemente überwacht wird (z. B. durch zwangsgeführte Rücklesekontakte am Ausgangsschütz). Damit würden viele technische Realisierungen von einkanaligen getesteten Systemen, die auf partieller Fehlererkennung, z. B. durch einen Watchdog für den Logikteil, beruhen, formell die bisherige Definition einer Kategorie 2 nicht erfüllen. Mit der vierten Normausgabe ist hier ein Paradigmenwechsel erfolgt, indem die pauschale „Testung der Sicherheitsfunktion“ durch einen mindestens partiellen Test aller Teile des Funktionskanals ersetzt wurde. Damit ist klargestellt, dass für Teilsysteme, in denen für den Eingangs-, Logik- oder Ausgangsteil nicht mindestens eine „niedrige“ Fehlererkennung möglich ist, Kategorie 2 nicht anwendbar ist.

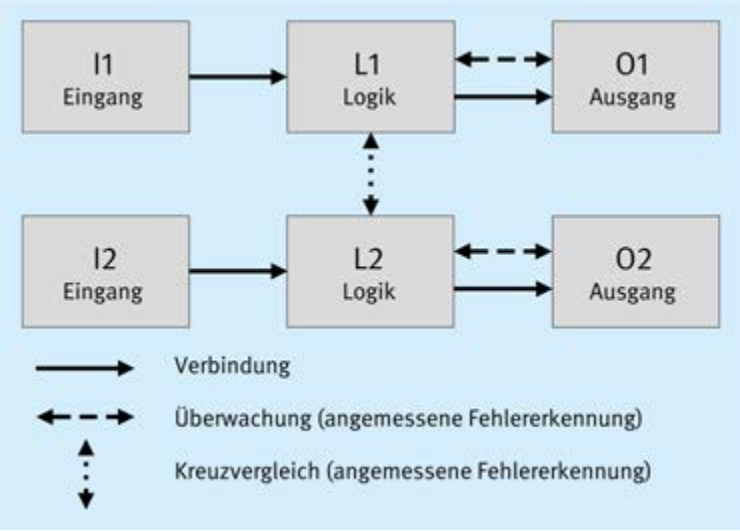


Abb. 8.4
Vorgesehene Architektur für Kategorie 3: gestrichelte Linien kennzeichnen vernünftigerweise durchführbare Fehlererkennung

Die quantitative Forderung eines mindestens niedrigen DC_{avg} ergibt sich aus der geänderten Definition der Kategorie 2 zwangsläufig. Trotzdem ist es nach wie vor empfehlenswert, dass die Diagnose immer möglichst nah an der „echten Ausführung der Teilfunktion" bleiben sollte.

- Der Hinweis „Die Testeinrichtung darf als Bestandteil des Funktionskanals oder getrennt davon vorgesehen sein." bedeutet, dass zwar durchaus ausführende Elemente der Testeinrichtung im Funktionskanal angesiedelt sein dürfen, z. B. um in einem aus Elektronik bestehenden Teilsystem Signale und Informationen bereitzustellen, die die Grundlage für eine Diagnose bilden. Der die Diagnosebefunde bewertende Teil der Testeinrichtung muss jedoch extern zum Funktionskanal, z. B. als separater Watchdog realisiert werden. Nur so können die Anforderungen zur Unabhängigkeit von Funktionskanal und Testkanal erfüllt werden. Die Diagnoseinformation für die Testeinrichtung sollte möglichst aussagefähig in Bezug auf die sicherheitsbezogene Funktionsfähigkeit der überwachten Teile des Funktionskanals sein. Sie sollte daher eine gewisse Mindestkomplexität (z. B. analoge oder dynamische Signale) aufweisen, sodass die Testeinrichtung eine fundierte Entscheidung über die Funktionsfähigkeit treffen kann. Die komplette Verschmelzung von TE mit dem Funktionskanal ist nicht akzeptabel, z. B. bei einem On-Chip-Watchdog ohne Trennung nach DIN EN 61508-2:2011, Anhang E (besondere Architekturanforderungen an integrierte Schaltkreise mit On-Chip-Redundanz) oder bei einer Testeinrichtung, die nur durch Software realisiert ist und über ein per Software generiertes Abschaltsignal direkt auf OTE zugreift.
- Abschnitt 8.2.14 und Anhang E geben weitere Hinweise, speziell auch zur erforderlichen Testhäufigkeit, zur Zuverlässigkeit der Testeinrichtung, zur Einleitung der Tests (automatisch, manuell, bei Anforderung der Sicherheitsfunktion) und zu Diagnosemaßnahmen.

8.2.6 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 Ausfall 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 möglich. Da nicht alle Fehler erkannt werden müssen oder die Fehleranhäufung unerkannter gefahrbringender Fehler zu einer Gefährdungssituation führen kann, reicht minimal ein niedriger DC_{avg}. Zur Frage der Testhäufigkeit siehe Abschnitt 8.2.14. Ausreichende Maßnahmen gegen CCF müssen angewendet werden.

Die Forderung nach Einfehlersicherheit bedeutet nicht zwangsweise eine Realisierung als zweikanaliges Teilsystem, da z. B. auch einkanalige Teile ohne gefahrbringendes Ausfallpotenzial (fehlersicheres Design) sicher gegen Einzelfehler sein können. Dasselbe gilt für Teilsysteme aus einem Funktionskanal mit hochwertiger Überwachung (Erkennung aller gefahrbringenden Fehler) in einem zusätzlichen Testkanal, der bei Anforderung der Teilfunktion durch einen eigenen Abschaltpfad eine Fehlerreaktion so schnell einleiten kann, dass ein gefährlicher Zustand bei jedem Einzelfehler vermieden wird. Trotzdem werden Kategorie-3-Systeme überwiegend zweikanalig realisiert, weshalb auch die zugehörige vorgesehene Architektur entsprechend gewählt wurde (**Abbildung 8.4**). Eine rein „logische Zweikanaligkeit", z. B. durch redundante Software auf einkanaliger Hardware, wird allerdings in der Regel nicht einfehlersicher gegen Hardwareausfälle sein.

Der mit Teilsystemen der Kategorie 3 erreichbare PL ist nicht pauschal begrenzt und kann bis PL = e gehen. Eine indirekte Begrenzung ergibt sich, wie bei allen anderen Kategorien auch, aus dem erreichten *PFH*-Wert.

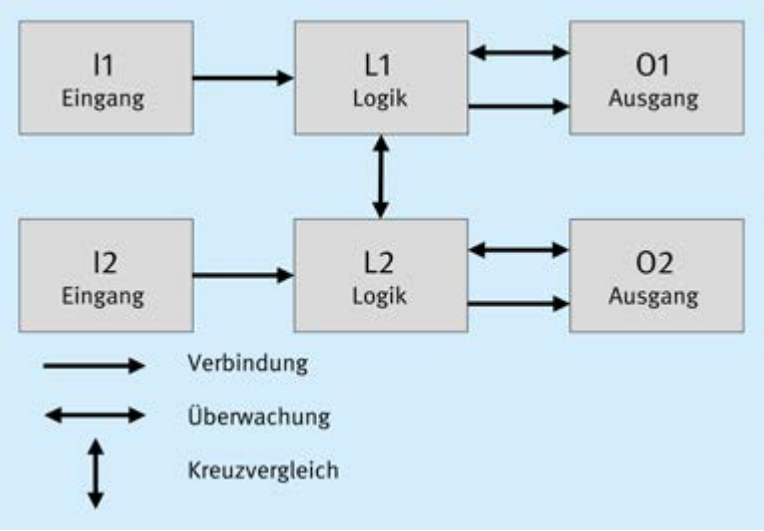


Abb. 8.5
Vorgesehene Architektur für Kategorie 4

8.2.7 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 Ausfall 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 Ausfall der Sicherheitsfunktion führen (in der Praxis kann die Betrachtung einer Fehlerkombination für zwei Fehler ausreichend sein).

Bei der Betrachtung der Fehlerkombinationen, typischerweise im Rahmen einer Ausfalleffektanalyse FMEA, ist es manchmal nicht möglich, 100 % der theoretisch denkbaren gefährlichen Fehler als erkennbar einzustufen. Daher wird in Kategorie 4 für die *PFH*-Berechnung „nur“ ein hoher *DC* von rechnerisch 99 % gefordert. Andererseits darf gemäß der Definition von Kategorie 4 die Anhäufung von (bis zu zwei) unerkannten gefährlichen Fehlern nicht zum Ausfall der Sicherheitsfunktion führen. Gäbe es daher tatsächlich einen unerkannten gefährlichen Fehler mit praktischer Relevanz, könnte der zweite gefährliche Fehler zum Versagen einer Kategorie 4-Struktur führen. Hier sorgt eine mit der vierten Normausgabe neu eingebrachte Anmerkung für mehr Klarheit: Gefährliche Fehler mit einer sehr niedrigen Wahrscheinlichkeit (theoretisch denkbar, praktisch aber nicht relevant) brauchen für die Fehleranhäufung nicht berücksichtigt zu werden – allerdings nur, wenn diese Fehlerbetrachtung dokumentiert und verifiziert wird.

Da es sich um die Kategorie mit der höchsten Widerstandsfähigkeit gegen Fehler handelt (höchster Beitrag zur Risikominderung), müssen sowohl die $MTTF_D$ jedes Kanals als auch der DC_{avg} hoch sein (zur Frage der Testhäufigkeit siehe Abschnitt 8.2.14) und ausreichende Maßnahmen gegen CCF angewendet werden. Folgerichtig kann mit Teilsystemen der Kategorie 4 ein PL = e erreicht 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 8.5**) ähnlich derjenigen für Kategorie 3. Allerdings symbolisieren die durchgezogenen Linien für die Überwachung den höheren DC_{avg}.

8.2.8 Blöcke und Kanäle

Zur vereinfachten Quantifizierung der Ausfallhäufigkeit ist eine Darstellung der inneren Struktur von Teilsystemen in Form von abstrahierten Blöcken und Kanälen hilfreich. Beispiele für diese Form der Darstellung sind die vorgesehenen Architekturen der Kategorien (Abbildungen 8.2 bis 8.5). Die Bezeichnung „Blöcke“ hat in diesem Zusammenhang eine eigene, feststehende Bedeutung. Es handelt sich hier um Funktionsblöcke nur in dem Sinne, dass die Teilfunktion und ihre Testung in kleineren, seriell und parallel angeordneten Einheiten ausgeführt wird. Für die Abbildung der Hardwarestruktur auf ein sicherheitsbezogenes Blockdiagramm können folgende Regeln gelten:

- Die Blöcke sollen in abstrakter Form alle Steuerungsbauteile abbilden, die sich auf die Ausführung der Sicherheitsfunktion beziehen.
- Wird die Teilfunktion 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 Teilfunktion 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 Gliederungshilfe 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 Ausfallhäufigkeit.
- Für jede sicherheitsrelevante Hardwareeinheit soll die Blockzugehörigkeit eindeutig festgelegt sein, z. B. als Stückliste. Dies erlaubt die Berechnung der mittleren Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$) des Blocks, basierend auf der $MTTF_D$ der Hardwareeinheiten, die zu diesem Block gehören (z. B. durch die Ausfalleffektanalyse FMEA oder das „Parts Count"-Verfahren, siehe Abschnitt 8.2.13).
- Nur rein zu Testzwecken verwendete Hardwareeinheiten, deren Ausfall die Ausführung der Sicherheitsfunktion in den verschiedenen Kanälen nicht direkt beeinträchtigen kann, können als separater Block zusammengefasst werden. Die Norm stellt für die Kategorien 3 und 4 keine direkten Anforderungen an dessen Zuverlässigkeit, aber Abschnitt 8.2.14 und Anhang E geben dazu Hinweise. Zudem sollten systematische Ausfälle und CCF berücksichtigt werden.

8.2.9 Sicherheitsbezogenes Blockdiagramm

Das sicherheitsbezogene Blockdiagramm ist dem bekannteren Zuverlässigkeitsblockdiagramm [36] entlehnt. Gemeinsam ist beiden das Prinzip, dass die (Sicherheits- oder Teil-)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 8.6** gezeigt.

Gemäß dieser Definition lassen sich folgende Regeln für die Darstellung eines Teilsystems 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 Teilfunktion nicht weiter ausführen.
- Die Parallelschaltung von Blöcken bzw. Kanälen symbolisiert die mehrfach redundante Ausführung der Teilfunktion oder entsprechender Teile davon. Zum Beispiel wird eine durch mehrere Kanäle ausgeführte Teilfunktion aufrechterhalten, solange mindestens ein Kanal keinen Ausfall hat.
- Nur für Testzwecke verwendete Blöcke, die bei ihrem Ausfall die Ausführung der Teilfunktion 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 in redundanten Systemen meist nur einen geringen Einfluss, solange die mehrkanalige Abarbeitung der reinen Sicherheitsfunktion in den einzelnen Kanälen weiter gewährleistet bleibt.

Die Definition der Blöcke und Kanäle geht einher mit der Bestimmung der Kategorie und ist der erste Schritt bei der quantitativen Bestimmung des PL. Dazu werden weitere Kennwerte benötigt: die Bewertung der Bauteilzuverlässigkeit ($MTTF_D$), der Tests (DC_{avg}) und der Relevanz von Ausfällen infolge gemeinsamer Ursache (CCF). Weitere Hinweise auf dem Weg „vom Schaltbild zum PL", speziell zur Ableitung des sicherheitsbezogenen Blockdiagramms, finden sich im SISTEMA-Kochbuch 1 [37]. Dort wird auch die Bezeichnung des „gekapselten Teilsystems" eingeführt. Dieses bezeichnet ein Teilsystem, für das der Hersteller bereits PL, *PFH* und Kategorie angibt und dessen genaue interne Struktur und Kennwerte nicht transparent sind. Diese Kennwerte setzen die Einhaltung der vom Hersteller spezifizierten Einsatzbedingungen voraus; dazu kann z. B. extern zu realisierende Diagnose gehören. Im sicherheitsbezogenen Blockdiagramm wird es auf Teilsystemebene einkanalig als Kreis in einem Block (siehe Teilsystem „SB1" in Abbildung 8.6) dargestellt, in die quantitative Bestimmung des PL geht es nur mit seinen Kennwerten *PFH* und PL ein. Die Angabe der Kategorie ist rein informativ.

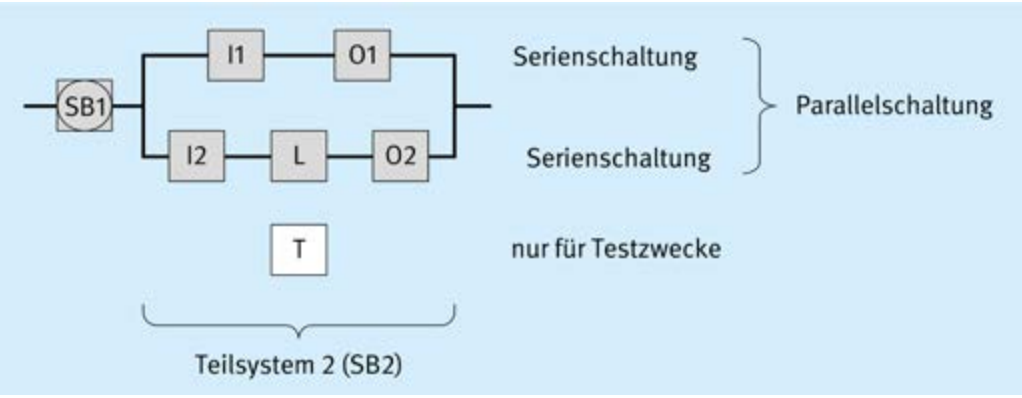


Abb. 8.6 Allgemeines Beispiel eines sicherheitsbezogenen Blockdiagramms; I1 und O1 bilden den ersten Kanal (Serienschaltung von SB2), während I2, L und O2 den zweiten Kanal von SB2 bilden (Serienschaltung); mit beiden Kanälen wird die Sicherheits- oder Teilfunktion redundant ausgeführt (Parallelschaltung); T wird nur für die Testung verwendet

8.2.10 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 Risikominderung),
- die allgemein anerkannte technische Erfahrung, unabhängig von der betrachteten Anwendung,
- die technischen Anforderungen in Bezug auf die Anwendung und auf die spezielle Gefährdung.

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

- Die Fehlerlisten stellen nur eine Auswahl dar. Daher müssen – wenn notwendig – neue Fehlermodelle erstellt werden (z. B. bei neuen Komponenten) oder je nach Applikation weitere Fehlerarten berücksichtigt werden. Dies ergibt sich z. B. auf der Grundlage einer FMEA.
- Folgefehler werden zusammen mit dem auslösenden Erstfehler als ein einzelner Fehler bewertet.
- Das gleichzeitige Auftreten von zwei oder mehreren Fehlern unterschiedlicher Ursache gilt als höchst unwahrscheinlich und braucht deswegen nicht betrachtet zu werden.

Mehrfachfehler, die eine gemeinsame Ursache haben, werden als CCF einer separaten Bewertung unterzogen (siehe Abschnitt 8.2.15).

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 ersichtlich ist (z. B. das Ablösen von Leiterbahnen bei richtig dimensioniertem Platinenlayout), muss eine genaue Begründung in der technischen Dokumentation gegeben werden.

Fehlerausschlüsse sind bei entsprechenden Voraussetzungen auch für Komponenten möglich, z. B. für die elektrischen Öffnerkontakte und die mechanische Betätigung von elektromechanischen Positionsschaltern oder Not-Halt-Geräten. Die Gültigkeit von Fehlerausschlüssen kann dabei auf niedrige PL begrenzt sein (siehe z. B. Tabelle D.8 der DIN EN ISO 13849-2 und Anhang D dieses Reports). Ein PL = e darf nach Norm nicht allein auf Fehlerausschlüssen beruhen und muss im Einzelfall begründet und geprüft werden. Für Komponenten mit Fehlerausschluss ist keine Berücksichtigung von Ausfallraten ($MTTF_D$) und Überwachungsmaßnahmen (DC) notwendig.

8.2.11 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 (Mean Time to Dangerous Failure, $MTTF_D$) 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, FIT steht für „Failure in Time“) notiert. Die Beziehung zwischen λ_D und $MTTF_D$ ist bei einer über die Lebensdauer konstanten Ausfallrate λ_D mit $MTTF_D = 1/\lambda_D$ gegeben, wobei die Umrechnung von Stunden auf Jahre natürlich zu berücksichtigen ist. Bei Bauteilen, die überwiegend durch ihre mechanische Betätigung verschleißen, ist es üblich, die Zuverlässigkeit in Schaltspielen, z. B. als B_{10D}-Wert anzugeben, d. h. die mittlere Anzahl von Zyklen, nach der 10 % der Bauteile gefährlich ausfallen. Hier kann eine Umrechnung in $MTTF_D$ durch Einbeziehen der in der Anwendung zu erwartenden mittleren Anzahl jährlicher Betätigungen n_{op} (Number of Operations) erfolgen. Mehr Einzelheiten dazu finden sich im Anhang D.

- „Gefahrbringend“ stellt klar, dass nur solche Ausfälle, die das Ausführen der Sicherheitsfunktion beeinträchtigen, letztlich in den PL einfließen (Ausfall zur unsicheren Seite). Im Gegensatz dazu können ungefährliche Ausfälle zwar den sicheren Zustand provozieren (Betriebshemmung) oder die Verfügbarkeit oder Produktivität einer Maschine herabsetzen, weiterhin wird aber die Sicherheitsfunktion erfolgreich ausgeführt oder der sichere Zustand eingeleitet bzw. aufrechterhalten. In redundanten Strukturen bezieht sich das Attribut „gefahrbringend“ allerdings auf jeden einzelnen Kanal. Führt ein Ausfall in einem Kanal zu einem Außerkraftsetzen der Sicherheits- oder Teilfunktion, so wird dieser Ausfall als gefahrbringend bezeichnet, selbst wenn ein weiterer Kanal noch erfolgreich arbeiten 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 am Teilsystem 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 8.2.10 näher beschrieben sind. Demnach können unter bestimmten Voraussetzungen z. B. Leitungskurzschlüsse oder bestimmtes mechanisches Versagen aufgrund der Konstruktion ausgeschlossen werden.

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

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

Seit der vierten Ausgabe der Norm werden auch Felddaten als potenzielle Datenquelle genannt, wenn die oben beschriebenen Methoden nicht anwendbar sind. An die Verlässlichkeit von Felddaten sind allerdings einige Anforderungen geknüpft: Die Felddaten müssen aus identischen Bauteil-Anwendungen in ähnlichen Umgebungen stammen und über eine aussagekräftige Zeitspanne gesammelt worden sein. Weiterhin müssen die Methoden zur Datenerfassung und -analyse ein vernünftiges Vertrauensniveau ergeben.

Sollte keine der hier beschriebenen Datenquellen verfügbar sein, kann als Abschätzung zur sicheren Seite für die $MTTF_D$ eines Bauteils der Wert von zehn Jahren angesetzt werden. Dieser sehr konservative Schätzwert begrenzt allerdings den erreichbaren PL sehr stark.

8.2.13 FMEA versus „Parts Count“-Verfahren

Sind die $MTTF_D$-Werte aller sicherheitsrelevanten Bauteile zusammengetragen, helfen einige simple Regeln, daraus den $MTTF_D$-Wert der Steuerung zu berechnen. Dabei gibt es verschiedene Methoden – aufwendig durch eine genaue Ausfalleffektanalyse (Failure Modes and Effects Analysis, FMEA) 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 ausgeglichen. 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. Dieser Näherungswert gilt während der angegebenen Gebrauchsdauer des Bauteils. Üblicherweise werden Frühausfälle vernachlässigt, da Komponenten mit ausgeprägten Frühausfällen den Verfügbarkeitsanforderungen an eine Maschinensteuerung nicht gerecht werden und daher im Markt nur eine geringe Rolle spielen. Dieses Vorgehen hat den Vorteil, dass die $MTTF_D$ immer gleich dem Kehrwert der zugehörigen gefährlichen Ausfallrate λ_D ist. Da sich die gefahrbringenden Ausfallraten λ_D der Bauteile in einem Block einfach aufsummieren, ergibt sich aus dem $MTTF_D$-Werten der beteiligten Bauteile (N Bauteile mit Laufindex i) in folgender Weise die $MTTF_D$ des Blocks:

$$\lambda_D = \sum_{i=1}^{N} \lambda_{Di} \quad \text{bzw.} \quad \frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}} \tag{8.1}$$

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 8.2**).

Tabelle 8.2 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

In Kategorie 4 beträgt die Obergrenze für „Hoch" 2 500 Jahre.

Weniger als drei Jahre mittlere (nicht garantierte!) Lebensdauer wird für Komponenten der Sicherheitstechnik als nicht angemessen betrachtet. Ergeben sich tatsächlich für einen Kanal weniger als drei Jahre, sollten die Bauteile durch solche mit höherer Zuverlässigkeit ausgetauscht werden, da sonst nicht einmal PL a erreicht werden kann. Mehr als 100 Jahre dürfen nur bei Kategorie 4 in Rechnung gestellt werden, um die Bauteilzuverlässigkeit gegenüber den anderen wichtigen Einflussgrößen wie Struktur oder Tests nicht überzubewerten. Diese Begrenzung ist vor allem mit Blick auf die in der $MTTF_D$ nicht erfassten systematischen Ausfälle (siehe Abschnitt 8.1.2) bewusst verankert. Mehr als 100 Jahre mittlere Lebensdauer sind nicht unüblich, tragen aber wegen der „Kappung" nicht mehr zum PL bei, da in der Bauteilzuverlässigkeit bereits der Höchstwert von 100 Jahren (in Kategorie 4 liegt der Höchstwert bei 2500 Jahren) in Rechnung gestellt wird.

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

$$MTTF_D = \frac{2}{3}\left(MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}} \right) \tag{8.2}$$

Bei ausgeglichenen Kanälen entspricht der so ermittelte $MTTF_D$-Wert der $MTTF_D$ jedes der beiden Kanäle. Bei unausgewogenen Kanälen ergibt sich eine mittlere $MTTF_D$, die minimal zwei Drittel des besseren Wertes betragen kann. Hier kann zusätzlich der Effekt auftreten, dass der bessere Kanal vorher auf 100 Jahre (bei Kategorie 4 sind es 2500 Jahre) $MTTF_D$ gekappt wurde und der symmetrisierte Wert dadurch weniger als 100 Jahre bzw. 2500 Jahre beträgt. Es ist daher in der Regel effektiver, möglichst Kanäle ausgeglichener Zuverlässigkeit zu realisieren. Das Resultat dieses Verfahrens ist in jedem Fall, unabhängig

von der Zahl und Ausführung der Kanäle, ein auf einen einzigen Steuerungskanal bezogener $MTTF_D$-Wert, der – über das Teilsystem gemittelt – das Niveau der Bauteilzuverlässigkeit angibt.

8.2.14 Diagnosedeckungsgrad von Test- und Überwachungsmaßnahmen – *DC*

Eine weitere einflussreiche Größe für den PL sind die (Selbst-)Test- und Überwachungsmaßnahmen in Teilsystemen. Durch wirksame Tests lässt sich z. B. eine schlechte Zuverlässigkeit der Komponenten teilweise kompensieren. Die Güte der Fehlererkennung durch Tests wird in DIN EN ISO 13849-1 mit dem sogenannten Diagnosedeckungsgrad (Diagnostic Coverage, *DC*) gemessen. Der *DC* ist definiert als Anteil der erkannten gefahrbringenden Ausfälle von allen möglichen gefahrbringenden Ausfällen, wobei die Bezugsgröße eine Komponente, ein Block oder das gesamte Teilsystem 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 gefahrbringenden erkennbaren Ausfallarten (dangerous detectable, DD) und gefahrbringenden nicht erkennbaren Ausfallarten (dangerous undetectable, DU) bzw. ihr Anteil an der Gesamtausfallrate gefahrbringender Ausfallarten (dangerous, D) bestimmt. Durch Summation und Verhältnisbildung ergibt sich schließlich der *DC*-Wert der entsprechenden Betrachtungseinheit:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{\sum \lambda_{DD}}{\sum \lambda_{D}} \qquad (8.3)$$

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 8.4) 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 Teilsystemen (Kategorie 2) dazu führt, dass ein zweites Abschaltelement vorhanden sein muss. Dieses ist nötig, um den sicheren Zustand einzuleiten bzw. aufrechtzuerhalten, wenn der Test ein Versagen des regulären Abschaltelements (Block „O“ im sicherheitsbezogenen Blockdiagramm) festgestellt hat. Nur bei niedrigem Risiko (bis PL_r = c) und wenn das Einleiten eines sicheren Zustands nicht möglich ist (z. B. durch Verschweißen des Kontakts des finalen Schaltglieds), kann es in Kategorie 2 ausreichen, wenn der Ausgang der Testeinrichtung (OTE) nur eine Warnung bereitstellt.
- Sowohl das Auslösen eines Tests, dessen Ausführung als auch die erforderliche Abschaltung sollten bevorzugt automatisch durchgeführt werden. Nur in Ausnahmefällen und wenn die Risikobeurteilung dies zulässt, ist es akzeptabel, hier auf eine manuelle Intervention, z. B. der Bedienperson einer Maschine, angewiesen zu sein. Denn die Praxis zeigt leider oft, dass die erforderlichen Maßnahmen aus Bequemlichkeit, wegen Arbeitsdrucks oder fehlerhafter Information bzw. Organisation nicht ausreichend umgesetzt werden. Hier ist eine enge Einbindung in den Arbeitsprozess oder ein hoher organisatorischer Aufwand und Disziplin nötig, um manuelle Tests wirksam umzusetzen. Gleichwohl berücksichtigt die Bestimmung des *DC* auch die Fehleraufdeckung bei Anforderung der Sicherheits- oder Teilfunktion, 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 Funktion erfolgen. Für die Fehleraufdeckung bei Anforderung muss die Häufigkeit der Anforderung der Sicherheitsfunktion berücksichtigt werden, um eine ausreichende Testhäufigkeit, wie im nächsten Spiegelstrich beschrieben, zu gewährleisten. Wenn dies technisch umsetzbar ist, sollte im Fall von nicht automatisch initiierten Tests die sicherheitsgerichtete Steuerung dazu genutzt werden, die Durchführung der Tests zu überwachen und sicherzustellen: Wenn in einem vorgesehenen Zeitintervall kein Test durchgeführt wird, sollte zunächst eine Warnung erfolgen. Wenn dann nach einer angemessenen Karenzzeit immer noch kein Test eingeleitet wurde, wird eine sicherheitsgerichtete Reaktion ausgelöst.
- Ein weiterer Aspekt ist die Frage nach der notwendigen Testhäufigkeit. Ein Test, der zu selten ausgeführt wird, wird unter Umständen durch das Eintreten eines Gefährdungsereignisses überholt und bietet damit nur trügerische Sicherheit. Als Faustregel gilt: Die Testhäufigkeit konkurriert immer mit anderen Häufigkeiten,

daher kann eine ausreichende Häufigkeit nicht generell genannt werden. Außerdem dienen Tests nicht nur zur Aufdeckung zufälliger, sondern auch systematischer Ausfälle.
Beim einkanalig getesteten System der Kategorie 2 muss der Test erfolgreich sein, bevor die nächste Anforderung der Sicherheitsfunktion – also eine potenzielle Gefährdung – erfolgt. Hier steht die Testhäufigkeit also in Konkurrenz zur Häufigkeit der Anforderung der Sicherheitsfunktion. In diesem Fall wird ein Faktor von 100 als ausreichend angesehen, also eine mindestens 100-mal höhere Testrate als die mittlere Anforderungsrate der Sicherheitsfunktion. Bis hinunter zu einem Faktor von 25 ergibt sich demgegenüber eine maximale Erhöhung der Ausfallhäufigkeit von ca. 10 % (siehe auch Abschnitt 4 in SISTEMA-Kochbuch 4 [30]. Darunter ist es wesentlich von der Synchronisation von Anforderung und Testung abhängig, ob die Testung überhaupt zur Geltung kommt. Falls in einkanalig getesteten Systemen allerdings der Test gleichzeitig mit der Anforderung der Sicherheitsfunktion so schnell ausgeführt wird, dass der sichere Zustand erreicht wird, bevor es zu einer Gefährdung kommt, dann werden keine Bedingungen an die Testhäufigkeit gestellt. Dies gilt – in Anlehnung an die unten genannten Empfehlungen für die Testhäufigkeit in zweikanaligen Systemen – solange von mindestens einer Anforderung im Jahr ausgegangen werden kann. Ein Spezialfall hiervon ist die kontinuierliche Testung (z. B. analoge Über-/Unterspannungsüberwachung), bei der die Anforderungen an die Testhäufigkeit immer erfüllt sind, wenn der sichere Zustand schnell genug erreicht wird.
In zweikanaligen Systemen der Kategorien 3 und 4 steht die Testhäufigkeit in Konkurrenz zur Häufigkeit des Auftretens eines zweiten gefahrbringenden Ausfalls. Denn erst, wenn der zweite Kanal ausfällt, bevor ein Test den Ausfall des ersten bemerkt hat, besteht die Gefahr der Nichtausführung der Sicherheitsfunktion – Kategorie-4-Systeme tolerieren gemäß Definition sogar die Anhäufung unerkannter Fehler. In der Praxis existieren verschiedene Empfehlungen für die minimal erforderliche Testrate in Kategorie 3 und 4.
In DIN EN 61800-5-2:2017-11 zur Sicherheit elektrischer Leistungsantriebssysteme werden für den Fall, dass die Testung nicht durchgeführt werden kann, ohne den Arbeitszyklus der Maschine zu unterbrechen, und wo keine vertretbare technische Lösung implementiert werden kann, folgende minimale Testhäufigkeiten als akzeptabel angesehen: ein Test pro Jahr für PL d mit Kategorie 3, ein Test pro drei Monate für PL e mit Kategorie 3 und ein Test pro Tag für PL e in Kategorie 4.
In DIN EN ISO 14119 [38] und in einer „Recommendation for Use“ der notifizierten Prüfstellen im Maschinensektor [39] wird für elektromechanische Ausgänge (Relais oder Schütze) ein automatischer oder manueller Test in folgender Häufigkeit gefordert: mindestens einmal pro Monat für PL e mit Kategorie 3 oder 4 und mindestens einmal in zwölf Monaten für PL d mit Kategorie 3. Der Test soll bevorzugt automatisch erfolgen oder das Testintervall soll automatisch überwacht werden und nur im Ausnahmefall durch organisatorische Maßnahmen sichergestellt werden.
Bei den hier genannten Testraten handelt es sich um Minimalanforderungen, die dann gelten, wenn keine häufigeren Tests möglich sind, z. B. weil der Test nur bei Anforderung der Sicherheitsfunktion durchgeführt werden kann (Signalwechsel erforderlich, z. B. bei Elektromechanik oder Fluidtechnik) oder weil dafür eine Unterbrechung des Arbeitszyklus der Maschine nötig ist, z. B. beim Start der Maschine zu Beginn der Schicht. Automatische Tests, die nicht diesen Einschränkungen unterliegen – z. B. Prozessor- oder Speichertests in elektronischen Systemen – können oft ohne großen Aufwand deutlich häufiger realisiert werden. Hier hat sich ein Test mindestens einmal pro Schicht für Kategorie 3 in der Praxis bewährt. In Kategorie 4 wurde schon zu Zeiten der Vorgänger-Norm DIN EN 954-1 eine minimale Testhäufigkeit von einmal je Stunde gewählt.

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

- Die Wirksamkeit einer bestimmten Testmaßnahme, z. B. Fehlererkennung durch den Prozess, kann sehr stark von der Anwendung abhängig sein und durchaus zwischen 0 und 99 % schwanken. Hier ist bei der Auswahl eines der *DC*-Eckwerte besondere Sorgfalt notwendig. Weitere Erläuterungen dazu gibt Anhang E.
- Bei der Bestimmung des DC_{avg}-Wertes für elektromechanische Kontakte ist eine ggf. vorliegende Reihenschaltung von Positionsschaltern zu berücksichtigen. Hier kann es zur Maskierung von Fehlern kommen, sodass der DC_{avg}-Wert und der erreichbare PL reduziert werden müssen. Details hierzu sind im Anhang E zu finden.
- Es kann vorkommen, dass Komponenten oder Blöcke durch mehrere Tests überwacht werden oder dass auf verschiedene Teile unterschiedliche Tests wirken und hieraus ein Gesamt-*DC* für die Komponente oder den Block ermittelt werden muss. Anhang E gibt einige Hilfestellungen zu diesen Fragen.
- Mit der DC_{avg}-Formel (8.4) ist es rechnerisch möglich, Blöcke mit unterschiedlichem *DC* so zusammenzufassen, dass die Mindest-DC_{avg}-Anforderungen für die realisierte Kategorie erfüllt sind, auch wenn einzelne Blöcke einen *DC* unter 60 % oder gar keine Diagnose (*DC* = 0 %) aufweisen. Hier ist im Einzelfall zu prüfen, ob diese Form der Realisierung mit den Anforderungen der Kategorie übereinstimmt. Kategorie 2 fordert einen Mindest-*DC* von „niedrig“ für jeden Block (I, L und O) des Funktionskanals. Kategorie 3 fordert z. B., dass – wenn immer in angemessener Weise durchführbar – ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden muss. Kategorie 4 fordert ebenfalls die Erkennung des einzelnen Fehlers und nur „wenn diese Erkennung nicht möglich ist“, die Ausführung der Teilfunktion auch bei Anhäufung unerkannter Fehler.
- Speziell bei programmierbaren elektronischen Systemen ist eine Vielzahl komplexer Fehler denkbar, sodass auch an die Komplexität der Tests entsprechende Anforderungen gestellt werden. Hier verlangt DIN EN ISO 13849-1, falls mehr als 60 % *DC* für die (programmierbare oder komplexe) Logik gefordert werden, mindestens eine Maßnahme für variante Speicher, invariante Speicher und die Verarbeitungseinheit – soweit vorhanden – mit mindestens je 60 % *DC*.

Sind die *DC*-Werte aller Blöcke schließlich bekannt, wird der DC_{avg}-Wert für das Teilsystem mit der Näherungsformel (8.4) berechnet. Diese gewichtet die einzelnen *DC* mit der zugehörigen $MTTF_D$, denn sehr zuverlässige Teile (mit hoher $MTTF_D$) sind weniger auf wirksame Tests angewiesen als unzuverlässigere Teile (die Summen in Zähler und Nenner werden über N Blöcke des gesamten Systems gebildet):

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}} \quad (8.4)$$

Mit dem DC_{avg}-Wert steht schließlich ein Kennwert bereit, der im Mittel über das gesamte Teilsystem 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 8.3**.

Tabelle 8.3 Die vier Klassen des Diagnosedeckungsgrades im vereinfachten Ansatz der DIN EN ISO 13849-1

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

Bei der anschließenden Weiterverwendung des DC_{avg} in der vereinfachten Quantifizierung durch das Säulendiagramm (siehe Abschnitt 8.2.16) 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 das Teilsystem überdurchschnittlichem *DC* durch eine zuverlässigere Komponente ersetzt wird (nähere Erläuterungen dazu am Ende von Anhang G).

8.2.15 Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF)

Der letzte Parameter, der bei der vereinfachten Quantifizierung der Ausfallhäufigkeit eine Rolle spielt, betrifft Ausfälle infolge einer gemeinsamen Ursache (Common Cause Failure, CCF). Dabei handelt es sich um zusammenhängende gefahrbringende Ausfälle, z. B. in beiden Kanälen eines redundanten Teilsystems, 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 z. B. die beabsichtigte Einfehlertoleranz außer Kraft setzen. Die Relevanz dieser Effekte in einem konkreten System lässt sich nur schwer quantitativ abschätzen (sie-

he auch Anhang F). Im Anhang D der DIN EN 61508-6 [40] wird dazu das sogenannte Beta-Faktor-Modell bemüht. Dieses setzt die Ausfälle infolge gemeinsamer Ursache als β mal λ_D ins Verhältnis zur gefahrbringenden Ausfallrate eines Kanals λ_D. Ohne eine genaue FMEA kann β für reale Teilsysteme 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),
- Verwendung bewährter Bauteile (5 Punkte),
- Ausfalleffektanalyse in der Entwicklung zur Aufdeckung potenzieller Ausfälle infolge gemeinsamer Ursache (5 Punkte),
- Schulung des Entwicklungspersonals hinsichtlich CCF und ihrer Vermeidung (5 Punkte),
- Schutz vor durch Verunreinigung (mechanische und fluidische Systeme) bzw. elektromagnetische Beeinflussung (elektrische Systeme) ausgelösten Ausfällen infolge gemeinsamer Ursache (25 Punkte),
- Schutz vor durch ungünstige Umgebungsbedingungen ausgelösten Ausfällen infolge gemeinsamer Ursache (10 Punkte).

Die für eine Gegenmaßnahme genannten Punkte sollen nur vollständig oder gar nicht vergeben werden. Eine „teilweise Umsetzung“ der Gegenmaßnahmen wird nicht durch Punkte belohnt. Allerdings können teilsystemweise unterschiedliche Maßnahmenbündel gegen CCF wirken. Wichtig ist auch, dass die Bewertung der Gegenmaßnahmen mit Blick auf die spezielle Anwendung und die dort relevanten Ursachen für CCF erfolgt. Wenn die Schutzmaßnahmen, z. B. hinsichtlich Überbelastung oder elektromagnetischer Beeinflussung, nicht auf Bauteilebene umgesetzt werden, so kann dieser Schutz durch externe Schutzeinrichtungen wie Schutzelemente, Filter oder Abschirmung erreicht werden. Diese Möglichkeit zum Erreichen eines akzeptablen Schutzniveaus für funktionale Sicherheit auf Systemebene ist besonders bei der Verwendung von Standardkomponenten, die nicht primär für sicherheitsbezogene Funktionen entwickelt wurden, hilfreich. Werden alle acht Gegenmaßnahmen erfüllt, ergibt sich eine maximale Summe von 100 Punkten. Allerdings fordert DIN EN ISO 13849-1 nur eine Mindestsumme von 65 Punkten – und dies auch nur für Teilsysteme in den Kategorien 2, 3 und 4. Bei Systemen der Kategorie 2 geht es darum, gefährliche Ausfälle in Test- und Funktionskanal durch gemeinsame Ursachen, die ein unerkanntes Auftreten eines gefährlichen Fehlers bewirken können, zu vermeiden. Bei der Erstellung des Säulendiagramms zur vereinfachten Quantifizierung wurden die 65 Punkte mit einem Beta-Faktor von 2 % gleichgesetzt. Hier wurde die Vergröberung gegenüber den fünf Kategorien und drei bzw. vier $MTTF_D$- und DC_{avg}-Klassen noch weiter forciert und auf eine simple Ja/Nein-Entscheidung reduziert. Während die Vorteile einer redundanten Struktur schon bei einem Beta-Faktor ab 10 % fast vollständig zunichte gemacht werden, minimiert ein Beta-Faktor von höchstens 2 % die Relevanz von Ausfällen infolge gemeinsamer Ursache auf ein vertretbares Maß.

8.2.16 Vereinfachte PL-Bestimmung durch das Säulendiagramm

Nachdem die vier wesentlichen quantitativen Parameter zur Ermittlung der Ausfallhäufigkeit bestimmt wurden (siehe Abbildung 8.1), ist es trotzdem keine einfache Aufgabe, hieraus den für das Teilsystem erreichten PL zu ermitteln. Obwohl dafür 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 (**Abbildung 8.7**).

Dieses Diagramm wurde auf der Grundlage der vorgesehenen Architekturen für die Kategorien durch Markov-Modellierung ermittelt. Weitere Erläuterungen dazu gibt Anhang G. Bei Anwendung des Säulendiagramms wird zunächst durch die erreichte Kategorie – dabei müssen für die Kategorien 2, 3 und 4 ausreichende Maßnahmen gegen CCF getroffen werden – in Kombination mit der erreichten DC_{avg}-Klasse auf der horizontalen Achse die relevante Säule bestimmt. Die Höhe der vom Teilsystem 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 mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde *PFH*, so helfen die Tabellen in Anhang K der Norm weiter. Ähnliches leistet auch die IFA Software SISTEMA (siehe Anhang H), die das Säulendiagramm quantitativ auswertet, und die handliche PLC-Drehscheibe des IFA (siehe Abbildung 8.12).

Bei der Ableitung des Säulendiagramms wurden nicht nur vorgesehene Architekturen und die an die Kategorien geknüpften Bedingungen berücksichtigt, sondern auch folgende Annahme vorausgesetzt, die bei dessen Anwendung beachtet werden muss:

- Als Gebrauchsdauer des Teilsystems werden 20 Jahre unterstellt, innerhalb derer die Bauteilzuverlässigkeiten durch konstante Ausfallraten beschrieben oder angenähert werden können. Durch Verwendung stark verschleißbehafteter Bauteile (siehe T_{10D}-Wert in Anhang D) oder aus anderen Gründen kann die tatsächliche Gebrauchsdauer die angenommenen 20 Jahre unterschreiten. Dann ist durch vorsorglichen Austausch der betroffenen Bauteile oder der betroffenen Teilsysteme die Anwendung des Säulendiagramms zu rechtfer-

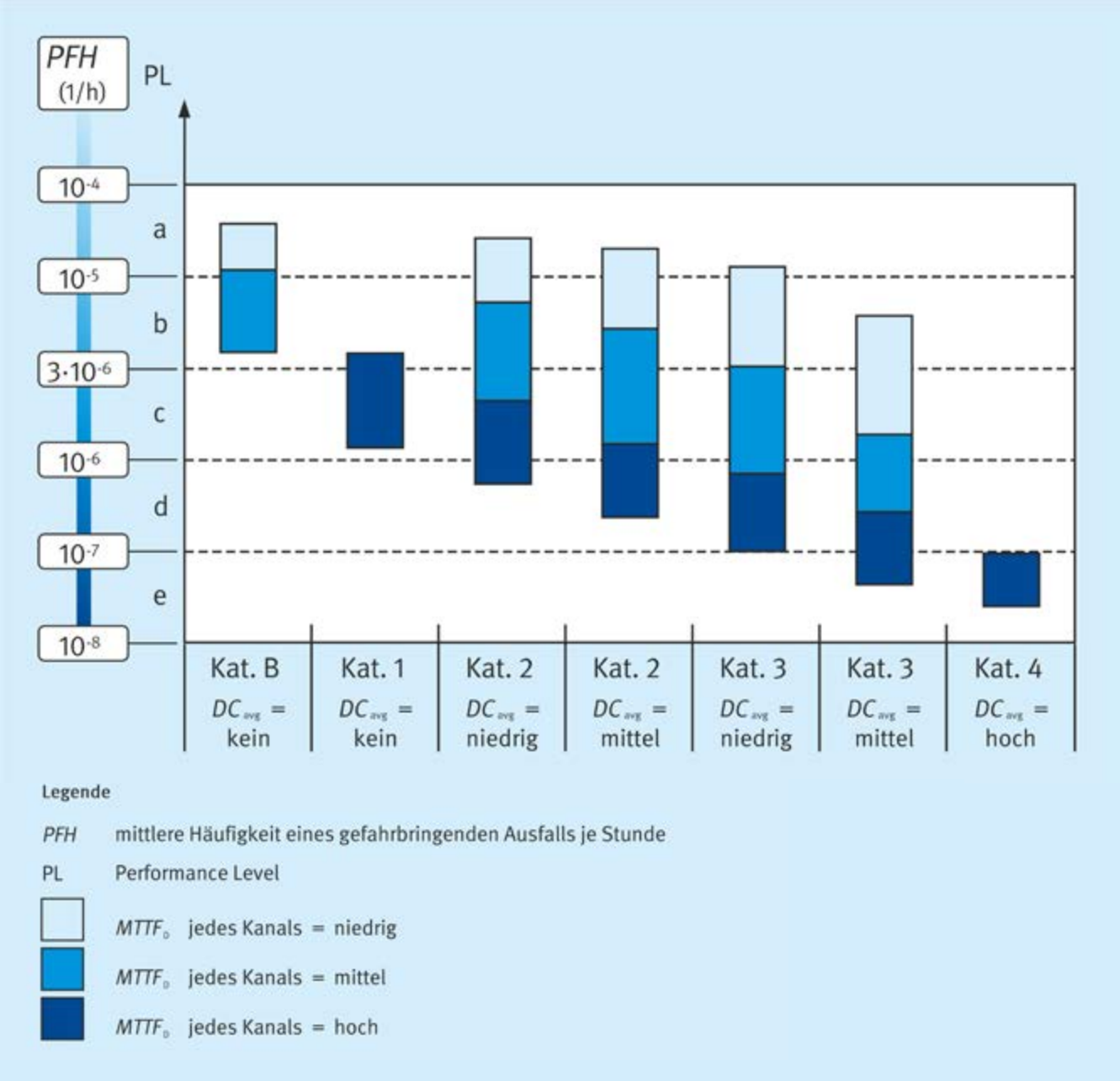


Abb. 8.7 Säulendiagramm zur vereinfachten PL-Bestimmung aus der Kategorie (Kat., inklusive Maßnahmen gegen CCF), dem DC_{avg} und der $MTTF_D$

tigen. Den Anwendenden sind diese Informationen in geeigneter Form mitzuteilen, z. B. über die Benutzerinformationen und durch Kennzeichnung auf den Teilsystemen. Soll die Gebrauchsdauer von vorneherein mehr als 20 Jahre betragen oder nachträglich über 20 Jahre hinaus verlängert werden, ergeben sich Abweichungen vom Säulendiagramm. In Anhang G ist dargestellt, wie damit umgegangen werden kann.

Durch die Begrenzung der anrechenbaren $MTTF_D$ jedes Kanals auf 100 Jahre – bei Kategorie 4 sind es 2500 Jahre – kann ein hoher PL nur mit bestimmten Kategorien erreicht werden. Obwohl dies mit dem vereinfachten Ansatz der vorgesehenen Architekturen und des Säulendiagramms zusammenhängt, gelten die damit verbundenen Einschränkungen auch bei einer unabhängigen Bestimmung der mittleren Häufigkeit eines gefahrbringenden 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.

Zusätzlich zum quantitativen Aspekt der Ausfallhäufigkeit müssen zum Erreichen eines bestimmten PL aber auch qualitative Aspekte beachtet werden. Zu diesen gehören systematische Ausfälle (siehe Abschnitt 8.1.1) und Softwarefehler, auf die in Kapitel 9 näher eingegangen wird.

8.2.17 Alternative PL-Bestimmung ohne $MTTF_D$

Als Reaktion auf Forderungen aus der praktischen Anwendung wurde in der dritten Ausgabe der Norm ein alternatives einfaches Verfahren zur Bestimmung der *PFH* und quantifizierbarer Aspekte des PL aufgenommen. Mit der vierten Normausgabe erfolgte eine Erweiterung des ursprünglich nur für den Ausgangsteil des SRP/CS beschriebenen Verfahrens auch auf den Eingangs- und Logikteil. Dieses alternative Verfahren ist allerdings nur in bestimmten Fällen anwendbar:

- wenn für mechanische, (elektro-)hydraulische oder (elektro-)pneumatische Bauteile (oder Bauteile gemischter Technologie, z. B. mechanische Bremsen mit pneumatischer Ansteuerung) keine Zuverlässigkeitsdaten ($MTTF_D$, Ausfallrate λ_D, B_{10D} o. ä.) verfügbar sind,
- wenn das „Verfahren guter ingenieurmäßiger Praxis“ (siehe Anhang D) nicht angewendet werden kann.

Die Vereinfachung der *PFH*-Bestimmung zielt hier hauptsächlich auf die realisierte Kategorie inklusive DC_{avg} und CCF. Eine Berechnung der (Kanal-)$MTTF_D$ entfällt, dafür müssen im Eingangs- und Ausgangsteil des SRP/CS durchgängig bewährte Bauteile (in Kategorien 1, 2, 3 und 4) verwendet werden. Der in der dritten Normausgabe erwähnte Einsatz betriebsbewährter Bauteile ist in der vierten Normausgabe wieder entfallen.

Tabelle 8.4 stellt in Anlehnung an Tabelle 8 der Norm – abhängig von der realisierten Kategorie und unter den an das Verfahren geknüpften Zusatzbedingungen – den abschätzbaren *PFH*-Wert und den damit erreichbaren PL für den Eingangs- und Ausgangsteil des SRP/CS dar.

Für den Logikteil des SRP/CS gilt innerhalb des alternativen Verfahrens ein anderer Ansatz als in Tabelle 8.4 dargestellt:

- In den Kategorien B, 2 und 3 kann für die $MTTF_D$ jedes Kanals pauschal ein Wert von zehn Jahren angesetzt werden.
- In Kategorie 1 kann für die $MTTF_D$ jedes Kanals pauschal ein Wert von 30 Jahren angesetzt werden, da Kategorie 1 die durchgehende Verwendung bewährter Bauteile voraussetzt.
- Kategorie 4 ist ausgeschlossen.

Durch die konservative Wahl der $MTTF_D$-Werte jedes Kanals kann im Logikteil maximal ein PL = c erreicht werden.

Folgende Zusatzbedingungen sind an das alternative Verfahren unabhängig vom Eingangs-, Logik- oder Ausgangsteil des SRP/CS geknüpft:

- Alle Anforderungen an die jeweilige Kategorie, außer denjenigen, die sich auf $MTTF_D$ beziehen, sind zu erfüllen.
- Gleichermaßen sind darüber hinaus alle Anforderungen für nicht quantifizierbare Aspekte wie systematische Ausfälle und Software zu erfüllen.
- Da die geschätzten *PFH*-Werte auf dem vereinfachten Verfahren zur Abschätzung eines PL (Säulendiagramm) beruhen, gelten dafür auch dieselben Voraussetzungen wie für die vorgesehenen Architekturen. Es werden also eine Gebrauchsdauer von 20 Jahren und konstante Ausfallraten innerhalb der Gebrauchsdauer unterstellt.
- Da die Basis für eine Ermittlung des T_{10D}-Wertes fehlt, wird dafür als konservative Schätzung ein Wert von zehn Jahren angenommen – für bewährte Bauteile sind auch 20 Jahre akzeptabel.
- Die Ermittlung von DC_{avg} gemäß Gleichung (8.4) reduziert sich mangels vorliegender $MTTF_D$-Werte auf den arithmetischen *DC*-Mittelwert über alle Blöcke des Teilsystems.

Tabelle 8.4 Alternative PL- und *PFH*-Bestimmung ohne $MTTF_D$ für den Eingangs- und Ausgangsteil des SRP/CS basierend auf Kategorie, DC_{avg} und der Verwendung bewährter Bauteile.

Kategorie	Zusätzliche Anforderungen		Abgeschätzte PFH_D in 1/h	Erreichbarer PL
B		⇢	$5{,}0 \cdot 10^{-6}$	PL b
1		⇢	$1{,}7 \cdot 10^{-6}$	PL c
2	ausschließlich bewährte Bauteile verwendet	⇢	$1{,}7 \cdot 10^{-6}$	PL c
3	ausschließlich bewährte Bauteile verwendet	⇢	$2{,}9 \cdot 10^{-7}$	PL d
4	ausschließlich bewährte Bauteile verwendet	⇢	$4{,}7 \cdot 10^{-8}$	PL e

Alle Anforderungen für die jeweilige Kategorie müssen erfüllt sein, außer die $MTTF_D$.

Der erreichbare PL deckt nur die quantifizierbaren Aspekte (zur Ermittlung der *PFH*) ab. Die zusätzlich geltenden Anforderungen für nicht quantifizierbare Aspekte wie systematischer Ausfall und Software müssen darüber hinaus erfüllt sein.

8.2.18 Bussysteme als „Verbindungsmittel“

Die einzelnen Blöcke Eingabeeinheit, Logik und Ausgabeeinheit einer vorgesehenen Architektur müssen nicht nur logisch, sondern auch physikalisch miteinander verbunden werden. Dazu definiert die Norm Verbindungsmittel, die als Teil der Teilsysteme betrachtet werden. Der Name Verbindungsmittel erscheint fachlich zunächst aus der Sicht der Elektro- oder Fluidtechnik merkwürdig, ist aber der Oberbegriff für elektrische sowie fluidtechnische Leitungen und sogar für mechanische Stößel usw. Somit gelten alle Anforderungen der Norm auch für diese „Verbindungsmittel“. Unter dem Aspekt der Fehlerbetrachtung ist also z. B. ein Leitungskurzschluss an einer Verbindungsstelle 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) [41] und die Norm DIN EN IEC 61784-3 [42] zu diesem Thema gibt. Bussysteme, die den in diesen Publikationen beschriebenen Anforderungen genügen, lassen sich ohne Weiteres auch unter dem Dach der DIN EN ISO 13849-1 einsetzen. Auf dem Markt gibt es eine größere Anzahl von Bussystemen, die für den sicherheitstechnischen Einsatz geeignet sind.

Die oben erwähnten Publikationen konzentrieren sich auf den Einsatz von feldbusbasierten, funktional sicheren Kommunikationssystemen basierend auf dem Prinzip des sogenannten Black Channels, d. h. an den Übertragungskanal des Feldbusses selbst werden keine speziellen Anforderungen zur sicherheitstechnischen Ertüchtigung gestellt.

Bei der Verwendung dieser Feldbusstrukturen müssen sämtliche notwendigen Maßnahmen zur Einrichtung einer sicheren Datenübertragung in Übereinstimmung mit den Anforderungen der DIN EN 61508 in einer zusätzlichen Sicherheitskommunikationsschicht (safety layer) ausgeführt werden.

Die Sicherheitskommunikationsschicht verfügt über passende Dienste und ein Protokoll, um sicherheitsrelevante Daten in ein Sicherheitstelegramm zu codieren und diese an den Black Channel weiterzugeben bzw. umgekehrt ein Sicherheitstelegramm vom Black Channel zu empfangen und die sicherheitsrelevanten Daten zu extrahieren.

Das in der Sicherheitskommunikationsschicht zu implementierende Protokoll muss dabei fehlererkennende Maßnahmen zur Beherrschung der möglichen Kommunikationsfehler Wiederholung, Verlust, Einfügung, falsche Reihenfolge, Verfälschung, Verzögerung, Maskerade und Adressierung berücksichtigen. Geeignete fehlererkennende Maßnahmen sind z. B. eine laufende Nummer, Zeitstempel, Zeiterwartung, Rückmeldung, Verbindungsauthentifizierung und Datensicherung.

Gerade die Betrachtung der Datensicherung ist oft mit komplexen Berechnungen verbunden. Ziel dieser Betrachtungen ist es, die Restfehlerwahrscheinlichkeit R und die daraus abgeleitete Gesamt-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 mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde (*PFH*) als Anteil für die Übertragung sicherheitsrelevanter Nachrichten einrechnen.

Bei der Abschätzung der Gesamt-Restfehlerrate Λ einer sicheren Datenübertragung sind die folgenden grundsätzlichen Sicherheitseigenschaften der sicherheitsrelevanten Nachrichten zu berücksichtigen:

- Datenintegrität: die korrekte Übermittlung des Nachrichteninhalts von einer Nachrichtenquelle zu einer oder mehreren zugeordneten Nachrichtensenke(n),
- Authentifizierung: die Nachrichtenübermittlung von einer korrekten Nachrichtenquelle zu einer oder mehreren zugeordneten Nachrichtensenke(n),
- Aktualität: die rechtzeitige Nachrichtenübermittlung von einer Nachrichtenquelle zu einer Nachrichtensenke innerhalb eines konfigurierten Zeitfensters.

Beide oben genannten Publikationen (GS-ET-26 und DIN EN IEC 61784-3) begrenzen den Wert der Restfehlerrate auf 1 % des maximal zulässigen *PFH*-Wertes. 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 Abbildung 3.2). Durch die 1 %-Regel ist der Beitrag zur *PFH* quasi vernachlässigbar bzw. kann den für die Teilsysteme ermittelten *PFH*-Werten hinzugerechnet werden. Umfassende Informationen zu Bussystemen für die Übertragung sicherheitsrelevanter Informationen gibt z. B. [43].

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

Kommt keines der bekannten, bereits beurteilten Profile für funktionale Sicherheit zum Einsatz, gilt es, die oben genannten Fehlerannahmen zu Übertragungsfehlern zu berücksichtigen, entsprechende (Gegen-)Maßnahmen zu implementieren und die Gesamt-Restfehlerrate Λ unter Berücksichtigung der typischen Bitfehlerwahrscheinlichkeit von 0,01 bei der Berechnung der *PFH* zu berücksichtigen. DIN EN IEC 61784-3 gibt Hinweise zur Berechnung der Gesamt-Restfehlerrate Λ.

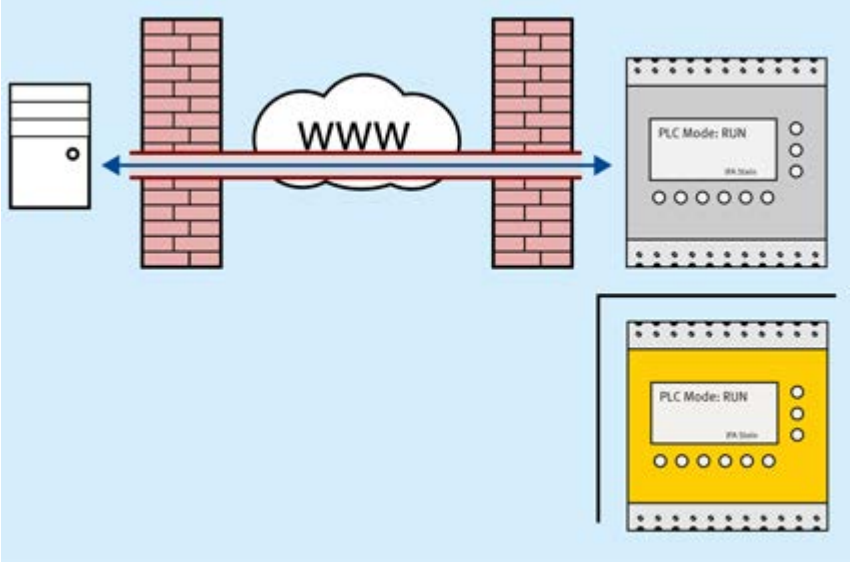


Abb. 8.8
Das SRP/CS wurde hier rückwirkungsfrei von der Maschinensteuerung mit Fernzugriffsmöglichkeit getrennt. Somit können Produktionsdaten ausgelesen und Rezepte angepasst werden, ohne dass der Fernzugriff auf die Funktion der SRP/CS wirken kann. Die Verbindung zwischen der Maschinensteuerung mit Fernzugriffsmöglichkeit und dem System in der Ferne wird über einen sicheren Tunnel gegen Datenverfälschungen geschützt.

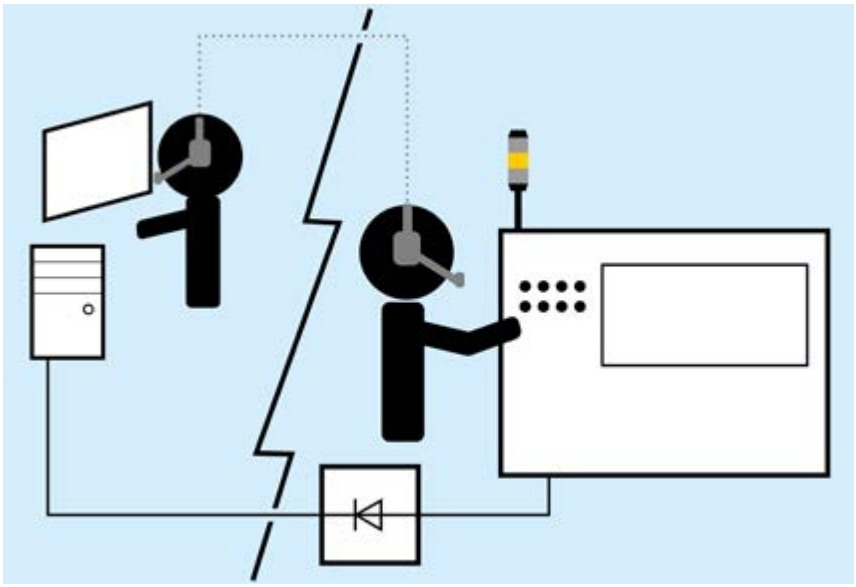


Abb. 8.9
Rückwirkungsfreier Fernzugriff mittels einer Datendiode kann eine sichere passive Fernwartung ermöglichen.

8.2.19 Remotezugang und Security-Hinweise

Der Fernzugriff auf das SRP/CS wird in der DIN EN ISO 13849-1 im Abschnitt 5.2.4 normativ erfasst. Falls eine Maschine für den Fernzugriff vorbereitet wurde, muss die Sicherheitssteuerung auch während des Fernzugriffs uneingeschränkt weiter funktionieren, wenn keine alternativen risikomindernden Maßnahmen in den Benutzerinformationen angegeben sind.

Typischerweise wird dies durch eine rückwirkungsfreie Trennung der SRP/CS von der Maschinensteuerung mit Fernzugriffsmöglichkeit wie in **Abbildung 8.8** dargestellt erreicht.

In vielen Fällen genügt es, beim Fernzugriff lediglich Produktionsdaten und Wartungsparameter einzuholen. Dazu ist es möglich, die Rückwirkungsfreiheit mit einer Datendiode sicherzustellen (**Abbildung 8.9**). Die Daten können dann etwa in einem verbindungslosem Protokoll kontinuierlich gesendet werden und werden in der Ferne von einem passenden System zur Analyse empfangen und ausgewertet. Damit ist dann auch eine passive Fernwartung möglich, bei der das Instandhaltungspersonal vor Ort die volle Kontrolle über die Maschine behält, während das Instandhaltungspersonal in der Ferne berät und über alle relevanten Daten verfügt.

Bei der Bereitstellung von Fernzugriffsmöglichkeiten stellen europäische Verordnungen weitgehende Forderungen, auf die im Anhang O verwiesen wird.

Bereits beim Entwurf der SRC/CS muss sichergestellt werden, dass keine gefährlichen Situationen entstehen können, wenn Personen unbemerkt während des Fernzugriffs im Innern oder in der Nähe der Maschine anwesend sind. Die Anwesenheit von Personen kann etwa mit Trittmatten, Laserlichtgittern oder Laserscannern überwacht werden. Beim Design der Maschine kann jedoch auch konstruktiv verhindert werden, dass sich Personen in bestimmten Bereichen aufhalten können.

8.3 Softwarebasierte Parametrierung

Um Teilsysteme individuell einsetzten zu können, werden diese von Herstellern wenn möglich programmierbar oder parametrierbar gestaltet. Ein bekanntes Beispiel sind Laserscanner, bei denen neben der Schutzfeldreichweite und Ansprechzeit oft noch viele andere Parameter eingestellt werden können. Bei einfachen Parametern könnte ein Anwender durch einen simplen Funktionstest noch überprüfen, ob der Parameter richtig gesetzt ist, aber eine komplexe Schutzfeldgeometrie wäre nur mit entsprechendem Aufwand verifizierbar. Wie aber ist sichergestellt, dass die Parametrierung eines Gerätes zuverlässig erfolgt? Neben technischen Fehlern bei der Parametrierung kann es zu unbeabsichtigten Fehleingaben oder gar nicht autorisierten Zugriffen kommen.

Hierzu listet DIN EN ISO 13849-1 im Abschnitt 6.3 Anforderungen an eine softwarebasierte Parametrierung sicherheitsbezogener Parameter auf. Diese sind nun bewusst vom übrigen Softwareteil der Norm gelöst. Außerdem wird betont, dass es nur um manuelle, softwarebasierte Parametrierung durch autorisierte Personen geht. Darunter fällt Parametrierung durch speziell qualifizierte Parametrierwerkzeuge (was sich in der Regel nur auf die Software bezieht), aber keine automatisierte Parametrierung oder direkte Steuerung einer Maschine durch eine Bedienperson, z. B. die Geschwindigkeitsregelung eines Gabelstaplers. Auch eine rein hardwarebasierte Parametrierung, beispielsweise durch DIP-Schalter (Dual In-Line Package), ist hier nicht gemeint.

Neu sind zusätzliche Informationen zu möglichen Einflüssen, die zu einer fehlerhaften Parametrierung führen könnten. Dazu zählen zum Beispiel Software- und Hardwarefehler des Parametrierwerkzeugs, Störungen während der Datenübertragung oder fehlerhafte Abspeicherung im sicherheitsbezogenen Gerät, aber auch falsche Eingaben durch den Anwender. Als Anforderungen zählt die Norm dann auf, u. a. die Integrität aller für die Parametrierung verwendeten Daten aufrechtzuerhalten. Dafür wird in der Praxis z. B. ein Handshakeverfahren verwendet: Bevor neue Daten im sicherheitsbezogenen Gerät aktiv gesetzt werden können, müssen diese dem Anwender zurückgespiegelt und von ihm bestätigt werden. Diese Maßnahmen, einhergehend mit einem Schutz gegen unbefugte Änderungen, muss der Hersteller oder Lieferant eines sicherheitsbezogenen Gerätes umsetzen. An den Anwender (das kann der Maschinenbauer oder auch das Wartungspersonal im Betrieb sein) richten sich dann die Anforderungen zur Dokumentation der Parametrierung. Hierbei wird er in der Regel von den Werkzeugen unterstützt.

8.4 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, das bereits in Abschnitt 6.8 begonnen wurde, gleichzeitig eine Brücke zu Kapitel 11, in dem eine große Anzahl von Schaltungsbeispielen verschiedener PL, verschiedener Kategorien und unterschiedlicher Technologie präsentiert wird.

Die im Folgenden separat dargestellten Textkästen entsprechen der Kurzbeschreibung im Stil von Kapitel 11. Darüber hinaus werden zusätzliche Erläuterungen gegeben, deren Erwähnung bei jedem Schaltungsbeispiel in Kapitel 11 den Rahmen sprengen würde.

8.4.1 Sicherheitsfunktionen

Das Steuerungsbeispiel einer Planschneidemaschine in Abschnitt 6.8 wird hier wieder aufgegriffen. Von den in 6.8.3 beschriebenen sechs Sicherheitsfunktionen wird exemplarisch die Realisierung von SF2 beschrieben, für die ein erforderlicher 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 [29] für die Absicherung an der Bedienseite zusätzlich zu einer Zweihandschaltung (ZHS), z. B. im Hinblick auf die Sicherheitsfunktion SF3, eine – hier nicht gezeigte – berührungslos wirkende Schutzeinrichtung (BWS).

Sicherheitsfunktion (SF2)

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

8.4.2 Realisierung

Realisiert als Zweihandschaltung lässt sich diese Sicherheitsfunktion folgendermaßen beschreiben: Beim Loslassen mindestens eines der beiden Stellteile S1 oder 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 so lange 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 siehe DIN EN ISO 13851, z. B. Anforderungen für den Typ IIIC und zur Manipulationssicherheit). 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 6 (siehe Abschnitt 6.3.2) enthält die Sicherheitsfunktion beide Aktoren – Pressbalken und Messer –, da sie sich an derselben Gefahrenstelle befinden. **Abbildung 8.10** zeigt in einem elektrohydraulischen Prinzipschaltbild, wie die sicherheitsrelevanten Steuerungsteile konkret realisiert werden. Die hier, wie auch im Kapitel 11, gewählte Darstellung als Prinzipschaltbild 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, elektromagnetische Störfestigkeit) 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 solches Prinzipschaltbild keine direkte Vorlage zum Nachbau ist, sondern die sicherheitstechnische Struktur illustrieren soll.

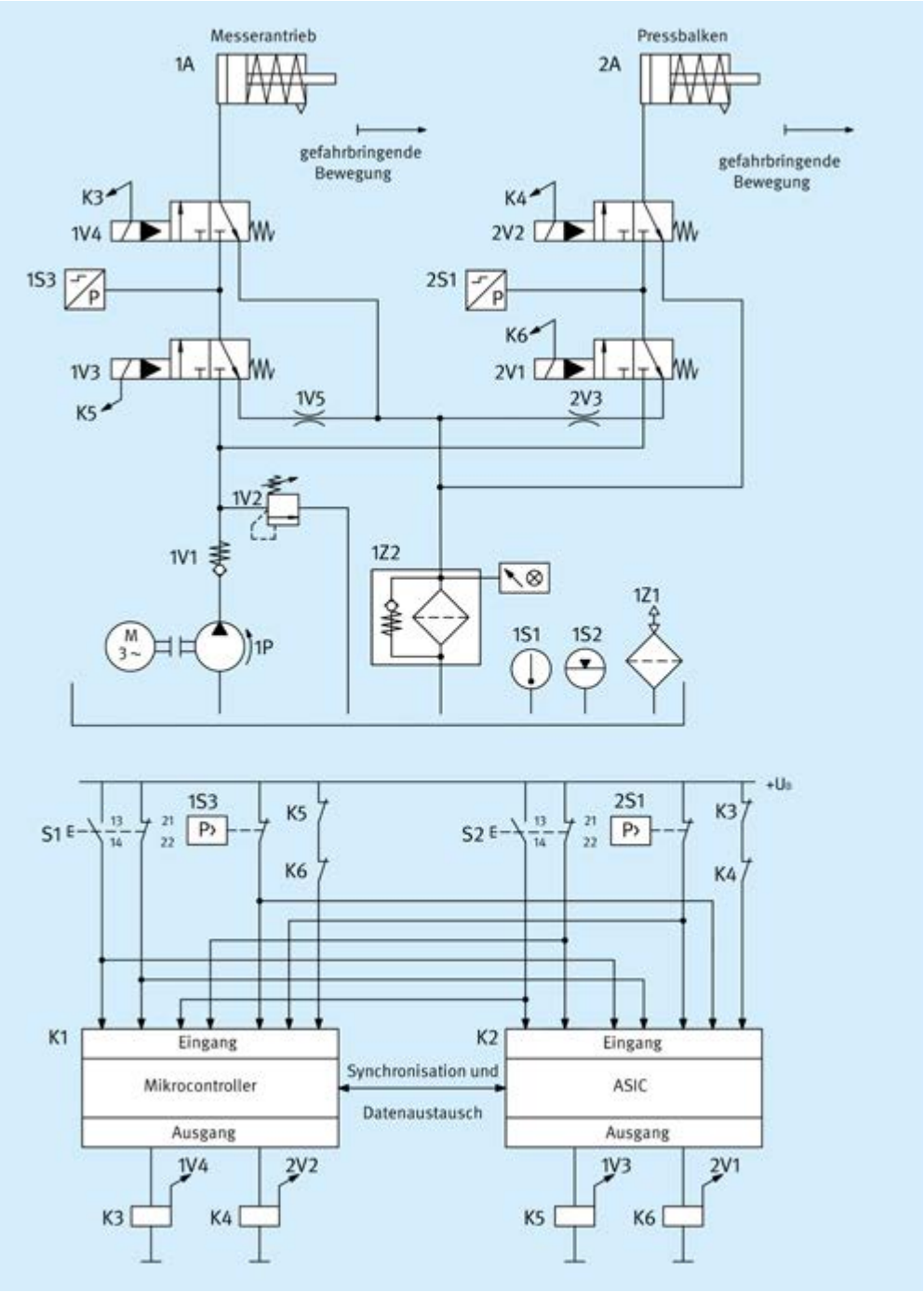


Abb. 8.10
Prinzipschaltbild der elektrischen und hydraulischen Ansteuerung eines Messerantriebs und eines Pressbalkens (wesentliche Bauelemente)

8.4.3 Funktionsbeschreibung

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

Zur Bewertung der sicherheitsbezogenen Zuverlässigkeit sind für die verwendeten Bauteile und ihre Verschaltung gegebenenfalls zusätzlich konstruktive Merkmale zu beachten. Diese werden in Abschnitt 10.10.2. unter dem Aspekt des Validierens der sicherheitsbezogenen Anforderungen genauer betrachtet.

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 Betätigen der Stellteile S1 und S2 werden die ansteigenden Flanken der Signale beider Verarbeitungskanälen K1 (Mikrocontroller) und K2 (ASIC) zugeführt. Erfüllen diese Signale die Anforderungen an die Gleichzeitigkeit (500 ms) nach der relevanten Norm DIN EN ISO 13851, 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. Es 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.

8.4.4 Sicherheitsbezogenes Blockdiagramm

Die Schaltungsbeschreibung in Verbindung mit dem Schaltplan und ggf. weiteren beschreibenden Dokumenten, wie der ausführlichen Spezifikation der Sicherheitsanforderungen (SRS), ermöglicht die Bestimmung einer Steuerungskategorie und die Abbildung der realen Schaltung auf ein abstrahiertes sicherheitsbezogenes Blockdiagramm (siehe **Abbildung 8.11**). In diesem Beispiel wird sehr schnell deutlich, dass die Sicherheitsfunktion in einem einzigen durchgehenden Teilsystem zweikanalig ausgeführt wird. Daher kommt Kategorie 3 oder 4 in Betracht. Wegen der hochwertigen Diagnosemaßnahmen, die auch Fehlerkombinationen beherrschbar machen, liegt Kategorie 4 nahe. Der konkrete Nachweis hierzu erfolgt als Verifikationsschritt in Kapitel 10, ebenso wie die Überprüfung der quantitativen Anforderungen an $MTTF_D$, DC_{avg} und CCF (siehe unten). Bei der Umsetzung in das sicherheitsbezogene Blockdiagramm sind die Erläuterungen in den Abschnitten 8.2.8 und 8.2.9 hilfreich. Es hat sich bewährt, dazu den Signalpfad, beginnend von 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. Das SISTEMA-Kochbuch 1 [37] erläutert diesen Schritt „Vom Schaltbild zum Performance Level“ genauer. In diesem Beispiel ist zu beachten, dass die Stellteile S1 und S2 zueinander nicht redundant sind, auch wenn dies auf den ersten Blick so erscheinen mag, denn jeder Taster schützt unabhängig eine Hand der Bedienperson. Die Redundanz beginnt vielmehr in jedem Taster durch Verwendung von elektrischen Öffner-Schließer-Kombinationen. Jeder Steuerungskanal überwacht beide Hände bzw. Stellteile durch Auswertung mindestens je eines elektrischen Schaltkontakts. Im sicherheitsbezogenen Blockschaltbild ist daher in jedem Kanal ein Schließerkontakt, z. B. S1/13-14, und ein Öffnerkontakt, z. B. S2/21-22, enthalten. Das sicherheitsgerichtete Blockdiagramm ist in Abbildung 8.11 dargestellt und unterscheidet sich hier deutlich vom funktionalen Schaltplan.

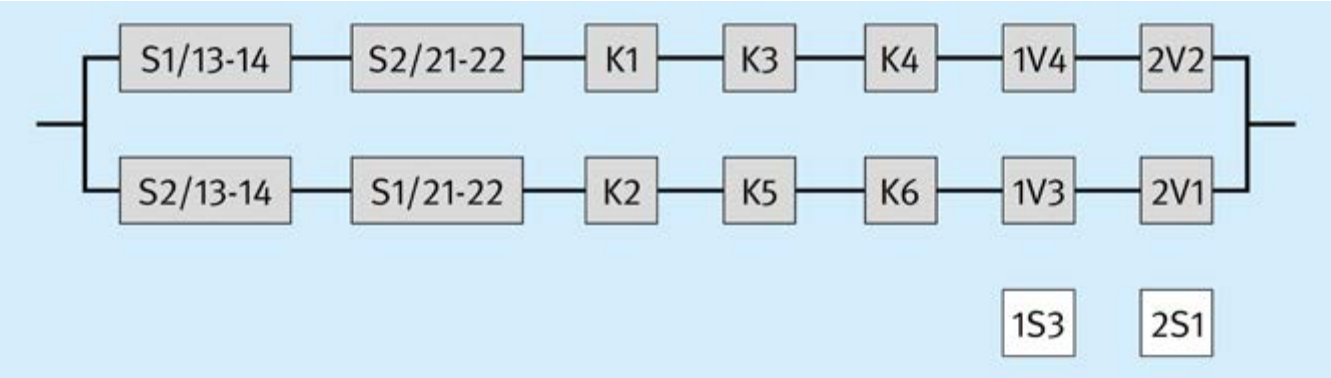


Abb. 8.11 Sicherheitsbezogenes Blockdiagramm zum SRP/CS für die ausgewählte Sicherheitsfunktion SF2 an der Planschneidemaschine

Aus der konkreten Realisierung der Sicherheitsfunktion ergeben sich unter Umständen Einschränkungen oder Empfehlungen für die Anwendung. Beispielsweise 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)

8.4.5 Eingangsgrößen zur quantitativen Bewertung des erreichten PL

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

Um die $MTTF_D$-Ermittlung zu erläutern, sei zunächst der Block „K1" vorgestellt: Obwohl das Prinzipschaltbild (siehe Abbildung 8.10) 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, elektromagnetischen Störfestigkeit oder zum 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 232) 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 8.5** gezeigt wird (Abbildung B.3 auf Seite 233 zeigt im Vergleich das Vorgehen bei einer Ausfalleffektanalyse).

Berechnung der Ausfallhäufigkeit

- ***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 eine $MTTF_D$ von 232 Jahren. Für den Mikrocontroller allein wird eine $MTTF_D$ von 1142 Jahren ermittelt. Der gleiche Wert wird auch für den ASIC eingesetzt. Zusammen mit der zugehörigen Beschaltung ergibt sich für die Blöcke K1 und K2 jeweils eine $MTTF_D$ von 806 Jahren. Für die Hydraulikventile 1V3, 1V4, 2V1 und 2V2 gibt der Hersteller eine $MTTF_D$ von jeweils 150 Jahren an. Diese Werte ergeben eine $MTTF_D$ jedes Kanals von 31,4 Jahren („hoch").
- ***DC*$_{avg}$:** Nach DIN EN ISO 13849-1, Anhang E, ergeben sich als *DC*-Werte für S1/S2: 99 % (Kreuzvergleich von Eingangssignalen ohne dynamischen Test mit häufigem Signalwechsel), für K1/K2: 90 % (Selbsttest durch Software und Kreuzvergleich), für K3 bis K6: 99 % (direkte Überwachung über zwangsgeführte Kontakte), für 1V3/2V1: 99 % (indirekte Überwachung durch den Druckschalter) und für 1V4/2V2: 99 % (indirekte Überwachung durch die Funktion und Messung einer geänderten Druckabfallzeit). Diese Werte ergeben einen DC_{avg} von 98,6 % (im Toleranzbereich von „hoch").
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL:** Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_D$ des Kanals (31,4 Jahre) und DC_{avg} = 98,6 %, im Toleranzbereich von „hoch". Damit ergibt sich eine *PFH* von $9{,}7 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Tabelle 8.5 „Parts Count"-Verfahren für den „Mikrocontroller"-Block K1, basierend auf Ausfallraten λ, die der Datensammlung SN 29500 [44] entnommen wurden (angegeben in FIT, d. h. 10^{-9}/h)

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

Die in der zweiten Spalte genannten Ausfallraten der Elemente wurden mithilfe der Datensammlung SN 29500 ermittelt. Die Validierung wird in der Fortsetzung dieses Beispiels in Abschnitt 10.6 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 Herstellerdaten verwendet. Da Zuverlässigkeitsdaten nur für S1/S2 insgesamt (Betätigungsmechanik plus Öffnerkontakt und Schließerkontakt) verfügbar sind, können diese Werte als Abschätzung zur sicheren Seite für jeden der Kanäle verwendet werden, obwohl in jeden Kanal neben der Betätigungsmechanik nur die Schließerkontakte (z. B. S1/13-14) oder die Öffnerkontakte (z. B. S2/21-22) eingehen. Die angenommenen B_{10D}-Werte werden mit den aus Anhang D bekannten Formeln in $MTTF_D$-Werte umgerechnet:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{Zyklus}} \cdot 3\,600\,\frac{s}{h} = \frac{240\ \text{Tage/Jahr} \cdot 8\ \text{h/Tag}}{80\ \text{s/Zyklus}} \cdot 3\,600\,\frac{s}{h} = 86\,400\,\frac{\text{Zyklen}}{\text{Jahr}} \tag{8.5}$$

$$MTTF_D = \frac{B_{10D}}{0{,}1 \cdot n_{op}} = \frac{2\,000\,000\ \text{Zyklen}}{0{,}1 \cdot 86\,400\ \text{Zyklen/Jahr}} = 231{,}5\ \text{Jahre} \tag{8.6}$$

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

$$T_{10D} = \frac{B_{10D}}{n_{op}} = \frac{2\,000\,000 \text{ Zyklen}}{86\,400 \text{ Zyklen / Jahr}} = 23{,}2 \text{ Jahre} \tag{8.7}$$

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

In der Summe für einen Kanal (S1, S2, K1, K3, K4, 1V4, 2V2) ergibt sich nach Abschnitt 8.2.13 eine $MTTF_D$ von 31,4 Jahren, also „hoch“:

$$\frac{1}{MTTF_D} = \frac{1}{232 \text{ Jahre}} + \frac{1}{232 \text{ Jahre}} + \frac{1}{806 \text{ Jahre}} + \frac{1}{232 \text{ Jahre}} + \frac{1}{232 \text{ Jahre}} + \frac{1}{150 \text{ Jahre}} + \frac{1}{150 \text{ Jahre}} = \frac{1}{31{,}4 \text{ Jahre}} \tag{8.8}$$

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

Die Validierung der angenommenen *DC*-Werte wird ebenfalls in Kapitel 10 näher beschrieben. Für K1 und K2 werden z. B. hochwertige Selbsttests durch Software und Kreuzvergleich inklusive der für Rechnersysteme erforderlichen speziellen Maßnahmen für variante und invariante Speicher und die Verarbeitungseinheit durchgeführt. In der Summe ergibt sich für das SRP/CS nach Abschnitt 8.2.14 ein DC_{avg} von 98,6 %, der unter Ausnutzung der 5-%-Toleranz im Bereich von „hoch“ liegt.

$$DC_{avg} = \frac{2 \cdot \left(\frac{99\,\%}{232 \text{ Jahre}} + \frac{99\,\%}{232 \text{ Jahre}} + \frac{90\,\%}{806 \text{ Jahre}} + \frac{99\,\%}{232 \text{ Jahre}} + \frac{99\,\%}{232 \text{ Jahre}} + \frac{99\,\%}{150 \text{ Jahre}} + \frac{99\,\%}{150 \text{ Jahre}} \right)}{2 \cdot \left(\frac{1}{232 \text{ Jahre}} + \frac{1}{232 \text{ Jahre}} + \frac{1}{806 \text{ Jahre}} + \frac{1}{232 \text{ Jahre}} + \frac{1}{232 \text{ Jahre}} + \frac{1}{150 \text{ Jahre}} + \frac{1}{150 \text{ Jahre}} \right)} = 98{,}6\,\% \tag{8.9}$$

Die im Kasten „Berechnung der Ausfallhäufigkeit“ auf S. 89 genannten Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) sind weitgehend selbsterklärend, dennoch wird die Validierung in Kapitel 10 näher erläutert. Zusätzlich wirkt im elektrischen Teilsystem die Maßnahme „Diversität“ und im hydraulischen Teilsystem 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.

8.4.6 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 (**Abbildung 8.12**). Die tabellarischen Werte in Anhang K der Norm oder die darauf basierende PLC-Drehscheibe des IFA liefern folgendes Ergebnis:

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

Sehr viel mehr Komfort bei der Verwaltung, Dokumentation und Berechnung aller Zwischenergebnisse bietet die vom IFA kostenlos zur Verfügung gestellte Software SISTEMA (siehe Anhang H). Alle bisher dargestellten quantitativen Anforderungen zur PL-Bestimmung lassen sich damit einfach erfassen und alle Rechenschritte inklusive der rechnerischen PL-Bestimmung sind automatisiert. Als besondere Option ist eine Berechnung mit den genauen DC_{avg}- und $MTTF_D$-Werten möglich. Für DC_{avg} wird mit dem genauen (hier schlechteren) Wert 98,6 % gerechnet, statt die 5 %-Toleranz zu DC_{avg} „hoch“ auszunutzen und gerundete 99 % anzusetzen (zu den Toleranzen bei *DC* und $MTTF_D$ vgl. Anmerkungen 2 in den Tabellen 6 und 7 der Norm). Die noch innerhalb des Toleranzbereichs liegende Unterschreitung der 99 %-Marke für Kategorie 4

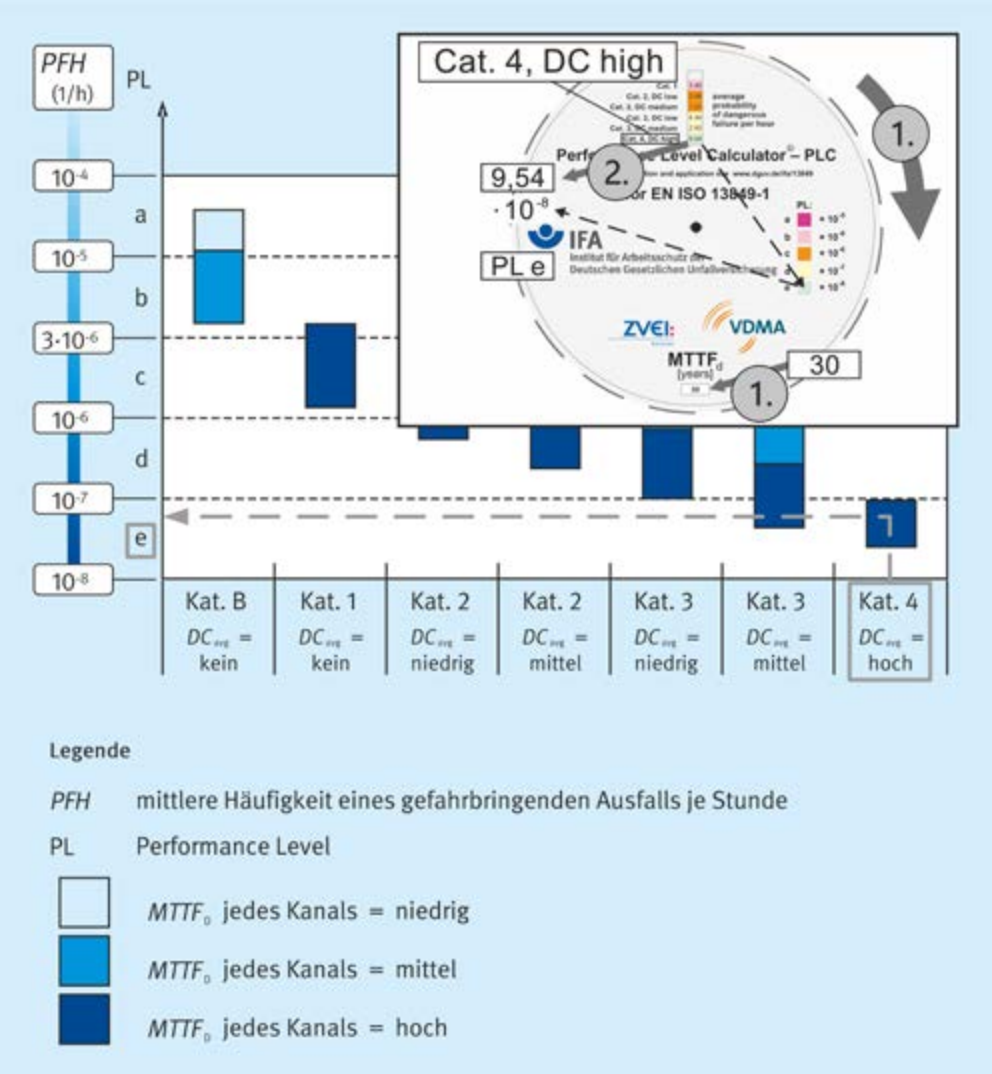


Abb. 8.12
PL-Bestimmung mithilfe des Säulendiagramms bzw. der Drehscheibe

wird von SISTEMA allerdings mit einem Warnhinweis versehen. Die Rechnung mit dem genauen $MTTF_D$-Wert von 31,4 Jahren bringt ein vergleichbares Ergebnis gegenüber der Rechnung mit dem abgerundeten Wert von 30 Jahren für $MTTF_D$ „hoch“. Es ergibt sich eine *PFH* von $9{,}7 \cdot 10^{-8}$/Stunde (**Abbildung 8.13**).

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

8.4.7 Systematische Ausfälle

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

- Verwendung des Ruhestromprinzips; hierdurch ist sichergestellt, dass der energielose Zustand nicht zu einem Ansteuersignal führen kann (z. B. bei einem Drahtbruch).
- Ausfallerkennung durch automatische Tests; hier werden in den beiden Steuerungskanälen jeweils verschiedene Tests ausgeführt, die frühzeitig Fehler erkennen können und jeweils unabhängig vom Nachbarkanal den sicheren Zustand selbst einleiten können.
- Testung durch redundante Hardware; hierdurch können mithilfe der konstruktionsbedingten Diversität zusätzlich Fehler durch Umwelteinflüsse beherrscht werden, die sich in den einzelnen Kanälen nicht gleichartig auswirken.
- 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.

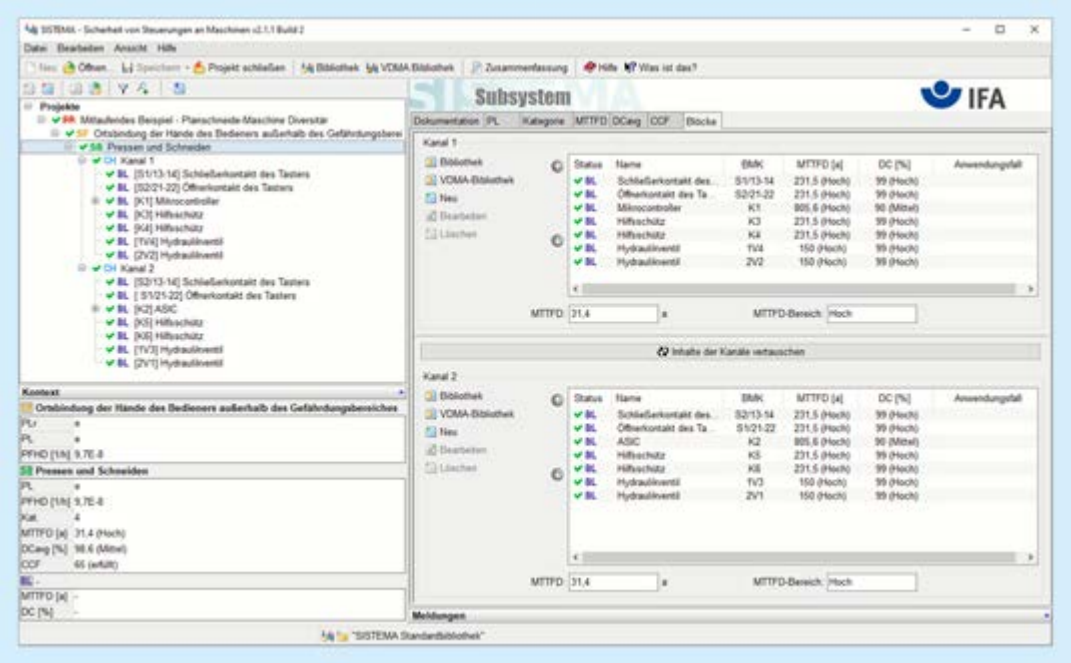


Abb. 8.13 PL-Bestimmung mithilfe von SISTEMA

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

- Bei der Gestaltung des Hydrauliksystems für Planschneidemaschinen ist der Papierstaubanfall zu berücksichtigen. So kann z. B. mit Papierstaub verunreinigtes Hydrauliköl die sichere Funktion einer Planschneidemaschine gefährden. Aus diesem Grund muss im Besonderen auf eine gute Filtrierung des Druckmediums geachtet werden. Weiterhin muss das externe Einbringen von Papierstaub in das Hydrauliksystem durch z. B. Abstreifringe an Kolbenstangen und Tankbelüftungsfilter verhindert werden.
- Fehlervermeidende Maßnahmen bei der ASIC-Entwicklung gemäß ASIC-Entwicklungs-Lebenszyklus nach DIN EN 61508-2: In dieser Norm ist für die Entwicklung eines ASICs ein V-Modell in Anlehnung an das aus der Softwareentwicklung bekannte V-Modell vorgesehen.

8.4.8 Ergonomische Aspekte

In diesem Beispiel gibt es eine sicherheitsrelevante Schnittstelle zwischen dem Benutzer und der Steuerung: die Zweihandschaltung (ZHS) mit den Stellteilen S1 und S2. Hier sind einige ergonomische Aspekte zu berücksichtigen, damit keine Person während der geplanten Verwendung und vernünftigerweise vorhersehbaren Fehlanwendung unmittelbar oder auf Dauer durch Fehlbelastungen gefährdet wird. Diese Benutzerschnittstellen können für die meisten Maschinen mit der Checkliste Ergonomische Maschinengestaltung, DGUV Informationen 209-068 und 209-069 [32], überprüft werden. Folgende Aspekte sind dabei u. a. zu betrachten:

- Höhe und Orientierung der Stellteile in Bezug auf die Bedienperson,
- Greif- und Beinraum bei der üblicherweise stehenden Bedienung,
- mit der Bedienaufgabe abgestimmte Anordnung und gute Erreichbarkeit außerhalb des Gefahrenraums,
- Beobachtbarkeit des Schneidevorgangs vom Ort der ZHS aus,
- Mindestabmessungen und Form der Stellteile (ergonomische Gestaltung unter Beachtung der Vorgaben nach DIN EN ISO 13851),
- 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.

8.4.9 Kombination von Teilsystemen

Da das gesamte SRP/CS durchgängig in einer Kategorie strukturiert ist und keine Teilsysteme kombiniert werden, ist eine diesbezügliche Betrachtung nach Kapitel 7 nicht notwendig. Gleichwohl müssen die verschiedenen Komponenten und Technologien an den Schnittstellen natürlich zueinander passen. Validierungsaspekte zur Integration werden in Kapitel 10 angesprochen.

8.4.10 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: Schneidemaschinen (6/2010). DIN Media, Berlin 2010
- DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (2/2011). DIN Media, Berlin 2011
- DIN EN ISO 13851: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte und Gestaltungsleitsätze (11/2019). DIN Media, Berlin 2019

Weitere Ausführungen, speziell hinsichtlich der Softwareanforderungen sowie der Verifikation und Validierung, folgen in der Fortsetzung dieses Beispiels einer Planschneidemaschine in den Kapiteln 9 und 10.

9 Entwicklung sicherheitsbezogener Software

„*Wer eine Software programmiert und darin jahrelange Erfahrung hat, macht selbstverständlich keine Fehler mehr.*“ Diese oder ähnliche Aussagen sind oft zu hören. Dabei ist gerade diese Selbstüberschätzung der größte Fehler, den man machen kann. Software ist in der Regel kompliziert und deshalb gibt es auch im Gegensatz zur Hardware zunehmend mehr Versagen durch Softwarefehler. Wie oft wundert man sich am PC, dass ein Peripheriegerät nicht mehr funktioniert, wie oft war es dann ein Teil der Software, der sich mit einem anderen, z. B. dem Treiber, nicht verträgt? Dagegen sind Hardwarefehler eher selten. Normale, das heißt Software für einfache Funktionen, hat nach [45] etwa eine Fehlerdichte von 25 Fehlern pro 1000 Programmzeilen. Gute Software hat eine Fehlerdichte von etwa zwei bis drei Fehlern pro 1000 Programmzeilen. Die Software im Space-Shuttle hatte (laut NASA) eine Fehlerdichte von weniger als einem 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. Diese Programmfehler „schlummern“ in den Produkten und werden sich unter bestimmten Bedingungen und in bestimmten Situationen auf die Funktion auswirken. Wie keine zweite Technologie übernimmt Software eine höhere Verantwortung als je zuvor und damit also auch die Programmierenden.

Als eine der wesentlichen Neuerungen der DIN EN ISO 13849-1 [7] gegenüber ihrer Vorgängernorm DIN EN 954-1 [46] wurden in der zweiten Ausgabe der Norm erstmals Anforderungen an die Software und deren Entwicklung gestellt. Um es vorweg deutlich herauszustellen: Die in der vierten Ausgabe der Norm in einem eigenen Abschnitt 7 zusammengefassten Anforderungen an die Entwicklung sicherheitsbezogener Software ermöglichen es, sicherheitsbezogene Software für alle SRP/CS im Maschinensektor und für alle erforderlichen Performance Level (PL) von a bis e zu entwickeln. Ausnahme bildet die Entwicklung von SRESW (safety-related embedded software – sicherheitsbezogene eingebettete Software) für den PL e. In diesem Fall gelten die Anforderungen des SIL 3 nach DIN EN 61508-3 [46], Abschnitt 7, wenn keine Softwarediversität für die beiden Kanäle in Kategorie 3 oder 4 vorliegt.

Dieses Kapitel richtet sich in erster Linie an Anwendungsprogrammierende, die Sicherheitsfunktionen für eine Maschine entwickeln, z. B. in einer applikationsorientierten Sprache auf einer speicherprogrammierbaren Steuerung (SPS). Für die Entwicklung von SRESW, also Firmware, ist dagegen der Neuigkeitswert der Anforderungen in DIN EN ISO 13849-1 nicht so hoch. Solche Embedded-Software-Entwicklungen für die meist zertifizierten Komponenten werden häufig unter den sehr komplexen Anforderungen der für IEC-Normen zur funktionalen Sicherheit verbindlichen Sicherheitsgrundnorm DIN EN 61508 ausgeführt. Die vierte Ausgabe der DIN EN ISO 13849-1 weist darauf hin, dass spezifische Anforderungen an Software, die künstliche Intelligenz nutzt, nicht berücksichtigt sind. Dies gilt gleichfalls für Themen wie agile Softwareentwicklung und objektorientierte Programmierung. Früher noch unter dem Thema Software beschriebene Anforderungen an eine softwarebasierte manuelle Parametrierung wurden in den Abschnitt 6.3 der Norm verschoben.

Die folgenden Darstellungen beschränken sich darauf, die normativen Anforderungen der DIN EN ISO 13849-1 zu sicherheitsbezogener Software kurz vorzustellen. Die Grundgedanken dieses Abschnitts können auf beide Softwaretypen bezogen werden. Einzelne Anforderungen werden aber eher für die Anwendungsprogrammierung von SRASW konkretisiert. Die Entwicklung der SRESW des in Abschnitt 6.8 begonnenen und in Abschnitt 8.4 fortgeführten Beispiels der Sicherheitssteuerung einer Planschneidemaschine mit diversitärer Redundanz in der Logiksteuerung (PL e) ist in Abschnitt 9.12 dargestellt.

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 zwei Sprachtypen unterschieden: Programmiersprache mit nicht eingeschränktem Sprachumfang (Full Variability Language, FVL) und Programmiersprache mit eingeschränktem Sprachumfang (Limited Variability Language, LVL). Sicherheitsbezogene Embedded-Software (SRESW) erfordert in der Regel eine FVL, während sicherheitsbezogene Anwendersoftware (SRASW) oft in einer LVL erstellt wird. Eine neue Entscheidungshilfe (Bild 15 der Norm) zur Einordnung der verwendeten Programmiersprache in FVL oder LVL ergänzt nun den Softwareabschnitt. Programmiersprachen in Übereinstimmung mit IFA Report 2/1016 „Sicherheitsbezogene Anwendungssoftware von Maschinen“ [13], konkret Kontaktplan, Funktionsbaustein-Sprache, Ablaufsprache und boolesche Algebra, gelten als LVL. Zusätzlich können durch Programmierrichtlinien, Compiler und Entwicklungswerkzeuge realisierte Beschränkungen, die einen definierten Programmfluss sicherstellen, zu einer Einordnung als LVL führen. Für SRASW, die in LVL programmiert ist, gelten die Anforderungen aus Abschnitt 7.4 der Norm. Sobald aber SRASW in FVL (z. B. eine SPS in der Hochsprache „C“ oder in Strukturiertem Text (ST) ohne Codierungsrichtlinien und -beschränkungen) programmiert wird, müssen die Anforderungen für SRESW, Abschnitt 7.3 der Norm, erfüllt werden. Soll PL e erreicht werden, muss die SRASW in diesem Fall wie oben bereits für SRESW erwähnt die Anforderungen der Norm DIN EN 61508-3, Abschnitt 7 erfüllen.

Für die Programmierung von SRASW als LVL ist der IFA Report 2/2016 erschienen. Er beschreibt die Matrixmethode des IFA zur Spezifikation, Verifizierung, Validierung und Dokumentation von SRASW als LVL. Diese Matrixmethode kann auch mit dem Tool SOFTEMA des IFA [18] angewendet werden. Der Report gibt darüber hinaus detaillierte, weiterführende Informationen zur Programmierung von SRASW als LVL.

Die Anforderungen für SRESW wurden bisher in der Norm nur sehr knapp beschrieben. Nun enthält die vierte Ausgabe für alle Basismaßnahmen und zusätzlichen Maßnahmen vertiefende beispielhafte Hinweise. Weiterführende Erläuterungen zum Thema SRESW enthält der IFA Report 1/2020 „Praxisgerechte Umsetzung der Anforderungen für sicherheitsbezogene Embedded-Software nach DIN EN ISO 13849-1“ [14].

9.1 Das V-Modell – 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 zur Risikominimierung beitragen soll, alles Angemessene getan werden, um Fehler zu vermeiden. Was angemessen ist, orientiert sich einerseits am erforderlichen 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, Design und Modifikation. Daher zielen die Anforderungen der Norm – und die Erläuterungen in diesem Abschnitt – besonders auf die Fehlervermeidung in diesen Phasen. Leider werden sie in der Praxis oft mit eher weniger Aufmerksamkeit bedacht.

Um eine gute Qualität sicherheitsbezogener Software zu erreichen, ist es nahe liegend, entsprechende aktuelle und bewährte Entwicklungsmodelle des „Software Engineering“ aufzugreifen. Für sicherheitsbezogene Systeme wird dabei meist auf das V-Modell referenziert [47]. 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 7.1, in einer vereinfachten Form (Abbildung 9.1) gefordert. Diese wird für die Bedingungen der SRP/CS im Maschinensektor und dort speziell für die Entwicklung von SRASW als praxisgerecht und zielführend bewertet. Im V-Modell des Software-Sicherheitslebenszyklus werden die Verifizierungsschritte (Reviews und Tests) und die Ergebnisse der Phasen genau benannt. Auch die auf dem absteigenden Ast entstehenden Dokumentationen, die mit jeder Spezifikationsphase immer feinteiliger werden, sind mit dargestellt. Neu in der vierten Ausgabe der Norm ist die in **Abbildung 9.2** gezeigte weiter vereinfachte zweistufige Variante des V-Modells für LVL. Voraussetzung ist der Einsatz bereits bewerteter sicherheitsbezogener Hard- und Softwaremodule, im Folgenden als validierte Funktionsblöcke bezeichnet, die als Anwendungsprogramm (SRASW) auf geprüfter Hardware laufen. Da die zugehörige Programmierung typischerweise nur einfache logische Verknüpfungen von Eingangs- und Ausgangsblöcken realisiert, können die Phasen Software-Systemdesign, Modul-

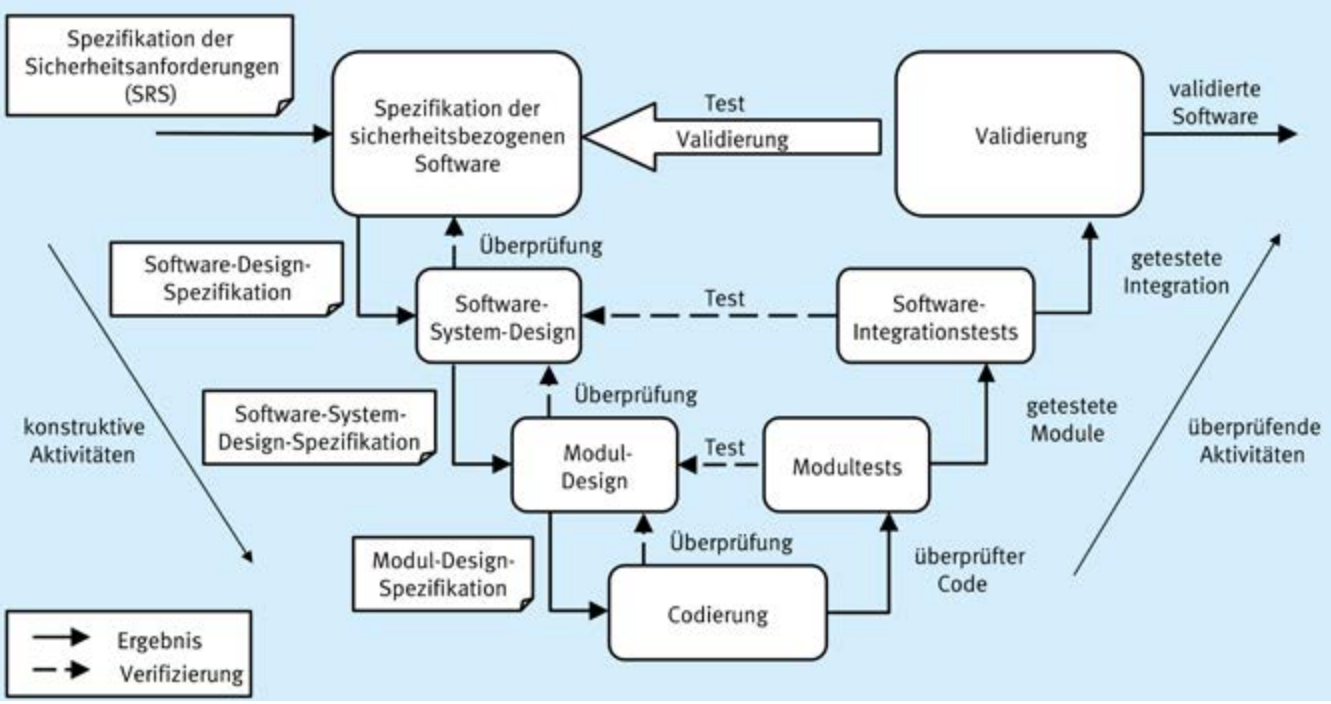


Abb. 9.1 Vereinfachtes V-Modell für die Entwicklung sicherheitsbezogener Software

Design, Modultests und Software-Integrationstests aus Abbildung 9.1 weggelassen werden und man kann direkt von der Phase der sicherheitsbezogenen Software-Spezifikation in die Codierungsphase übergehen. Abschließend muss die Validierung durchgeführt werden. Das Ziel bei der Anwendung des V-Modells ist es, lesbare, verständliche, testbare und wartbare Software zu erhalten. Diese Anforderungen empfinden Programmierende, die üblicherweise keine sicherheitsrelevante Software erstellen, aus Erfahrung eher als mühsam. Die Erfüllung dieser Anforderungen gibt ihnen aber die Bestätigung, die Software hinreichend gut entwickelt zu haben.

Neben den Phasen sind in Abbildung 9.1 wichtige Begriffe dargestellt, deren Bedeutung (auf Software bezogen) vorab definiert werden soll.

Ergebnis

Bezeichnet das, was in einer Phase erstellt wurde, z. B. die Software-Design-Spezifikation, die Modul-Design-Spezifikation, den überprüften Code und als abschließendes Ergebnis die validierte Software. Es kann aber z. B. auch ein Testplan sein, als Ergebnis der Spezifikationsphase, der erst in einer 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.

Verifizierung

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 das in der Modul-Design-Spezifikation vorgegebene Modul-Design realisiert und dabei die Programmierrichtlinien eingehalten wurden.

Validierung

Die Software-Validierung ist hier eine abschließende spezielle Form der Verifizierung der gesamten Software. Es wird geprüft, ob die Anforderungen der Software-Design-Spezifikation 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 abwärts gerichtete Teil des „V“ beschreibt die konstruktiven und der aufwärtsgerichtete die überprüfenden Aktivitäten der Entwicklung.

9.2 Phase „Spezifikation der sicherheitsbezogenen Software“ – Schnittstelle zur Gesamtsicherheit

Ausgehend von der übergeordneten Spezifikation der Sicherheitsanforderungen (SRS) der SRP/CS wird in der Software-Design-Spezifikation beschrieben, welche Teilfunktionen davon die Software realisieren muss. Weiterhin werden u. a. dargestellt:

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

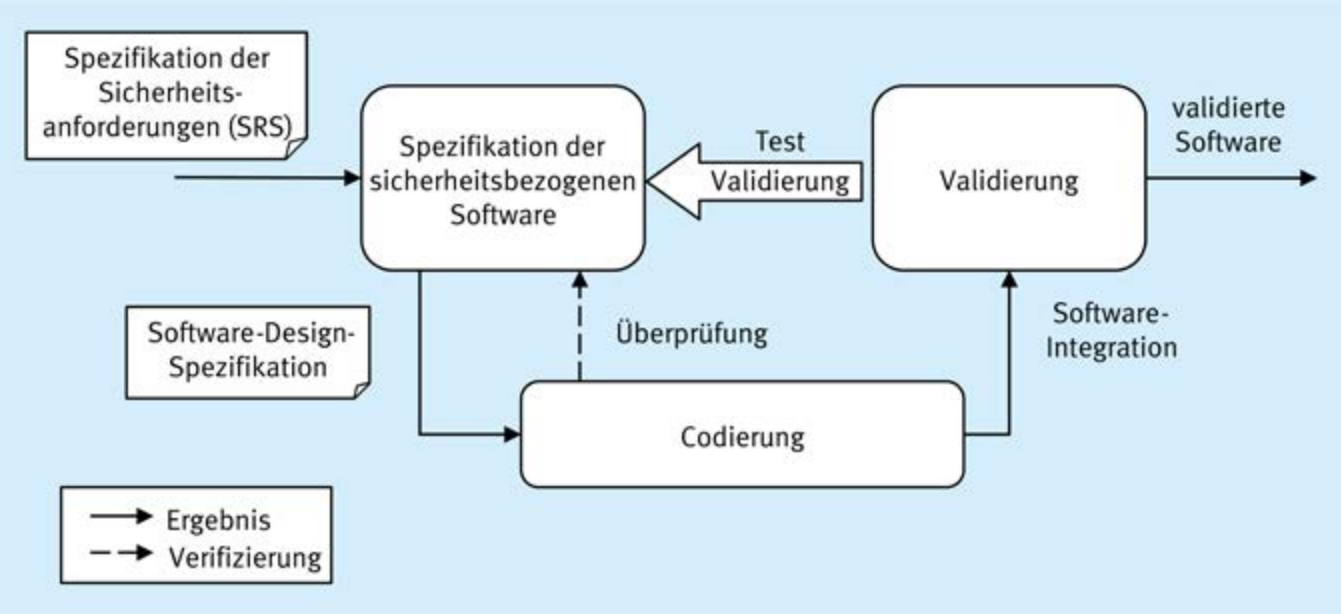


Abb. 9.2 Vereinfachtes V-Modell für Software, die validierte Funktionsblöcke verwendet und als Anwendungsprogramm (SRASW) in Kombination mit LVL auf geprüfter Hardware läuft

Neben diesen funktionalen Anforderungen ist auch der von den Sicherheitsfunktionen zu erreichende PL, der PL_r, anzugeben, damit die notwendigen fehlervermeidenden Maßnahmen (siehe Abschnitt 9.6) ausgewählt werden können.

Die Software-Design-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 das Lastenheft mit der übergeordneten Spezifikation der Sicherheitsanforderungen übereinstimmt, und zweitens, dass auch die Anforderungen an die Form, wie eine Software-Design-Spezifikation zu schreiben ist, erfüllt sind. Die Software-Design-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 und Software) gewährleistet. Hier ist also eine Beschreibung der Sicherheit für die Maschine bzw. Maschinenanlage in Form einer SRS notwendig. Das Dokument muss nicht Hunderte von Seiten umfassen, sondern kann sich durchaus in verständlicher Form auf das Wesentliche beschränken. Nach den Festlegungen zur Gesamtheit der Maschine oder Maschinenanlage wird es eine Teilmenge von Arbeiten für Programmierende geben. Die Software-Design-Spezifikation ist damit Teil des Gesamtkonzepts und folglich als „Vertrag“ mit einem „Unterauftrag“ zur Programmierung zu bewerten.

Zunächst macht die Software-Design-Spezifikation Vorgaben für das Design 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 Software-Design-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 Software-Design-Spezifikation auch eine vertragsverbindliche Schnittstelle zu externen oder internen Dienstleistern sein.

9.3 Phasen „Software-System-Design“ und „Modul-Design“ für das „sicherheitsbezogene Softwarepflichtenheft“

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

Die Dokumentation des Software-System-Designs (Software-System-Design-Spezifikation) sollte Aufbau und Ablauf der Software durch Grafiken auch für außenstehende Personen verständlich beschreiben. Dies kann umso kompakter sein, je mehr das Programm auf wiederverwendeten, bereits validierten Softwarefunktionen basiert, die schon an anderer Stelle dokumentiert sind. In der Phase Modul-Design werden in der Modul-Design-Spezifikation zusätzlich die projektspezifisch neu zu erstellenden Softwarefunktionen, ihre Schnittstellen und Testfälle für deren Modultest spezifiziert. Die Phasen Software-System-Design und Modul-Design können bei weniger komplexen SRP/CS zusammengefasst werden und ergeben das „sicherheitsbezogene Softwarepflichtenheft“.

9.4 Phase „Codierung“ – endlich programmieren

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

- Lesbaren und verständlichen Code schreiben, damit dieser später leichter getestet und fehlerfreier modifiziert werden kann. Verbindliche Programmierrichtlinien helfen z. B., das Programm besser zu kommentieren und die Variablen bzw. Bausteine selbsterklärend zu benennen.
- Defensiv programmieren, das heißt, immer mit internen oder externen Fehlern rechnen und diese aufdecken. Kennt man z. B. das zeitliche Verhalten von Eingangssignalen, so kann man mit dieser Erwartungshaltung Fehler der peripheren Beschaltung aufdecken. Wird eine Zustandsmaschine programmiert, dann wird die Zustandsvariable auf gültigen Wertebereich überwacht usw.
- Der Code muss statisch, d. h. ohne Ausführung, analysiert werden: Für niedrige PL reicht ein Code-Review, für PL d und e sollte der Daten- und Steuerfluss zusätzlich – möglichst werkzeugbasiert – überprüft werden. Typische Fragen sind: Entspricht der Code der Modul-Design-Spezifikation? 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?

9.5 Phasen „Modultest“, „Software-Integrationstest“ und „Validierung“ – prüfe, was sich ewig bindet

Im Modultest werden die projektspezifisch neu entwickelten Softwarefunktionen getestet und simuliert, um zu prüfen, ob sie so codiert sind, wie in dem Modul-Design spezifiziert. Spätestens beim Software-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 dem Software-System-Design (Verifizierung) getestet. Beides sind noch Verifizierungsmaßnahmen, d. h., man schaut dabei in die Software „hinein“. Ob die Teilfunktionen 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 die resultierende neue Teilfunktion zu validieren. Auch bei zertifizierten Bausteinen kann es aufgrund falscher Parametrierung und Verknüpfung zu gefahrbringenden systematischen Ausfällen kommen.

9.6 Struktur der normativen Anforderungen

Nachdem der Entwicklungsprozess skizziert ist, werden normative Anforderungen an die Software selbst, an die benutzten Entwicklungswerkzeuge und 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 mit zunehmendem PL_r sinnvoll gesteigert.

Es fällt nicht leicht die Anforderungen für den konkreten Anwendungsfall unter Berücksichtigung des PL_r und bei eventuell vorhandener Softwarediversität direkt eindeutig zu identifizieren. Hier soll der erste Teil des neuen informativen Anhangs N helfen: Zunächst wird im Hinblick auf die Anwendung mit Tabelle N.1 einer von vier Einsatzfällen bestimmt. Die Fälle berücksichtigen den PL_r (a/b, c, d oder e) und je nachdem unter welchen Umständen die Software eingesetzt wird, können die Anforderungen um eine Stufe herabgesetzt werden. Diese Abstufung ist für Software im Testkanal von Kategorie 2 oder in diversitären Funktionskanälen (gemeint sind Software-Funktionskanäle) von Kategorie 3 oder 4 möglich. **Tabelle 9.1** hebt die möglichen Abstufungen hervor. Danach werden mit dem zutreffenden Fall in Tabelle N.2 bzw. Tabelle N.3 die empfohlenen und verbindlichen Einzelmaßnahmen abgelesen.

Tabelle 9.1 Gruppierung von Fällen für die Auswahl von Maßnahmen (Tabelle N.1 der DIN EN ISO 13849-1)

PL_r	Kategorie	Software verwendet in	Fall
a und b	B	Funktionskanal	Fall 1
a, b und **c**	2	**Testkanal**	
a und b	2	Funktionskanal	
a und b	3	bereits bewertete Plattform	
a und b	3	Kanal 1 UND 2	
a, b und **c**	3	**Kanal 1 ODER 2**	
c	2	Funktionskanal	Fall 2
c	3	bereits bewertete Plattform	
c	3	Kanal 1 UND 2	
d	2	**Testkanal**	
d	3 und 4	**Kanal 1 ODER 2**	
d	2	Funktionskanal	Fall 3
d	3 und 4	bereits bewertete Plattform	
d	3 und 4	Kanal 1 UND 2	
e	3 und 4	**Kanal 1 ODER 2**	
e	3 und 4	bereits bewertete Plattform	Fall 4
e	3 und 4	Kanal 1 UND 2	

Der zweite Teil des neuen Anhangs N demonstriert die Softwarevalidierung durch Analyse und Tests am Beispiel einer SRASW, die auf validierte Funktionsblöcke zurückgreift. Das Beispiel für die Realisierung von SRESW im informativen Anhang J wurde an das aktuelle V-Modell des Software-Sicherheitslebenszyklus angepasst.

Abbildung 9.3 zeigt die Vorgehensweise zur Auswahl der Anforderungen für die verschiedenen Softwaretypen zum Design sicherheitsbezogener Software in einer Übersicht. Für nicht zugängliche Embedded-Software industrieller Standardkomponenten gelten die Anforderungen nach Abschnitt 7.3.2 der Norm. Für SRESW und SRASW in FLV bzw. SRASW in LVL erfolgt zunächst die Fallbestimmung, bevor die konkreten Maßnahmen für alle Aktivitäten der Softwareerstellung aus der zutreffenden Tabelle ermittelt werden.

Abbildung 9.4 zeigt, dass es sowohl bei SRASW als auch bei SRESW für alle PL ein geeignetes Bündel von grundlegenden Maßnahmen (Basismaßnahmen) gibt. Diese können als softwarespezifische grundlegende Sicherheitsprinzipien verstanden werden. Sie genügen für die Entwicklung von Software für PL a oder b. Für Software, die in Teilsystemen für PL c bis e eingesetzt wird, gelten neben den Basismaßnahmen zusätzliche fehlervermeidende Maßnahmen. Bei SRASW werden die zusätzlichen Maßnahmen für PL c mit geringerer Wirksamkeit, für PL d mit mittlerer Wirksamkeit und für PL e mit höherer Wirk-

samkeit gefordert. Für SRESW ist das Konzept steigender Wirksamkeit nicht im normativen Text beschrieben. Bei der Fußnote dazu in Tabelle N.3 der Norm handelt es sich aus Sicht der Autoren um einen Kopierfehler.

Zu dem Aspekt steigender Wirksamkeit folgendes Beispiel: Der Aspekt „höhere Wirksamkeit" bezieht sich auf den zunehmenden Grad der Fehlervermeidung. Dies soll an der wichtigen Aktivität der Software-Design-Spezifikation illustriert werden. So kann es z. B. für PL c ausreichend sein, wenn Programmierende die Software-Design-Spezifikation selbst verfassen und andere sie gegenlesen („internes Review"). Soll aber die gleiche Software für PL e eingesetzt werden, so muss ein höherer Grad der Fehlervermeidung erreicht werden. Dann wird es notwendig sein, dass nicht die Programmierenden selbst die Software-Design-Spezifikation erstellen, sondern z. B. der „Projektleiter Software". Darüber hinaus würde das Review dieser Software-Design-Spezifikation gemeinsam mit einer Person größerer Unabhängigkeit durchgeführt, die z. B. für die Hardware-Projektierung zuständig ist. Eine größere Anzahl von Personen deckt (meist) auch mehr Fehler auf.

Nachfolgend sind noch einige besondere Fälle rund um das Thema normative Anforderungen zu sicherheitsrelevanter Software aufgeführt:

- Häufig realisiert die gesamte Software eines Teilsystems oder SRP/CS mehrere Sicherheitsfunktionen SFx mit jeweils unterschiedlichem 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 d oder e realisiert. Wird in einem Kanal eines Teilsystems eine programmierbare Elektronik und im anderen Kanal eine diversitäre Redundanz mit einer anderen Technologie (z. B. fluidtechnisch) eingesetzt, werden die Anforderungen um eine PL-Stufe abgesenkt, was in Tabelle N.1 der Norm berücksichtigt ist. Es ergibt sich außer für niedrige PL ein anderer Fall im Vergleich zu einer Lösung ohne Diversität. Der Normensetzer berücksichtigt bei Realisierung von Diversität die geringe Wahrscheinlichkeit, dass in beiden Kanälen jeweils ein systematischer Softwarefehler vorliegt, der zu einem gefahrbringenden Ausfall der Sicherheitsfunktion führen könnte.
- Verwendung von Standard-SPS: Die Schaltungsbeispiele in diesem Report (siehe Kapitel 11) zeigen, dass sicherheitsbezogene Steuerungen prinzipiell auch mit Standard-SPS aufgebaut werden können. Für PL a bis d werden die Softwareanforderungen an die nicht zugängliche Embedded-Software in der Standard-SPS im Abschnitt 9.10 beschrieben. Zusätzlich müssen bei der Anwendungsprogrammierung die Anforderungen zur

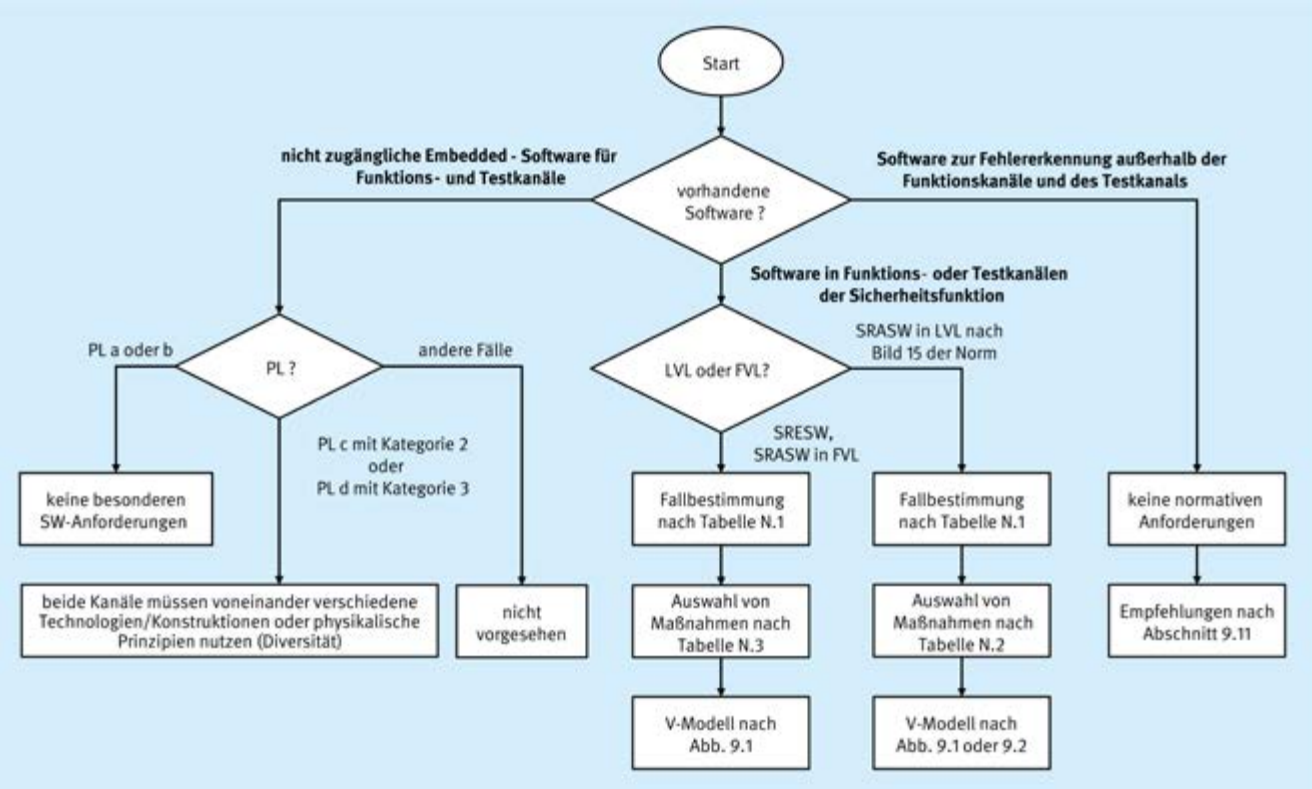


Abb. 9.3 „Software-Flow" zur Auswahl der Anforderungen an Software

Fehlervermeidung bei SRASW (Abschnitte 7.1 und 7.3 der Norm) entsprechend dem PL_r erfüllt werden.
- Bonus bei der Erstellung diversitärer SRESW: Bei zweikanaligen SRP/CS für Sicherheitsfunktion(en) mit PL_r e kann die SRESW beider Kanäle verschieden realisiert werden. Geht der Grad dieser Diversität so weit, dass der Code, das Design und sogar die Software-Design-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 ein SRP/CS verschiedene oder zwei identische Hardwarekanäle hat. Auch bei anderen PL_r wird Softwarediversität prinzipiell „belohnt“, indem z. B. ein anderer Fall daraus resultiert. Allerdings legt der Normensetzer nicht fest, welcher Umfang von Softwarediversität dafür erforderlich ist. Geht es z. B. darum, den Aufwand zur Überprüfung von Teilen der Software zu vermindern, in dem statt des Prüfens jeder Codezeile nur strukturelle Aspekte berücksichtigt werden, kann Diversität in Entwurf und Codierung ausreichen.

9.7 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 der Normung zur IEC 61508 wird das Thema Eignung von Softwarewerkzeugen ausgiebig diskutiert. DIN EN ISO 13849-1 betont folgende vier Elemente:
- Entwicklungswerkzeuge:
  Zur Entwicklung sind geeignete und für den Einsatz bewährte Werkzeuge gefordert. In der Regel werden für SRASW zertifizierte Werkzeuge für Sicherheitskomponenten eingesetzt. Merkmale wie die Vermeidung und Aufdeckung von semantischen Fehlern, Einhaltung von Sprachteilmengen oder Überwachung von Programmierrichtlinien entlasten die Programmierenden und erhöhen die Softwarequalität.
- Bibliotheken:
  Das Software-System-Design sollte vorhandene oder mitgelieferte Bibliotheken berücksichtigen und validierte Funktionen – soweit praktikabel – einsetzen. Es gilt: Je mehr das Programm auf bereits validierten oder sogar zertifizierten Funktionen basiert, umso weniger projektspezifische Softwareteile sind vor Inbetriebnahme noch zu validieren. Zur Systemintegration ist man gut beraten, für typische wiederkehrende Funktionen entsprechende Bausteine/Module mit dem notwendigen Aufwand nach DIN EN ISO 13849-1 selbst zu entwickeln, sodass sie wieder verwendbar sind. Auch die Erstellung einzelner Bibliotheksfunktionen erfordert die Aktivitäten Spezifikation, Design, Testplan, Validierung usw.
- Geeignete Programmiersprachen:
  Für SRASW werden applikationsorientierte Sprachen, z. B. gemäß DIN EN 61131-3 [48], empfohlen. Selbst diese Sprachen sind bereits über das notwendige Maß hinaus sehr umfangreich und enthalten teilweise fehlerträchtige Konstrukte. Daher sollten Programmierende die Syntax nur eingeschränkt einsetzen. Entsprechende Sprachteilmengen werden meist durch das Werkzeug vorgegeben.
- Programmierrichtlinien:
  Zur Codierung der Softwarefunktionen sind geeignete Programmierrichtlinien zu beachten, z. B. MISRA C [49]. 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.

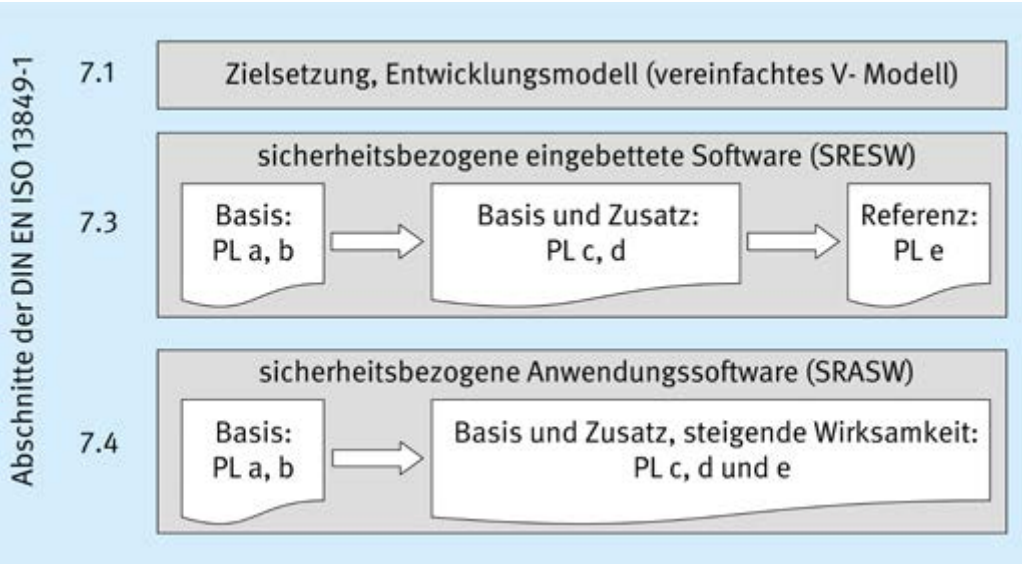


Abb. 9.4
Abstufung der Anforderungen an sicherheitsbezogene Software

Diese Werkzeuge und Richtlinien sollten in den Design-Spezifikationen vorgegeben werden.

9.8 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 Software-Design-Spezifikation der realisierten Sicherheitsfunktionen (Lastenheft), die Dokumentation des Software-System-Designs und Modul-Designs (sicherheitsbezogenes Softwarepflichtenheft) sowie das gut kommentierte Programm gemeint. Zusätzlich sind die benutzten zertifizierten oder selbst validierten Bibliotheksfunktionen mit ihrer Identifikation (Versionsnummer, Autor, Datum usw.) aufzulisten. Die Anwendung von eigenen Programmierrichtlinien und Sprachteilmengen ist ebenfalls zu dokumentieren. Falls das Werkzeug diese bereits enthält, genügt ein entsprechender Hinweis auf diese Merkmale. Bleibt noch die Dokumentation der Testaktivitäten: Oft werden Software-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 welchem Teilsystem bzw. SRP/CS geladen?

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

9.9 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 Software-Design-Spezifikation nicht mehr passt: Sie müsste eigentlich überarbeitet werden. Durch geänderte Sicherheitsfunktionen an der einen Seite der Anlage/Maschine können auch die anderen, zunächst nicht modifizierten Sicherheitsfunktionen betroffen sein. Oder es ergeben sich durch die Modifikationen Lücken im Sicherheitskonzept. Dies gilt es zu überprüfen und gegebenenfalls die notwendigen Phasen des V-Modells zu wiederholen.

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

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

Im Prinzip muss man nach einer Modifikation wieder dort im Entwicklungsprozess, also im V-Modell, einsteigen, wo etwas geändert wurde (Abbildung 9.1), z. B.:

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

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

9.10 Anforderungen an nicht zugängliche Embedded-Software industrieller Standardkomponenten

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. Eine Ausnahmeregelung gibt es jedoch für nicht zugängliche Embedded-Software.

Die Verwendung von zugekauften industriellen Standardkomponenten, die nicht speziell für den Einsatz in Sicherheitsfunktionen entwickelt wurden, die aber nicht zugängliche Embedded-Software enthalten, wurde erst in der dritten Ausgabe der DIN EN ISO 13849-1 thematisiert. Es gibt in der Praxis viele SRP/CS-Beispiele, die solche Standardkomponenten wie SPS, Frequenzumrichter oder Sensoren verwenden und die Sicherheit z. B. durch diversitäre Redundanz mit Fehlererkennung auf Systemebene realisieren. Ein solches Beispiel mit einer Standard-SPS und einem Standard-Frequenzumrichter ist in Anhang I der Norm dargestellt. Da für solche Standardkomponenten die Einhaltung der SRESW-Anforderungen in der Regel durch den Hersteller nicht bestätigt wird und durch den Integrator nicht nachträglich geleistet werden kann, stellt sich die Frage, ob Standardkomponenten eingesetzt werden können, und wenn ja, unter welchen Bedingungen.

Abschnitt 7.3.2 der Norm erlaubt für solche Standardkomponenten einen Verzicht auf den Nachweis der SRESW-Anforderungen unter folgenden Bedingungen (siehe Abbildung 9.3):

- Das Teilsystem ist auf PL a oder PL b begrenzt und verwendet Kategorie B, 2 oder 3.
- Das Teilsystem ist auf PL c mit Kategorie 2 oder PL d mit Kategorie 3 begrenzt. Es werden die Diversitätsanforderungen der CCF-Betrachtung erfüllt, indem beide Kanäle unterschiedliche Technologien, Entwürfe oder physikalische Prinzipien verwenden. Die geforderten diversitären Technologien/Konstruktionen oder physikalischen Prinzipien in beiden Kanälen führen dazu, dass die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des SRP/CS durch jeweils einen Fehler in der unterschiedlichen Embedded-Software sehr gering ist.
- Unabhängig von den beiden vorgenannten Bedingungen sind die zugehörige Hardware und die Anforderungen an SRASW gemäß den Anforderungen der Norm zu bewerten, insbesondere für Ausfälle gemeinsamer Ursache (Common Cause Failure, CCF), siehe Anhang F der Norm.

Neben den Anforderungen an die nicht zugängliche Embedded-Software sind beim Einsatz von Standardkomponenten für SRP/CS nach Norm weitere, mehr hardwarebezogene Anforderungen zu beachten, z. B. hinsichtlich Vermeidung und Beherrschung systematischer Fehler oder Eignung für die zu erwartenden Umweltbedingungen, z. B. Klima, Vibration, elektromagnetische Verträglichkeit (EMI). Diese Anforderungen gelten unabhängig von der Embedded-Software weiterhin. Dazu gehört auch, dass bereits ab Kategorie B grundlegende Sicherheitsprinzipien und ab Kategorie 1 bewährte Sicherheitsprinzipien verwendet werden müssen. Für alle Kategorien sind außerdem folgende Basisanforderungen der Kategorie B zu erfüllen: Das SRP/CS muss mindestens in Übereinstimmung mit den zutreffenden Normen gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert sein, also z. B. in Übereinstimmung mit DIN EN 61131-2 für SPS oder DIN EN IEC 61800-1/-2 für Frequenzumrichter.

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

Tabelle 9.2 zeigt einen Überblick zum Einsatz nicht zugänglicher Embedded-Software industrieller Standardkomponenten. Im Gegensatz zur dritten Ausgabe der Norm ist es nun nach der vierten Ausgabe nicht mehr zulässig, Standardkomponenten mit nicht zugänglicher Embedded-Software in Sicherheitsfunktionen für PL d mit Kategorie 2 zu verwenden. Realisierungen in Kategorie 1 sind nicht vorgesehen, da Kategorie 1 generell nicht für die Verwendung mit komplexen Bauteilen vorgesehen ist.

Tabelle 9.2 Überblick zum Einsatz nicht zugänglicher Embedded-Software industrieller Standardkomponenten (nach DIN EN ISO 13849-1)

PL	Einsatz nicht zugänglicher Embedded-Software
a, b	erlaubt
c	erlaubt mit Kategorie 2 oder 3 plus Diversität
d	erlaubt mit Kategorie 3 plus Diversität
e	grundsätzlich nicht erlaubt

Bleibt noch zu klären, was technologische bzw. konstruktive Diversität bedeutet. Das Ziel systematische Ausfälle und Ausfälle infolge gemeinsamer Ursache zu verhindern, wird bei folgenden Ansätzen üblicherweise als erfüllt angesehen.

- Ein Kanal (Funktionskanal oder Testkanal) enthält Bauteile mit Embedded-Software. Der zweite Kanal enthält ausschließlich Bauteile ohne Embedded-Software, also mechanische, elektronische, elektromechanische, pneumatische oder hydraulische Bauteile.
- Beide Kanäle verwenden diversitäre Embedded-Software zur Realisierung der sicherheitsbezogenen Funktionen einschließlich grundsätzlich verschiedener Betriebssysteme, auf gleicher oder unterschiedlicher Hardware.
  Anmerkung: Bei Verwendung gleicher Hardware ergibt sich eine höhere Anfälligkeit für Ausfälle gemeinsamer Ursache (CCF).

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

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

Die Anforderungen an SRASW von speicherprogrammierbaren Standardkomponenten (SPS) orientieren sich an dem PL, den das Teilsystem mit der Standardkomponente erreichen soll. Wird z. B. eine Standardkomponente in einem Kanal in diversitärer Redundanz mit einer anderen Technologie (z. B. fluidtechnisch) in dem anderen Kanal in Kategorie 3 oder 4 eingesetzt, dann werden nach Tabelle N.1 der Norm die Anforderungen für SRASW im PL um eine Stufe abgesenkt. Es ergibt sich z. B. Fall 2 für PL d, anstatt Fall 3. Bei Kategorie 2 werden nur die Anforderungen für die SRASW des Testkanals abgesenkt. In PL d gilt z. B. nach Tabelle N.1 der Norm zwar Fall 3 für die SRASW des Funktionskanals, aber Fall 2 für SRASW im Testkanal. Tabelle 9.1 hebt die möglichen Abstufungen der Tabelle N.1 der Norm hervor. Weitere Fälle werden im Kapitel 9 des IFA Reports 2/2016 beschrieben; weitere Details zur SRASW siehe vorherige Abschnitte im Kapitel 9.

9.11 Anforderungen an Software von fehlerkennenden Elementen außerhalb der Funktionskanäle und des Testkanals

Bisher wurden Anforderungen an das Design von Software in Komponenten in sicherheitsbezogenen Teilen von Steuerungen besprochen, die Bestandteil der Funktionskanäle in den Kategorien B, 2, 3 oder 4 oder des Testkanals in Kategorie 2 sind. Dabei wurden Anforderungen an das Design von sowohl zugänglicher als auch nicht zugänglicher Embedded-Software berücksichtigt (siehe Abbildung 9.3).

Zusätzlich zu diesen Komponenten als Bestandteil eines Funktionskanals bzw. eines Testkanals ist es auch Praxis, dass Komponenten eingesetzt werden, die sich außerhalb dieser Strukturen befinden und allein zur Fehlererkennung von Komponenten dienen, die sich innerhalb dieser Strukturen befinden. Ein Ausfall einer solchen Komponente führt nicht zu einem gefahrbringenden Ausfall einer Sicherheitsfunktion. Ausfälle dieser Komponenten werden auch nicht bei der Berechnung der Ausfallhäufigkeit berücksichtigt. Kapitel 11 enthält einige Beispiele mit solchen Komponenten.

Wie geht man nun mit diesen Komponenten um, zumal in der Norm keine Anforderungen an diese Komponenten oder deren Software zu finden sind? Als sinnvoll erweist sich die Berücksichtigung folgender Empfehlungen:

- Die Software programmierbarer Komponenten realisiert die Fehlererkennung für Komponenten innerhalb der Sicherheitsfunktion. Daher ist es wichtig, die korrekte Umsetzung der Diagnose durch Prüfung nachzuweisen und zu dokumentieren.
- An das Design einer nicht zugänglichen Embedded-Software in der Komponente bestehen darüber hinaus keine normativen Anforderungen.
- Eine qualitätsgesicherte Entwicklung der Komponente sollte immer angestrebt werden. Gleiches gilt für die Einhaltung grundlegender Sicherheitsprinzipien, die unter anderem die Anwendung vorhandener Produktnormen, z. B. DIN EN 61131-2 für eine SPS erfordert.
- Fehlererkennende Software sollte vom Anwender möglichst nicht auf einfache Weise deaktiviert werden können.

Diese Empfehlungen schließen nicht aus, dass eine Fehlererkennung außerhalb der Funktionskanäle oder des Testkanals z. B. mithilfe eines Mikrocontrollerboards oder einer Soft-SPS realisiert wird. Soweit die Software (SRESW und SRASW) hier zugänglich ist, ist die Anwendung der jeweiligen Basismaßnahmen für Fall 1 nach Tabelle 9.1 als Orientierungshilfe empfohlen.

9.12 Umsetzung der Software-Anforderungen, speziell SRESW, am Beispiel einer Planschneidemaschine mit diversitärer Redundanz in der Logiksteuerung (PL e)

Im Folgenden wird das in Abschnitt 6.8 begonnene und in Abschnitt 8.4 fortgeführte Beispiel der Sicherheitssteuerung einer Planschneidemaschine mit diversitärer Redundanz in der Logiksteuerung (PL e) fortgeführt. In diesem Abschnitt wird die Realisierung der sicherheitsbezogenen Firmware für den Mikrocontroller K1 beispielhaft dargestellt. Es handelt sich um eine Embedded-Software (SRESW). Aufgrund des diversitären Ansatzes für die Logiksteuerung – der zweite Kanal wird als ASIC ausgeführt – können die Anforderungen entsprechend der Anmerkung in Abschnitt 7.3.1 der Norm heruntergestuft werden: *„Wenn Diversität in Spezifikation, Entwurf und Codierung in beiden Kanälen des Teilsystems in Kategorie 3 oder 4 verwendet wird, kann ein PL_r e mit den oben erwähnten zusätzlichen Maßnahmen für PL_r c oder d erreicht werden.“* Nach Tabelle N.1 der Norm liegt Fall 3 vor.

Der Entwicklungsprozess für die Firmware orientiert sich am V-Modell in Abbildung 9.1 und ist in das zertifizierte Qualitätsmanagement des Herstellers eingebettet. Auf Basis der SRS der gesamten sicherheitsbezogenen Steuerung wird zunächst die Software-Design-Spezifikation 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, die von der Software zu implementierende Fehlererkennung einschließlich der Reaktion bei erkannten Fehlern, Schnittstellen zu anderen Teilsystemen, Abhängigkeiten von Betriebsarten usw. Zusätzlich werden alle nach Abschnitt 7.3.1 der Norm für PL c oder d geforderten fehlervermeidenden Maßnahmen festgelegt. Die Software-Design-Spezifikation wird dann z. B. vom „Projektleiter Sicherheit“ gegengelesen (Review) und gegebenenfalls werden Änderungen eingepflegt. Nach Freigabe der Software-Design-Spezifikation kann das Software-System-Design 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.

Das Design der Softwarearchitektur wird in der Software-System-Design-Spezifikation (Pflichtenheft zum Modul-Design) festgelegt. 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 Verifizierung der Codierung festgelegt. Die Planung von Software-Integrationstests wird ebenfalls in diesem Dokument festgeschrieben. Nach einem erneuten Review z. B. durch den „Entwicklungsleiter Software“ wird das Pflichtenheft als Vorgabe für das Modul-Design freigegeben. In diesem Review wird auch verifiziert, ob die Anforderungen der Software-Design-Spezifikation erfüllt sind.

Das Design der erforderlichen Softwaremodule und Funktionen zur Realisierung der oben beschriebenen Software wird in der Modul-Design-Spezifikation (Pflichtenheft zur Codierung) festgelegt. Die Planung von Modultests wird ebenfalls in diesem Dokument festgeschrieben. Nach einem Review wird das Pflichtenheft als Vorgabe für die Codierung freigegeben.

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) Verifizierung des fertigen Codes gegen die Modul-Design-Spezifikation (Pflichtenheft) führen Programmierende im Kollegenkreis einen 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 dem Modul-Design 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 Software-Integrationstest kann sich ergeben, dass der Mikrocontroller nicht so leistungsfähig ist wie vorher angenommen. In diesem Fall muss die Softwarearchitektur, konkret die zeitliche Einplanung der Tasks und auch die Zuordnung von Funktionen zu den Tasks, geändert werden. Die Software-Design-Spezifikation wird sich dadurch nicht ändern. Aber das Software-System-Design und Modul-Design muss angepasst und erneut einem Review unterzogen werden, um die Übereinstimmung mit der Software-Design-Spezifikation zu gewährleisten. Dies ist ein Beispiel dafür, wie notwendige technische Änderungen während der Entwicklung zu einem erneuten Durchlauf des V-Modells führen, damit die Änderungen qualitätsgesichert umgesetzt werden. Die Änderungen werden codiert und die Modultests sowie Software-Integrationstests müssen erneut durchgeführt werden.

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

9.13 Software in der Maschinenverordnung (EU) 2023/1230

Die Maschinenverordnung (EU) 2023/1230 enthält neu das Sicherheitsbauteil „Software, die Sicherheitsfunktionen wahrnimmt“. Für das Sicherheitsbauteil Software ist vorgesehen, dass der Hersteller die erforderliche Konformitätsbewertung mit dem Verfahren der internen Fertigungskontrolle (Modul A nach Anhang VI) durchführt. Eine Ausnahme bilden Software bzw. Systeme mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens, die Sicherheitsfunktionen gewährleisten. Solche Software bzw. Systeme fallen in den Anhang I, Teil A und machen die Einbindung einer notifizierten Stelle z. B. für eine EU-Baumusterprüfung zwingend. In den meisten Fällen wird sicherheitsrelevante Software jedoch Bestandteil einer Maschine bzw. deren Steuerung oder eines zugehörigen Produktes sein und somit unter den jeweils dafür geltenden Bestimmungen Gegenstand der Konformitätsbewertung sein. Eine solche Software erfüllt auch nicht die Definition eines Sicherheitsbauteils, da sie nicht gesondert in Verkehr gebracht wird. Ändert ein Betreiber die sicherheitsrelevante Software einer Maschine gilt es zu prüfen, ob daraus eine wesentliche Veränderung resultiert, was der Fall sein könnte, wenn eine neue Gefährdung entsteht oder sich ein bestehendes Risiko erhöht. Diese hätte dann außer bei Eigengebrauch durch nichtprofessionelle Nutzer eine neue Konformitätsbewertung zur Folge.

10 Verifikation und Validierung

Änderung gegenüber dem IFA Report 2/2017

- Der gesamte Abschnitt wurde überarbeitet, die inhaltliche Struktur wurde enger an den Ablauf des V&V-Prozesses angelehnt, eine neue Liste der relevanten Aspekte gibt eine einleitende Übersicht.
- Auf Fragen zur Vorqualifizierung von Teilsystemen wird eingegangen.
- Die Dokumentationsprüfung zu Modifikationsverfahren wird neu aufgegriffen.
- Das Beispiel zur Verifikation und Validierung der Planschneidemaschine wurde aktualisiert.

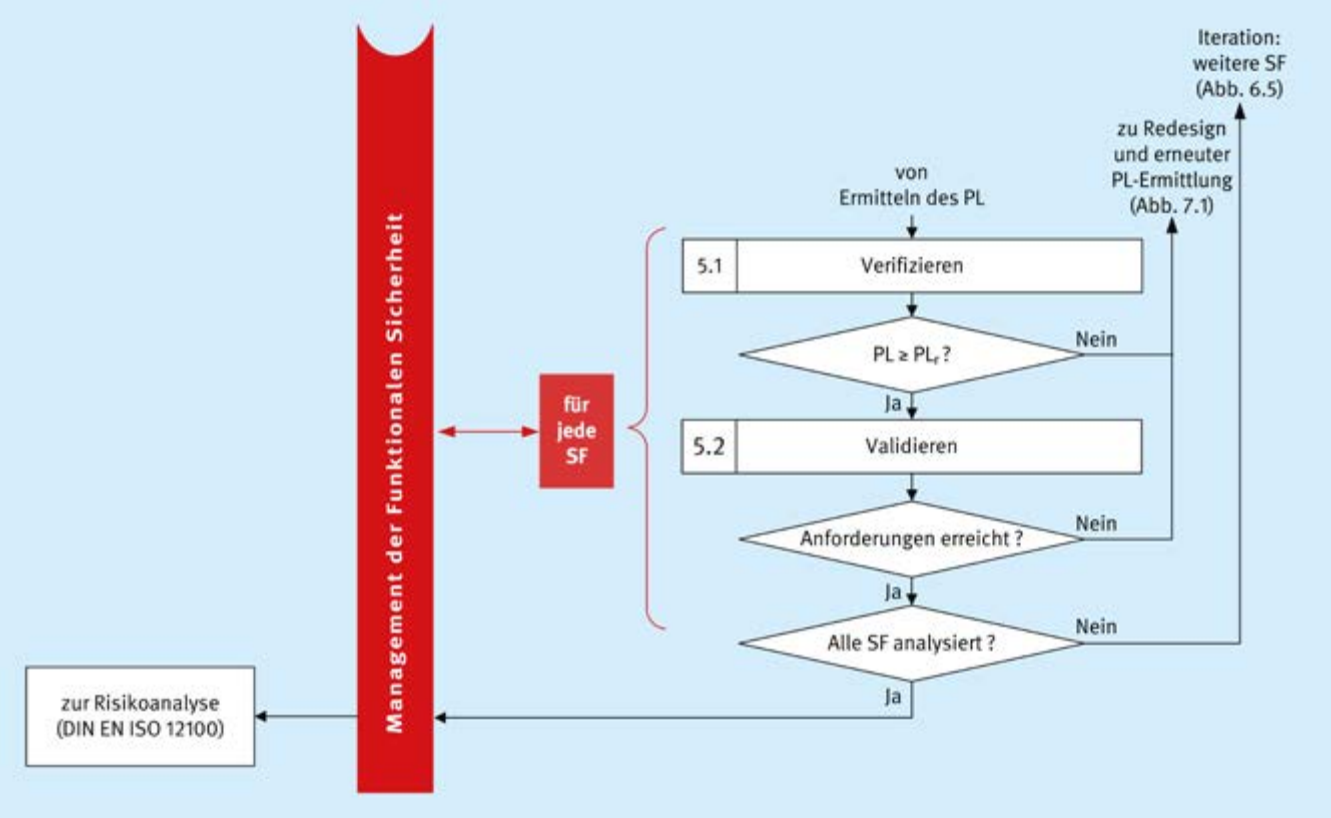


Abb. 10.1 V&V-Anbindung im Entwicklungsprozess

DIN EN ISO 13849-1 [7] behandelt in ihrer Neufassung auch umfassend das Thema Validierung. Die nun enthaltenen Anforderungen zu Verifikation und Validierung (V&V) im Entwicklungsprozess ersetzen mit Ausnahme der informativen Anhänge die Anforderungen aus DIN EN ISO 13849-2 [8]. In der Anwendung der Validierung wird dem Teil 1 nun Priorität gegeben und Teil 2 noch stärker ein erläuternder Part übertragen. Da der Sachstand zur Validierung jedoch weitgehend unverändert geblieben ist, kann für den Übergang bis zur Neufassung von Teil 2 davon ausgegangen werden, dass die Validierungsanforderungen des neuen Teils 1 auch erfüllt werden, wenn jene aus dem bestehenden Teil 2 umgesetzt sind. Mit der Übertragung in den normativen Teil ist V&V im Entwicklungs- und Integrationsprozess sicherheitsbezogener Teilsysteme und SRP/CS nun deutlich betont. Auch wenn die Norm das Validieren des SRP/CS beschreibt, sind die dort genannten Anforderungen auch auf das Verifizieren und Validieren von Teilsystemen anzuwenden, die nach der Norm entwickelt werden. Die Anwendung der entsprechenden Aktivitäten ist Bedingung dafür, eine Übereinstimmung mit DIN EN ISO 13849 zu erreichen. Dieser Abschnitt des Reports soll die Anwendung der Norm in Bezug auf Verifizieren und Validieren unterstützen.

V&V sind elementare Maßnahmen zur Fehlervermeidung und Qualitätssicherung in einem SRP/CS-Entwicklungsprojekt mit dessen Teilen und Inhalten Spezifikation, Systemauslegung (Entwurf), technische Realisierung (Umsetzung) und Begleitdokumentation. Sie leisten einen wesentlichen Beitrag zur Vermeidung und Aufdeckung systematischer Fehler, angefangen bei Denkfehlern beim

Spezifizieren bis zu Umsetzungsfehlern, z. B. bedingt durch ungeeignete Entwicklungswerkzeuge.

Verifikation und Validierung eines sicherheitsbezogenen Steuerungssystems, eines Teilsystems oder Teilbereiche davon nehmen die folgenden Aspekte in den Fokus:

Mit Verifizieren und Validieren fokussierte Aspekte

- jede in der Spezifikation der Sicherheitsanforderungen (SRS) enthaltene Anforderung,
- die Ausführung aller für das SRP/CS spezifizierten Sicherheitsfunktionen oder für Teilsysteme spezifizierten Teilfunktionen; für jede Sicherheitsfunktion werden alle spezifizierten Merkmale, Kennwerte, Eigenschaften, Bedingungen, Ablaufverhalten und Schnittstellen – also die vollständige Definition – relevant,
- Rückwirkungs- bzw. Wechselwirkungsfreiheit, Priorisierung und Reihenfolge bei mehreren gleichzeitig aktiven Sicherheitsfunktionen als auch bei gleichzeitig aktiven Standardfunktionen, insofern diese gemeinsam auf Teilsystemen implementiert sind,
- die Sicherheitsintegrität (Wirksamkeit der Sicherheitsfunktionen) in Form des erreichten Performance Levels (PL) über die Kennwerte: Kategorie (Architektur, Fehlertoleranz, Sicherheitsprinzipien etc.), $MTTF_D$-, *DC*- und *PFH*-Werte zusammen mit den eingesetzten Maßnahmen zur Vermeidung von Ausfällen infolge gemeinsamer Ursache (CCF), den Maßnahmen gegen systematische Ausfälle und zur Vermeidung systematischer Fehler in der sicherheitsbezogenen Software,
- das Verhalten unter Fehlerbedingungen (Ausfallverhalten) zusammen mit den technischen, auch softwaretechnischen Maßnahmen der selbsttätigen Fehlerdiagnose (Ausfallerkennung) einschließlich Fehlerakkumulation bzw. Mehrfachfehlerannahme auch mit Ausfall einer Diagnose bei Kategorie 4.

Darüber hinaus:

- als Teil der jeweiligen Sicherheitsfunktion oder separat die Ausführung der Mensch-SRP/CS-Schnittstelle und -Interaktion,
- als Teilaspekt der Sicherheitsfunktion sämtliche Zustandswechsel, Einschalten und Hochlauf, Neustart etc. und als Teilaspekt des Verhaltens im Fehlerfall: Einnehmen und Verlassen des Fehlerzustandes,
- als Eigenschaft der Sicherheitsfunktion deren funktionale sowie technisch-konstruktive Maßnahmen zum Schutz vor Umgehung (Manipulation) bzw. auch vor vorhersehbarer Fehlanwendung,
- die Funktion unter Betriebsbeanspruchung und Umgebungsbedingungen (Grenzbedingungen),
- die Begleitdokumentation.

Die Verifikation (das Verifizieren) umfasst Analysen und Tests für SRP/CS bzw. deren Teilaspekte und Teilsysteme, die feststellen, ob die erzielten Resultate einer Entwicklungsphase bzw. eines Konstruktionsabschnitts den Vorgaben für diese Phase entsprechen. Beispielsweise wird beurteilt, ob das Schaltungslayout dem Schaltungsentwurf entspricht oder ob in der Spezifikation die für die vorgesehenen Anwendungen relevanten Anforderungen umfassend (d. h. vollständig) zusammengestellt sind und ob eine Kombination/Integration von Teilsystemen korrekt erfolgt.

Die Verifikation ist also ein Verfahren der Überprüfung, ob die spezifizierten Sicherheitsanforderungen (als Eingaben) im Entwicklungsprozess entlang der Entwicklungsschritte mit deren Ergebnissen (als Ausgaben) erfüllt sind. Damit wird festgestellt, ob die Ergebnisse der einzelnen Phasen im Entwicklungsprozess korrekt und vollständig im Sinne der gestellten Anforderungen sind. Verifizieren beginnt bei der Spezifikation (SRS). Fehler und Abweichungen sollen frühzeitig erkannt werden, was nicht allein mit der Frage verknüpft ist, ob der erreichte PL dem PL_r entspricht, so wie es mit einem kurzen Blick auf Abschnitt 8 und Bild 4 der DIN EN ISO 13849-1 interpretiert werden könnte. Die vereinfachte Darstellung der Aktivität des Verifizierens in Box 5.1 der **Abbildung 10.1** entspricht daher genaugenommen mehreren Verifikationsschritten, die in den Entwicklungsprozess integriert sind. Typische, hier beispielhaft genannte Methoden des Verifizierens sind: Inspektion, Review, Walk-through, formale/mathematisch-modellbasierte Verifikation, Simulation, Emulation, statische Analyse, dynamische Analyse, Black-Box-Test, Grey-Box-Test und White-Box-Test, Funktionsprüfung als Integrationstest (für Teilsysteme, Komponenten, Module, Hardware mit Software, Parametrierungswerkzeug mit Komponente, einschl. der Schnittstellen) und Funktionsprüfung als Systemtest. Andere in der Literatur genannte Verfahren wie Prototyping oder enge Releasezyklen werden im Kontext funktionaler Sicherheit nicht als probate Verifikationsaktivitäten angesehen.

Als Validierung (Validieren) wird die Nachweisführung darüber bezeichnet, ob eine Eignung bezogen auf die gestellten Anforderungen und für die beabsichtigte Verwendung gegeben ist. Es wird also während oder am Ende des Ent-

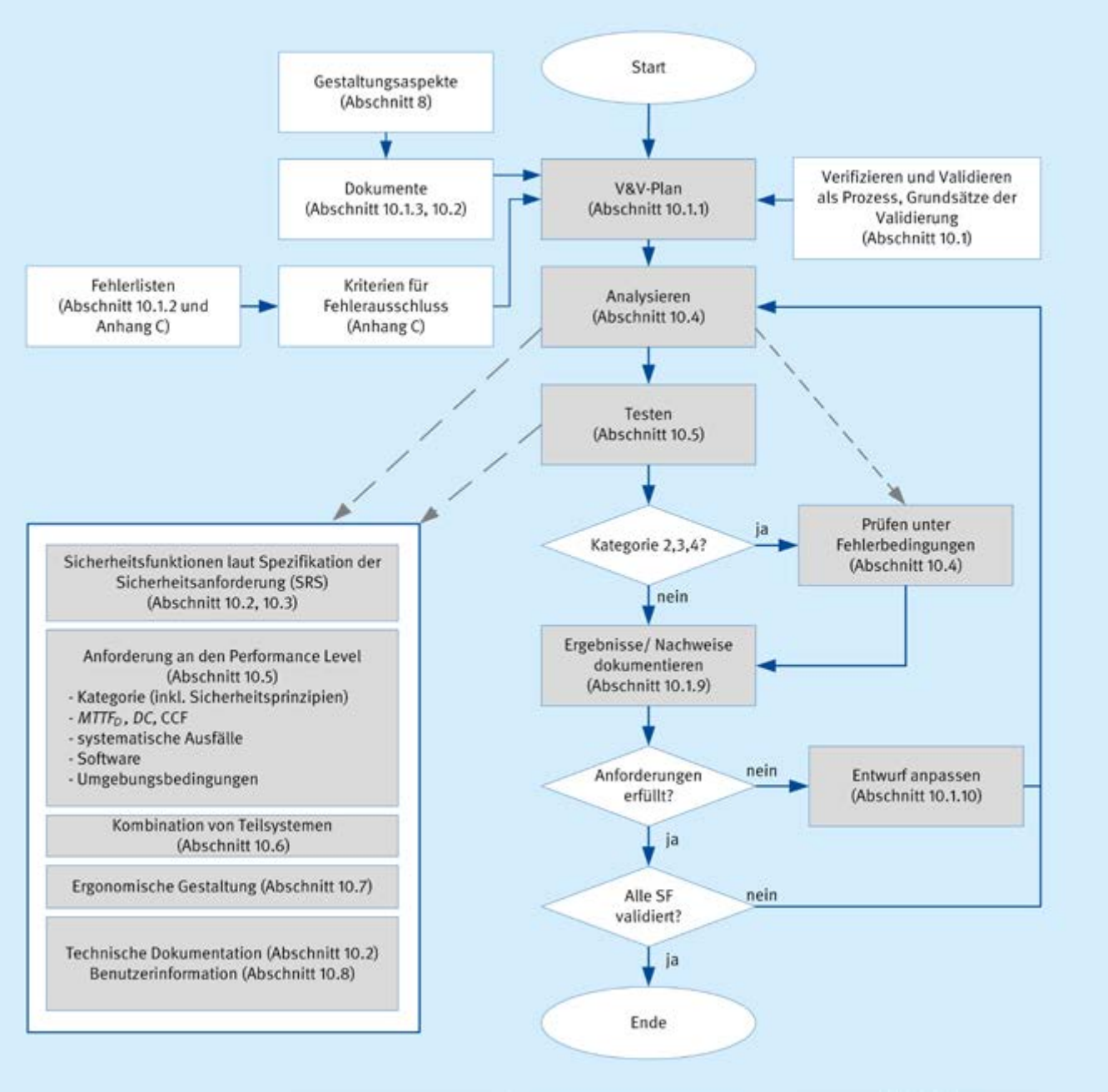


Abb. 10.2 Übersicht zum Verifikations- und Validierungsprozess

wicklungsprozesses überprüft, ob im Allgemeinen die spezifizierten funktionalen und konstruktiven Anforderungen an den sicherheitsrelevanten Teil der Maschinensteuerung erreicht wurden, bzw. im Konformitätskontext der DIN EN ISO 13849, ob das SRP/CS für jede Sicherheitsfunktion die entsprechenden Anforderungen dieser Norm erfüllt.

Typische, hier beispielhaft genannte Methoden der Validierung sind: Funktionsprüfung als Systemtest für die Sicherheitsfunktion mit deren Leistungsmerkmalen und -daten, erweiterte Funktionsprüfung mit ungewöhnlichen, unerwarteten und besonderen Testfällen, Ausfalleffektprüfung (entspricht dem Testen durch Fehlerimplementierung), Funktionsprüfung unter Betriebs- und Umgebungsbedingung (Umweltprüfung, Störfestigkeitsprüfung) und Teilfunktionsprüfung der Mensch-System-Schnittstelle.

Eine erweiterte Funktionsprüfung ist unter Umständen mit entsprechenden Analyse- oder Testfällen auch dazu geeignet, die Immunität gegen mögliche Einflüsse bzw. Rückwirkungen durch die Maschinensteuerung (den nicht sicherheitsrelevanten Teil) festzustellen.

Statistische Prüfungen (Tests), die in anderen Branchen bei Akzeptanztests von Sicherheitssystemen Verwendung finden, sind bei SRP/CS nicht anwendbar. Sogenannte Assessments, wie sie in der Anlagentechnik und Prozessindustrie regelmäßig zur Anwendung kommen, sind in der DIN EN ISO 13849 nicht vorgesehen. Ebenso wenig die dort typischen Wiederholungsprüfungen (sog. Proof Tests), bei denen Komponenten manuell überprüft und gewartet werden.

10.1 Das Verfahren der Verifikation und Validierung

Der Prozess der Beurteilung einer Sicherheitsfunktion in ihrer Realisierung durch SRP/CS ist also ein Zusammenspiel aus Verifikations- und Validierungsschritten, das sowohl Teilaspekte und Teilsysteme behandelt als auch die Gesamtheit des SRP/CS zum Gegenstand hat.

Dieses Kapitel hat das Ziel, die Planung der Durchführung von V&V-Aktivitäten mit den dort relevanten Tätigkeiten und einem sinnvollen Vorgehen informativ zu unterstützen. Die Norm selbst gibt zwar Anforderungen, aber kein eigenes Durchführungsverfahren mit dezidierten (festen) V&V-Aktivitäten vor. Damit liegt es in der Verantwortung des Herstellers, mit den Zielen und allgemeinen Anforderungen der Norm bzgl. Planung, Durchführung und Dokumentation von Analysen und Tests diese auszuführen und Nachweise davon bereitzustellen (siehe **Abbildung 10.2**).

Der Prozess der Verifikation und Validierung liegt mit der Planung, Lenkung und Überwachung in der Verantwortung des Managements der Funktionalen Sicherheit, wo auch der Übergang zum Qualitätsmanagement der Entwicklung organisiert sein soll. Im Kontext der DIN EN ISO 13849 ist V&V auf SRP/CS beschränkt. Die Norm befasst sich nur am Rande mit der Validierung auf Maschinenebene (Gesamtvalidierung und Zusammenführung mit dem nicht sicherheitsbezogenen Teil der Maschinensteuerung), die auch für jede individuelle Maschine bzw. jeden spezifischen Maschinentyp gefordert wird. An dieser Stelle setzt die Validierung der Auswirkungen der Integration von SRP/CS auf die verbleibende Steuerung und deren Rückwirkungsfreiheit auf SRP/CS auf Maschinenebene an. Informationen und Anforderungen hierfür werden in der Regel über die relevante C-Norm abgedeckt. Maßnahmen und Methoden der V&V sind nicht abhängig vom PL abgestuft; z. B. durch eine Mindestanzahl für Testfälle. Über einen ausreichenden Umfang wird in der V&V-Planungsphase entschieden. Das Verhältnis von Analysen und Tests darf in Abhängigkeit von Technologieaspekten und dem PL gewählt werden. Hierbei ist die Verfügbarkeit von Analyse- und Testwerkzeugen ebenso ein Auswahlaspekt. Weitere Orientierungen zur Festlegung der V&V-Aktivitäten finden sich in diesem Kapitel.

Verifikation und Validierung sind nicht ersetzbar durch andere fehlervermeidende Maßnahmen in der Konstruktion (z. B. den Einsatz bewährter Bauteile bei Hardware oder der Verwendung einer Programmiersprache mit eingeschränktem Sprachumfang bei Software).

Jede für die Konstruktion, Entwicklung oder Herstellung eines SRP/CS verantwortliche Organisationseinheit muss mit ihrem Management der Funktionalen Sicherheit dafür Sorge tragen – und hierfür bestmöglich Leitsätze aufstellen –, dass Fehler während der Verifizierung und Validierung (z. B. durch Instrumentierungen) vermieden werden bzw. diese offenkundig werden und daraus keine Auswirkungen auf die Sicherheit der SRP/CS resultieren.

10.1.1 Verifikations- und Validierungsplan

Ein Verifikations- und Validierungsplan ist dazu vorgesehen, die Durchführung des V&V-Verfahrens auszulegen und zu beschreiben. Eine Konformität mit DIN EN ISO 13849 setzt die Anwendung eines V&V-Verfahrens voraus, legt jedoch weder Form noch Inhalt im Detail dafür fest. In einem V&V-Plan werden alle den Entwicklungsverlauf begleitende V&V-Aktivitäten verbindlich festgelegt. Er sollte folgende Angaben enthalten:

- Identifikationen der betrachteten SRP/CS, ggf. ihrer Komponenten sowie möglicher Varianten und Variationen,
- Identifikation der Sicherheitsfunktionen mit Zuordnung der beteiligten SRP/CS und Teilsysteme,
- Referenzenliste aller Bezugsdokumente (einschließlich der anzuwendenden Normen und technischen Regeln) mit Anforderungsbeschreibungen, Spezifikationen und Lasten aus dem Anwendungsbereich zum betrachteten SRP/CS sowie firmeninterne Gestaltungsregeln wie eigene Hardwaredesignregeln und Programmierregeln (als Programmierleitfaden),
- Referenzenliste der anzuwendenden Prüfnormen. Dies sind Normen zu Prüfverfahren und zur Prüfungsdurchführung, nicht zu Produktanforderungen (beispielsweise die DIN EN 60068-Reihe zu Umgebungseinflüssen),
- die durchzuführenden Analysen und Tests; ggf. mit zusätzlichen Hinweisen auf eine erforderliche Abfolge,
- Kennzeichnung, ob und welche Konformitäten und Qualifizierungen für einzelne Komponenten oder Teilsysteme bereits vorliegen; mit Nennung der Verweise auf die früheren Nachweisdokumente,
- anzuwendende Fehlerlisten (siehe auch Abschnitt 10.1.2),
- weitere Referenzen zu Dokumenten mit Bezug zur Erstellung von Nachweisen; z. B. QM-Handbuch, Verfahrensanweisungen, Vorlagen/Muster für V&V-Aktivitäten,
- für die jeweiligen Analysen und Tests verantwortliches Personal (Person, Abteilung oder Stelle/ggf. Prüfstelle),
- einzuhaltende Prüfungs-Umgebungsbedingungen und einzusetzende Ausrüstung, Prüfmittel, Werkzeuge oder Hilfsmittel zur Durchführung der Analysen und Tests sowie weitere einzuhaltende Betriebsbedingungen; diese Angaben können auch in den Ergebnisdokumenten der einzelnen V&V-Aktivitäten aufgelistet sein,
- die Identifikation der zu erstellenden Ergebnisdokumentation (Bericht bzw. Protokolle) sowie der weiterführenden Dokumentation zur Durchführung der V&V-Aktivitäten (z. B. Prüfspezifikationen, Test(fall) spezifikationen, Checklisten),
- Bewertungskriterien für Analyse- und Testergebnisse einschließlich der Maßnahmen, die durchzuführen sind, wenn eine Analyse bzw. ein Test nicht bestanden wurde (wahlweise auch als Annahme-/Freigabekriterien bezeichnet),

- formale Aspekte (Metadaten) mit Projektbezug, Dokument-Identifikation, Version/Stand und Änderungshistorie, Autoren/Verantwortliche, Freigabevermerke, Unterschriften etc.

Den V&V-Plan erstellt man sinnvollerweise in einer frühen Entwicklungsphase – zu empfehlen ist parallel zur Spezifikation. Zudem ist es bewährte Praxis, den V&V-Plan durch eine im Bereich des Qualitätsmanagements oder Managements der Funktionalen Sicherheit kompetente Person überprüfen zu lassen.

Es besteht die Möglichkeit, im V&V-Plan festzuhalten, welche Validierungen erst nach einem Einbau in eine Maschine leistbar sind. Ebenfalls kann vermerkt werden, ob hierfür ersatzweise Simulationen (z. B. per „Hardware-in-the-loop Simulation“) vorgesehen werden sollen oder müssen. Die Eignung, Angemessenheit und Leistungsfähigkeit der zum Einsatz kommenden V&V-Methoden muss vom Management der Funktionalen Sicherheit (im Plan der Funktionalen Sicherheit) bestätigt, d. h. freigegeben worden sein. V&V-Plan und Plan der Funktionalen Sicherheit können nach Festlegung des Herstellers separat erstellt werden oder in einem Dokument zusammengefasst sein.

10.1.2 Fehlerlisten

Im V&V-Prozess ist das Verhalten des SRP/CS bei Ausfällen zu beurteilen. Die Grundlage einer Fehlerbetrachtung ist die Fehlerliste, die alle zu betrachtenden Fehler (im Sinne anzunehmender Fehler) zusammen mit den anwendbaren Fehlerausschlüssen enthält. In der DIN EN ISO 13849-2 sind diese in den Anhängen A bis D zu finden. Im Anhang C dieses Reports werden zu Fehlerlisten, anzunehmenden Fehlern, Ausfallarten und Fehlerausschlüssen weitere Informationen gegeben. Diese allgemeinen Fehlerlisten stützen sich auf Erfahrungen und wurden im fachlichen Konsens festgelegt. Die Norm DIN EN 61508-2:2011 [57] zur Funktionalen Sicherheit programmierbarer elektronischer Systeme enthält im Anhang A.2, Tabelle A.1, noch einige Präzisierungen zu Fehlern z. B. bei CPU, RAM, ROM und Takt. Weitere Normen, z. B. zu sicherheitsbezogener Datenübertragung, dienen als Fundstellen für spezifische Technologien oder Baugruppen. Für eine Teilsystementwicklung im Rahmen der DIN EN ISO 13849 kann ggf. noch das Fehlermodell für hochintegrierte Bauteile der Mikroelektronik (Mikroprozessoren, DSP, ASIC, FPGA, SoC, etc.) relevant werden oder von Interesse sein. Vorteilhaft ist es, wenn zur Fehlerdiagnose Standardmaßnahmen – in Software und Hardware – verwendet werden. Solche Standardmaßnahmen, z. B. für Speicher-Selbsttests namens „Galpat“, „March“, „Checkerboard“ etc. oder für IEC 61508-/IEC 26262-Anwendungen kommerzialisierte Watchdog-/Überwachungsbausteine, sind exakt auf die beschriebenen Ausfallarten ausgelegt. Für Bauteile, die in den Fehlerlisten der DIN EN ISO 13849-2 nicht enthalten sind, sollen eigene spezielle Fehlerlisten mit anzunehmenden Fehlern und Fehlerausschlüssen in vergleichbarer Weise ergänzt werden. Um Fehlerausschlüsse geltend machen zu können, müssen diese ausreichend begründet sein. Der Teil individuell ergänzter Fehlerlisten zählt dann zu der zu bewertenden technischen Dokumentation.

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

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

10.1.3 Dokumente für V&V-Aktivitäten

Für die Durchführung jeder V&V-Aktivität sind eingehende technische Dokumentationen erforderlich. Diese – insbesondere die Spezifikationen – sind dann im gesamten V&V-Verfahren oder nur bei einzelnen Analysen und Tests einzusetzen. Empfohlen ist, auf ausreichend dokumentierte Inhalte zu achten, die beispielweise in folgender Form vorliegen können:

- vollständige Spezifikation der Anforderungen an die Sicherheitsfunktionen sowie der Anforderungen an den Entwurf des SRP/CS; die Beschreibung der Anforderungen muss alle Bemessungsdaten, Leistungsmerkmale, Eigenschaften, Betriebsarten, Zustands- und Ablauferwartungen enthalten, aus denen Bewertungskriterien abzuleiten sind, darunter u.a. Betriebs- und Umgebungsbedingungen mit Bemessungsdaten, die sich aus den vorgesehenen Anwendungen bzw. aus anzuwendenden Normen ergeben,
- Funktionsbeschreibung zur Ausführung sämtlicher Sicherheitsfunktionen mit Zustands- und Ablaufbeschreibungen; die Behandlung von Ausfällen/Fehlern im SRP/CS, d.h. die Reaktionen und Zustände des SRP/CS bei den möglichen Ausfall-/Fehlerarten, ebenso das Bedienkonzept mit allen Interaktionen,
- Konstruktionsbeschreibung der SRP/CS (mit Spezifikationen für eingesetzte mechanische, elektrische, elektronische, hydraulische und pneumatische Bauteile) mittels angemessener Zeichnungen/Skizzen, Diagramme, Pläne, Daten, Nennwerte und erläuternden Texten; dies sind z. B. Übersichtszeichnungen, Struktur-/Blockdiagramme, Ablauf-/Zustandsübergangsdiagramme, Verdrahtungspläne und Anschluss- bzw. Schnittstellenbeschreibungen, Prinzipschaltpläne, Schaltpläne, Elektropläne, Fluid(schalt)pläne, Montagepläne, Tabellen

technischer Daten bzw. Bemessungsdaten für Komponenten, ggf. Datenblätter,
- Ausfalleffektanalyse (FMEA/FMEDA) unter Berücksichtigung der angewandten Fehlerlisten; für Kategorie 4 einschließlich Fehleranhäufung,
- ausführliche Beschreibung der getroffenen technischen Maßnahmen zur Fehlerbeherrschung (Fehlerdiagnosemaßnahmen),
- Darstellung der bei der Gestaltung berücksichtigten grundlegenden und bewährten Sicherheitsprinzipien und für den Entwurf und der Realisierung zugrunde gelegte Gestaltungsregeln wie Designregeln für Analog- und Digitalschaltungen, Programmierrichtlinien u. ä.,
- Angabe der getroffenen Maßnahmen gegen systematische Ausfälle,
- vollständige Softwaredokumentation (siehe auch Kapitel 9),
- dokumentierte Ermittlung der quantifizierbaren Werte *PFH*, Kategorie, Ausfallraten, $MTTF_D$, *DC* und CCF für den PL. Ggf. Nachweise zu erreichten Zuverlässigkeits-Kennwerten, wenn diese auf eine andere Weise als der nach DIN EN ISO 13849 erreicht wurden,
- Nachweise (Zertifikate, Prüfberichte, Ergebnisprotokolle) zu bereits validierten Bauteilen, Komponenten, Software-Bibliotheken oder Teilsystemen sowie Angaben und ggf. Nachweise zu bewährten Bauteilen; aus diesen muss ersichtlich sein, dass die Ergebnisse auch die Verwendung in der angestrebten Applikation zulassen,
- vollständige Begleitinformation (Montage-/Einbau-, Betriebs- und Wartungs-/Instandhaltungsanleitung), ggf. Kurzanleitungen und andere Begleitmedien
- spezifische weitere Dokumentation, sofern sie für die Validierung notwendig sind, z. B. bei Werkstoffanalysen.

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

10.1.4 Analysen

Die Beurteilung eines SRP/CS, Teilsystems oder dessen Teilaspekte erfolgt neben Tests auch durch Analysen. Dabei kommen sowohl manuell leistbare Analysemethoden zum Einsatz wie Inspektionen, Reviews oder Walk-throughs für die Spezifikation, von technischen Unterlagen, der Benutzerinformationen und Prozessbeschreibungen (hier z. B. des Modifikationsprozesses) als auch werkzeuggestützte Analysen wie die Schaltungssimulation, statische und dynamische Hardware-/Softwareanalyse, FMEA-/FMEDA, Fehlersimulation und modellbasierte Simulation. Virtuelle Verfahren werden zukünftig als weitere neue Analyseverfahren und Analysewerkzeuge hinzukommen. Die Entscheidung, wo sich verschiedene einzelne analytische Verfahren ergänzen müssen und wo Tests erweiternd zur Anwendung hinzukommen, erfolgt beim Management und wird im V&V-Plan dokumentiert.

10.1.5 Tests

Tests kommen zumeist anhand real ausführbarer Entwicklungsstufen wie Prototypen, Funktionsmuster oder Code bei Software zum Nachweis der korrekten Funktion zur Anwendung. Aber auch dort, wo in einer FMEDA Unsicherheit über die möglichen Auswirkungen einzelner Ausfälle besteht, kann durch Testen mit Fehlerimplementierung das reale Systemverhalten festgestellt werden – erfahrungsgemäß auch mit von der FMEDA abweichenden Ergebnissen. Die Testverfahren stehen auf den verschiedenen Integrationsebenen als Modultest, Schnittstellentest, Integrationstest und Systemtest zur Verfügung und werden mit zunehmender Testtiefe als Funktionstest, Black-Box-Test, Grey-Box-Test und White-Box-Test durchgeführt. Sogenannte Leistungstest oder Stresstests stellen keine grundsätzlich anderen Verfahren dar. In jeder V&V-Planung ist für alle betreffenden Teilaspekte eine in Umfang, Tiefe und Entwicklungs-/Konstruktionsabschnitt passende Strategie für Tests auszulegen. Die Testergebnisse erlangen eine umso höhere Aussagekraft, je näher sie an der vorgesehenen Betriebskonfiguration durchgeführt werden – unter welchen Bedingungen ist vorher in der Planung festzulegen. Eine automatisierte, werkzeuggestützte Durchführung von Tests ist ebenso möglich wie eine manuelle.

10.1.6 Validierung von Teilsystemen mit einer Vorqualifizierung nach DIN EN ISO 13849

Bei Teilsystemen mit einer formell belegten Übereinstimmung mit DIN EN ISO 13849 ist zu ermitteln, welche Validierungsfälle bei der Integration des Teilsystems noch anstehen. Dazu zählen auch alle Einstellungen, Konfigurationen, Parametrierungen und Anwendungsprogrammierungen mit Einfluss auf Eigenschaften der Sicherheitsfunktion. Aufgabe der V&V-Planung ist es, diesen Umfang zu identifizieren und dafür V&V-Aktivitäten festzulegen. Bestmöglich wird die Validierung am Teilsystem bzw. der Sicherheitskomponente selbst vorgenommen, da sich nach Integration mit weiteren Teilsystemen in der Regel Einschränkungen bei der Bewertbarkeit oder beim Bewertungsumfang ergeben.

10.1.7 Validierung von Teilsystemen, die mithilfe anderer Normen der Funktionalen Sicherheit entwickelt wurden

Die Möglichkeit Teilsysteme in SPR/CS einzusetzen, die mit einer anderen Norm für funktionale Sicherheit entwickelt wurden, ist in gleicher Weise wie in 10.1.6 gegeben. Im Fall einer Sicherheits-SPS mit Zertifizierung gemäß IEC 61508 oder DIN EN 61131-6 [58] treffen die noch notwendigen Validierungsaktivitäten auf alle Elemente der Anwendungssoftware (Programm, Variablen) zu. Dies setzt voraus, dass für das gewählte Anwendungssoftware-Entwicklungswerkzeug ein Konformitätsnachweis vor-

liegt. Für die sicherheitsrelevante Anwendungssoftwareentwicklung gelten die zutreffenden Anforderungen von DIN EN ISO 13849 wiederum als Maßstab. Liegen bereits validierte Anwendungssoftwareelemente (Funktionen, Funktionsbausteine, Bibliotheken, etc.) vor, gilt für diese gleichfalls das Folgende:

Für Teilsysteme, die für funktionale Sicherheit validiert sind, z. B. mit MPLa (Machine Performance Level) nach DIN EN ISO 19014-1, mit AgPL (Agricultural Performance Level) nach DIN EN ISO 25119-1, mit SIL nach IEC 61511, mit ASIL (Automotive Safety Integrity Level) nach ISO 26262 oder als High Availability Software nach EN 50128, muss festgestellt werden, ob die Einzelanforderungen des maßgeblichen PL nach DIN EN ISO 13849 erreicht sind. Zu dessen Analyse ist die Verwendung einfacher Vergleichs- oder Korrelationstabellen mit Entsprechungen zwischen PL, MPLa, AgPL, SIL und ASIL allein nicht ausreichend, ebenso wenig wie eine Übereinstimmung einzig anhand der angegebenen *PFH* anzunehmen ist. Gegenstand der vergleichenden Analyse muss u. a. auch der geleistete Validierungsumfang sein. Ein allgemein gültiges Analyseschema hierfür kann an dieser Stelle jedoch nicht skizziert werden; sind die Differenzen zwischen DIN EN ISO 13849 und anderen Branchenspezialisierungen doch zu groß. Im Fall einer bereits nach DIN EN IEC 62061 [10] erfolgten Validierung vereinfacht sich die Analyse zur Umsetzung der Einzelanforderungen, da diese weitgehend mit denen aus DIN EN ISO 13849 kompatibel sind. Das Analyseergebnis, das zum einen den Teil der Übereinstimmung bei Einzelanforderungen wiedergibt, muss zum anderen alle sich nicht entsprechenden Eigenschaften bzw. nicht abgedeckte Anforderungen darstellen. Alle Einzelanforderungen der letzteren Gruppe werden zum Gegenstand der Planung von V&V-Aktivitäten für das Teilsystem.

10.1.8 Verifikation und Validierung von Teilsystemen, Hardware oder Software mithilfe von (zertifizierten) Werkzeugen

Werden bei der SRP/CS- oder Teilsystementwicklung Werkzeuge zur Verifikation oder Validierung eingesetzt, müssen deren Leistungseigenschaften im Detail bekannt, d. h. beschrieben sein. Dies betrifft auch Teilaufgaben des Testfalldesigns, über die eigentliche Ausführung bis zur Aufzeichnung (Ergebnisberichte) sowie kommerzielle dedizierte Analyse- und Test-Produkte, in Werkzeuge der Entwicklungsumgebungen integrierte Funktionen oder in Eigenentwicklung erstellte Lösungen (Automaten, Softwarewerkzeuge etc.). Diese Dokumentation soll Teil der allgemeinen technischen Dokumentation sein. Mit ihr soll auch eine Einschätzung zum Vollständigkeitsgrad der geplanten und realisierten Test- und Analysefälle möglich werden. Im Rahmen des Managements der Funktionalen Sicherheit wird festgelegt, ob und für welche Aufgaben die Werkzeuge geeignet sind.

DIN EN ISO 13849-2 adressiert mit den informativen Anhängen A bis D “Validierungswerkzeuge” für mechanische, pneumatische, hydraulische und elektrische Systeme. Sie führt darin allerdings weder Empfehlungen zu Werkzeugtypen noch zu Anforderungen auf, die von Test-/Analyse-Werkzeugen zu erfüllen sind. Hier liegt der Fokus auf der Validierung der Kategorieanforderungen mithilfe der Tabellen “Grundlegende Sicherheitsprinzipien”, “Bewährte Sicherheitsprinzipien”, “Bewährte Bauteile” und “Fehler und Fehlerausschlüsse”. Die Norm IEC 61508 ist, wenngleich auf elektrische und elektronische Systeme begrenzt, bei der Beschreibung von Anforderungen informativer. Sie behandelt Werkzeuge zum Zweck der Spezifikation, des Entwurfs, des Testens und des Konfigurations- oder Änderungsmanagements sogar im normativen Teil. Im Kontext von V&V-Werkzeugen ist eine informelle Anleihe bei IEC 61508 also empfehlenswert. Die darin allgemein formulierten Anforderungen an Werkzeuge betreffen die Übersichtlichkeit der Bedienung und Funktionalität samt Verständlichkeit (Durchschaubarkeit) für Anwendende, die Korrektheit und Wiederholbarkeit von Ergebnissen und die Anwendung entsprechender Qualitätssicherungsmaßnahmen (z. B. Kalibrierung). Die Messunsicherheiten bei Nachweisen durch Prüfung müssen der DIN EN ISO 13849-2 folgend angemessen sein. Sie gibt Hinweise auf einzuhaltende Grenzen.

Bei der Auswahl sind betriebsbewährte Werkzeuge zu bevorzugen. Sofern zertifizierte Werkzeuge zur Verfügung stehen, vereinfacht deren Einsatz den Nachweis der Eignung. In jedem Fall ist die (reale) Leistungsfähigkeit des Werkzeugs ein zu priorisierendes Auswahlkriterium. Die Norm kennt bzw. benennt keine Grenzen in Bezug auf Technologien. Somit stehen viele moderne Werkzeuge offen, so u. a. die XIL-Techniken (XIL: X-in-the-Loop) für Modelle (MIL), Software (SIL), Hardware (HIL), Prozessor (PIL) sowie für die Testumgebung und Simulation.

Im Entwicklungsprojekt müssen selbstverständlich ebenso die manuellen werkzeugunterstützten V&V-Aktivitäten in der Planung erfasst und die Ergebnisse dokumentiert werden. Ein Beispiel hierfür sind FME(D)A-Tools zur Unterstützung der systematischen Erfassung des Ausfallverhaltens.

10.1.9 Ergebnis-/Nachweisdokumentation (Validierungsbericht)

Alle im V&V-Plan festgelegten und mit ergänzenden Angaben versehenen Analyse- und Testaktivitäten erhalten für ihre Durchführung, Ergebnisse und Bewertung die entsprechende Dokumentation. Es steht zur Wahl, ob ein zentraler, alle Aktivitäten umfassender Bericht oder jeweils ausführliche Einzeldokumente und ein zusammenfassender Bericht erstellt werden. Hierbei ist es wichtig (dies zur Hilfestellung hier gelistet), dass die herangezogenen Anforderungsspezifikationen und Beurteilungsgrundlagen mit ihrer Version referenziert werden und das

unter Analyse/Test stehende Objekt (Dokument, Software, Prüfling, Teilsystem etc.) eindeutig identifiziert wird. Eingestellte Konfigurationen müssen festgehalten, die Analyse-/Testbedingungen samt verwendeter Analyse-/Testwerkzeuge (Prüf-/Messmittel), Aufbau und Ablauf wiedergegeben und alle Verifikations-/Validierungspunkte/-fälle samt Ergebnissen aufgezeichnet werden. Formale Angaben wie Dokumentidentifikation, Durchführende, Datum, Unterschrift etc. dürfen natürlich ebenso wenig fehlen wie, als Referenz, der versionierte V&V-Plan, aus dem vorbereitend die Vorgaben für die jeweiligen Aktivitäten stammen. Je nach Automationsgrad und zum Einsatz kommender Werkzeuge wird auch die Ergebnisdokumentation variieren. Jedoch sollten die genannten Inhalte als minimaler Dokumentationsumfang im Validierungsbericht gelten. Sind umfangreiche Einzelaufzeichnungen (Nachweise) entstanden, genügt die Ergebnisnotation samt Referenz auf entstandene Protokolle, Dateien etc. mit den Details – diese selbstredend versioniert. Alle von Zulieferern oder Dritten zur Geltung kommenden Ansprüche auf Übereinstimmung mit den Sicherheitsanforderungen – das können Zertifikate, Prüfberichte u. a., ggf. Datenblätter sein – sind Bestandteil der Ergebnisdokumentation. Ein Dokumentationsmanagement ist also auch aus den Bedarfen des V&V-Verfahrens abgeleitet angemessen. Jedwede Unterstützung mit Hilfsmitteln hierfür, z. B. Protokollvorlagen bis zum Dokumentenmanagementsystem, dürfen als wertvoll angesehen werden.

10.1.10 Abschluss oder Iteration

Wurden die V&V-Aktivitäten für alle Sicherheitsfunktionen mit dem Ergebnis abgeschlossen, dass alle Anforderungen umgesetzt wurden, so ist nach Norm deren Bewertung abgeschlossen. Ansonsten muss das V&V-Verfahren mit den noch offenen Sicherheitsfunktionen und deren Kombinatorik fortgesetzt werden, siehe auch Kapitel 10.3. Im Fall, dass nicht alle in der SRS festgelegten Anforderungen erfüllt sind, d. h. negative Analyse- oder Testergebnisse vorliegen, wird im Rahmen des Managements der Funktionalen Sicherheit entschieden, ob die Prüfung fortgeführt werden kann oder ob eine Änderungsanforderung zu stellen ist.

Eine Änderungsanforderung identifiziert die Bestandteile des V&V-Verfahrens, die nicht bestanden wurden, benennt, wohin im Gestaltungs- und Realisierungsprozess zurückgesprungen wird, und ordnet zu, mit welchen V&V-Aktivitäten dieser neu zu durchlaufen ist. Hierzu kann der V&V-Plan geeignete Elemente enthalten und benennen.

Im Management des Entwicklungsprozesses muss also der Fall negativer Ergebnisse berücksichtigt sein. Bei in Serie hergestellten und einzeln in Verkehr (in den Markt) gebrachten SRP/CS oder Teilsystemen schließt dies die Herstellung (Fertigung) bis zur Auslieferung ein. Der Hersteller muss hier einen QM-Prozess mit Maßnahmen vorweisen, um abzusichern, dass die sicherheitsbezogenen Anforderungen der DIN EN ISO 13849 von allen ausgelieferten Stücken/Einheiten eingehalten bzw. Fehler aufgedeckt werden. Ein Vorbild für den Prozess kann der DIN EN ISO 9001 [59] entstammen, die (Qualitäts-)Kriterien stehen jedoch im Kontext der Anforderungen von DIN EN ISO 13849. Das geforderte Management schließt die relevante Dokumentation, Konfigurationen, Personal und Ressourcen allgemein ein.

10.2 Verifizieren der Spezifikation und der Technischen Dokumentation

Das auch für die Validierung eines SRP/CS oder Teilsystems grundlegende Dokument neben der DIN EN ISO 13849 selbst ist dessen SRS bezüglich der Sicherheitsfunktionen und Sicherheitsintegrität zusammen mit der vorgesehenen Verwendung, den vorgesehenen Betriebs- und Umgebungsbedingungen und den Angaben der Verwendungsgrenzen. Zur besseren Handhabung als auch Sorgfalt in puncto Vollständigkeit ist es bewährte Praxis, Sicherheitsanforderungen systematisiert zu erfassen (z. B. per Nummerierung) und mit Zuweisungen zu versehen. Rückverfolgbare Referenzierungen erleichtern den Prozess der V&V-Aktivitäten genauso wie den Entwurfsprozess selbst.

In Bezug auf die sicherheitsrelevanten funktionalen Eigenschaften und die Sicherheitsintegrität haben alle Anforderungen der Norm die höchste Priorität, insbesondere vor individuellen Kundenanforderungen an die Funktion. In der Spezifikation sollten daher die Anforderungen an die funktionale Sicherheit klar erkennbar sein und von anderen Anforderungen getrennt sein.

Eine Verifikation der Spezifikation (SRS) erfolgt als Inspektion und Review. Bewährt hat sich hierbei eine Zweiteilung in der Vorgehensweise – zum einen und zuerst die Verifikation durch erfahrenes Personal beim Hersteller selbst und zusätzlich durch eine kompetente externe Person, Stelle oder ggf. eine Prüfinstitution mit einem höheren Grad der Unabhängigkeit. DIN EN ISO 13849 beschränkt anders als weitere Normen zur Funktionalen Sicherheit das Maß der Unabhängigkeit auf nicht an dem Entwurf beteiligte Personen. Dies gilt für alle V&V-Aktivitäten, nicht nur die Bewertung von Dokumentationen.

Eine Verifikation der Technischen Dokumentation schließt die in DIN EN ISO 13849-1, Abschnitt 12 gelisteten Entwicklungs-/Konstruktionsdokumente (bzw. Inhalte) ein. Als Verifikationsaktivitäten sind Analysen angemessen. Inspektion, Review und Walk-through gelten als typische Methoden hierzu. Bei Bedarf können u. a. in IEC 61508-7 [51] kurze Erläuterungen zu diesen Methoden nachgelesen werden.

10.3 Validieren der Sicherheitsfunktion(en)

Das Validieren einer Sicherheitsfunktion bezieht sich auf deren Bestandteile (auslösendes Ereignis, sicherheitsgerichtete Reaktion, gefahrbringendes Maschinenteil) und Leistungsmerkmale (z. B. Nachlaufzeit) zusammen mit den Grenzen bzw. den Grenzmerkmalen (z. B. den Verwendungsgrenzen). Hierzu gehört die umfassende Funktionsprüfung jeder Sicherheitsfunktion. Validiert werden alle Sicherheitsfunktionen separat als auch in der beabsichtigten Kombination, wenn mehrere Sicherheitsfunktionen gleichzeitig aktiv sein können. Hierbei muss das Erreichen der gestellten Anforderungen zur Priorisierung, zu zeitlichen Vorgaben und der Wechselwirkungsfreiheit Gegenstand von Validierungsfällen sein, einschließlich der Rückwirkungsfreiheit nicht sicherheitsgerichteter Funktionen/Teilfunktionen und Daten im selben Teilsystem auf Sicherheitsfunktionen. Dieses Erfordernis geht aus DIN EN ISO 13849-1 nicht klar hervor, darf aber keinesfalls versäumt werden. Neben einer dementsprechenden Analyse sind insbesondere der Schnittstellentest und die erweiterte Funktionsprüfung dafür geeignet. Bestandteil der Validierung sind in jedem Fall die Schnittstellen (hier der Funktionen). Die typischen Validierungsaktivitäten umfassen den Funktionstest, den sogenannten erweiterten Funktionstest (mit Testfällen zum Verhalten des SRP/CS bei unüblichen, nicht erwarteten, im Ablauf inkorrekten oder außerhalb der Spezifikation liegenden bzw. ungültigen Eingangssignalen, Bedienungsabläufen oder Benutzereingaben) und den Leistungstests (funktionale Kennwerte, Reaktionszeit, etc.). Validieren von Sicherheitsfunktionen mittels Simulation erlangt zunehmende Bedeutung bzw. Aufmerksamkeit. Wenn Simulationen jedoch nur eingeschränkte Rückschlüsse auf das Verhalten des realen SRP/CS in realen Einsatzbedingungen zulassen, sollten diese nur ergänzend ausgeführt werden.

Zur Validierung der Sicherheitsfunktion an der Maschine gehören eine Reihe weiterer Aspekte, z. B. die Bemessung von Nachläufen und Sicherheitsabständen. Aus der vorgesehenen Verwendung der Maschine leiten sich dann noch die Validierungsfälle unter den vorgesehenen Betriebs- und Umgebungsbedingungen ab.

10.4 Verifizieren und Validieren des Verhaltens unter Fehlerbedingungen

Die wirksamsten Aktivitäten zur Identifizierung gefahrbringender Ausfälle, die zum Verlust der Sicherheitsfunktion bzw. deren Eigenschaften oder Leistungsmerkmalen führen können, sind Ausfalleffektanalyse unter Einbeziehung der Diagnose FMEDA und die Tests durch Fehlerimplementierung. Beide schließen eine Bewertung der Diagnosefunktionen mit deren Diagnosefähigkeit und die Reaktionsfunktion mit ein. Sie gehören damit zum Pflichtprogramm einer Bewertung der Maßnahmen zur Vermeidung systematischer Ausfälle und der Eigenschaft zur Fehlerbeherrschung. Mit den Ausfalltests wird zudem verifiziert, ob die vorhergesagten Ausfallarten und Ausfalleffekte der FMEDA richtig enthalten sind. In welcher Tiefe die Prüfungen vorzunehmen sind – ob nur an Schnittstellen der Teilsysteme, Komponenten oder sogar Bauelemente –, ist in der DIN EN ISO 13849 nicht explizit vorgegeben. Wenn das Ausfallverhalten nicht vorab vollständig bestimmt ist, so muss die Betrachtungseinheit genauer untersucht werden. Eine höhere Aussagekraft der Testfälle wird mit steigendem PL und beanspruchtem Diagnosedeckungsgrad erforderlich. Als qualitatives Ziel gilt, dass die spezifischen Fehler und Ausfälle, die in den referenzierten Fehlerlisten angesprochen werden, betrachtet werden. Die zur Anwendung kommenden Methoden sind austauschbar, z. B. eine Fehlerbaumanalyse (FTA) anstelle einer FMEA. Die Bewertung zufälliger Hardwarefehler und systematischer Ausfälle kann auch analytisch, per Simulation oder Emulation erfolgen. Entscheidend bei der Methodenauswahl ist deren Leistungsfähigkeit zusammen mit der Kompetenz des Personals sie einzusetzen. Bei allen Analysefällen ist die Notation des Fehler-Reaktionsverhaltens, insbesondere bei Kombination mehrerer Teilsysteme und bei komplexen Systemen, nicht trivial. Sie muss der Spezifikationen der Fehlerreaktion entsprechen und sollte reproduzierbar sein. Die Einnahme oder ggf. Aufrechterhaltung des definierten sicheren Zustandes muss Gegenstand der SRP/CS-Validierung sein, d. h. für alle Analyse-/Testfälle bestätigt werden können. Bei Relevanz schließt dies auch die maximale Fehlerreaktionszeit, also die Zeitdauer vom Ausfalleintritt bis zum Erreichen des sicheren Zustands, ein. Für einfehlersichere Steuerungsstrukturen muss der Nachweis auch den Teilaspekt beinhalten, dass die Sicherheitsfunktion mit Vorhandensein eines Fehlers weiterhin ausführbar bleibt, d.h. die Kanäle sich im Fehlerfall nicht gegenseitig beeinträchtigen. Jede von der Norm abweichende Ausfallart, ggf. das Ausfallmodell, eine individualisierte Wirkungskette oder ein anderer Fehlerzustand, muss spezifiziert und validiert werden. Ein degradierter Fortbetrieb bei fehlertoleranten Strukturen ist in der DIN EN ISO 13849 nicht vorgesehen.

10.5 Verifizieren des PL

Bei der Bewertung der erreichten Sicherheitsintegrität geht es um die umgesetzten Anforderungen zur Kategorie und den probabilistischen Kennwerten $MTTF_D$ (mittlere Zeit bis zum gefährlichen Ausfall eines Kanals in Jahren), *DC* (Diagnosedeckungsgrad) und CCF (Abschätzungen der Ausfälle infolge gemeinsamer Ursache) sowie der *PFH*. Die in der Entwicklung vorgenommene Berechnung wird hier abschließend überprüft. Bei Teilsystemen entfällt die Verifikation des PL in den Fällen, in denen die benötigten Sicherheitsintegritäts-Kennwerte vom Hersteller dokumentiert vorliegen (z. B. mittels Prüfbescheinigung). Bei selbst entwickelten Teilsystemen soll beurteilt werden,

ob die Bestimmungsmethoden für die *PFH* und die Kennwerte $MTTF_D$, *DC* und CCF korrekt angewendet wurden und die errechneten Ergebnisse bis zur *PFH* und zum PL plausibel sind. Die Anwendung eines zweiten Werkzeugs oder Hilfsmittels zur Abschätzung der probabilistischen Kennwerte des PL wird empfohlen, sofern kein validiertes oder ausreichend betriebsbewährtes Werkzeug bei der Entwicklung genutzt wurde. Im einfachsten Fall wird für die eigentlichen Berechnungen ein solch validiertes Werkzeug, z. B. SISTEMA, verwendet. So muss nur noch eine Plausibilisierung aller Kennwerte für jede Sicherheitsfunktion als Verifizierung vorgenommen und bestätigt werden. Verifizieren des PL umfasst dann natürlich noch die getroffenen Maßnahmen zu systematischen Ausfällen und speziell zu sicherheitsbezogener Software, siehe folgend 10.5.1 bis 10.5.6

10.5.1 Verifizieren der Kategorie

Ziel ist es zu bestätigen, dass im jeweiligen Entwicklungsschritt alle an die Kategorie gestellten Anforderungen erfüllt werden. Folgende Analysen werden hierzu in der Regel durchgeführt:

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

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

10.5.2 Verifizieren der $MTTF_D$-Werte

Die zur Bestimmung des PL eingesetzten $MTTF_D$-Werte sollen mindestens auf ihre Plausibilität überprüft werden. Dazu zählt typischerweise die Beurteilung, ob geeignete Quellenangaben zur Herkunft der Werte vorliegen und genaue Begründungen der Werte enthalten sind. Dazu können u. a. die im Anhang D genannten Datenquellen herangezogen werden. Die Zuverlässigkeitsdaten von Bauteilen plausibilisieren sich bestmöglich über das jeweilige Datenblatt, ansonsten über einen Vergleich mit weiteren Quellen. Für die Werte B_{10D}, T_{10D} und n_{op} wird deren angemessene Bestimmung analytisch nachvollzogen und abschließend die korrekte Berechnung mindestens auf Plausibilität kontrolliert.

10.5.3 Verifizieren der *DC*-Werte

Für die angesetzten Diagnosedeckungsgrade (Prozentwerte) soll ein Review mit qualitativer Abschätzung erfolgen, ob die individuell entwickelten Diagnosemaßnahmen diese beanspruchten Werte auch erreichen können. Dabei ist besonders bei *DC*-Maßnahmen mit einer Spanne erreichbarer *DC*-Werte zu einem konservativen Ansatz geraten. Als Gegenkontrolle eignet sich die Abschätzung der Rate der zufälligen Hardwareausfälle, die einen gefahrbringenden Systemausfall hervorrufen können und nicht durch Diagnose entdeckt werden. Die Kontrolle schließt die Überprüfung der spezifizierten Diagnoseintervalle ein, die seit der vierten Ausgabe der Norm den *DC*-Schätzwert nach Tabelle E.2 dieses Reports limitieren können. Bei programmierbarer Hardware stehen ggf. vorqualifizierte Diagnosemaßnahmen mit bekanntem Diagnose-Deckungsgrad, wie Selbsttest-Bibliotheken, zur Verfügung. Deren Verifikation muss nicht wiederholt werden.

Zusammen mit den Tests zum Verhalten des SRP/CS unter Fehlerbedingungen (Ausfalleffektprüfung bzw. Tests durch Fehlerimplementierung) nach Abschnitt 10.4 soll gezeigt werden, dass durch die Diagnosemaßnahmen auch eine korrekte Fehleraufdeckung gegeben ist.

10.5.4 Verifizieren der Maßnahmen gegen CCF

Zur Bewertung der ausgewählten Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) beschreibt Anhang F dieses Reports ein Verfahren basierend auf einem Punkteschema. Neben der Kontrolle für das Erreichen der Gesamtpunktzahl und der Klärung, dass die ausgewählten Maßnahmen in den entsprechenden Dokumenten umfassend beschrieben und begründet sind, wird durch Analyse oder Test gezeigt, dass die Maßnahmen tatsächlich umgesetzt wurden. Zu den typischen V&V-Aktivitäten zählen hierzu ergänzend die statische Hardwareanalyse und die Funktionsprüfung unter Umgebungsbedingungen (Grenzbedingungen).

10.5.5 Verifizieren der technischen Maßnahmen zur Vermeidung und Beherrschung von systematischen Ausfällen

Für systematische Ausfälle sind die exakten Auswirkungen und damit die spezifischen Ausfallarten oder Ausfallmodelle und Ausfallraten oder Anteile ungefährlicher Ausfälle nicht vorauszusagen. Damit gibt es auch keine quantifizierbare Kenngröße zur Wirksamkeit von Gegenmaßnahmen wie einen Diagnosedeckungsgrad für diesen Anteil möglicher Ausfälle zu bestimmen und zu verifizieren. Die auslösenden Ursachen für systematische Ausfälle werden über entsprechende Entwurfsmaßnahmen, Maßnahmen im Herstellungsprozess und im Zusammenhang mit der betriebs- und umgebungsbedingten Beanspruchung weitgehend vermieden. Auf eine systematische

Eignung von Komponenten zu achten, ist also ein elementarer Aspekt in der Entwicklung. Verifizieren bedeutet an diesem Punkt Kontrollen durchzuführen, u. a. zu den umgesetzten Sicherheitsprinzipien, aber auch zu den festgelegten Einsatzgrenzen. Alle spezifizierten und entwickelten technischen Maßnahmen (z. B. Diagnosefunktionen) zur Beherrschung zufälliger Fehler wie systematischer Ausfälle werden auf ihre Wirksamkeit hin geprüft. Mit Entwicklungswerkzeugen realisierte Maßnahmen zur Fehleraufdeckung erfordern keine zusätzlichen Nachweise, wenn diese Leistungsumfänge ausgewiesen und validiert oder zertifiziert worden sind. Gleiches trifft auf softwarebasierte Werkzeuge zur Parametrierung zu (vergl. Abschnitt 6.3.4 von DIN EN ISO 13849-1), bei denen ebenso Verifizierungsaktivitäten gefordert sind oder alternativ eine Bestätigung der Eigenschaften bzgl. der geforderten Fehlervermeidung bzw. Fehlererkennung vorhanden ist. Ein Verifizierungsschwerpunkt bei Software (SRASW und SRESW) sollen deren programmiertechnische Möglichkeiten zur Fehlererkennung wie Programmlaufüberwachung, Plausibilitätsprüfungen, Zustandsbewertungen, Datenintegritätsprüfungen und Zusicherungen/Vorbedingungen (englisch: Assertions) sein. Bei Hardware sind dies Überwachungsmaßnahmen, Diversität und Schutzbeschaltungen bei der Energieversorgung und an Schnittstellen. Die Beachtung des grundlegenden Sicherheitsprinzips der Überdimensionierung bei der Auswahl von Bauteilen gehört zu den Basismaßnahmen einer funktional sicheren Entwicklung. Die Verifikation hierzu liegt hauptsächlich in der Analyse der vorhandenen Implementierung und Bestätigung ihrer Wirksamkeit zur Fehlerbeherrschung. Für organisatorische Maßnahmen zur Vermeidung systematischer Ausfälle in der Entwicklung, der Herstellung und dem Betrieb sind entsprechend Managementaktivitäten (bzw. Prozesse) zu beurteilen.

10.5.6 Verifizieren und Validieren der sicherheitsbezogenen Software

Sicherheitsbezogene Software als integraler Bestandteil des SRP/CS oder eines Teilsystems erfordert Verifikations- und Validierungsmaßnahmen zu Software-Sicherheitsanforderungen im Entwicklungsprozess und im Modifikationsprozess.

An dieser Stelle wird auf die speziellen Angaben zu diesem Thema in Abschnitt 9 dieses Reports verwiesen. Mit dem IFA Report 1/2020 „Praxisgerechte Umsetzung der Anforderungen für sicherheitsbezogene Embedded-Software nach DIN EN ISO 13849-1“ [7] und dem IFA Report 2/2016 „Sicherheitsbezogene Anwendungssoftware von Maschinen“ [13] sind sowohl zu SRESW als auch SRASW Veröffentlichungen des IFA verfügbar, die u. a. auf Verfahren der Software-Verifikation und Software-Validierung ausführlich eingehen.

Eine besondere Herausforderung besteht im Nachweis, dass in Software realisierte Sicherheitsfunktionen von nicht sicherheitsbezogenen Funktionen nicht bzw. nicht kritisch beeinflussbar sind (vergl. Abschnitt 7.1 von DIN EN ISO 13849-1). Jede Softwaremodifikation führt hier unweigerlich zur notwendigen Einflussanalyse und ggf. zur Neuverifikation. Teilen sich beide Softwareteile dieselbe Hardware-Umgebung, so ist der Einsatz vorqualifizierter Betriebsmittel wie Echtzeit-Betriebssysteme für Sicherheitsanwendungen (sog. Safety RTOS) zu empfehlen. Deren Vorteil besteht u. a. genau in dieser inhärenten Eigenschaft und damit einhergehend einer erheblichen Aufwandsreduktion bei Nachweisen auch zur Rückwirkungsfreiheit.

10.6 Verifizieren der Kombination von SRP/CS-Teilsystemen

Die einzelnen Teilsysteme des SRP/CS sind vor der Kombination separat zu prüfen. Um systematische Fehler während der Kombination bzw. Integration von Teilsystemen zu vermeiden, sind folgende sich ergänzende, aber nicht austauschbare V&V-Aktivitäten typisch:

- Inspektion der Konstruktionsdokumente, die insgesamt die Realisierung der jeweiligen Sicherheitsfunktion beschreiben,
- Abgleich der Kenndaten/Leistungsdaten der Schnittstellen zwischen den Teilsystemen und Schnittstellentest,
- Ausfalleffektanalyse, ggf. unter Einbeziehung der Diagnose (FMEDA), bezogen auf die Kombination bzw. Integration,
- Funktionstest und erweiterter Funktionstest,
- Kontrolle der vereinfachten Bestimmung des Gesamt-PL aus den PL der einzelnen SRP/CS-Teilsysteme wie in Abschnitt 7.2 beschrieben.

Integration von mehreren SRP/CS-Teilsystemen bedeutet noch nicht deren Inbetriebnahme mit der dazugehörenden Inbetriebnahmeprüfung an einer Maschine.

10.7 Verifizieren und Validieren der Mensch-System-Schnittstelle (Benutzerschnittstelle)

Zur relevanten Schnittstelle der Mensch-SRP/CS-Interaktion samt Eingabe-/Bedien- und Anzeige-Komponenten beschränkt sich DIN EN ISO 13849-1 im Abschnitt 9 auf eine knappe Darstellung von Anforderungen zu Entwurfsaspekten der Ergonomie. Es werden Referenzen für Leitlinien zur Ergonomie angegeben, nach denen dann auch die Validierung erfolgen sollte. Spezifische Validierungsfälle davon richten sich auf die explizit genannten Vorkehrungen zur technisch-funktionalen Verhinderung ungewollter Bedienungsfehler. Vorgaben zur ergonomischen Gestaltung der sicherheitsbezogenen Benutzerschnittstelle beziehen sich

in DIN EN ISO 13849 auf universelle Gestaltungsziele, wie die Vorbeugung vor gefährlichem Handeln und Umgehen der SRP/CS bzw. deren Manipulation, sowie auf allgemeine ergonomische Prinzipien wie Einfachheit, Benutzerfreundlichkeit und Mitbetrachtung menschlicher Faktoren, die mit DIN EN ISO 12100 [5] auch referenziert werden. Die Eignung von Gegenmaßnahmen und deren Umsetzung gilt es mit der Validierung zu bestätigen.

Benötigt man bei der Verifikation ergonomischer Aspekte der Benutzerschnittstellen über die in DIN EN ISO 12100 Abschnitt 6.2.8 verwiesenen Normen hinaus weitere Grundlagen, so kann die Anwendung von Gestaltungsleitlinien, z. B. der Richtlinie VDI/VDE 3850 „Gebrauchstaugliche Gestaltung von Benutzungsschnittstellen für technische Anlagen“ [34], des VDMA-Leitfadens „Software-Ergonomie, Gestaltung von Bedienoberflächen“ [52] oder der Normen DIN EN ISO 9241-11 „Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte“ [53] hilfreich sein.

Bei allen Elementen der Mensch-Maschine-Schnittstelle wie Befehlsgeber, Stellteilen etc., die Anteil an einer Sicherheitsfunktion haben, müssen diese selbstverständlich mit verifiziert und validiert werden. Dies kann ebenso auf Anzeigemittel zutreffen wie bei der Muting-Zustandsanzeige der Muting-Funktion von berührungslos wirkenden Schutzeinrichtungen, wenn an diese bestimmte Anforderungen gestellt sind.

10.8 Verifizieren der Benutzerinformation

Die Begleitdokumentation bzw. Benutzerinformation (mit Betriebsanleitung, Montageanleitung, Instandhaltungsanleitung etc.) beschreibet u. a. den sicheren Betrieb des SRP/CS sowie die Phasen Inbetriebnahme und Instandhaltung. Dort werden Validierungsfälle auf SRP/CS-Ebene und ggf. für die Gesamtvalidierung der Maschine verbindlich festgelegt. In aller Regel müssen die Validierungsfälle in der Begleitdokumentation identifiziert und per Inspektion und/oder Review auf Angemessenheit bzw. spezifische Eignung analysiert werden.

Für Instandhaltungsaufgaben werden in den meisten Fällen eigene Betriebsarten und ggf. auch Sicherheitsfunktionen festgelegt. Deren Validierung bereits mit der Entwicklung des SRP/CS und eine Verifikation der Dokumentation zur Durchführung ist Bestandteil der V&V-Aktivitäten.

10.9 Beurteilung der Modifikationsverfahrensbeschreibung

Jede Modifikation am SRP/CS oder eines der Teilsysteme in der Betriebsphase ist dann noch einmal eine spezielle Phase für V&V-Aktivitäten. Eine Modifikation wird im Rahmen des Managements der Funktionalen Sicherheit aufgegriffen, gelenkt und freigegeben. Festzulegen sind u. a. alle Validierungsaktivitäten sowohl für den Fall anwendungsnaher Änderungen (im Sinne einer Wiederinbetriebnahme) als auch für den Fall entwicklungsrelevanter Änderungen, z. B. nach Ausfällen im Betrieb, mit Wiederholungs-Verifikationen und -Validierungen bei der Änderungs-Realisierung, dem Entwurf und ggf. auch der Spezifikation dafür.

Bei der Verifikation der Beschreibungsteile in der Begleitinformation ist neben den zu Modifikationen notwendigen Tätigkeiten mit den entsprechenden Verantwortlichkeiten noch der neu oder wiederholt durchzuführenden Verifikation und Validierung des SRP/CS Aufmerksamkeit zu widmen. Erwartungsgemäß enthält die Begleitdokumentation nur den Teil der anwendungsnahen Modifikationen. Für entwicklungsrelevante Änderungen am SRP/CS sind weitergehende Beschreibungen wie der Sicherheitsplan und ggf. die spezifische Prozessdokumentation zu analysieren.

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

Begleitend zur allgemeinen Beschreibung der Verifikation und Validierung von Sicherheitsfunktionen und PL werden in diesem Abschnitt die V&V-Aktivitäten am praktischen Beispiel der Planschneidemaschine aus den Abschnitten 6.8 und 8.4 erläutert. An dieser Stelle wird unterstellt, dass alle notwendigen Dokumente und ein Prototyp der Maschine vorhanden sind. Auf Basis der Dokumente sollen hier stellvertretend für eine der Sicherheitsfunktionen, „SF2 – Ortsbindung der Hände des Bedieners außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung“ (Abschnitt 6.8.3), die Schritte der Verifikation und Validierung gezeigt werden. Zu den vorhandenen Dokumenten gehört auch der Verifikations- und Validierungsplan, der die jeweils notwendigen Aktivitäten in den verschiedenen Phasen beschreibt (Abschnitt 10.1.1). Aufgrund der Höhe des Gefährdungspotenzials ist es ratsam, die Arbeiten durch unabhängige Personen, z. B. aus einer anderen Abteilung, durchführen zu lassen.

In diesem Abschnitt soll die Definition für Verifikation und Validierung aus der Einleitung zu diesem Kapitel verwendet werden. Oft sind die Grenzen jedoch unscharf und eine exakte Zuordnung ist schwierig. So wird z. B. das Testen von Software, um festzustellen, ob Programme oder Programmteile den spezifizierten Zweck erfüllen, in der Literatur auch der Validierung zugeordnet. Nach dem in diesem Kapitel beschriebenen Verständnis wäre es auch möglich, diese Schritte als Verifizierungsaktivität zu bezeichnen.

10.10.1 Verifizieren des erreichten PL

Anhand einer Risikoeinschätzung wurde ermittelt, dass für die auszuführende Sicherheitsfunktion SF2 ein erforderlicher PL_r e erreicht werden muss. Diese Analyse steht im Einklang mit der Forderung aus DIN EN 1010-1 [54], die im Verweis auf die Anforderungen der entsprechenden Norm zu Zweihandschaltungen DIN EN ISO 13851 [55] die technischen Anforderungen weiter präzisiert. In der Systemspezifikation sind die zu erfüllenden Randbedingungen genannt und durch eine Validierung bestätigt worden. Die jetzt stattfindende Verifikation bestätigt die korrekte Umsetzung der Vorgaben, hier durch die Bestimmung der quantifizierbaren Aspekte des PL unter Zuhilfenahme des Softwaretools SISTEMA. Auch werden alle Anforderungen an die qualitativen Aspekte wie das Verhalten der Sicherheitsfunktion unter Fehlerbedingungen, einschließlich der umgesetzten fehlererkennenden Maßnahmen in der sicherheitsbezogenen Software, die Maßnahmen gegen systematische Ausfälle und das Verhalten unter Umgebungsbedingungen für einen PL e hinreichend erfüllt.

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

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

10.10.2 Validieren der sicherheitsbezogenen Anforderungen

Fehlerlisten

Bei der PL-Bestimmung werden die Fehlerlisten nach DIN EN 13849-2 [8] zugrunde gelegt.

Dokumente

Wie bereits in Abschnitt 10.1.3 erwähnt bilden Schaltpläne, Stücklisten, die vollständige Spezifikation, Funktionsbeschreibung, die Konstruktionsbeschreibung, Fehler-/Fehlerauswirkungsanalyse, die Softwarespezifikation und Softwaredokumentation u. a. die Grundlage für die Analyse bzw. Prüfung.

Dokumentation

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

Validieren der Sicherheitsfunktion

Zur Überprüfung der funktionalen Anforderungen an die Sicherheitsfunktion wird ein Funktionstest, ergänzt um einen erweiterten Funktionstest, durchgeführt, um das Verhalten der Sicherheitsfunktion bei seltenen oder nicht festgelegten Eingaben zu überprüfen. Ein Beispiel für einen solchen Test könnte die Überprüfung der Reaktion des SRP/CS sein, wenn zu einer gültigen Schnittanforderung der Zweihandschaltung ein Fehlersignal, z. B. an der Peripherie oder durch einen Stoppbefehl, ausgelöst durch ein Lichtgitter erfolgt. Weiter werden Leistungstests zu funktionalen Aspekten durchgeführt. Hierzu zählt z. B. die Überprüfung der nach der Norm DIN EN ISO 13851 einzuhaltenden Zeit für eine synchrone Betätigung. Nur wenn beide Stellteile S1 und S2 in einem Zeitabschnitt ≤ 0,5 Sekunden betätigt werden, dürfen Ausgangssignale zur Ansteuerung des Pressbalkens und des Messers erzeugt werden.

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

Verifikation des PL des SRP/CS

- Verifikation der Kategorie:

Auf Basis der SRS sind in einem frühen Stadium der Entwicklung wesentliche Weichenstellungen zur Kategorie des SRP/CS erfolgt. Zum ermittelten PL_r e wurde ebenfalls die Kategorie 4 gewählt. Die Verifikation der Schaltungsstruktur (diversitäre Redundanz, siehe auch Abschnitt 8.4.2) ergab, dass diese den Anforderungen für eine Kategorie 4 genügt.

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

gen Prüfprotokoll wird für jeden Fehlereinbau die erwartete sicherheitsgerichtete Reaktion beschrieben und das Verhalten des SRP/CS mit dem Bewertungskriterium „bestanden“ oder „nicht bestanden“ kommentiert.

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

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

- Verifikation der $MTTF_D$-Werte:

Beispielhaft für die Verifikation der $MTTF_D$-Werte wird hier der für die Ventile 1V3, 1V4, 2V2 und 2V1 angesetzte Wert von 150 Jahren betrachtet (siehe Abbildung 8.8). Die Angabe des Herstellers entstammt einer zuverlässigen Quelle und wurde durch Vergleich mit dem entsprechenden Wert aus Tabelle C.1 der DIN EN ISO 13849-1 erfolgreich auf Plausibilität überprüft (siehe Tabelle D.2 dieses Reports). Die für die Annahme des $MTTF_D$-Wertes vom Hersteller genannten Bedingungen (z. B. Filtrierung des Druckmediums, Ölwechsel) werden in der Betriebsanleitung beschrieben und es wird unterstellt, dass die Bedingungen im Betrieb eingehalten werden.

Konstruktive Merkmale

- Die Anforderungen von Kategorie B, grundlegende und bewährte Sicherheitsprinzipien, werden eingehalten. Durch diversitär redundante Verarbeitungskanäle (Mikrocontroller K1 und ASIC K2) führt ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion und systematische Fehler werden weitgehend vermieden.
- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1 [56].
- K1 ist ein Standard-Mikrocontroller, der im Datenaustausch mit einem ASIC (K2) steht.
- K3 bis K6 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Die zugehörigen Öffner-Kontakte zur Überwachung der Schließer-Kontakte werden im jeweiligen Nachbarkanal überwacht.
- Die hydraulischen Wegeventile 1V3, 1V4, 2V1 und 2V2 haben eine ausreichende positive Überdeckung und eine Federrückstellung.
- Alle Signale führenden Anschlussleitungen sind entweder getrennt oder gegen mechanische Beschädigung geschützt verlegt.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung aller elektrischen Signale, auch die der Druckschalter, erfolgt in einer mehrkanaligen Steuerung.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel über den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm).
- **Software:** Die Programmierung der Software (SRESW) von K1 erfolgt entsprechend Fall 3 (herabgestuft wegen Diversität) mit Maßnahmen nach Tabelle N.3 der Norm und den Hinweisen in Kapitel 9. Fehlervermeidende Maßnahmen bei der ASIC-Entwicklung von K2 sind entsprechend den Anforderungen des ASIC-Entwicklungs-Lebenszyklus (V-Modell) der Norm DIN EN 61508-2 [57] für SIL 2 (herabgestuft wegen Diversität) durchgeführt.

- Verifikation der *DC*-Werte:

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

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

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

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

- Verifikation der Maßnahmen gegen CCF:

Mit 65 Punkten für Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache werden die Mindestanforderungen erfüllt. Zusätzlich wirken in Teilen der Steuerung weitere Maßnahmen. Für die Umsetzung der Maßnahme „physikalische Trennung zwischen den Signalpfaden“ werden beispielsweise 15 Punkte berücksichtigt. Die richtige Umsetzung der Maßnahme ist anhand der Analyse von Entwicklungsunterlagen, wie Schaltplänen, und durch Prüfungen an der Hardware zu zeigen.

- Verifikation der Maßnahmen gegen systematische Ausfälle:

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

Neben den Prüfungen erfolgt entwicklungsbegleitend eine Inspektion der Dokumentationen, in der die angewandten grundlegenden und bewährten Sicherheitsprinzipien und die Maßnahmen zur Beherrschung und Vermeidung systematischer Ausfälle nach Abschnitt 8.1.1 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 des SRP/CS gegen die festgelegten Umgebungsbedingungen zu zeigen, finden eine Analyse zu EMI (Pfad C) sowie Prüfungen zu erwarteten und vorhersehbar widrigen Bedingungen für u. a. Temperatur und Feuchte statt. Dies ist ein weiteres Beispiel für eine Maßnahme zur Vermeidung systematischer Ausfälle. Die Grenzen für Temperatur und Feuchte, in denen die Planschneidemaschine betrieben werden darf, sind in der Spezifikation festgeschrieben und dort durch Verifikation des Dokuments bestätigt worden.

- Verifikation der Software:

Die Entwicklung und Validierung der Software wird ausführlich in Kapitel 9 beschrieben. An dieser Stelle wird ergänzend die Verifikation der Software durchgeführt, d. h. die Prüfung der Funktion und auch der Reaktionszeiten der auf der Hardware integrierten Software. Geprüft wird mit funktionalen Tests (Blackbox-Tests) und erweiterten Funktionstests, bei denen einerseits die sicherheitsrelevanten Eingangssignale korrekt zu sicherheitsrelevanten Ausgangssignalen verarbeitet werden müssen und andererseits Testfälle mit eingebauten Fehlern ausgeführt werden, um die spezifizierten Fehlerreaktionen der Firmware des Mikrocontrollers K1 zu verifizieren. Das heißt, es wird geklärt, ob die Vorgaben der Spezifikation in der Software korrekt umgesetzt worden sind.

- Kontrolle der Abschätzung des PL:

Zur Abschätzung des PL wurde das vereinfachte Verfahren nach DIN EN ISO 13849-1 angewendet. Dessen korrekte Anwendung wird nachvollzogen. Die Berechnung der $MTTF_D$ nach Abschnitt 8.2.11 und Anhang D sowie des durchschnittlichen Diagnosedeckungsgrades DC_{avg} nach Abschnitt 8.2.14 und 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 8.7.

- Verifikation der Benutzerinformation:

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

- 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 Schnitt-

stellenkenndaten zwischen den eingesetzten Technologien sowie Funktionstests und erweiterte Funktionstests.

10.10.3 Prüfung, ob alle Sicherheitsfunktionen analysiert wurden

Die hier für SF2 gezeigten V&V-Aktivitäten werden für alle vom SRP/CS ausgeführten Sicherheitsfunktionen (SF1 bis SF6) durchgeführt. Der Mehraufwand ist allerdings gering, da viele Sicherheitsfunktionen auf dieselbe Hardware zurückgreifen. Die Analysen und Prüfungen 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.

11 Schaltungsbeispiele für SRP/CS

Änderung gegenüber dem IFA Report 2/2017

- Weggefallene Beispiele: Nr. 4, 6, 7, 8, 26, 28, 30, 36
- Neues Beispiel Nr. 30
- Alle Sicherheitsfunktionen in den Beispielen wurde durchgehend nummeriert und inhaltlich um Aussagen zur Software und elektromagnetischer Störung erweitert.
- Kürzel [D], [G], [H] und [N] zur Kennzeichnung der unterstellten Quellen für die Zuverlässigkeitsdaten $MTTF_D$, B_{10D} usw. entfernt

Dieser Report geht zunächst allgemein auf die Gestaltung sicherer Steuerungen ein. Die Abschnitte 6.8, 8.4 und 10.10 illustrieren 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 beiden Teilen der DIN EN ISO 13849 zwar Schritt für Schritt beschrieben, einige dieser Schritte, z. B. die Ableitung des sicherheitsbezogenen Blockdiagramms aus dem Schaltplan, erfordern jedoch einige Übung. Im SISTEMA-Kochbuch 1 [37] werden Hinweise zur Ableitung des sicherheitsbezogenen Blockdiagramms und der SISTEMA-Datei aus dem Schaltplan gegeben. Die einzelnen Schritte lassen sich aufgrund der Vielfalt möglicher Sicherheitsfunktionen und ihrer Realisierung aber nur schwer allgemein beschreiben. Daher wird nun in diesem Kapitel die Bewertung einer Vielzahl von Schaltungsbeispielen vorgestellt, die Sicherheitsfunktionen in verschiedenen Kategorien bzw. Performance Leveln (PL) und in verschiedenen Technologien realisieren. Mit dem Begriff Steuerung sind in den Schaltungsbeispielen im Allgemeinen nur die sicherheitsbezogenen Teile von Steuerungen (SRP/CS) oder deren Teilsysteme erfasst. Die Beispiele beschränken sich auf wesentliche Gesichtspunkte und dienen deshalb primär dazu, die Methodik der *PFH*-Berechnung und quantitativen PL-Bestimmung zu verdeutlichen. Bei deren Auswahl wurde auf ein breites Spektrum von Technologien und möglichen Anwendungen Wert gelegt. Im Vergleich zum IFA Report 2/2017 [60] wurden einige nicht mehr aktuelle Beispiele entfernt, andere wurden hinzugenommen. Die Beispiele sind eine Interpretation der Kategorien und wurden von den Autoren aufgrund langjähriger Erfahrungen mit sicherheitsbezogenen Maschinensteuerungen und Mitwirkung in nationalen und europäischen Normungsgremien zusammengestellt, um eine wirksame Hilfestellung für die Konstruktion eigener Entwicklungen zu geben. Da sie von verschiedenen Autoren erstellt wurden, ist naturgemäß eine Varianz, z. B. in der Darstellung von Details vorhanden. Alle Berechnungen für die Schaltungsbeispiele wurden mithilfe der Software SISTEMA (siehe Anhang H) in der zum Zeitpunkt der Erstellung dieses Reportes verfügbaren Version 2.1 ausgeführt. Weitere Schaltungsbeispiele inklusive SISTEMA-Dateien sind auch im IFA Report 4/2018 „Sichere Antriebssteuerungen mit Frequenzumrichtern“ [12] beschrieben.

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

- Sicherheitsfunktion,
- Funktionsbeschreibung,
- konstruktive Merkmale,
- Bemerkungen,
- Berechnung der Ausfallhäufigkeit,
- weiterführende Literatur.

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

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

Unter „Konstruktive Merkmale“ sind die Besonderheiten im Entwurf des jeweiligen Beispiels, wie die Anwendung bewährter Sicherheitsprinzipien oder die Verwendung bewährter Bauteile, aufgelistet. Auf zusätzliche Anforderungen, beispielsweise Software und elektromagnetische Störfestigkeit, wird kurz hingewiesen.

Die Schaltbilder sind Prinzipschaltbilder, die sich ausschließlich darauf beschränken, Sicherheitsfunktionen oder deren Teilfunktionen mit den hierzu notwendigen relevanten Komponenten zu zeigen. Nicht dargestellt werden zwecks besserer Übersicht solche schaltungstechnischen Maßnahmen, die in der Regel immer zusätzlich realisiert sein müssen, um z. B. den Berührungsschutz sicherzustellen, Über- und Unterspannungen bzw. Überdruck/Unterdruck zu beherrschen, Isolationsfehler, Erd- und Kurzschlüsse z. B. auf extern verlegten Leitungen

aufzudecken oder die erforderliche Störfestigkeit gegen elektromagnetische Einwirkungen zu garantieren. Für die Bestimmung des sicherheitsbezogenen Blockdiagramms unwesentliche Schaltungsdetails wurden somit bewusst weggelassen. Dazu gehören in der Elektrik Schutzbeschaltungen wie Sicherungen und Dioden, z. B. als Freilaufdioden. Ebenfalls nicht aufgeführt sind Entkopplungsdioden in Schaltungen, in denen z. B. Sensorsignale redundant in mehrere Logikeinheiten eingelesen werden. Diese sollen verhindern, dass bei Redundanz im Fehlerfall ein Eingang zu einem Ausgang wird und damit den zweiten Kanal beeinflusst. Um eine Steuerung nach einer Kategorie und einem PL zu realisieren, sind alle diese genannten Bauelemente unerlässlich. Selbstverständlich muss gemäß den Fehlerlisten aus DIN EN ISO 13849-2 beispielsweise 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. In den technologiebezogenen Bemerkungen zur Fluidtechnik sind weitere Beispiele aufgeführt.

Es wird nur eine Auswahl derjenigen konstruktiven Merkmale genannt, die für die beschriebenen Sicherheitsfunktionen wichtig sind. Meist ist dies eine „sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung“. Andere Sicherheitsfunktionen, wie 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 gibt Abschnitt D.2.5.7 zusätzliche Hinweise.

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

Unter „Berechnung der Ausfallhäufigkeit“ wird, basierend auf dem aus dem Prinzipschaltplan abgeleiteten sicherheitsbezogenen Blockdiagramm, die rechnerische Bestimmung des PL für die verschiedenen Teilsysteme 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 können in der Praxis als Herstellerwerte, typische Werte aus Datenbanken oder als Werte aus der Norm DIN EN ISO 13849-1 (siehe Tabelle D.2 dieses Reports) herangezogen werden. Die Norm sieht eine Priorisierung von Herstellerdaten vor.

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

Der Schwerpunkt in der Darstellung liegt eher auf den Kategorien in Form der „Widerstandsfähigkeit gegen Fehler“, dem Blockdiagramm und den „rechnerischen“ Methoden zur Bestimmung des PL. Einige Teilschritte, z. B. Fehlerausschlüsse, grundlegende und bewährte Sicherheitsprinzipien, Maßnahmen gegen systematische Fehler (inklusive Software) oder Maßnahmen für die erforderliche Störfestigkeit gegenüber elektromagnetischen Störungen (EMI), sind dagegen nur in kurzer Form erwähnt. Dies gilt auch für das Management der funktionalen Sicherheit (siehe Abschnitt 5.1), das hier nicht beschrieben wird. Auf diese zusätzlichen wichtigen Aspekte muss bei einer Realisierung entsprechendes Augenmerk gerichtet werden, da Fehleinschätzungen oder unzureichende Umsetzungen bei diesen Maßnahmen die Fehlertoleranz oder Ausfallhäufigkeit verschlechtern können. Als Hilfe zum Verständnis der Schaltungsbeispiele und für die praktische Umsetzung sei daher insbesondere auf Kapitel 10 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“ in verketteten Teilsystemen erfolgt.

11.1 Grundlegende technologiebezogene Bemerkungen zu den Steuerungsbeispielen

11.1.1 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. Dieses 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 [27] 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 Anhang K der DIN EN 60947-5-1 [56].

Detaillierte Informationen zur Modellierung elektromechanischer Bauteile sind im Abschnitt D.2.5 enthalten.

11.1.2 Fluidtechnische Steuerungen

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

Bei hydraulischen Anlagen (**Abbildung 11.1**) 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 11.1 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 Flüssigkeitsbehäl-

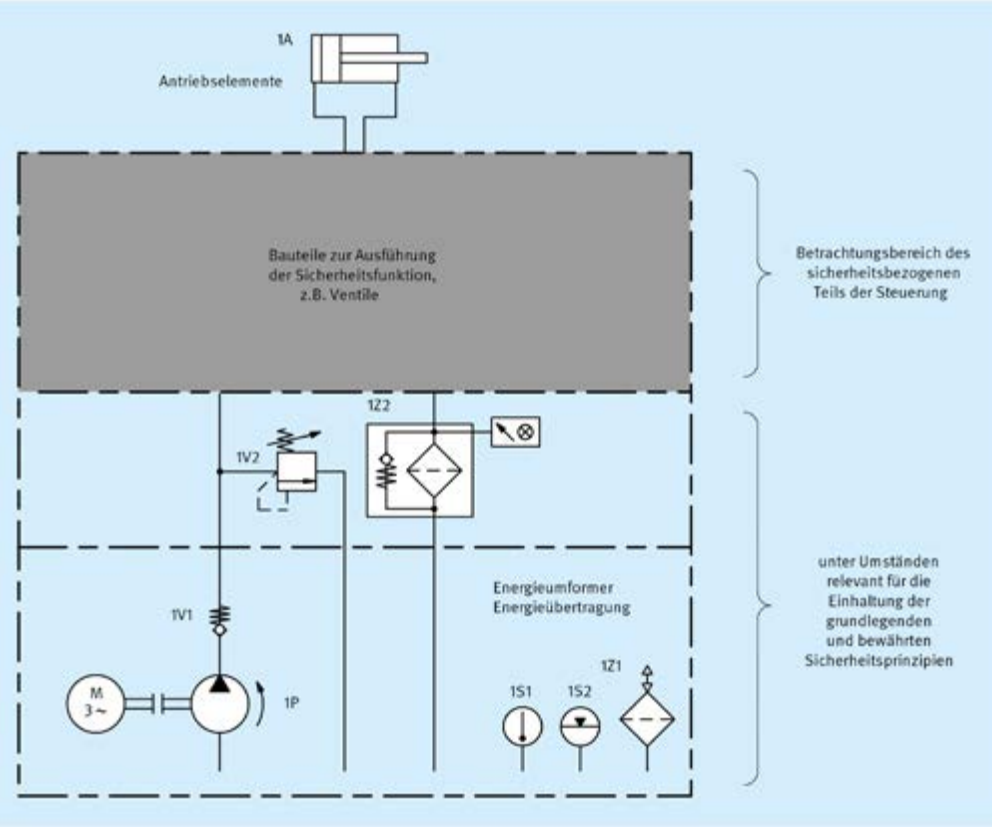


Abb. 11.1
Anwendungsbereich der DIN EN ISO 13849 bei hydraulischen Anlagen

ter 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 auch Anhang C).

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

Bei pneumatischen Anlagen (**Abbildung 11.2**) 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 (Abbildung 11.2) 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 [61, 62] zu entnehmen. Als weitere zutreffende Normen sind [63 bis 66] zu nennen.

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

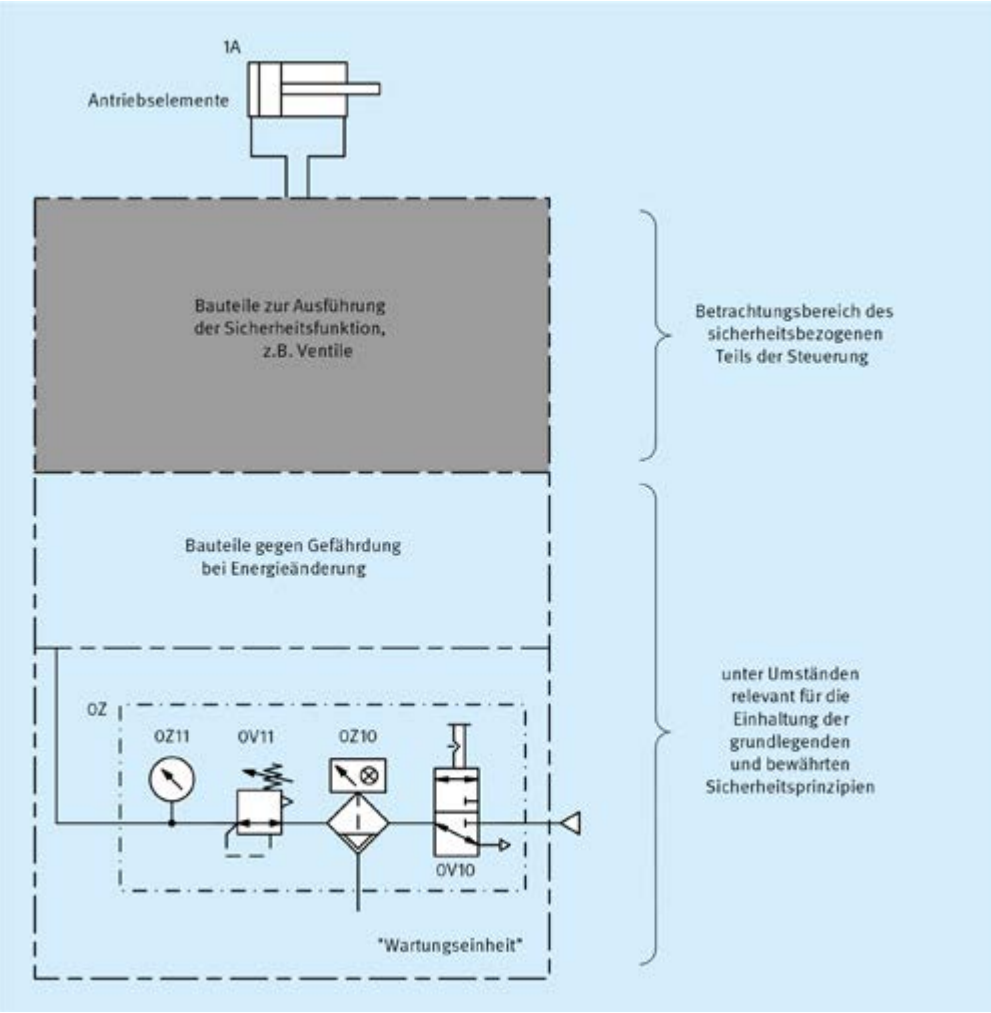


Abb. 11.2
Anwendungsbereich der DIN EN ISO 13849 bei pneumatischen Anlagen

Die geforderte Teilfunktion 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 oder Teilfunktion 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.

11.1.3 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 und 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 Soft Errors, bei denen durch hochenergetische Teilchen wie α-Teilchen eine Kondensatorumladung innerhalb eines Chips erfolgt, sind in der Regel nur schwer zu entdecken und hauptsächlich durch strukturelle Maßnahmen zu beherrschen.

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

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

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

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

Teilsysteme 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 PL, Maßnahmen zur Fehlervermeidung bzw. Fehlerbeherrschung erforderlich sind. Weitere Ausführungen dazu enthält Abschnitt 9. Werden im Rahmen einer Entwicklung ASICs eingesetzt, so sind im Entwicklungsprozess fehlervermeidende Maßnahmen erforderlich. Solche enthält zum Beispiel die Norm DIN EN 61508-2 [57], die für die Entwicklung eines ASICs ein V-Modell in Anlehnung an das aus der Softwareentwicklung bekannte V-Modell vorsieht.

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

- Zwei Kanäle eines Teilsystems 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 etc. 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.

11.2 Schaltungsbeispiele

Tabelle 11.1 zeigt eine Übersicht der Schaltungsbeispiele 1 bis 30. Weitere Beispiele finden sich im IFA Report 4/2018 „Sichere Antriebssteuerungen mit Frequenzumrichtern“ [12]. **Tabelle 11.2** nennt alphabetisch sortiert die wichtigsten in den Schaltungsbeispielen verwendeten Abkürzungen.

Hinweise

- Bei Beispielen mit mehreren Sicherheitsfunktionen (13, 14, 15, 18, 19) wird jeweils nur die erste Sicherheitsfunktion im sicherheitsbezogenen Blockdiagramm dargestellt.
- Die Berechnung der Ausfallhäufigkeit der Schaltungsbeispiele wurde mit den Standardeinstellungen des SISTEMA Tools vorgenommen. Dies umfasst die Experten-Einstellung „*DC*-Zwischenstufen verwenden“, mit der genauere *PFH*-Werte ermittelt werden.

Tabelle 11.1 Übersicht der Schaltungsbeispiele

Erreichter PL	Realisierte Kategorie	Technologie/Beispiel Nr.		
		Pneumatik	Hydraulik	Elektrotechnik
b	B			1,
c	1	2	3, 29	4,
c	2			5
c	3			6, 24
d	2	7	8	9, 30
d	3	10	11, 12	11, 12, 13, 14, 15, 16, 17, 18, 19
e	3	20	21	22
e	4	23	24, 25	25, 26, 27, 28

Tabelle 11.2 Übersicht der in den Schaltungsbeispielen verwendeten Abkürzungen

Abkürzung	Bedeutung
µC	Mikrocontroller
B_{10}	Nominale Lebensdauer: mittlere Zahl von Schaltspielen bzw. Schaltzyklen, bis 10 % der betrachteten Einheiten ausgefallen sind
B_{10D}	Nominale Lebensdauer: mittlere Zahl von Schaltspielen bzw. Schaltzyklen, bis 10 % der betrachteten Einheiten gefährlich ausgefallen sind
BKK	Brems-/Kupplungskombination
BWS	Berührungslos wirkende Schutzeinrichtung
CCF	Ausfall infolge gemeinsamer Ursache (Common Cause Failure)
CPU	Mikroprozessor (Central Processing Unit)
DC	Diagnosedeckungsgrad (Diagnostic Coverage)
DC_{avg}	Durchschnittlicher Diagnosedeckungsgrad (average Diagnostic Coverage)
EMI	Elektromagnetische Störung (Electromagnetic Interference)
FIT	Ausfälle in 10^9 Betriebsstunden (Failures In Time)
FMEA	Ausfalleffektanalyse (Failure Mode and Effects Analysis)
FU	Frequenzumrichter
M	Motor
MFST	Multifunktionsstellteil
$MTTF_D$	Mittlere Zeit bis zum gefahrbringenden Ausfall (Mean Time To Dangerous Failure)
n_{op}	Mittlere Anzahl jährlicher Betätigungen (Number of Operations)
PFH	Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde (Average Frequency 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 6.2)
SPS	Speicherprogrammierbare Steuerung
SRASW	Sicherheitsbezogene Anwender-Software (Safety-Related Application Software)
SRESW	Sicherheitsbezogene eingebettete Software (Safety-Related Embedded Software)
SRP/CS	Sicherheitsbezogener Teil einer Steuerung
SS1-r, SS1-t	Sicherer Stopp 1 (Safe Stop 1, siehe Tabelle 6.2)
SS2-r, SS2-t	Sicherer Stopp 2 (Safe Stop 1, siehe Tabelle 6.2)
STO	Sicher abgeschaltetes Moment (Safe Torque Off, siehe Tabelle 6.2)
T_{10D}	Zeit, bis 10 % der betrachteten Bauteile gefährlich ausgefallen sind
ZHS	Zweihandschaltung

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

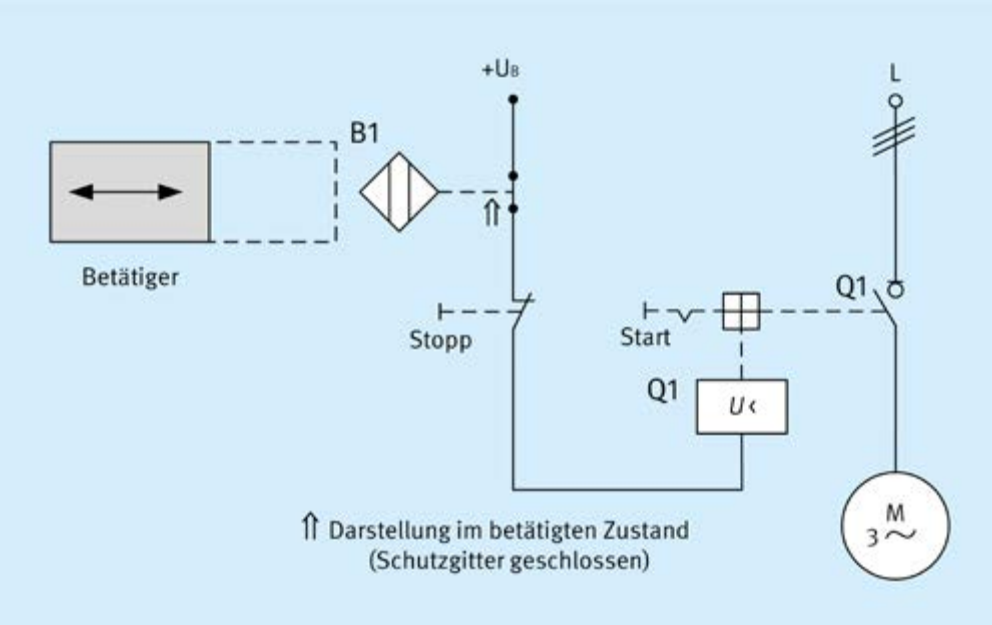


Abb. 11.3
Stellungsüberwachung verriegelter trennender Schutzeinrichtungen mittels Näherungsschalter

Sicherheitsfunktion

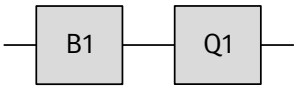
- SF1.1: Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Die Betätigung des Näherungsschalters beim Öffnen der verriegelten trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion Sicher abgeschaltetes Moment (STO) ein.

Funktionsbeschreibung

- Das Öffnen des Schutzgitters wird durch den Näherungsschalter B1 erfasst, der auf den Unterspannungsauslöser Q1 wirkt. Durch das Abfallen von Q1 werden gefahrbringende Bewegungen stillgesetzt.
- 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.
- Durch das Betätigen der Starttaste wird der Motor gestartet. Die Stopptaste öffnet die Versorgungspannung des Unterspannungsauslösers, der somit die Lastversorgung für den Motor unterbricht.

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 11 beschrieben, sind vorgesehen. Als ein grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip für den Unterspannungsauslöser verwendet.
- Ein stabiler Aufbau des Schutzgitters 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 den verdeckten Einbau (siehe auch DIN EN ISO 14119).
- Die Spannungsversorgung der gesamten Maschine wird durch den Unterspannungsauslöser oder den Stopp-Taster abgeschaltet (Stopp-Kategorie 0 nach DIN EN 60204-1).
- Das Teilsystem wird in geeigneter Umgebungsbedingung eingesetzt. Dies beinhaltet die Mindestanforderungen der Kategorie B. Die Anforderungen hinsichtlich elektromagnetische Störfestigkeit, mechanische Bedingungen wie Schock- und Vibrationsfestigkeit der Komponenten und Umwelteinflüsse für das Teilsystem werden eingehalten.
- B1 enthält keine internen Überwachungsmaßnahmen. Es sind keine weiteren Maßnahmen zur Fehlererkennung vorgesehen.
- Q1 ist ein Unterspannungsauslöser der als elektromechanischer Schalter den Motor startet, wenn der Start-



knopf gedrückt wird. Der Unterspannungsausschalter ist für die industrielle Anwendung geeignet. Der Schalter erfüllt die Anforderungen der Norm DIN EN 60947-1.

EMI: Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel über den Industriestandard der DIN EN IEC 61000-6-2 nachgewiesen (Pfad B nach Anhang L der Norm). Alle eingesetzten Bauteile des Teilsystems erfüllen laut Hersteller die normativen Anforderungen, wenn sie nach Vorgabe installiert werden.

Software: Dieses Beispiel enthält keine zu bewertende Software.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Diese Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie B.
- ***MTTF*$_D$:** Bei B1 handelt es sich um einen Näherungsschalter an einem Schutzgitter mit $MTTF_D$ = 1100 Jahren. Für die Unterspannungsauslösung des Motorstarters Q1 entspricht der B_{10}-Wert näherungsweise der elektrischen Lebensdauer von 10 000 Schaltspielen. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Bei täglicher Betätigung des Näherungsschalters ergibt sich mit n_{op} = 365 Zyklen/Jahr für Q1 eine $MTTF_D$ von 548 Jahren. Die Kombination von B1 und Q1 ergibt $MTTF_D$ = 365 Jahre für den Kanal. Dieser Wert wird auf 100 Jahre („hoch“) gekürzt.
- ***DC*$_{avg}$:** DC Maßnahmen sind in Kategorie B nicht relevant.
- **CCF:** Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie B nicht relevant.
- **PL:** Die elektromechanische Steuerung entspricht Kategorie B mit hoher $MTTF_D$ (100 Jahre). Als Berechnungsgrundlage zur *PFH*-Bestimmung nach dem vereinfachten Verfahren wird der Maximalwert für Kategorie B, also 27 Jahre („mittel“), benutzt. Für SF1.1 ergibt sich damit eine mittlere Häufigkeit gefährlicher Ausfälle von $4{,}2 \cdot 10^{-6}$/Stunde. Dies entspricht dem maximal mit Kategorie B erreichbaren PL b.

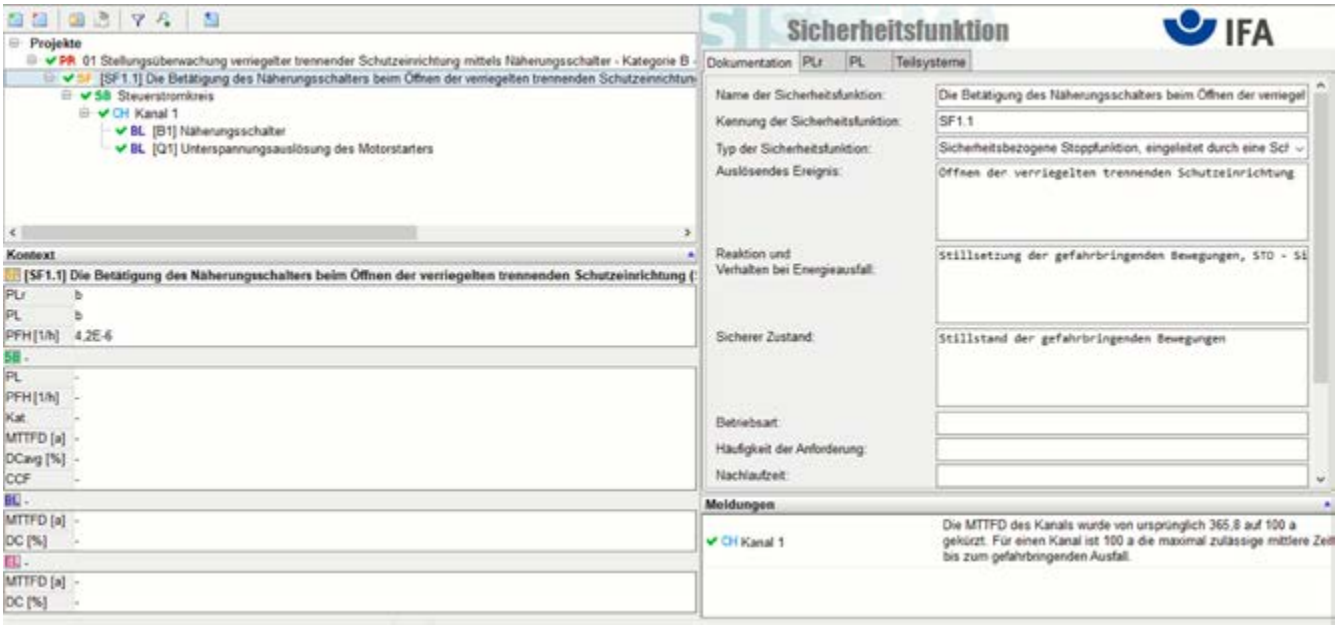


Abb. 11.4 PL-Bestimmung mithilfe von SISTEMA

11.2.2 Pneumatisches Ventil (Teilsystem) – Kategorie 1 – PL c (Beispiel 2)

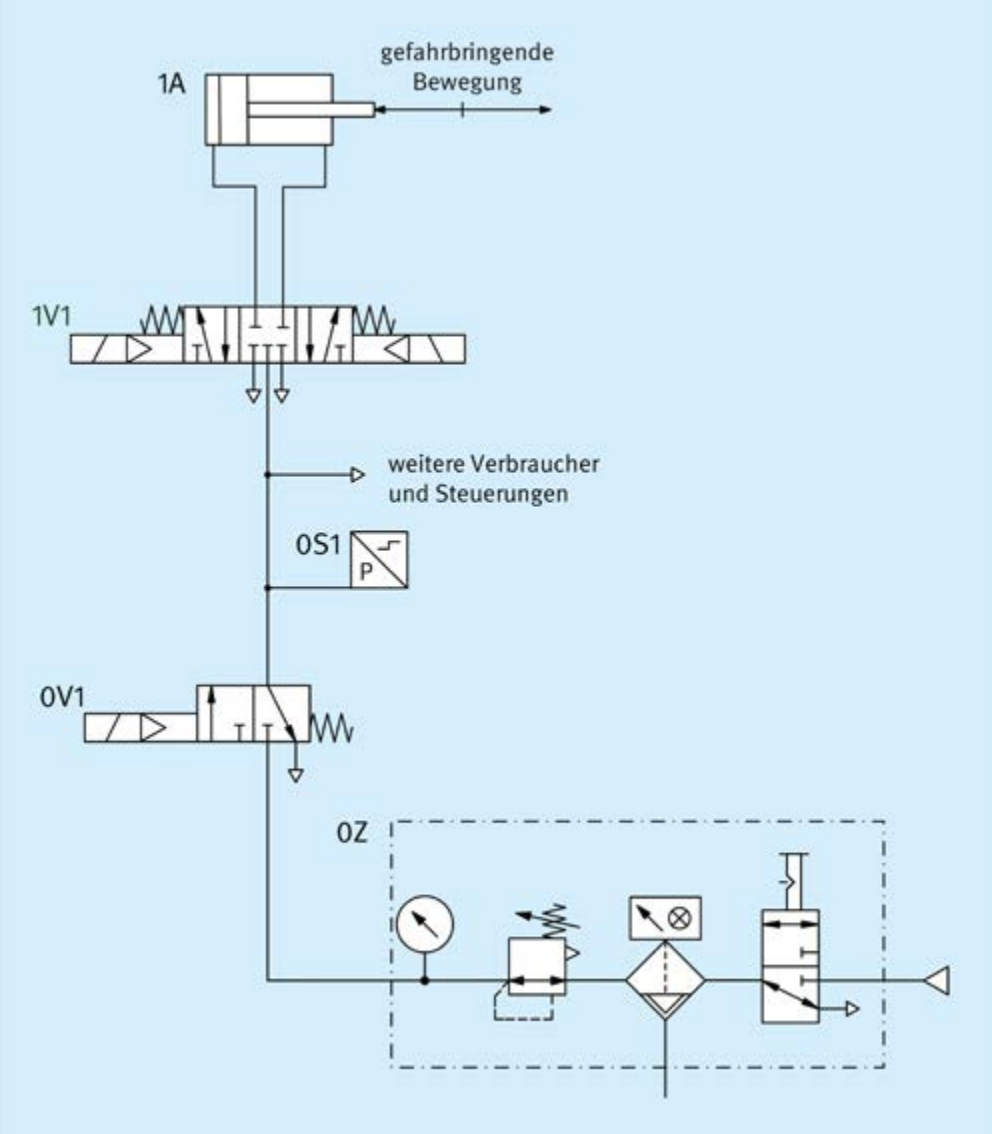


Abb. 11.5
Pneumatisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- SF2.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktion SSC.
- Hier ist nur der pneumatische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme hinzuzufügen.

Funktionsbeschreibung

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

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V1 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Bestätigung für das Wegeventil als sicherheitstechnisch bewährtes Bauteil (ausreichend hohe Zuverlässigkeit) erfolgt durch den Hersteller/Anwender.
- Die Sicherheitsfunktion kann auch durch eine Verknüpfung von entsprechenden Ventilen erreicht werden.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das pneumatische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 1.
- ***MTTF*$_D$:** Für das Wegeventil 1V1 wird ein B_{10D}-Wert von 20 000 000 Schaltspielen [H] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr und $MTTF_D$ = 145 Jahre. Dies ist gleichzeitig der $MTTF_D$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- ***DC*$_{avg}$:** Überwachungsmaßnahmen sind in Teilsystemen der Kategorie 1 nicht relevant.
- **CCF:** Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Teilsystemen der Kategorie 1 nicht relevant.
- **PL:** Die pneumatische Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Für SF2.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer. Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Wegeventil 1V1 folgende Bewertung. Die Gebrauchsdauer des verschleißbehafteten Elements 1V1 endet nach Ablauf von T_{10D} = 14 Jahren. Danach verliert die *PFH*-Berechnung ihre Grundlage. Ein rechtzeitiger Austausch wird empfohlen.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022).DIN Media, Berlin 2022.

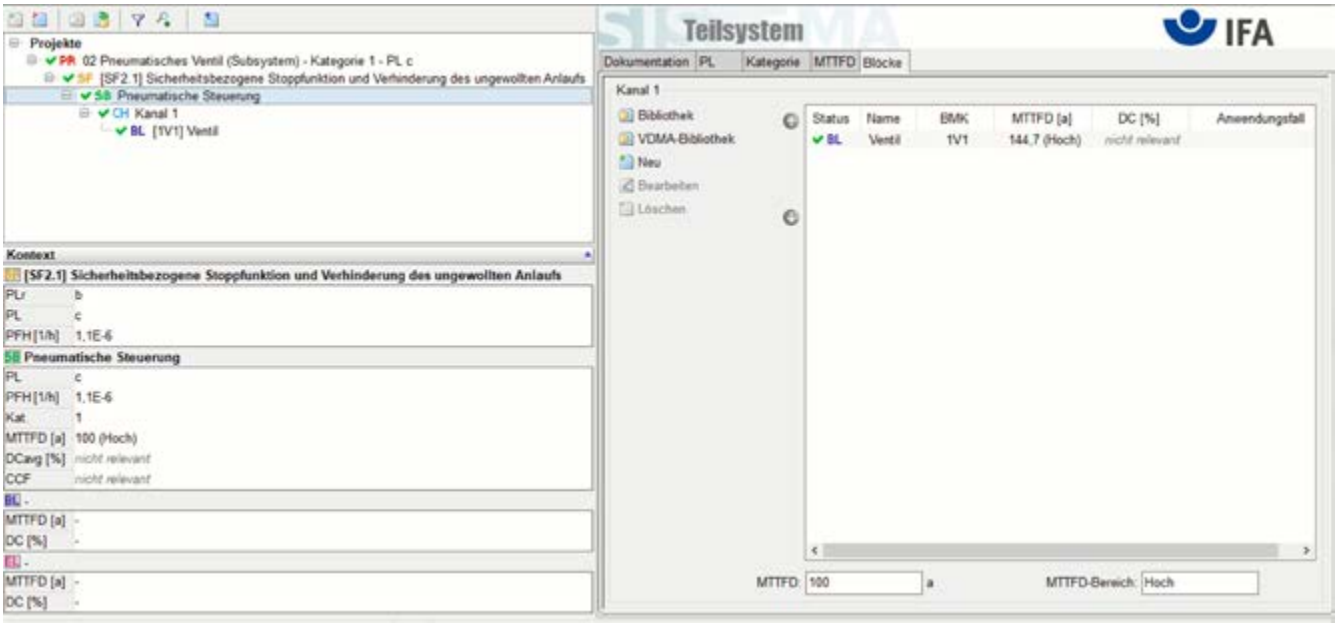


Abb. 11.6 PL-Bestimmung mithilfe von SISTEMA

11.2.3 Hydraulisches Ventil (Teilsystem) – Kategorie 1 – PL c (Beispiel 3)

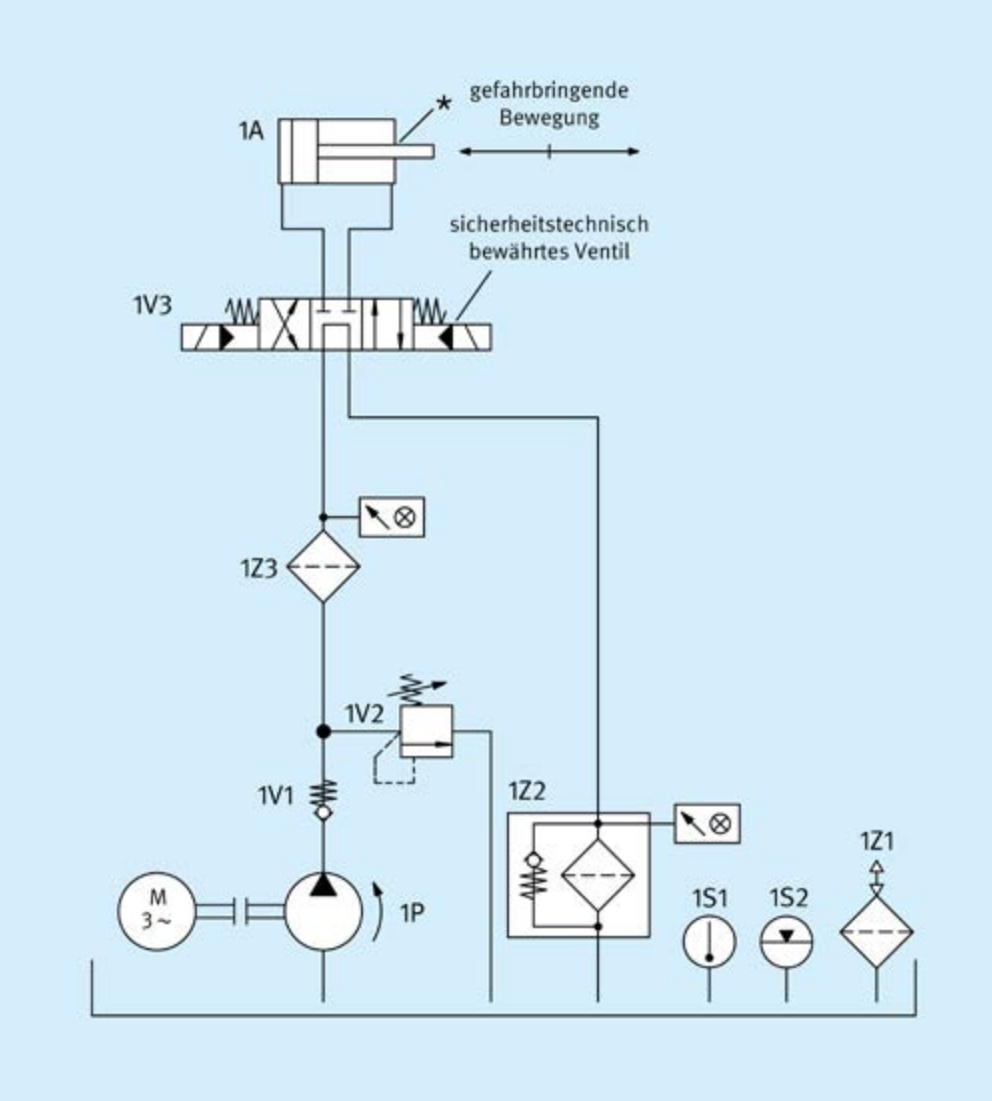


Abb. 11.7
Hydraulisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- SF3.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktion SSC.
- Hier ist nur der hydraulische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme 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.

1V3

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 11.7) vorgesehen.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das hydraulische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 1.
- ***MTTF*$_D$:** Für das Wegeventil 1V3 wird eine *MTTF*$_D$ von 150 Jahren angenommen. Dies ist gleichzeitig der *MTTF*$_D$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- ***DC*$_{avg}$:** Überwachungsmaßnahmen sind in Teilsystemen der Kategorie 1 nicht relevant.
- **CCF:** Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Teilsystemen der Kategorie 1 nicht relevant.
- **PL:** Die hydraulische Steuerung entspricht Kategorie 1 mit hoher *MTTF*$_D$ (100 Jahre). Für SF3.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022.

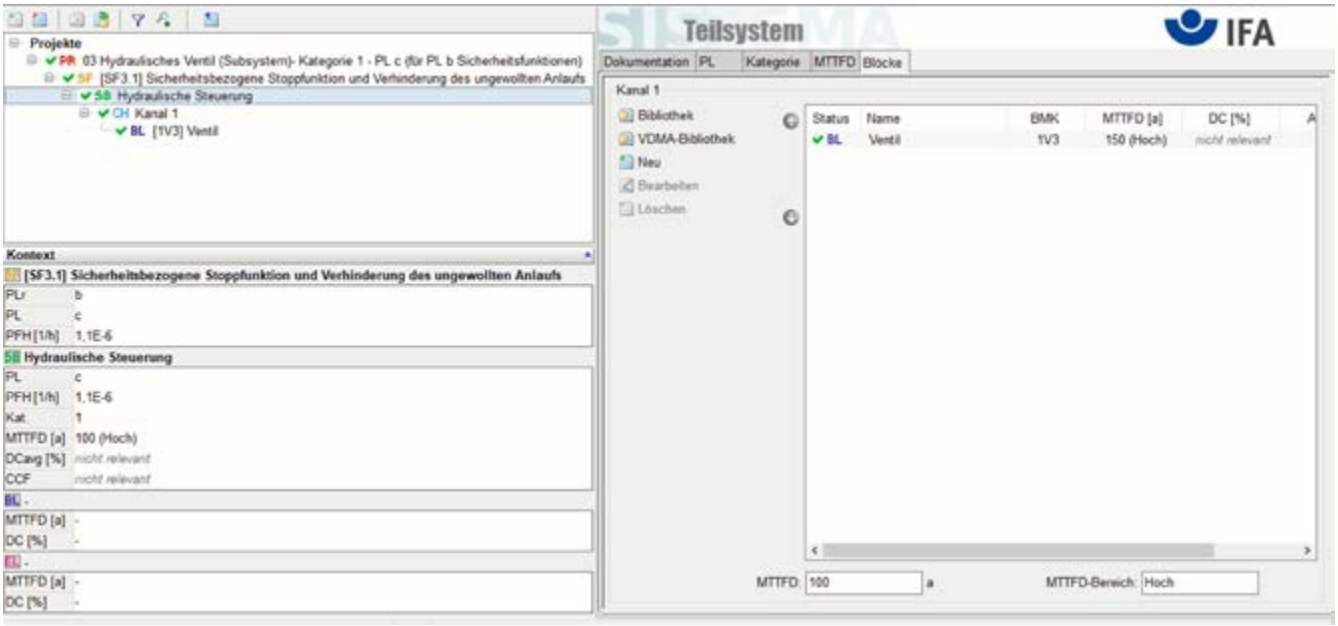


Abb. 11.8 PL-Bestimmung mithilfe von SISTEMA

11.2.4 Stellungsüberwachung verriegelter trennender Schutzeinrichtungen – Kategorie 1 – PL c (Beispiel 4)

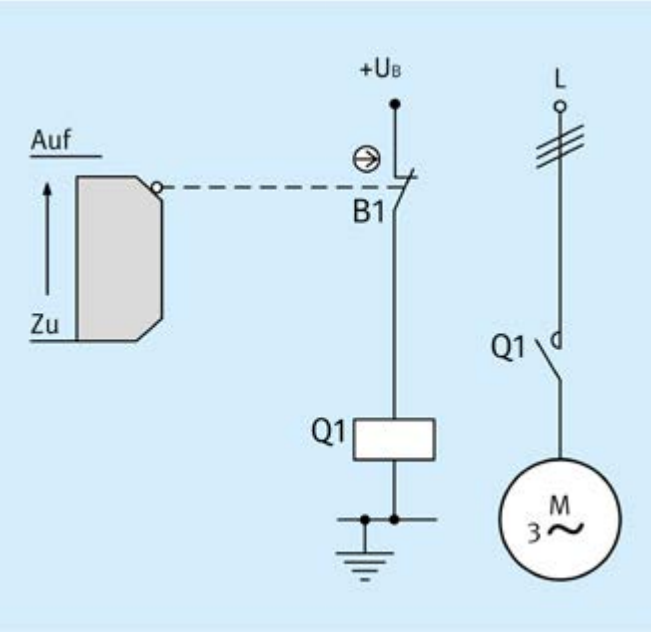


Abb. 11.9
Stellungsüberwachung verriegelter trennender Schutzeinrichtungen zur Verhinderung von gefahrbringenden Bewegungen (Sicher abgeschaltetes Moment, STO)

Sicherheitsfunktion

- SF4.1: Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der verriegelten trennenden Schutzeinrichtung leitet die Sicherheitsfunktion Sicher abgeschaltetes Moment (STO) ein.

Funktionsbeschreibung

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

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 beschrieben, sind vorgesehen. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip verwendet. Die Erdung des Steuerkreises ist als bewährtes Sicherheitsprinzip zu betrachten.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K, und wird daher als bewährtes Bauteil angesehen. Der Öffnerkontakt unterbricht den Stromkreis mechanisch zwangläufig, wenn die Schutzeinrichtung sich nicht in Schutzstellung befindet.
- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.3 der DIN EN 13849-2.
- Die Stellungsüberwachung erfolgt durch einen Positionsschalter. Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt. Die Betätigungselemente des Positionsschalters sind gegen Lageveränderung gesichert. Es werden nur starre mechanische Teile (keine Federelemente in Wirkrichtung der Betätigungskraft) verwendet.
- Der Betätigungshub für den Positionsschalter erfolgt nach Herstellerangabe.
- Das Teilsystem wird in geeigneter Umgebungsbedingung eingesetzt. Dies beinhaltet die Mindestanforderungen der Kategorie B. Die elektromagnetische Störfestigkeit, mechanische Bedingungen wie Schock- und

B1 Q1

Vibrationsfestigkeit der Komponenten und die Temperatureinflüsse für das Teilsystem werden eingehalten.

- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 1.
- ***MTTF*$_D$:** Für B1 ist eine B_{10D} von 20 000 000 Schaltspielen angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 35 040 Zyklen/Jahr und $MTTF_D$ = 5 707 Jahre. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10} -Wert der elektrischen Lebensdauer von 1 300 000 Schaltspiele. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} ergibt sich für Q1 eine $MTTF_D$ von 742 Jahren. Die Kombination von B1 und Q1 ergibt für den Kanal eine $MTTF_D$ = 656 Jahre, die auf 100 Jahre („hoch“) gekürzt wird.
- ***DC*$_{avg}$:** Überwachungsmaßnahmen sind in Teilsystemen der Kategorie 1 nicht relevant.
- **CCF:** Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Teilsystemen der Kategorie 1 nicht relevant.
- **PL:** Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Für SF4.1 ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

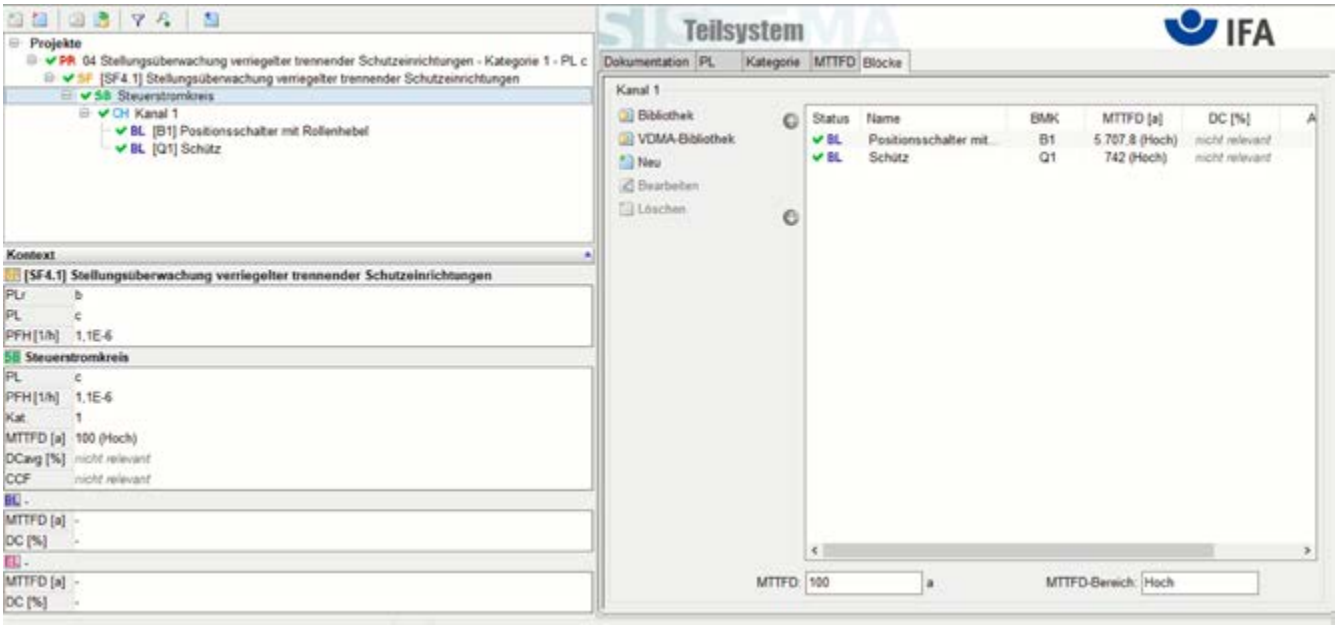


Abb. 11.10 PL-Bestimmung mithilfe von SISTEMA

11.2.5 Getestete Lichtschranken – Kategorie 2 – PL c mit nachgeschaltetem Kategorie-1-Ausgangsschaltelement (Beispiel 5)

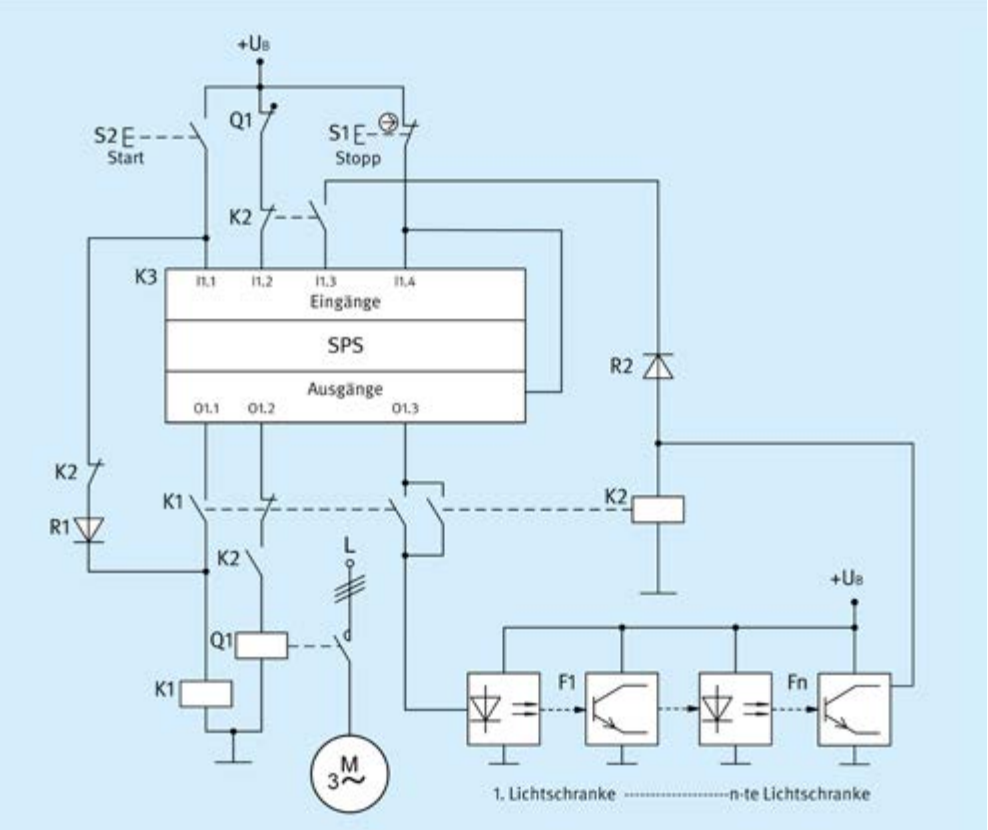


Abb. 11.11
Testung von Lichtschranken mit einer Standard-SPS

Sicherheitsfunktion

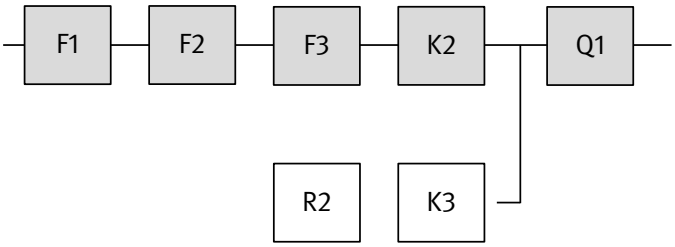
- SF5.1: Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Bei Lichtstrahlunterbrechung wird die gefahrbringende Bewegung stillgesetzt (Sicher abgeschaltetes Moment, STO).

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 O1.2 des Testkanals ein Abschaltbefehl erzeugt. Das Stillsetzen der gefahrbringenden Bewegung erfolgt dann über das Hauptschütz Q1.
- Die Testung der Lichtschranken erfolgt vor jedem Start der gefahrbringenden Bewegung nach dem Betätigen der Start-Taste S2 durch softwaregesteuertes Ausschalten der Lichtschrankensender mittels SPS-Ausgang O1.3. Die Überwachung der Empfängerreaktion (K2 fällt wieder ab) erfolgt über die SPS-Eingänge I1.2 und I1.3. Bei fehlerfreiem Verhalten gelangt K2 über O1.3 in Selbsthaltung und S2 kann zum Einleiten der gefahrbringenden Bewegung losgelassen werden. K1 wird über O1.1 entregt und über O1.2 wird das Hauptschütz Q1 angesteuert.
- Im Falle eines durch die Testung aufgedeckten Fehlers in einer Lichtschranke oder in K2 werden die Ausgänge O1.2 und O1.3 deaktiviert und es erfolgt keine weitere Ansteuerung des Hauptschützes Q1.
- Beim unterstellten globalen Versagen der SPS (Ausgang O1.1 führt Low-Potenzial, O1.2 und O1.3 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 O1.2 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 11 beschrieben, sind vorgesehen.



- Es werden spezielle Lichtschranken mit geeigneten optischen Eigenschaften (optischer Öffnungswinkel, Fremdlichtsicherheit usw.) nach DIN EN IEC 61496-2 verwendet.
- Mit nur zwei SPS-Eingängen und einem Relais bzw. Hilfsschütz können mehrere Lichtschranken kaskadiert und überwacht werden.
- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Das Hauptschütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN IEC 60947-4-1, Anhang F.
- Die Lichtschranken F1 bis Fn sind Standardkomponenten ohne Software und in Elektronik ohne komplexe Bauteile wie Mikrocontroller, ASICs oder FPGAs aufgebaut.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel über die Sicherheitsfachgrundnorm für Schutzeinrichtungen DIN EN IEC 61496-1 nachgewiesen (Pfad A nach Anhang L der Norm).
- **Software:** Für die Standardkomponente K3 ist die Einhaltung der SRESW-Anforderungen durch den Hersteller der SPS nicht bestätigt und kann durch den Integrator nicht nachträglich geleistet werden (nicht zugängliche Embedded-Software). Nach Abschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da das Teilsystem auf PL c mit Kategorie 2 begrenzt ist und die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Entwurfsprinzipien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt. Die Programmierung der Software (SRASW) der Standardkomponente K3 im Testkanal erfolgt entsprechend Fall 1 (herabgestuft wegen Testkanal) mit Basismaßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9. Die SRASW realisiert die erforderliche Fehlererkennung für F1 bis Fn und K2.
- Die Start-Taste S2 muss außerhalb des Gefahrenbereiches und mit Einblick in den Gefahrenbereich bzw. in die Gefahrstelle angeordnet sein.
- Die Anzahl, Anordnung und Höhe von Lichtstrahlen muss DIN EN ISO 13855 und DIN EN IEC 62046 entsprechen.
- Ist bei der Absicherung von Gefahrbereichen ein „Hintertreten“ möglich, sind weitere Maßnahmen wie 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.
- Beim Einsatz von Lichtschranken, die komplexe Bauteile wie Mikrocontroller, ASICs oder FPGAs mit Software ohne Sicherheitsbewertung durch den Hersteller enthalten (d. h. die Anforderungen für sicherheitsbezogene Embedded-Software sind nicht erfüllt), ist nach Norm der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da das Teilsystem auf PL c mit Kategorie 2 begrenzt ist und die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Entwurfsprinzipien erfüllt werden.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Zur Berechnung der Ausfallhäufigkeit wird das Gesamtsystem in die zwei Teilsysteme „Lichtschranken“ in Kategorie 2 und „Hauptschütz“ (Q1) in Kategorie 1 aufgeteilt.
- Bei der Berechnung der Ausfallhäufigkeit 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.

Für das Teilsystem „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 Ausfallhäufigkeit nicht beteiligt.
- ***MTTF*$_D$:** Für F1 bis F3 liegen folgende Herstellerangaben vor: für den Sender $MTTF_D$ = 176 Jahre und für den Empfänger $MTTF_D$ = 231 Jahre. Für K2 gilt ein B_{10D}-Wert von 20 000 000 Zyklen. Mit 240 Arbeitstagen, 16 Arbeitsstunden und 180 Sekunden Zykluszeit ist n_{op} = 76 800 Zyklen/Jahr. Durch die oben beschriebene Testung verdoppelt sich dieser Wert auf n_{op} = 153 600 Zyklen/Jahr mit einer $MTTF_D$ = 1302 Jahre für K2. Diese Werte ergeben eine $MTTF_D$ des Funktionskanals von 32 Jahren („hoch“). Für K3 liegt die Herstellerangabe $MTTF_D$ = 46 Jahre vor. Der $MTTF_D$-Wert von 228 311 Jahren für die Entkopplungsdiode R2 ist im Vergleich dazu unbedeutend.
- ***DC*$_{avg}$:** DC = 60 % für F1 bis F3 begründet sich durch den beschriebenen Funktionstest, *DC* = 99 % für K2 folgt aus der direkten Überwachung in K3 mithilfe zwangsgeführter Kontakte. Die Mittelungsformel für DC_{avg} ergibt 61 % („niedrig“).
- **CCF:** 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 Teilsystem „Lichtschranken“ entspricht Kategorie 2 mit hoher $MTTF_D$ des Funktionskanals (32 Jahre) und niedrigem DC_{avg} (61 %). Damit ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls PFH von $1{,}9 \cdot 10^{-6}$/Stunde.

Für das Teilsystem „Hauptschütz“ gilt:

- ***MTTF*$_D$:** B_{10D} = 1300 000 Zyklen mit n_{op} = 76 800 Zyklen/Jahr. Dies führt zu einer $MTTF_D$ von 169 Jahren, die nach Norm auf 100 Jahre begrenzt wird.
- Die Struktur entspricht Kategorie 1, daher sind DC_{avg} und Ausfälle infolge gemeinsamer Ursache nicht relevant. Es ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls von $1{,}1 \cdot 10^{-6}$/Stunde.
- **PL:** Die Addition der mittleren Häufigkeiten eines gefahrbringenden Ausfalls beider Teilsysteme ergibt eine PFH von $3{,}0 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.
- Ist abzusehen, dass die Sicherheitsfunktion häufiger als für die vorgesehene Architektur der Kategorie 2 zugrunde gelegt angefordert wird (das Verhältnis 100 : 1 wird unterschritten, d. h. häufiger als einmal in fünf Stunden), so kann dies gemäß Anmerkung 1 der Norm in Anhang K bis zu einem Verhältnis von 25 : 1 mit einem Zuschlag von 10 % berücksichtigt werden. Im vorliegenden Fall mit drei Lichtschranken erreicht das Teilsystem „Lichtschranken“ noch eine *PFH* von $2{,}1 \cdot 10^{-6}$/Stunde. Die mittlere Häufigkeit eines gefahrbringenden Ausfalls *PFH* von $3{,}2 \cdot 10^{-6}$/Stunde erreicht allerdings nur noch PL b. Um PL c zu erreichen, müssten z. B. die Anzahl der Lichtschranken reduziert oder Komponenten mit höherer $MTTF_D$ eingesetzt werden.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Bauteil Q1 folgende Bewertung. Die Gebrauchsdauer des verschleißbehafteten Elements Q1 endet nach Ablauf von T_{10D} = 17 Jahren. Danach verliert die *PFH*-Berechnung ihre Grundlage. Ein rechtzeitiger Austausch wird empfohlen.

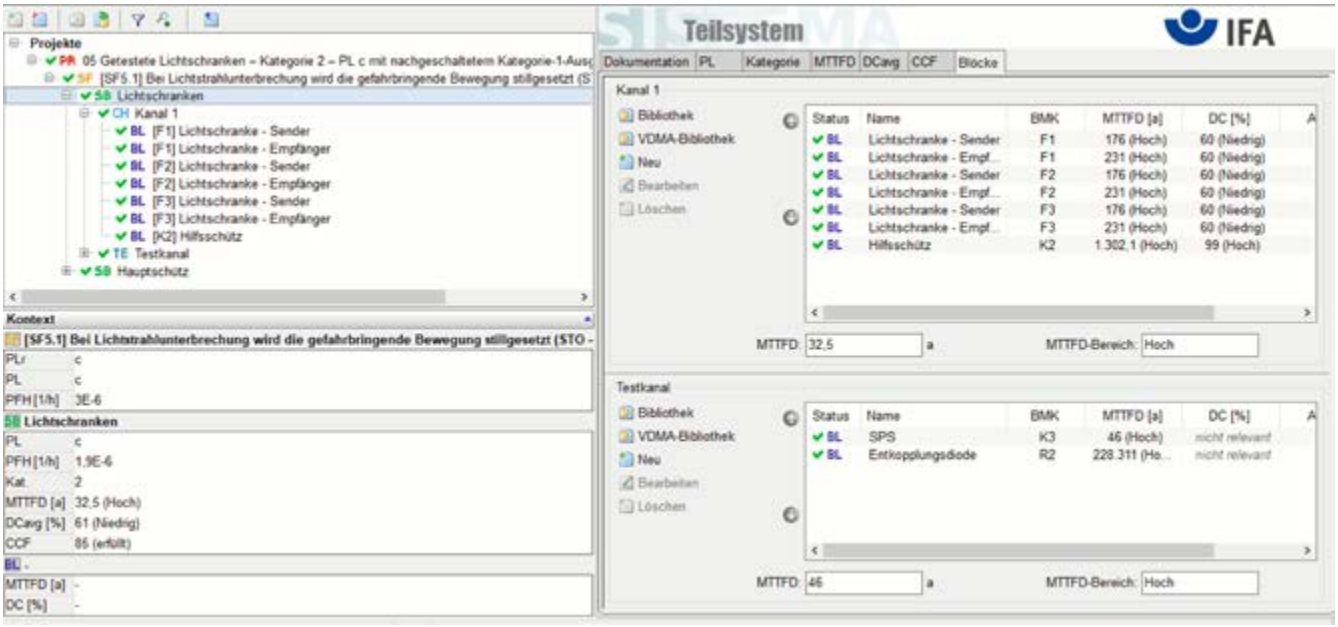


Abb. 11.12 PL-Bestimmung mithilfe von SISTEMA

Weiterführende Literatur

- DIN EN IEC 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (6/2021). DIN Media, Berlin 2021
- DIN EN IEC 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, die aktive optoelektronische Schutzeinrichtungen (AOPD) verwenden (8/2021). DIN Media, Berlin 2021
- DIN EN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zur Anwesenheitserkennung von Personen (3/2019). DIN Media, Berlin 2019
- DIN EN ISO 13855: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (10/2010). DIN Media, Berlin 2010

11.2.6 Sicheres Stillsetzen eines SPS-gesteuerten Antriebs mit Not-Halt – Kategorie 3 – PL d (Beispiel 6)

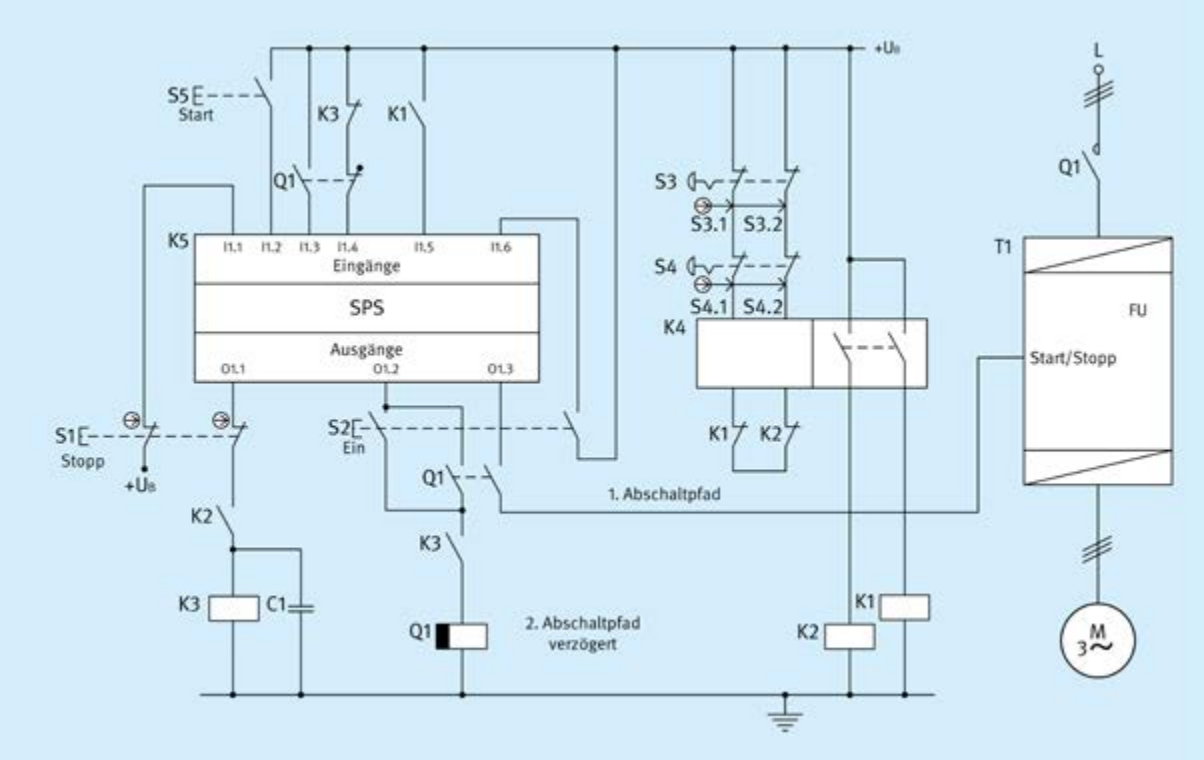


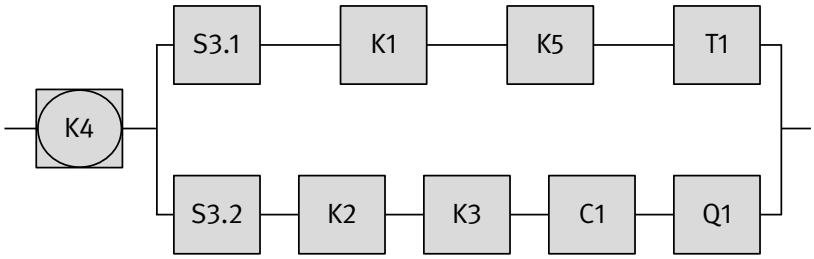
Abb. 11.13 Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Not-Halt-Befehl

Sicherheitsfunktion

- SF6.1: Bei Betätigung des Not-Halt-Gerätes S3 wird der Antrieb gesteuert stillgesetzt (SS1-t – Sicherer Stopp 1 mit STO nach Verzögerungszeit).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird stillgesetzt, falls entweder die Stopp-Taste S1 oder eines der Not-Halt-Geräte S3 bzw. S4 betätigt wird. In diesem Beispiel wird nur die Betätigung mittels Not-Halt-Gerät S3 betrachtet. Das Stillsetzen des Antriebs im Notfall erfolgt nach Betätigung von S3 zuerst durch Deaktivierung des Not-Halt-Sicherheitsschaltgerätes K4 einhergehend mit dem Entregen der Hilfsschütze K1 und K2. Das Öffnen des Schließerkontaktes K1 am Eingang I1.5 der SPS K5 bewirkt über den SPS-Ausgang O1.3 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 I1.1 und die Absteuerung des FU mit dem Rücksetzen des SPS-Ausgangs O1.3. Redundant dazu wird das Hilfsschütz K3 – abfallverzögert mithilfe des Kondensators C1 – entregt. Nach Ablauf der Bremszeitvorgabe wird die Ansteuerung für das Netzschütz Q1 unterbrochen.
- Bei einem einzelnen Versagen der SPS K5, des Umrichters T1, des Netzschützes Q1, der Hilfsschütze K1/K2 oder des abfallverzögerten Hilfsschützes K3 wird trotzdem das Stillsetzen des Antriebs sichergestellt, weil immer zwei voneinander unabhängige Abschaltpfade vorhanden sind. Ein Nichtabfallen der Hilfsschütze K1 und K2 wird durch Überwachung der zwangsgeführten Öffnerkontakte innerhalb des Not-Halt-Sicherheitsschaltgerätes K4 spätestens nach dem Entriegeln des betätigten Not-Halt-Gerätes aufgedeckt. Das Nichtabfallen des Hilfsschützes K3 wird wegen der vorhandenen Rückführung des zwangsgeführten Öffnerkontaktes in den SPS-Eingang I1.4 spätestens vor einem erneuten Ingangsetzen der Maschinenbewegung aufgedeckt. Der Nichtabfall des Netzschützes Q1 wird über den in SPS-Eingang I1.4 eingelesenen Spiegelkontakt aufgedeckt. Ein Verschweißen dieses Spiegelkontaktes wird durch den hiermit zwangsgeführten



Schliesser-Hilfskontakt am SPS-Eingang I1.3 erkannt. Bei einem Fehler im Kondensator C1 weicht die gemessene Abfallzeit des Hilfsschützes K3 von der Zeitvorgabe in der SPS ab. Der Fehler wird erkannt und führt zur Abschaltung und Betriebshemmung der Maschine. Durch organisatorische Maßnahmen wird sichergestellt, dass jedes Not-Halt-Gerät mindestens einmal pro Jahr betätigt wird.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 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 im Fehlerfall verzögerte Erreichung des Stillstands nur über den zweiten Abschaltpfad darf nicht mit einem verbleibenden inakzeptabel hohen Restrisiko verbunden sein.
- Der sicherheitsrelevante Steuerungsteil des Not-Halt-Sicherheitsschaltgerätes K4 erfüllt alle Anforderungen für Kategorie 3 und PL d.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt werden (siehe Anhang L der Norm).
- **Software:** Für die Standardkomponenten K5 und T1 ist die Einhaltung der SRESW-Anforderungen durch die Hersteller nicht bestätigt und kann durch den Integrator nicht nachträglich geleistet werden (nicht zugängliche Embedded-Software). Nach Abschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da das Teilsystem auf PL d mit Kategorie 3 begrenzt ist und die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Technologien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt. Die Programmierung der Software (SRASW) der Standardkomponente K5 erfolgt entsprechend Fall 2 (herabgestuft wegen Diversität) mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9. Die SRASW realisiert die erforderliche Fehlererkennung. T1 wird mittels softwarebasierter manueller Parametrierung mit dem dafür vorgesehenen Parametrierungswerkzeug des Herstellers eingestellt. Die Anforderungen zur softwarebasierten manuellen Parametrierung nach Abschnitts 6.3 der Norm sind erfüllt.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion besteht aus zwei Teilsystemen der Kategorie 3. Im ersten Teilsystem wurde Not-Halt-Gerät und die redundante Abschaltung zusammengefasst. Das zweite Teilsystem besteht aus dem gekapseltem Teilsystems des Not-Halt-Schaltgeräts.
- Das Not-Halt-Gerät S3 ist mit zwei Öffnerkontakten S3.1 und S3.2 ausgestattet. Für die Blöcke S3.1 und S3.2 gibt der Hersteller jeweils einen B_{10D} = 127 500 Zyklen an. Bei einer jährlichen Betätigung und einem n_{op} = 1 Zyklus/Jahr ergibt sich für jeden Kontakt eine $MTTF_D$ = 1275 000 Jahre. Das Not-Halt-Sicherheitsschaltgerät K4 liegt als geprüftes Sicherheitsbauteil der Kategorie 3, PL d vor. Seine Ausfallhäufigkeit beträgt $3{,}0 \cdot 10^{-7}$/Stunde und wird am Ende der Berechnung addiert.
- ***MTTF*$_D$:** Die SPS K5 hat eine $MTTF_D$ von 10 Jahre. Der Frequenzumrichter hat eine $MTTF_D$ von 35 Jahre. Der Kondensator C1 geht mit $MTTF_D$ von 45 662 Jahren in die Berechnung ein. Für K1 und K2 ergibt sich bei einem B_{10D}-Wert von 5 000 000 Zyklen und einer Schalthäufigkeit von täglichem Einschalten an 240 Arbeitstagen eine $MTTF_D$ von 208 333 Jahren. Für K3 ergibt sich bei einem B_{10D}-Wert von 2 000 000 Zyklen und bei 240 Arbeitstagen, 16 Arbeitsstunden und 3 Minuten Zykluszeit eine n_{op} = 76 800 Zyklen/Jahr eine $MTTF_D$ von 260 Jahren. Für Q1 ergibt sich bei einem B_{10D}-Wert von 600 000 Zyklen und bei 240 Arbeitstagen, 16 Arbeitsstunden und 3 Minuten Zykluszeit eine n_{op} = 76 800 Zyklen/Jahr eine $MTTF_D$ von 78 Jahren.
- ***DC*$_{avg}$:** Eine ausreichende Testhäufigkeit der Not-Halt Geräte ist gewährleistet (siehe Hinweise in den Abschnitten 6.2.14 und D.2.5.1). Die Fehlererkennung der Blöcke S3.1 und S3.2 erfolgt durch einen Kreuzvergleich in K4 (*DC* = 90 %). Fehlererkennung durch den Prozess

bei Ausfall der Ansteuerung der Bremsrampe führt auf einen *DC* von 90% für K5. Für T1 ergibt sich ein *DC* von 60 % ebenfalls aus der Fehlererkennung durch den Prozess. Zur Bestimmung der *DC* ist die bekannte Zyklenzahl von 76 800 als Prozessdiagnoserate (Testrate r_t) zugrunde gelegt worden. Bei eine jährlichen Anforderungsrate r_d für die Sicherheitsfunktion führt dies zum Verhältnis $r_t/r_d = 76\,800$. Dies entspricht laut Norm Tabelle E.1 Anmerkung 3 einem *DC*-Wert von 99 %.
K1 und K2 weisen eine *DC* von 99 % durch die integrierte Fehlererkennung in K4 auf und für K3 gilt ein *DC* von 99 % wegen der Fehlererkennung durch K5. Für C1 gilt *DC* = 60 % durch Testung des Zeitglieds bei spannungsfreiem FU über die Abfallzeit von Hilfsschütz K3 in der SPS. Für Q1 folgt ein *DC* von 99 % durch eine direkte Überwachung in K5. Die Mittelungsformel für DC_{avg} ergibt 64,5 % („niedrig“).

- ***CCF***: Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte): Trennung (15), Diversität (20), FMEA (5) und Umgebungsbedingungen (25 + 10).
- Die Gebrauchsdauer des verschleißbehafteten Elements Q1 endet nach Ablauf von T_{10D} = 7,8 Jahren. Danach verliert die PFH-Berechnung ihre Grundlage. Ein rechtzeitiger Austausch wird empfohlen
- **PL:** Bei der Kombination des Teilsystems des redundanten Stillsetzens und des Not-Halt-Geräts ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von *PFH* = $4{,}4 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Die Gesamtausfallhäufigkeit für SF6.1 wird durch Addition der *PFH* von K4 zur Häufigkeit gefährlicher Ausfälle von $6{,}9 \cdot 10^{-7}$/Stunde ermittelt. Dies entspricht PL d.

Weiterführende Literatur

- *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld, R.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA-Report 4/2018. Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2018. https://publikationen.dguv.de/forschung/ifa/ifa-report/3500/sichere-antriebssteuerungen-mit-frequenzumrichtern-ifa-report-4/2018
- IEC 61800-5-2:2016-04 Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional. IEC Central Office, Switzerland CH-1211, Geneva 2016

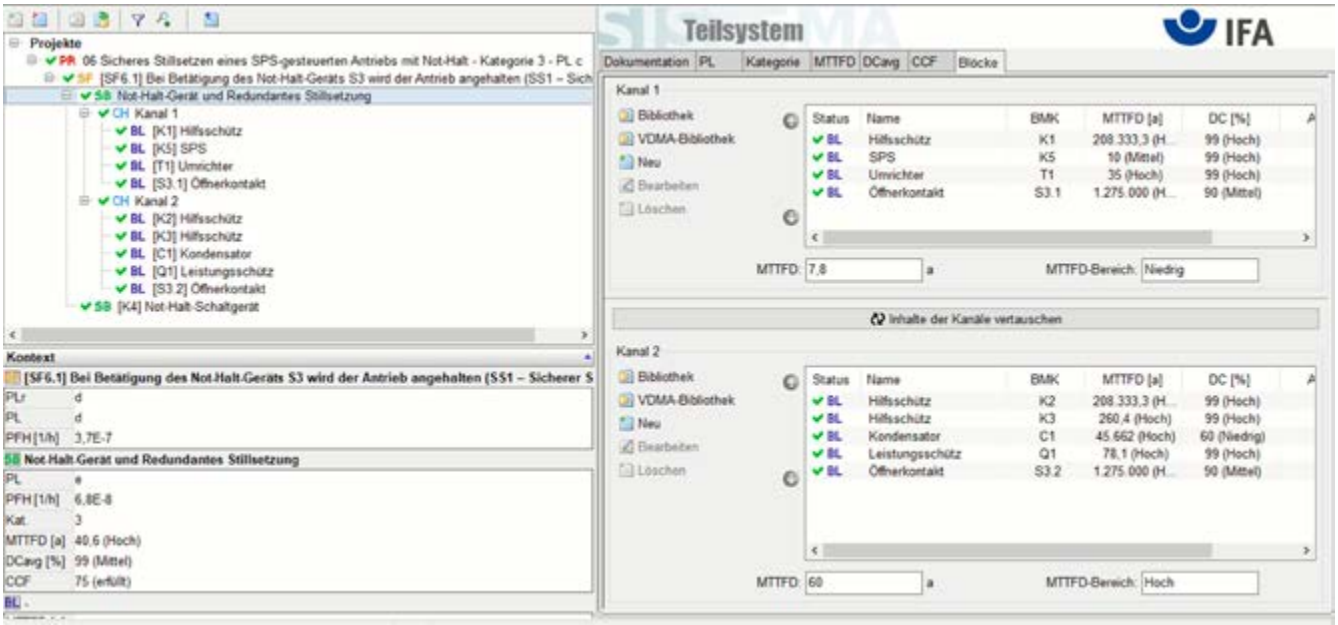


Abb. 11.14 PL-Bestimmung mithilfe von SISTEMA

11.2.7 Getestetes pneumatisches Ventil (Teilsystem) – Kategorie 2 – PL d (Beispiel 7)

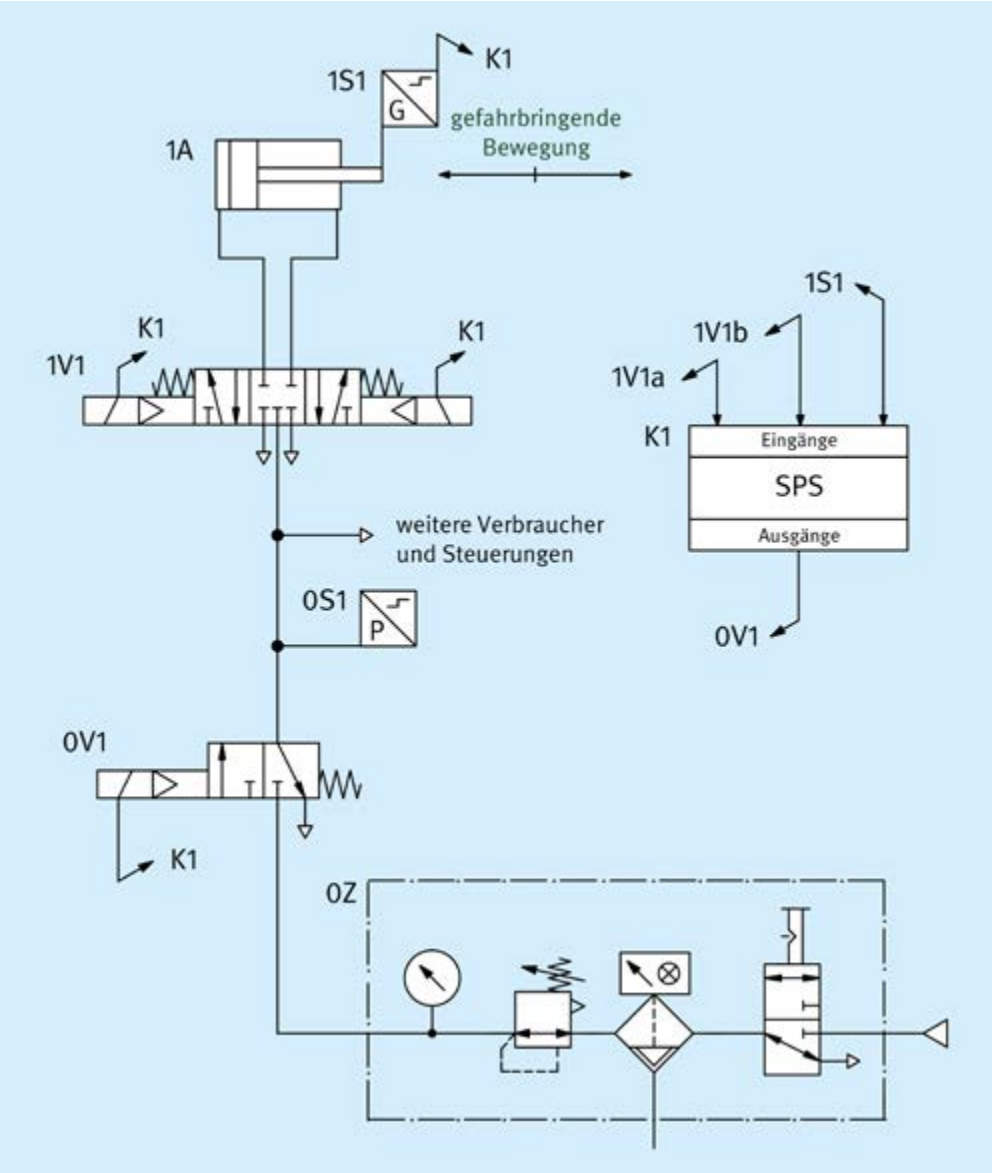


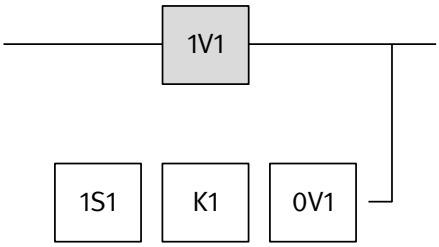
Abb. 11.15
Pneumatisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- SF7.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, durch die Sicherheits-Teilfunktion SSC und bei erkannten Fehlern (Ausfallerkennung) durch die Sicherheits-Teilfunktion SDE.
- Hier ist nur der pneumatische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch ein Wegeventil 1V1 gesteuert.
- Der Ausfall des Wegeventils 1V1 zwischen den Funktionstests kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion über die SPS K1 mithilfe eines Wegmesssystems 1S1 in geeigneten Zeitabständen und beim Anfordern der Sicherheitsfunktion. Das Erkennen des Ausfalls von 1V1 führt zum Abschalten des Entlüftungsventils 0V1.
- Das Unterbrechen der gefahrbringenden Bewegung über das Entlüftungsventil 0V1 ergibt in der Regel einen verlängerten Nachlaufweg. Der Abstand zum Gefahren-



bereich muss auf den verlängerten Nachlaufweg ausgelegt sein.
- Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.
- Wenn durch eingesperrte Druckluft eine weitere Gefährdung auftreten kann, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V1 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Testung erfolgt z. B. durch Überprüfung des Weg-/Zeitverhaltens (Wegmesssystem 1S1) der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einer SPS (K1).
- Die elektrische Ansteuerung von 1V1 darf nicht aus K1 erfolgen.
- In geeigneten Zeitabständen, z. B. täglich, wird zur Verhinderung eines systematischen Ausfalls die übergeordnete Abschaltfunktion (in diesem Beispiel auf das Entlüftungsventil 0V1 wirkend) überprüft.
- Für den Einsatz in Anwendungen mit seltenem Eingriff in den Gefahrbereich vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2 erfüllt werden. Die Anforderung besagt, dass die Testung unmittelbar bei Anforderung der Sicherheitsfunktion erfolgt und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand, beispielsweise unter Berücksichtigung des Nachlaufweges, der u. a. von der Entlüftungszeit und den Schaltzeiten der Ventile abhängt (hier wird über das Ventil 0V1 übergeordnet entlüftet), kürzer ist als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855 und vgl. Abschnitt 6.2.14).
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das pneumatische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Für die Standardkomponente K1 im Testkanal reduzieren sich die Anforderungen an die SRESW um einen Performance Level von PL d nach PL c. Die Einhaltung der SRESW-Anforderungen ist durch die Hersteller nicht bestätigt und kann durch den Integrator nicht nachträglich geleistet werden (nicht zugängliche Embedded-Software). Nach Abschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da für die Standardkomponente K1 im Testkanal die Anforderungen auf PL c reduziert wurde und zusätzlich die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Technologien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt.
- Die Programmierung der Software (SRASW) der Standardkomponente K1 erfolgt entsprechend Fall 2 (herabgestuft wegen Testkanal) mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9. Die SRASW realisiert die erforderliche Fehlererkennung für 1V1.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 2.
- ***MTTF*$_D$** des Funktionskanals: Für das Wegeventil 1V1 wird ein B_{10D}-Wert von 20 000 000 Schaltspielen 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 angenommen. Für die SPS K1 wird ein $MTTF_D$-Wert von 50 Jahren angenommen. Für das Entlüftungsventil 0V1 gilt ein B_{10D}-Wert von 20 000 000 Zyklen. 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“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).

- **PL**: Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_D$ (72,3 Jahre) und niedrigem DC_{avg} (60 %). Für SF7.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $7{,}6 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer. Die Gebrauchsdauer des verschleißbehafteten Elements 1V1 endet nach Ablauf von $T_{10D} = 7$ Jahren. Danach verliert die *PFH*-Berechnung ihre Grundlage. Ein rechtzeitiger Austausch wird empfohlen.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022.

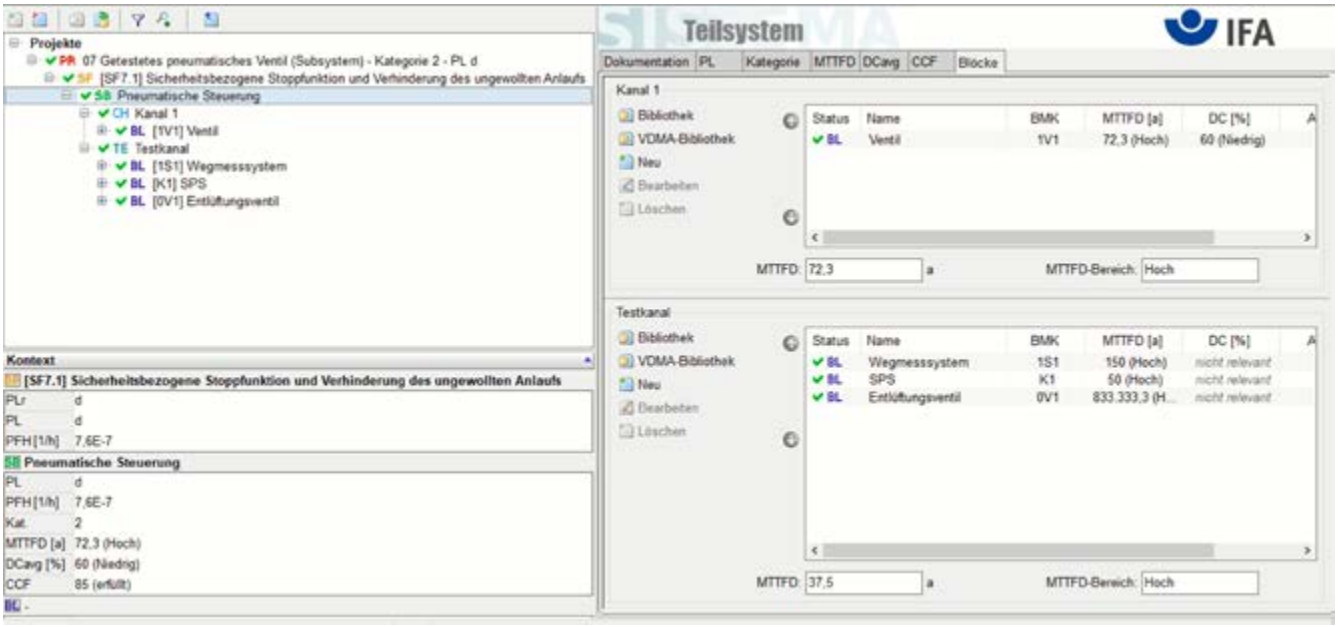


Abb. 11.16 PL-Bestimmung mithilfe von SISTEMA

11.2.8 Getestetes hydraulisches Ventil (Teilsystem) – Kategorie 2 – PL d (Beispiel 8)

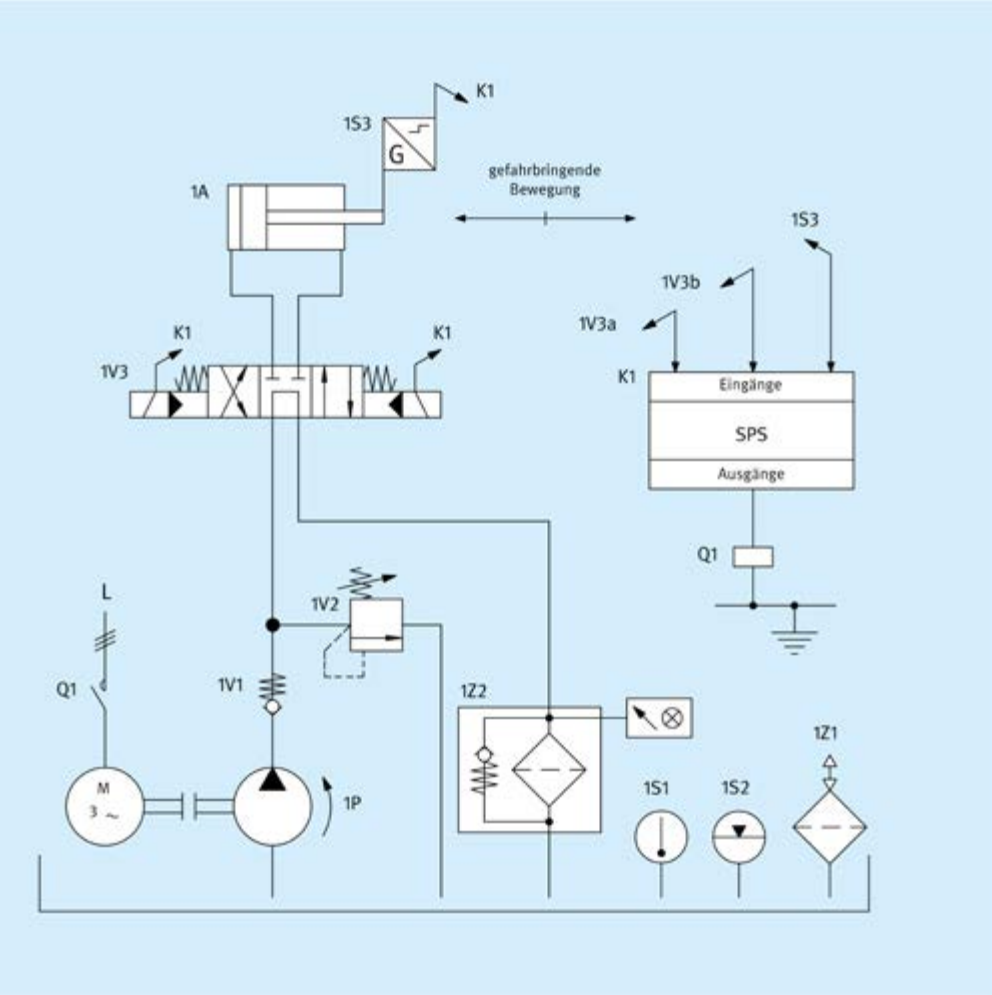


Abb. 11.17
Hydraulisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

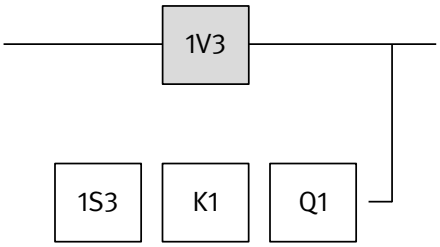
- SF8.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, durch die Sicherheits-Teilfunktion SSC und bei erkannten Fehlern (Ausfallerkennung) durch die Sicherheits-Teilfunktion SDE.
- Hier ist nur der hydraulische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme 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 Ausfallhäufigkeit hängt von der Zuverlässigkeit des Wegeventils ab.
- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion über die SPS K1 mithilfe eines Wegmesssystems 1S3 in geeigneten Zeitabständen und beim Anfordern der Sicherheitsfunktion. Das Erkennen des Ausfalls von 1V3 führt zum Abschalten der Hydraulikpumpe 1M bzw. 1P mittels Leistungsschütz Q1.
- Das Unterbrechen der gefahrbringenden Bewegung über die Hydraulikpumpe ergibt in der Regel einen verlängerten Nachlaufweg. Der Abstand zum Gefahrenbereich muss auf den verlängerten Nachlaufweg ausgelegt sein.
- Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V3 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.



- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Testung erfolgt z. B. durch Überprüfung des Weg-/Zeitverhaltens (Wegmesssystem 1S3) der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einer SPS (K1). Die elektrische Ansteuerung von 1V3 darf nicht aus K1 erfolgen.
- In geeigneten Zeitabständen, z. B. täglich, wird zur Verhinderung eines systematischen Ausfalls die übergeordnete Abschaltfunktion (in diesem Beispiel auf die Hydraulikpumpe wirkend) überprüft.
- Für den Einsatz in Anwendungen mit seltenem Eingriff in den Gefahrbereich vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2 erfüllt werden. Die Anforderung besagt, dass die Testung unmittelbar bei Anforderung der Sicherheitsfunktion erfolgt und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand, beispielsweise unter Berücksichtigung des Nachlaufweges, kürzer ist als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855 und vgl. Abschnitt 6.2.14).
- **EMI**: Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das hydraulische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Für die Standardkomponente K1 im Testkanal reduzieren sich die Anforderungen an die SRESW um einen Performance Level von PL d nach PL c. Die Einhaltung der SRESW-Anforderungen ist durch die Hersteller nicht bestätigt und kann durch den Integrator nicht nachträglich geleistet werden (nicht zugängliche Embedded-Software). Nach Abschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da für die Standardkomponente K1 im Testkanal die Anforderungen auf PL c reduziert wurde und zusätzlich die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Technologien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt.
- Die Programmierung der Software (SRASW) der Standardkomponente K1 erfolgt entsprechend Fall 2 (herabgestuft wegen Testkanal) mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9. Die SRASW realisiert die erforderliche Fehlererkennung für 1V3.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 2.
- ***MTTF*$_D$** des Funktionskanals: Für das Wegeventil 1V3 wird eine $MTTF_D$ von 150 Jahren angenommen. Dies ist gleichzeitig der $MTTF_D$-Wert für den Funktionskanal, der zunächst auf 100 Jahre gekürzt wird.
- ***MTTF*$_D$** des Testkanals: Für das Wegmesssystem 1S3 wird ein $MTTF_D$-Wert von 91 Jahren angenommen. Für die SPS K1 wird ein $MTTF_D$-Wert von 50 Jahren angenommen. Für das Leistungsschütz Q1 gilt ein B_{10D}-Wert von 1300 000 Zyklen. Bei täglichem Einschalten an 240 Arbeitstagen ergibt sich ein $MTTF_D$-Wert für Q1 von 54 166 Jahren. Damit beträgt die $MTTF_D$ des Testkanals 32,3 Jahre. Die $MTTF_D$ des Funktionskanals muss deshalb nach dem zugrunde liegenden Berechnungsmodel auf 64,5 Jahre gekürzt werden.
- ***DC*$_{avg}$:** DC = 60 % für 1V3 gründet sich auf den Vergleich des Weg-/Zeitverhaltens der gefahrbringenden Bewegung in Verbindung mit dem Schaltzustand des Wegeventils. Dies ist gleichzeitig der DC_{avg} („niedrig“).
- **CCF**: Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- **PL**: Die Kombination der Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_D$ (75 Jahre) und niedrigem DC_{avg} (60 %). Für SF8.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $8{,}7 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022.

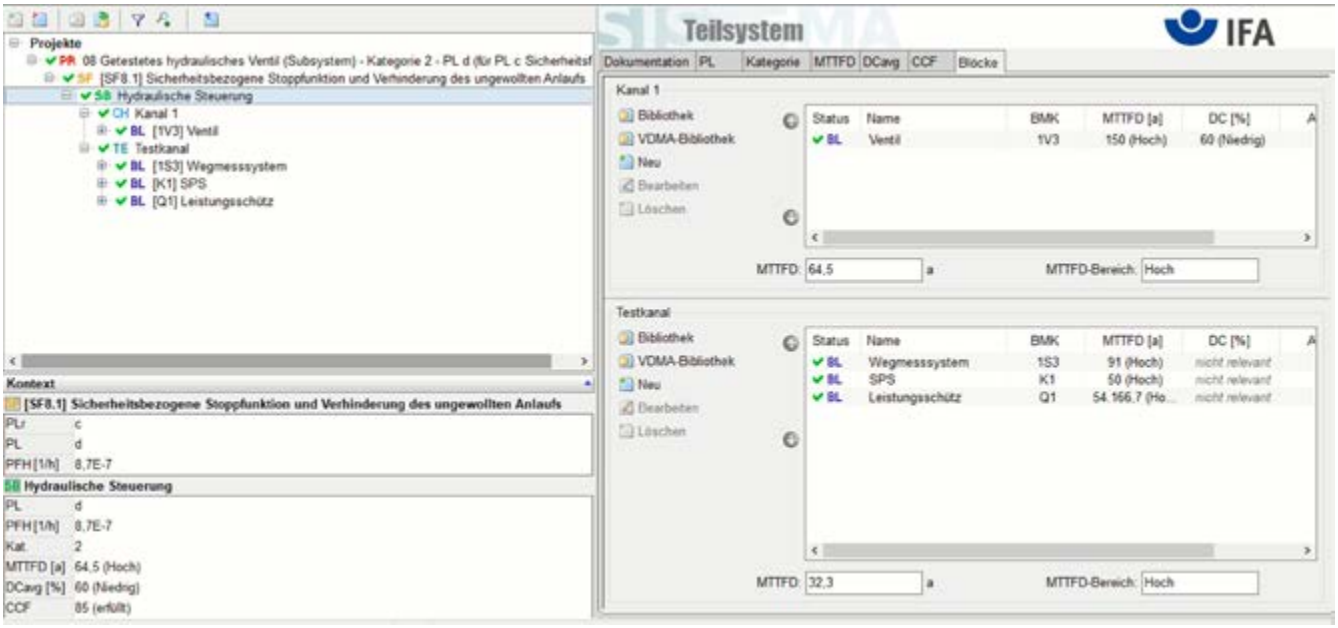


Abb. 11.18 PL-Bestimmung mithilfe von SISTEMA

11.2.9 Unterlasterkennung für Leuchtenhänger – Kategorie 2 – PL d (Beispiel 9)

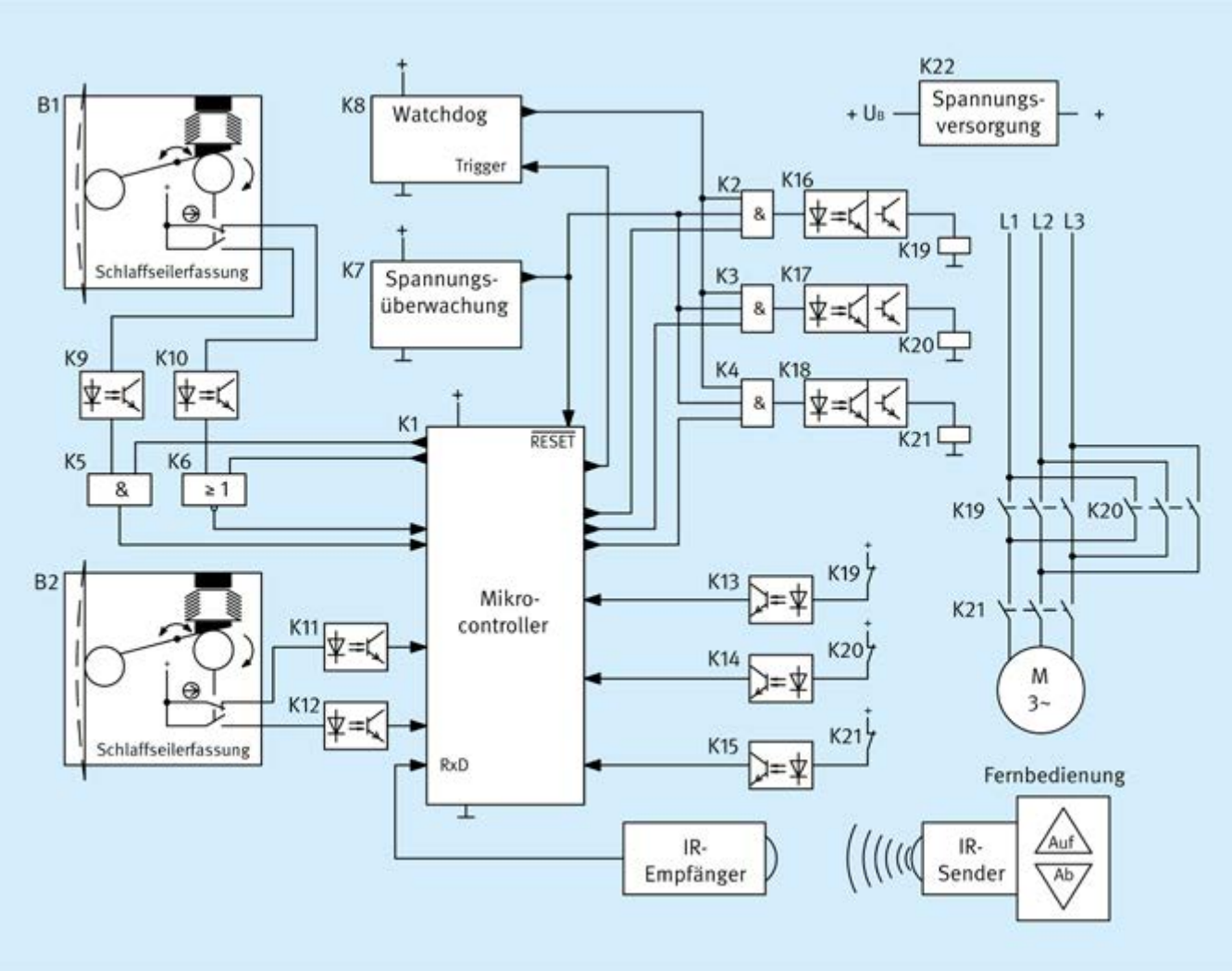


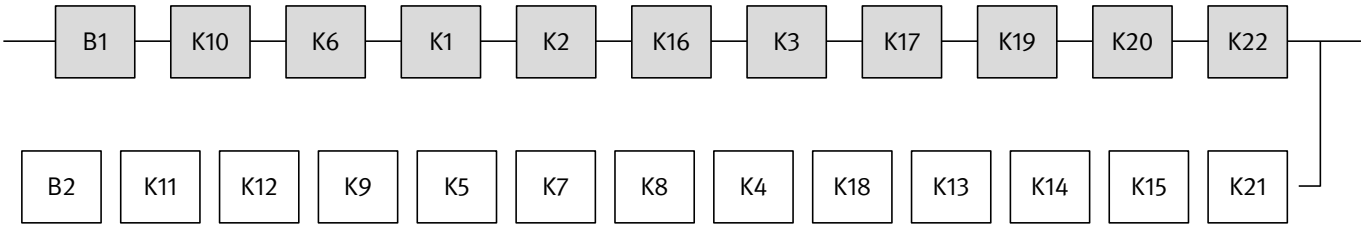
Abb. 11.19 Kombinierte elektromechanische und programmierbare elektronische Steuerung zur Verhinderung der Unterlast von Leuchtenhängern

Sicherheitsfunktion

- SF9.1: Unterlast- bzw. Schlaffseilerkennung: Bei Erkennung der Unterlast eines Leuchtenhängers (schlaffes Tragmittel/Seil) wird die Abwärtsbewegung gestoppt (Sicher abgeschaltetes Moment, STO).

Funktionsbeschreibung

- In der Studio- und Bühnentechnik werden zahlreiche elektromotorisch betriebene Leuchtenhänger eingesetzt. Bei der Abwärtsbewegung besteht die Gefahr, dass Unterlast (d. h. das Tragmittel wird schlaff) durch Verklemmen oder Verkanten der geführten Last oder durch Aufsetzen auf andere Gegenstände auftritt. Hierbei besteht die Gefahr, dass z. B. das Hindernis plötzlich nachgibt, die Last durchschlägt und in der Folge Personen in diesem Bereich gefährdet werden.
- Auf- und Abwärtsbewegungen des Leuchtenhängers können z. B. über eine Infrarot-Fernbedienung gesteuert werden. Diese Funktion wird hier nicht bewertet, sie ist aber immer sicherheitsgerichtet auszuführen.
- Um einen Absturz des Leuchtenhängers durch Reißen eines Tragmittels zu vermeiden, wird die Last von zwei Tragmitteln getragen. An jedem Tragmittel befindet sich ein Schlaffseilschalter B1 bzw. B2 mit einer Öffner-Schließer-Kombination.
- Der Mikrocontroller K1 wertet die Schaltzustände der Schlaffseilschalter B1 und B2 aus. Weiterhin steuert K1 über Logikgatter K2/K3 und optoentkoppelte Transistorverstärker K16/K17 die Hilfsschütze K19 und K20 für die Auf- bzw. Abwärtsbewegung des Leuchtenhängers an.
- Die Schaltzustände der Kontakte der Schlaffseilschalter B1 und B2 werden vom Mikrocontroller K1 ausgewertet und auf Plausibilität geprüft. Zur Testung der verwendeten Eingänge des Mikrocontrollers werden die Signale des Schlaffseilschalters B1 zwangsdynamisiert.



Hierzu erzwingt der Mikrocontroller über Logikgatter K5 und K6 einen kurzzeitigen Wechsel der Signale, um festzustellen, ob die Eingänge den Signalwechsel noch übertragen können. Die Zwangsdynamisierung der Signale eines Schlaffseilschalters ist ausreichend.

- Im Mikrocontroller K1 werden Selbsttests der integrierten Einheiten wie Recheneinheit, Arbeits- und Festwertspeicher durchgeführt. Die Spannungsüberwachung K7 überwacht die mit K22 erzeugte Versorgungsspannung. Fehler im Mikrocontroller werden durch eine zeitliche Programmlaufüberwachung im Watchdog K8 erkannt. Die Bauteile K19 bis K21 zur Steuerung der Auf- bzw. Abwärtsbewegung des Leuchtenhängers werden mithilfe einer Rücklesung – entkoppelt durch Optokoppler K13 bis K15 – im Mikrocontroller überwacht. Im Falle eines erkannten Fehlers erfolgt eine übergeordnete Abschaltung über das Hilfsschütz K21 – angesteuert durch Logikgatter K4 und entkoppelt durch Optokoppler K18 – durch das fehlererkennende Bauteil. Wird der Watchdog K8 nicht rechtzeitig vom Mikrocontroller K1 retriggert, erfolgt ausgehend von K8 über alle Logikgatter K2 bis K4 ein Stillsetzen der Bewegung des Leuchtenhängers.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 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.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Die Programmierung der Software (SRESW) von K1 erfolgt entsprechend Fall 3 mit Maßnahmen nach Tabelle N.3 der Norm und den Hinweisen in Kapitel 9.

Bemerkungen

- DIN 56950-2 fordert in Abschnitt 5.2.1 zwei Tragmittel, um den Absturz eines Leuchtenhängers und seiner Last zu verhindern.
- In geeigneten Zeitabständen sind Sichtprüfungen bzw. Wartungen der Tragmittel vorzunehmen.
- Die gezeigte Schaltungsstruktur ist in Teilen nicht explizit dazu ausgelegt, mögliche Gefährdungen durch unerwartete Bewegungen des Leuchtenhängers zu verhindern.
- Die verwendete Schaltungsstruktur erreicht für die betrachtete Sicherheitsfunktion – wie die Berechnung der Ausfallhäufigkeit zeigt – PL d. Die Anwendung des Risikographen zur Bestimmung der erforderlichen Performance Level PL_r mit den Parametern S2, F1 und P1 führt nach DIN 56950-2, Abschnitt A.1.2.3.3 unter der Voraussetzung, dass der Betrieb mit Beaufsichtigung erfolgt und dass die Leuchtenhänger nur von Fachleuten betrieben werden, auf einen PL_r = c. Ist dies nicht der Fall, ist PL_r = d erforderlich.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 2.
- Zur besseren Übersicht werden in Abbildung 11.19 Bauteile zusammengefasst. K9 bis K15 enthalten je einen Optokoppler und zwei Widerstände. K16 bis K18 enthalten zusätzlich je einen Transistor zur Ansteuerung der nachfolgenden Hilfsschütze.
- Zur Anwendung des vereinfachten Verfahrens für die Abschätzung des erreichten PL werden die Bauteile der Schaltung wie folgt den Blöcken der vorgesehenen Architektur für Kategorie 2 zugewiesen:
  I: B1
  L: K10, K6, K1, K2, K16, K3, K17, K22
  O: K19, K20
  TE: B2, K11, K12, K9, K5, K7, K8, K4, K18, K13, K14, K15
  OTE: K21
- ***MTTF*$_D$:** Die für die Berechnung benötigten $MTTF_D$-Werte stammen vorrangig aus DIN EN ISO 13849-1, SN 29500-2 und SN 29500-14. Für B1 und B2 liegen folgende Kennwerte vor: B_{10D} = 100 000 Zyklen, n_{op} = 10 Zyklen/Jahr. Für die Hilfsschütze K19 bis K21 gilt: B_{10D} = 400 000 Zyklen, n_{op} = 10 Zyklen/Tag an 365 Arbeitstagen. Für den Mikrocontroller K1 wird eine

$MTTF_D$ von 1142 Jahren angesetzt. Für die elektronischen Bauteile werden folgende $MTTF_D$-Werte angesetzt: 4566 Jahre für den Watchdog K8, 5707 Jahre für die Optokoppler K9 bis K18, 22831 Jahre für die Logikgatter K2 bis K6, 38052 Jahre für die Spannungsüberwachung K7 und 45662 Jahre für Transistoren bzw. 228310 Jahre für Widerstände. Für die Spannungserzeugung K22 liegt die Herstellerangabe $MTTF_D$ = 228 Jahre vor. Durch Aufsummierung der Ausfallraten aller Bauteile des Funktionskanals (Blöcke I, L und O) ergibt sich eine $MTTF_D$ von 128 Jahren. Diese wird gemäß den Anforderungen der Norm auf 100 Jahre begrenzt („hoch“).

- Die $MTTF_D$ des Testkanals ergibt sich durch Aufsummierung der Ausfallraten aller Bauteile der Blöcke TE und OTE. Sie beträgt 389 Jahre und ist damit größer oder gleich der Hälfte der $MTTF_D$ des Funktionskanals.
- **DC_{avg}:** DC = 90 % für B1, K10 und K6 durch Kreuzvergleich von B1 und B2 in K1 gemäß Anmerkung 4 der Tabelle E.1 der Norm zum Effekt der Testrate ($r_t \geq 1$/Jahr).
  DC = 60 % für K1 durch zeitliche Programmlaufüberwachung und Selbsttests einfacher Wirksamkeit.
  DC = 99 % für K2, K3, K16, K17, K19 und K20 durch direkte Überwachung über zwangsgeführte Kontakte. Für K22 ist DC = 99 %. Die Mittelungsformel für DC_{avg} ergibt 94 % („mittel“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10)
- **PL:** Die Kombination der Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_D$ des Funktionskanals (100 Jahre) und mittlerem DC_{avg} (94 %). Für die SF9.1 ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls PFH von $2{,}3 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN 56950-2: Veranstaltungstechnik – Maschinentechnische Einrichtungen – Teil 2: Sicherheitstechnische Anforderungen an bewegliche Leuchtenhänger (9/2014). DIN Media, Berlin 2014
- DGUV Information 215-310: Sicherheit bei Veranstaltungen und Produktionen – Leitfaden für Theater, Film, Hörfunk, Fernsehen, Konzerte, Shows, Events, Messen und Ausstellungen (bisher BGI 810). Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2016. http://publikationen.dguv.de/dguv/pdf/10002/215-310.pdf
- SN 29500: Ausfallraten Bauelemente, Erwartungswerte. Hrsg.: Siemens AG, CT TIM Regulation & Standardization, München 2004-2016

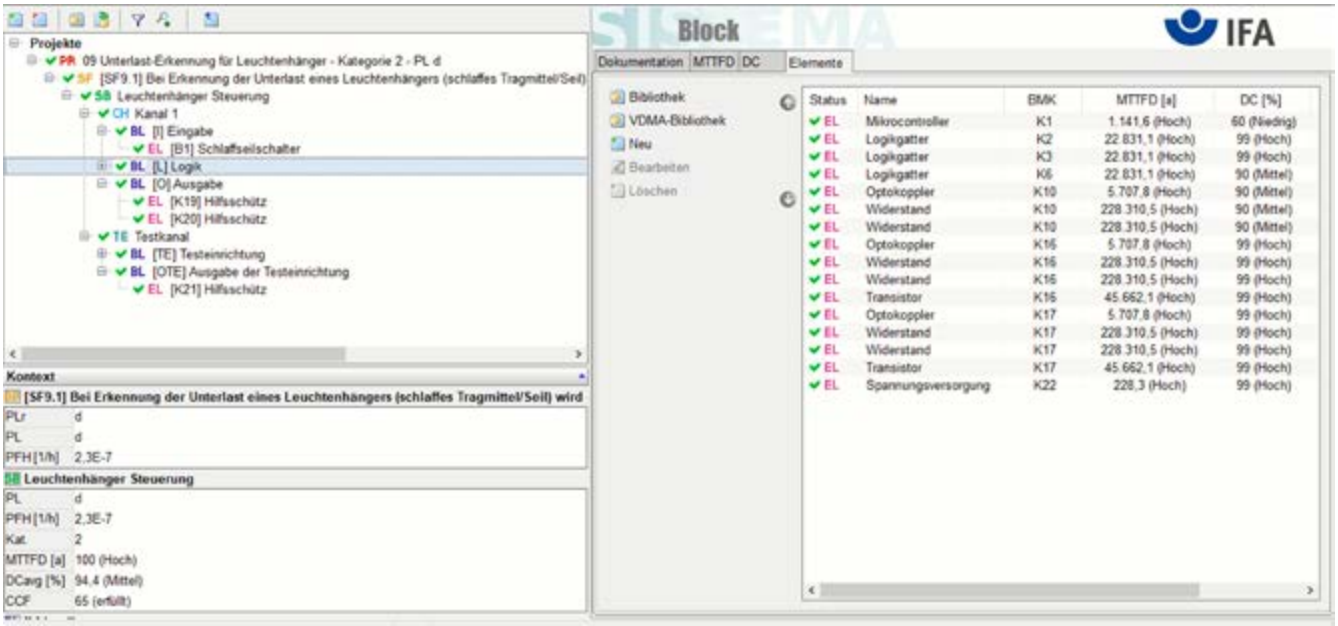


Abb. 11.20 PL-Bestimmung mithilfe von SISTEMA

11.2.10 Pneumatische Ventilsteuerung (Teilsystem) – Kategorie 3 – PL d (Beispiel 10)

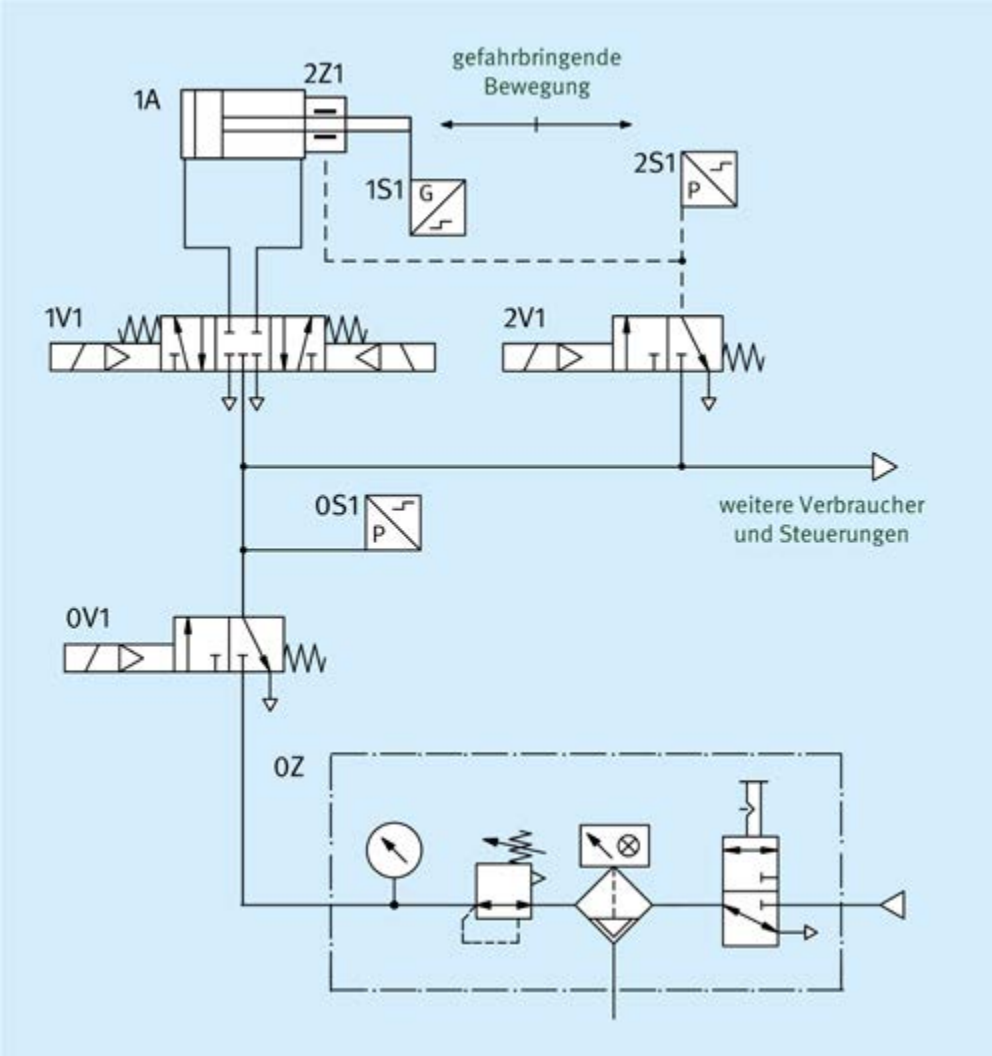


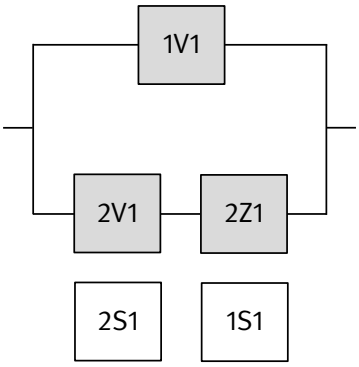
Abb. 11.21
Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- SF10.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktionen SSC und SBC.
- Hier ist nur der pneumatische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme 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.
- Die Wegeventile und die 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 acht Arbeitsstunden.
- Durch den Ausfall der Bremse darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zum Ausfall der Bremse führen.
- Kann durch eingesperrte Druckluft eine weitere Gefährdung auftreten, sind weitere Maßnahmen erforderlich.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Das Wegeventil 1V1 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das pneumatische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Die Signalverarbeitung der Drucküberwachung 2S1 und des Wegmesssystems 1S1 erfolgt beispielsweise in einer einkanaligen SPS außerhalb der Funktionskanäle (nicht dargestellt). Die Programmierung der Software (SRASW) realisiert die erforderliche Fehlererkennung für 2V1 und 2Z1. Es wird durch ein herstellerinternes Verfahren sichergestellt, dass die zur Fehlererkennung erforderliche SRASW auch tatsächlich in der SPS implementiert ist. An die nicht zugängliche Embedded-Software in der einkanaligen SPS zur Diagnose außerhalb der Funktionskanäle werden keine Anforderungen gestellt.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 3.
- ***MTTF*$_D$:** Für die Wegeventile 1V1 und 2V1 werden B_{10D}-Werte von 20 000 000 Zyklen angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 15 Sekunden Zykluszeit ist n_{op} = 921600 Zyklen/Jahr. Für 1V1 und 2V1 ergibt sich damit eine $MTTF_D$ = 217 Jahre. Für die mechanische Bremse an der Kolbenstange 2Z1 wird ein B_{10D}-Wert von 5 000 000 Schaltspielen eingesetzt. Das ergibt für die mechanische Bremse $MTTF_D$ = 54 Jahre. Insgesamt ergibt sich ein symmetrisierter $MTTF_D$-Wert pro Kanal von 75 Jahren („hoch“).
- Die Gebrauchsdauer des verschleißbehafteten Bremse 2Z1 endet nach Ablauf von T_{10D} = 5 Jahren. Danach verliert die *PFH*-Berechnung ihre Grundlage. Ein rechtzeitiger Austausch wird empfohlen.
- ***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 (Prozessdiagnoserate sehr viel größer als die Anforderungsrate der Sicherheitsfunktion). DC = 75 % für 2Z1 folgt aus einer Anlauftestung der mechanischen Bremse. Durch Mittelung ergibt sich damit ein DC_{avg} von 77 % („niedrig“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL**: Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (75 Jahre) und niedrigem DC_{avg} (76 %). Für SF10.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $1{,}1 \cdot 10^{-7}$ / Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022.

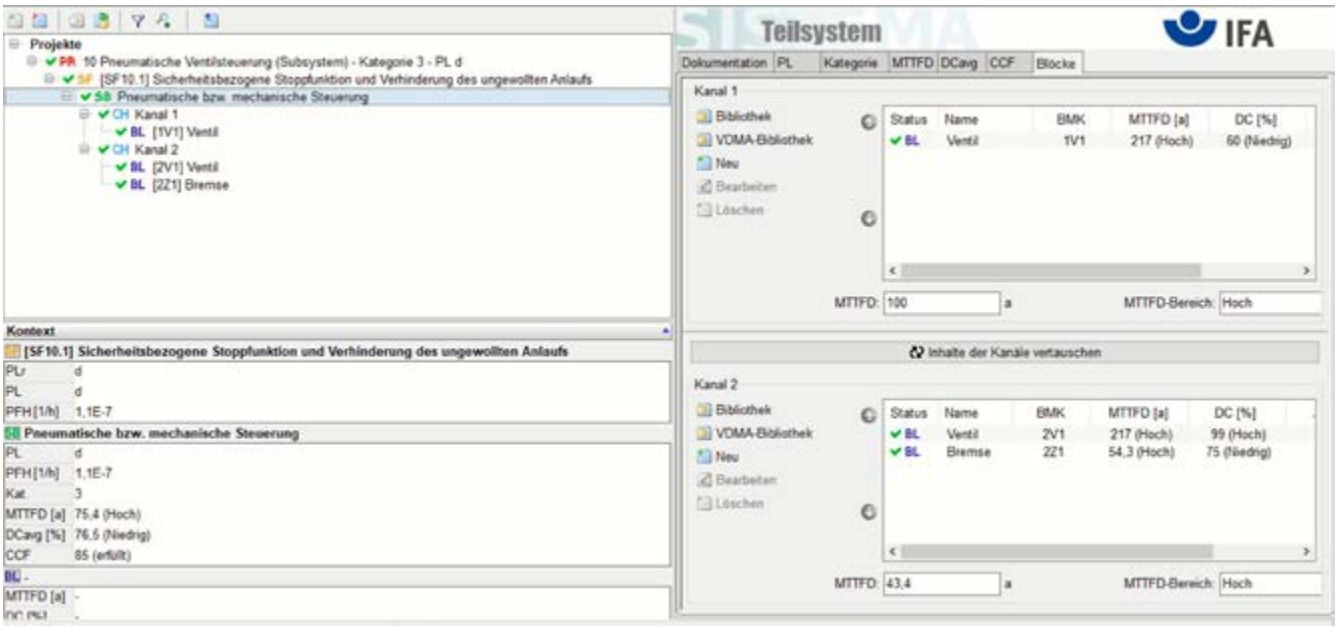


Abb. 11.22 PL-Bestimmung mithilfe von SISTEMA

11.2.11 Schutzeinrichtung und SPS-gesteuerte Hydraulik – Kategorie 3 – PL d (Beispiel 11)

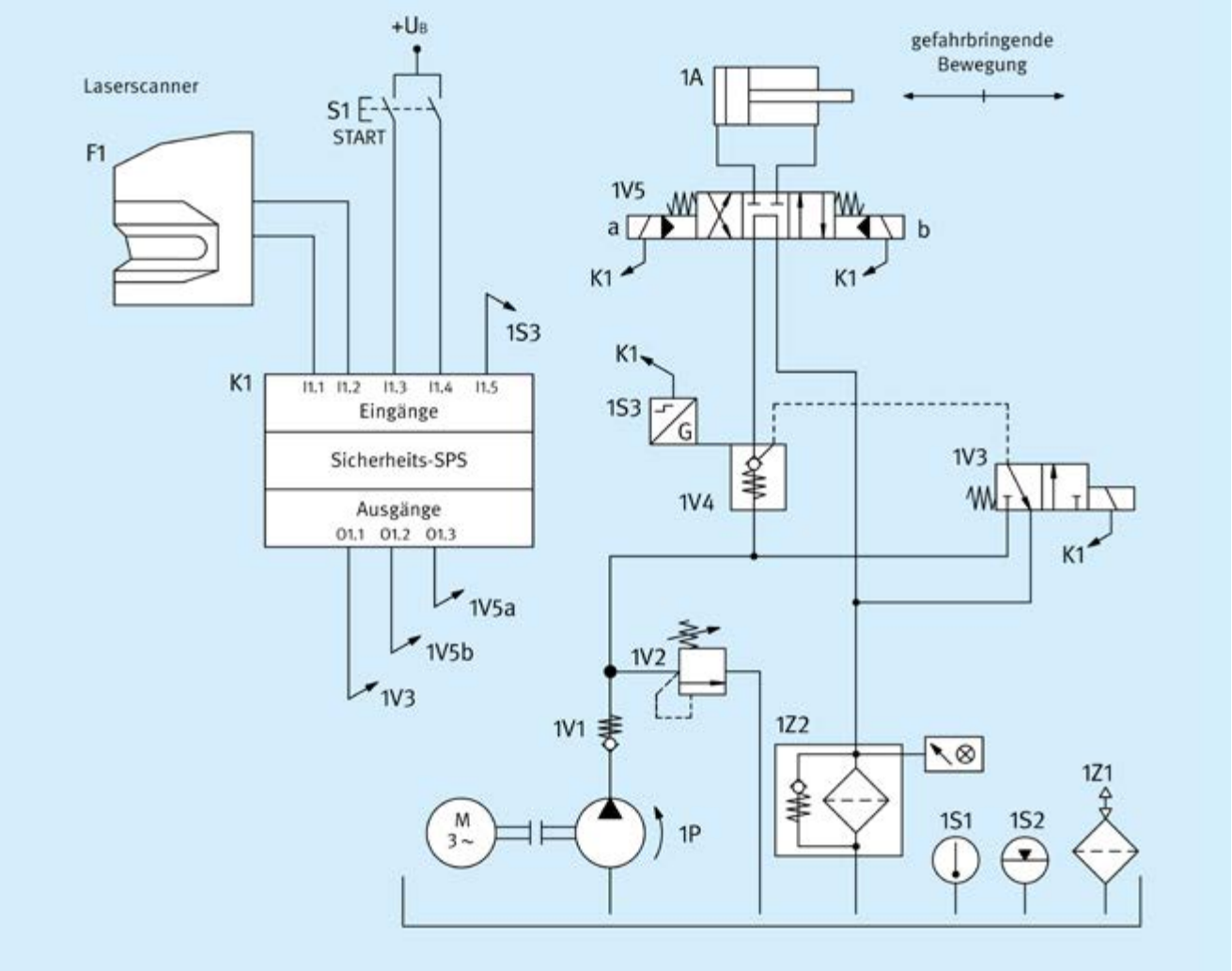


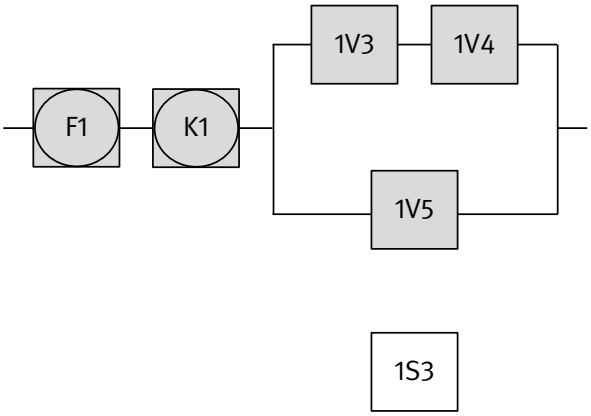
Abb. 11.23 Schutzfeld-Überwachung durch Laserscanner mit elektrohydraulischer Abschaltung der gefahrbringenden Bewegung

Sicherheitsfunktion

- SF11.1: Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Ein Eindringen in das Schutzfeld des Laserscanners führt zu einem Stillsetzen der gefahrbringenden Bewegung.

Funktionsbeschreibung

- Der Laserscanner F1 überwacht mit seinem Schutzfeld den Bereich, in dem die Bewegung des Zylinders 1A für die Bedienperson gefährlich werden kann. Das Ausgangssignal des Laserscanners wird zweikanalig in die Sicherheits-SPS K1 eingelesen. Nach jeder Schutzfeldverletzung muss eine erneute Bewegung durch die Betätigung eines in K1 ausgewerteten Start-Tasters S1 freigegeben werden (Wiederanlaufsperre). K1 steuert mithilfe des hydraulischen Teilsystems die Bewegung von 1A.
- Das hydraulische Teilsystem ist zweikanalig aufgebaut. Der erste Kanal besteht aus dem Wegeventil 1V3, das auf das entsperrbare Rückschlagventil 1V4 wirkt. In gesperrter Stellung blockiert 1V4 Bewegungen von 1A. Der zweite Kanal besteht aus dem Richtungsventil 1V5, das in Sperr-Mittelstellung ebenfalls eine Bewegung von 1A verhindert.
- 1V5 wird zyklisch im Prozess angesteuert, 1V3 und 1V4 schließen nur bei einer Verletzung des Schutzfeldes (Anforderung der Sicherheitsfunktion), jedoch mindestens einmal pro Schicht.
- Als Maßnahme zur Fehlererkennung ist an 1V4 eine direkte Stellungsüberwachung 1S3 vorgesehen, die in K1 ausgewertet wird. Fehler in 1V5 können funktionsbedingt über den Prozess erkannt werden. Die Anhäufung unentdeckter Fehler im hydraulischen Steuerungsteil kann zum Verlust der Sicherheitsfunktion führen.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 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 entsprechen. Der Laserscanner F1 entspricht auch Typ 3 nach Produktnorm.
- 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.
- 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.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Die Programmierung der Software (SRASW) von K1 erfolgt entsprechend Fall 3 mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus drei Teilsystemen der Kategorie 3.
- Da der Laserscanner F1 und die Sicherheits-SPS K1 als zuvor validierte Teilsysteme vorliegen, werden deren Ausfallhäufigkeiten am Ende der Berechnung addiert (F1: PFH = $8{,}0 \cdot 10^{-8}$/Stunde, K1: PFH = $2{,}5 \cdot 10^{-9}$/Stunde). Für das hydraulische Teilsystem wird die Ausfallhäufigkeit im Folgenden berechnet.
- ***MTTF*$_D$:** Für die Ventile 1V3, 1V4 und 1V5 werden Werte von je 150 Jahren angenommen. Damit ergibt sich insgesamt ein symmetrisierter *MTTF*$_D$-Wert von 88 Jahren („hoch“) für die beiden Kanäle.
- ***DC*$_{avg}$:** *DC* = 99 % für 1V4 ergibt sich durch die direkte Überwachung in K1 mithilfe der Stellungsüberwachung 1S3. Wegen der engen Kopplung von 1V3 und 1V4 wird 1V3 dadurch mit einem *DC* von 99 % indirekt mit überwacht. *DC* = 60 % für 1V5 gründet sich auf die Fehlererkennung im Prozess bei zyklischer Ansteuerung (Prozessdiagnoserate sehr viel größer als die Anforderungsrate der Sicherheitsfunktion). Durch Mittelung ergibt sich damit ein *DC*$_{avg}$ von 86 % („niedrig“).
- **CCF**: 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 Teilsystem entspricht Kategorie 3 mit hoher MTTF$_D$ pro Kanal (88 Jahre) und niedrigem *DC*$_{avg}$ (86 %). Damit ergibt sich für die Hydraulik eine mittlere Häufigkeit gefahrbringender Ausfälle von $6{,}2 \cdot 10^{-8}$/Stunde.
- **PL**: Für SF11.1: beträgt die mittlere Häufigkeit gefahrbringender Ausfälle
  PFH = $(8{,}0 + 0{,}25 + 6{,}2) \cdot 10^{-8}$/Stunde = $1{,}4 \cdot 10^{-7}$/Stunde.
  Dies entspricht PL d.

Weiterführende Literatur

- *Bömer, T.*: Hinweise zum praktischen Einsatz von Laserscannern (Kennzahl 310 243). In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 02/2020. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. 2. Aufl. 2003. Erich Schmidt, Berlin 2003 – Losebl.-Ausg. https://www.ifa-handbuchdigital.de/IFA-HB_310243
- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022.

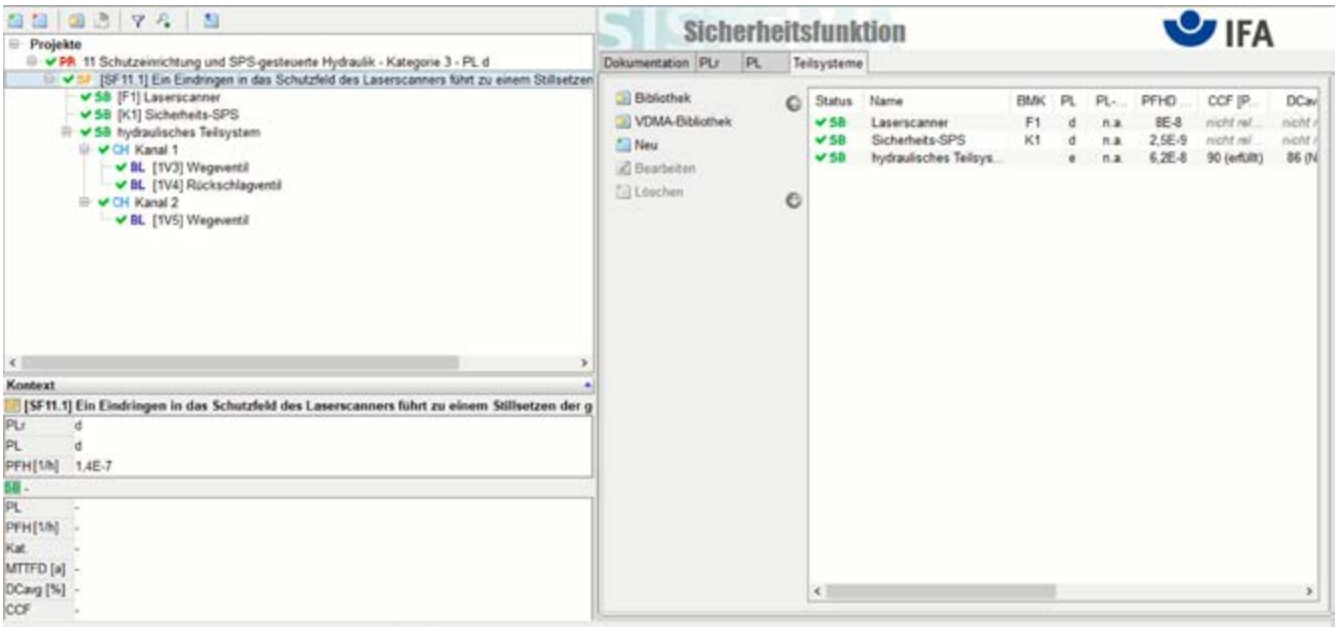


Abb. 11.24 PL-Bestimmung mithilfe von SISTEMA

11.2.12 Erdbaumaschinensteuerung mit Bussystem – Kategorie 2 bzw. 3 – PL d (Beispiel 12)

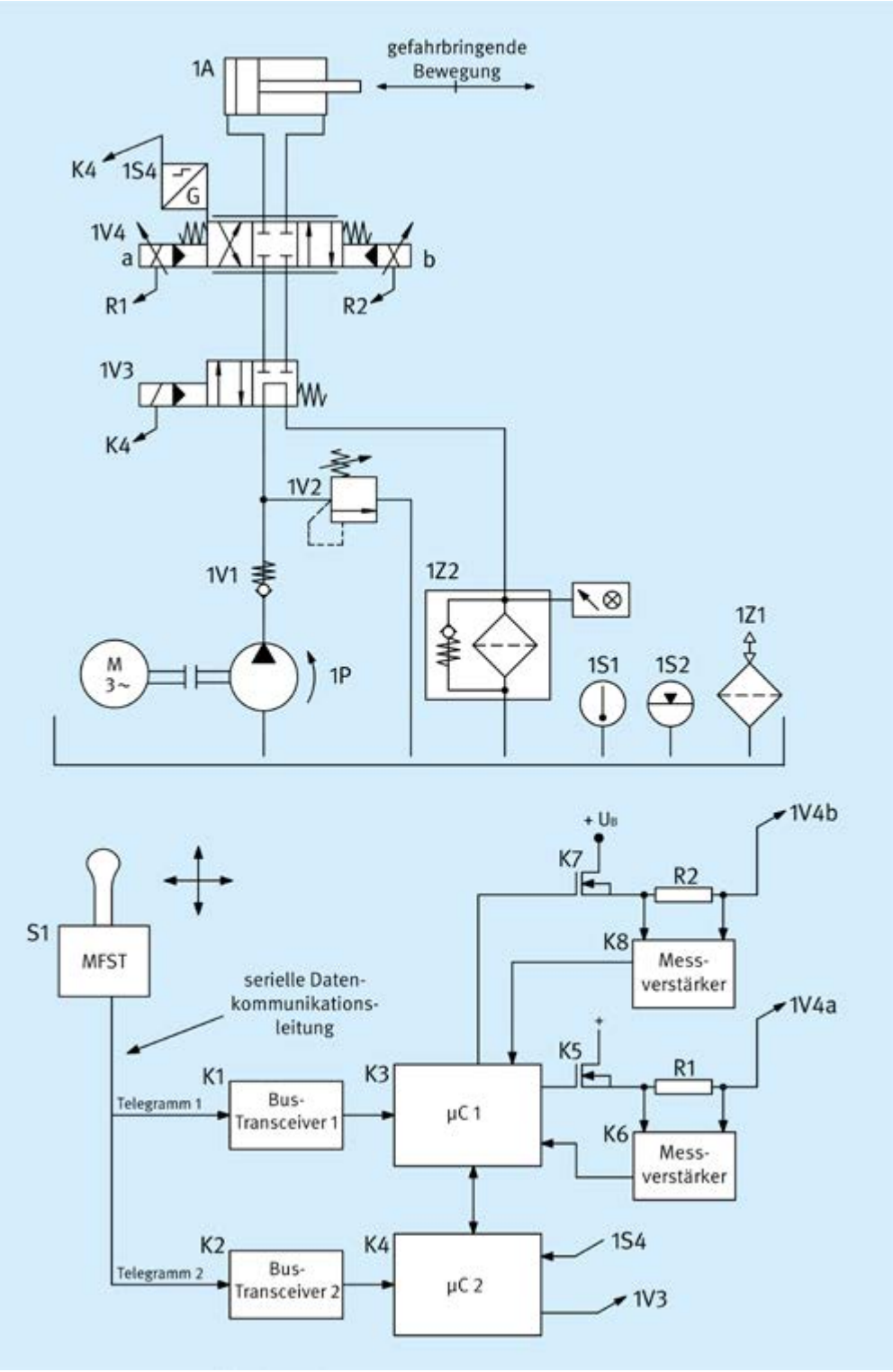
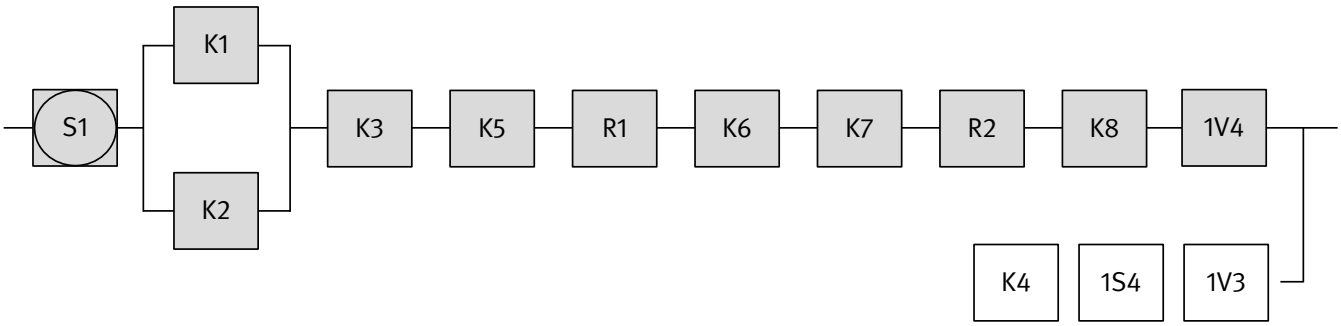


Abb. 11.25
Ansteuerung von gefahrbringenden Bewegungen einer Erdbaumaschine

Sicherheitsfunktion

- SF12.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage der Arbeitsgeräte von Erdbaumaschinen, realisiert durch die Sicherheits-Teilfunktion SSC (safe stopping and closing).
- Weitere sicherheitsrelevante Funktionen, wie Verhinderung der Anwahl einer fehlerhaften Bewegungsrichtung der Arbeitsgeräte der Erdbaumaschine, sind in diesem Beispiel nicht betrachtet.



Funktionsbeschreibung

- Das Multifunktionsstellteil (MFST) S1 wandelt die vom Bediener ausgeführte manuelle Auslenkung des MFST in elektronische Datentelegramme um. Es sendet diese Telegramme zyklisch über eine serielle Datenkommunikationsleitung (Bussystem) zur Logiksteuerung, die Ansteuersignale für die Hydraulik zur Ausführung der von der Bedienperson vorgesehenen Arbeitsbewegung der Erdbaumaschine erzeugt.
- Das vom MFST S1 gesendete Telegramm 1 gelangt über den Bus-Transceiver K1 in den Mikrocontroller K3. Dieser erzeugt aus Telegramm 1 gemäß den in der Software abgelegten Algorithmen die erforderlichen analogen Signale zur Ansteuerung des Proportionalventils 1V4. Die Widerstände R1/R2 und die Messverstärker K6/K8 dienen zur Regelung der Ausgangsströme für das Proportionalventil. Der Mikrocontroller K4 erhält ein redundantes Telegramm 2 von S1 über den Bus-Transceiver K2. K4 überprüft die korrekte Auslenkung des Proportionalventils 1V4 über das in 1V4 integrierte Wegmesssystem 1S4 innerhalb der Reaktionszeit bzw. Prozesssicherheitszeit auf Plausibilität gegen die aus Telegramm 2 ermittelte Sollstellung. Bei erkannten Fehlern schaltet K4 übergeordnet das Wegeventil 1V3 ab, sperrt den hydraulischen Druck und bringt damit 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 11 beschrieben, sind vorgesehen.
- Bei dem MFST handelt es sich um ein für den Einsatz in PL d geeignetes Sicherheitsbauteil, das der Kategorie 3 entspricht.
- Gemäß der Funktionsbeschreibung erfolgen die Verarbeitung der Steuerinformationen und die Ansteuerung der Ventile in einer Kategorie-2-Struktur. Dabei bilden K4 und 1S4 den Testkanal mit 1V3 als Abschaltelement des Testkanals.
- Aufgrund der kontinuierlichen Überwachung von 1V4 durch K4 über 1S4 kann ein Ausfall von 1V4 erkannt werden, sobald die Sicherheitsfunktion angefordert wird. 1V3 muss innerhalb der Reaktionszeit die sicherheitsgerichtete Reaktion ausführen, damit die Struktur der Steuerung der Kategorie 2 entspricht. Ein abruptes übergeordnetes Schalten von 1V3 darf nicht zu Gefährdungen führen.
- Das Proportionalventil 1V4 und das Wegeventil 1V3 haben eine Sperrstellung bzw. Sperr-Mittelstellung, Federrückstellung bzw. Federzentrierung und eine ausreichend positive Überdeckung.
- Die Datenübertragung vom MFST zur Logiksteuerung ist nach GS-ET-26 bzw. DIN EN IEC 61784-3 abgesichert. Das verwendete Datenkommunikationsprotokoll enthält redundante Telegramme mit Vergleich zwischen K3 und K4 und Maßnahmen, um folgende Übertragungsfehler zu erkennen: Wiederholung, Verlust, Einfügung, falsche Reihenfolge, Verfälschung, Verzögerung, Maskerade und fehlerhafte Adressierung (siehe auch Abschnitt 8.2.18). Die Restfehlerrate Λ ist geringer als $1 \cdot 10^{-8}$/Stunde und trägt damit wie von den Beurteilungsgrundlagen vorgesehen weniger als 1 % zur maximal zulässigen mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde der Sicherheitsfunktion bei. Die Modellierung erfolgt in Kategorie 4, der sich ergebende Anteil in der Berechnung der Gesamtausfallhäufigkeit ist vernachlässigbar.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel über die Produktnormen DIN EN ISO 13766-1 und DIN EN ISO 13766-2 nachgewiesen (Pfad A nach Anhang L der Norm).
- **Software:** Die Programmierung der Software (SRESW) von K3 erfolgt entsprechend Fall 3 mit Maßnahmen nach Tabelle N.3 der Norm und den Hinweisen in Kapitel 9. Die Programmierung der Software (SRESW) von K4 erfolgt entsprechend Fall 2 (herabgestuft wegen Testkanal) mit Maßnahmen nach Tabelle N.3 der Norm und den Hinweisen in Kapitel 9.

Bemerkung

- Eine eventuell erforderliche Notlauffunktion der Erdbaumaschine ist hier nicht dargestellt und übergeordnet zu realisieren.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Zur Berechnung der Ausfallhäufigkeit wird das Gesamtsystem in drei Teilsysteme „MFST“ Kategorie 3, „Datenkommunikation“ Kategorie 4 und „Logik- und Hydrauliksteuerung“ Kategorie 2 aufgeteilt.
- Das MFST S1 liegt als handelsübliches Sicherheitsbauteil vor. Die zugehörige Ausfallhäufigkeit wird am Ende der Berechnung addiert ($PFH = 3{,}0 \cdot 10^{-7}$/Stunde). Für den übrigen Steuerungsteil wird die Ausfallhäufigkeit im Folgenden berechnet.
- ***MTTF*$_D$** der Datenkommunikation: Für die Bus-Transceiver K1 und K2 wird eine $MTTF_D$ von 11 416 Jahren angesetzt. Diese wird in Kategorie 4 auf den Maximalwert von 2 500 Jahren begrenzt.
- ***DC*$_{avg}$** der Datenkommunikation: $DC = 99$ % für K1 und K2 durch Kreuzvergleich der Telegramme in den Mikrokontrollern K3 und K4.
- Die Ausfallhäufigkeit der Datenkommunikation ergibt sich zu $PFH = 9{,}1 \cdot 10^{-10}$/Stunde.
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10). Diese Betrachtung gilt auch für die nachfolgenden Steuerungsteile.
- ***MTTF*$_D$** des Funktionskanals der Logik- und Hydrauliksteuerung: Für den Mikrocontroller K3 einschließlich seiner Peripherie wird nach SN 29500-2 eine $MTTF_D$ von 878 Jahren berücksichtigt. Für die weiteren elektrischen Bauteile werden folgende Kenndaten angesetzt: 45 662 Jahre für die Schalttransistoren K5 und K7, 228 311 Jahre für die Widerstände R1 und R2 und 1 142 Jahre für die Messverstärker K6 und K8. Für das Proportionalventil 1V4 wird eine $MTTF_D$ von 150 Jahren angenommen. Damit beträgt der $MTTF_D$-Wert des Funktionskanals 104 Jahre.
- **MTTF$_D$** des Testkanals der Logik- und Hydrauliksteuerung: Für den Mikrocontroller K4 einschließlich seiner Peripherie wird nach SN 29500-2 eine $MTTF_D$ von 878 Jahren berücksichtigt. Für das Wegmesssystem 1S4 liegt die Herstellerangabe $MTTF_D = 75$ Jahre vor. Für das Wegeventil 1V3 wird eine $MTTF_D$ von 150 Jahren angenommen. Damit beträgt die $MTTF_D$ des Testkanals 47 Jahre. Für das in der Norm beschriebene vereinfachte Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL ist eine Bedingung, dass die $MTTF_D$ des Testkanals größer als die Hälfte der $MTTF_D$ des Funktionskanals ist. Daher wird die $MTTF_D$ des Funktionskanals auf 94 Jahre begrenzt.
- ***DC*$_{avg}$** des Funktionskanals der Logik- und Hydrauliksteuerung: $DC = 60$ % für K3 durch Kreuzvergleich mit K4 und Selbsttests einfacher Wirksamkeit durch Software; $DC = 90$ % für die restlichen elektrischen Bauteile durch Fehlererkennung in K4 mittels Wegmesssystem 1S4. $DC = 99$ % für 1V4 durch direkte Überwachung des Weges über 1S4 in K4. Die Mittelungsformel für DC_{avg} ergibt 93 % („mittel“).
- **PL**: Die Logik- und Hydrauliksteuerung entspricht Kategorie 2 mit hoher $MTTF_D$ des Kanals (94 Jahre) und mittlerem DC_{avg} (93 %). Damit ergibt sich eine durchschnittliche Häufigkeit eines gefahrbringenden Ausfalls von $PFH = 2{,}5 \cdot 10^{-7}$/Stunde.
- Die durchschnittliche Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion SF12.1 ergibt sich durch Addition der Anteile der Teilsysteme „MFST“, „Datenkommunikation“ und „Logik- und Hydrauliksteuerung“ und beträgt $PFH = 5{,}5 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN EN ISO 19014-2: Erdbaumaschinen – Funktionale Sicherheit – Teil 2: Entwurf und Bewertung von Hardware- und Architekturanforderungen für sicherheitsrelevante Teile des Steuerungssystems (11/2022). DIN Media, Berlin 2022
- DIN EN IEC 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile (2/2022). DIN Media, Berlin 2022
- Grundsätze für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“ (GS-ET-26) (3/2014). Hrsg.: DGUV Test, Prüf- und Zertifizierungsstelle der Deutschen Gesetzlichen Unfallversicherung, Köln 2014 https://www.dguv.de/dguv-test/prod-pruef-zert/pruefgrundsaetze-erfahrung/pruefgrundsaetze/elektrotechnik/index.jsp
- DIN EN ISO 13766-1: Erdbaumaschinen und Baumaschinen - Elektromagnetische Verträglichkeit von Maschinen mit internem elektrischen Bordnetz – Teil 1: Allgemeine EMV-Anforderungen unter typischen EMV-Umgebungsbedingungen (4/2019). DIN Media, Berlin 2019
- DIN EN ISO 13766-2: Erdbaumaschinen und Baumaschinen - Elektromagnetische Verträglichkeit von Maschinen mit internem elektrischen Bordnetz – Teil 2: Zusätzliche EMV-Anforderungen für die funktionale Sicherheit (12/2018). DIN Media, Berlin 2018
- SN 29500: Ausfallraten Bauelemente, Erwartungswerte. Hrsg.: Siemens AG, CT TIM Regulation & Standardization, München 2004-2016
- VDMA-Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022

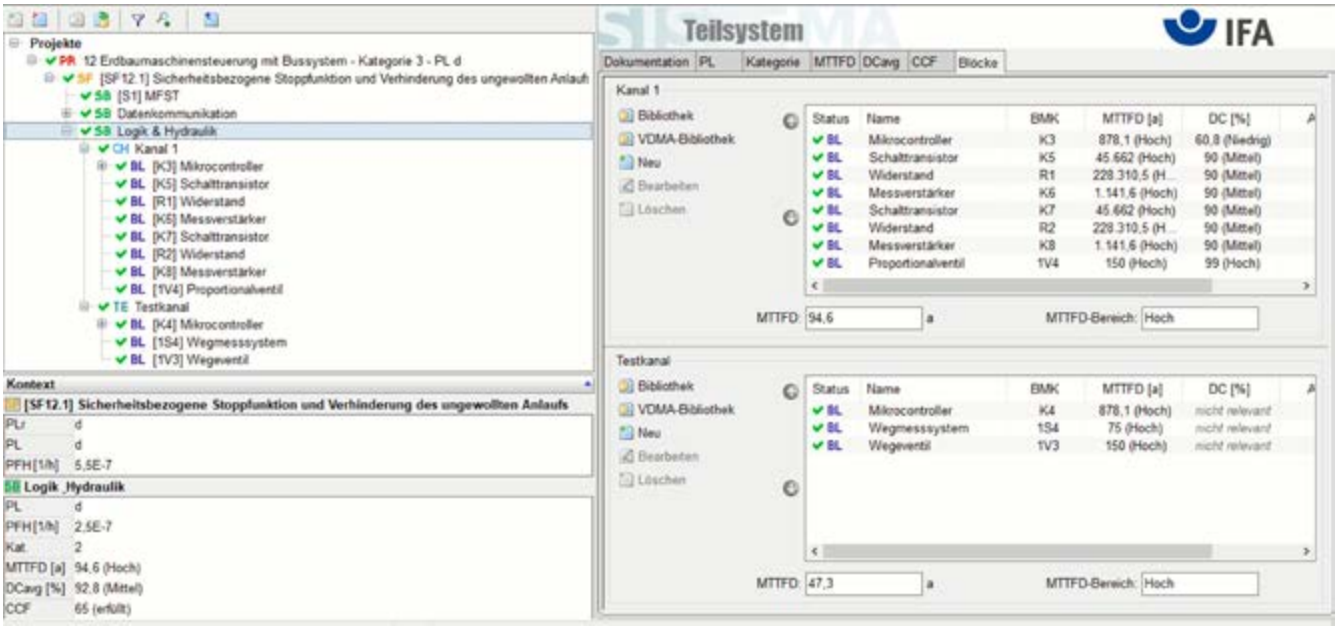


Abb. 11.26 PL-Bestimmung mithilfe von SISTEMA

11.2.13 Kaskadierung von Schutzeinrichtungen mittels Sicherheitsschaltgeräten – Kategorie 3 – PL d (Beispiel 13)

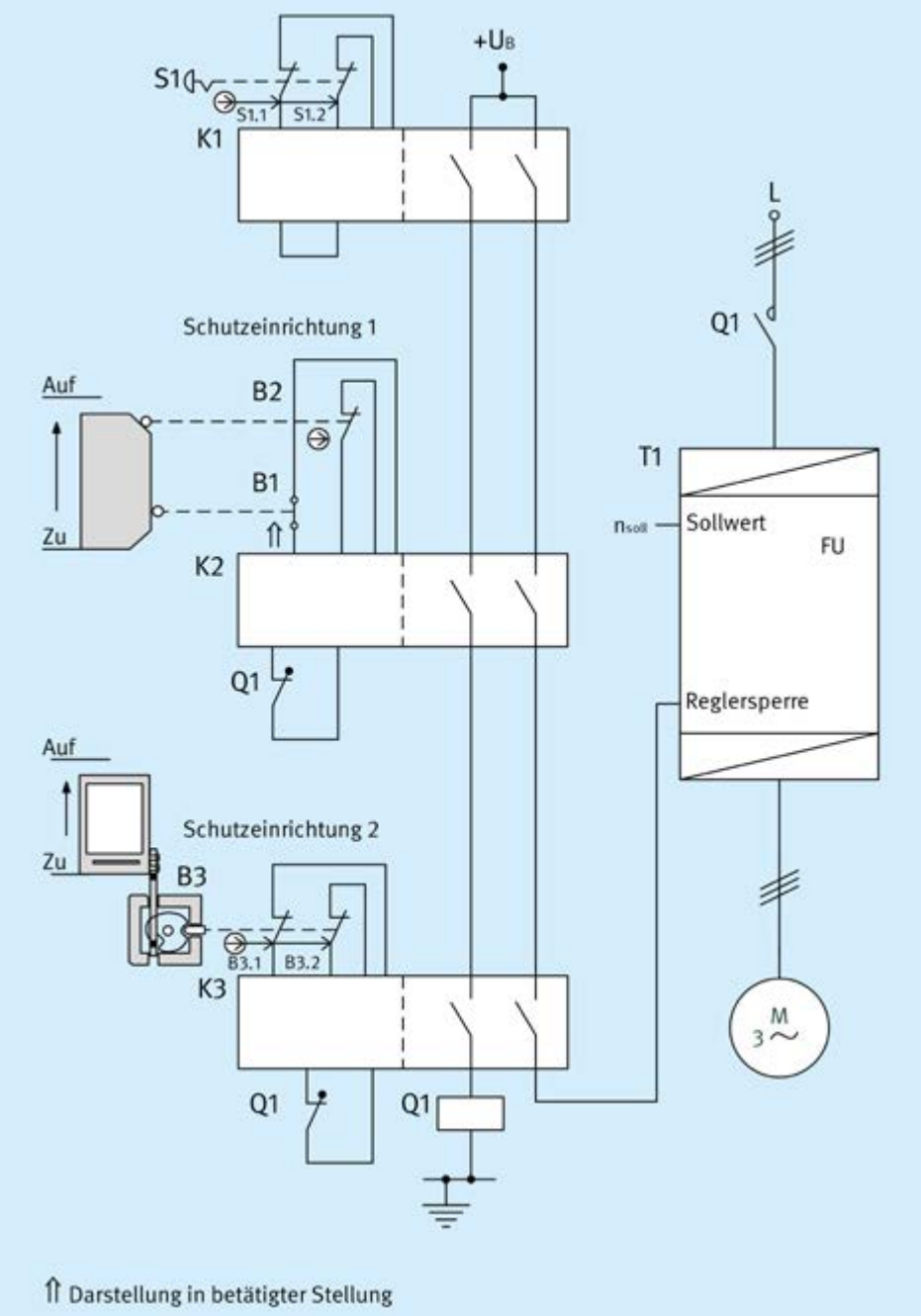


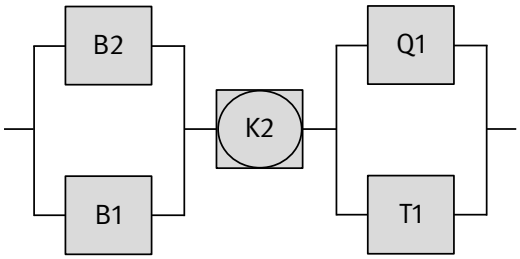
Abb. 11.27
Kaskadierung von Schutzeinrichtungen mittels Sicherheitsschaltgeräten (Not-Halt-Funktion, STO)

Sicherheitsfunktionen

- SF13.1: Das Öffnen der beweglichen trennenden Schutzeinrichtung 1 zur Beladung leitet die Sicherheitsfunktion Sicher abgeschaltetes Moment (STO) ein.
- SF13.2: Das Öffnen der beweglichen trennenden Schutzeinrichtung 2 zur Entladung leitet die Sicherheitsfunktion STO ein.
- SF13.3: Bei Betätigung des Not-Halt-Gerätes wird der Antrieb des Motors in STO geschaltet

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Geräts S1 mit zwei zwangsöffnenden Kontakten über das Sicherheitsschaltgerät K1 redundant durch Unterbrechung der Steuerspannung von Schütz Q1 und Anwahl der Reglersperre des Frequenzumrichters T1 abgeschaltet.
- Das Öffnen der Schutzeinrichtung 1 wird durch zwei Positionsschalter (Bauart 1) B1/B2 in Öffner-Schließer-Kombination erfasst und in einem Sicherheitsschaltgerät K2 ausgewertet. Dieser kann in gleicher Weise wie K1 gefahrbringende Bewegungen oder Zustände unterbrechen bzw. verhindern. Die Überwachung der Schutzeinrich-



tung 2 erfolgt durch einen Positionsschalter der Bauart 2 mit den Kontakten B3.1 und B3.2 und einem Sicherheitsschaltgerät K3, der ebenfalls auf Q1 und T1 wirkt.
- Bei Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten.
- Die meisten Bauteilausfälle werden erkannt und führen zur Betriebshemmung. Die Positionsschalter B1 und B2 an Schutzeinrichtung 1 werden im zugehörigen Sicherheitsschaltgerät, der auch über interne Diagnosemaßnahmen verfügt, auf Plausibilität überwacht.
- Die elektrischen Kontakte B3.1 und B3.2 werden im zugehörigen Sicherheitsschaltgerät K3, das ebenfalls über interne Diagnosemaßnahmen verfügt, auf Plausibilität überwacht.
- Fehler im Schütz Q1 werden über die Rücklesung des Spiegelkontakts in K2 und K3 erkannt. Eine zusätzliche Rücklesung in K1 ist nicht erforderlich, da die Diagnose indirekt über K2 und K3 realisiert ist und die Not-Halt-Funktion viel seltener angefordert wird. Ein großer Anteil der Fehler in T1 wird durch den Prozess erkannt. Einige wenige Fehler werden von der Steuerung nicht erkannt.
- Durch organisatorische Maßnahmen wird sichergestellt, dass das Not-Halt-Gerät mindestens einmal pro Jahr betätigt wird.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) und CCF-Maßnahmen, wie in den ersten Abschnitten von Kapitel 10 beschrieben, sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtungen zur Betätigung der Positionsschalter ist sichergestellt.
- Das Not-Halt-Gerät S1 mit den zwangsöffnenden Kontakten S1.1 und S1.2 entspricht DIN EN ISO 13850.
- Die Kontakte der Positionsschalter B2 und B3 sind zwangsöffnend entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern B1, B2 und B3 sind getrennt oder geschützt verlegt.
- Das Schütz Q1 besitzt Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F.
- Die Sicherheitsschaltgeräte K1, K2 und K3 erfüllen alle Anforderungen für Kategorie 4 und PL e mit PFH = $2{,}3 \cdot 10^{-9}$/Stunde.
- Der Frequenzumrichter T1 verfügt über keine integrierten Sicherheitsfunktionen.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt werden (siehe Anhang L der Norm).
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Bemerkungen

- Die Not-Halt-Funktion ist eine ergänzende Schutzmaßnahme nach DIN EN ISO 12100:201103.
- Zur Kaskadierung von Schutzeinrichtungen ist es erforderlich den Diagnosedeckungsgrad entsprechend TR 24119 anzupassen. In diesem Beispiel sind die Schutzeinrichtungen einzeln auf Sicherheitsbausteine geführt, daher muss die *DC* nicht reduziert werden.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die drei Sicherheitsfunktionen lassen sich in jeweils drei Teilsysteme darstellen. Das sicherheitsbezogene Blockdiagramm ist nur für die Sicherheitsfunktion 1 dargestellt. Für die zweite Schutzeinrichtung gilt eine vergleichbare Sicherheitsfunktion (SF13.2) mit nahezu identischer Berechnung der Ausfallhäufigkeit. Für den Betätiger des Positionsschalters B3 ist ein Fehlerausschluss für das Brechen zu begründen.
- ***MTTF*$_D$ (SF13.1):** Bei dem Schalter B1 handelt es sich um einen Positionsschalter mit Schließerkontakt. Der B_{10D} für den Schließerkontakt beträgt 100 000 Schaltspiele. Für den zwangsöffnenden Positionsschalter B2 mit Rollenbetätigung beträgt der B_{10D} = 20 000 000 Schaltspiele. Bei 220 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 21120 Zyklen/Jahr und $MTTF_D$ beträgt für B1 47,3 Jahre und für B2 9 469 Jahre. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes auf 2 000 000 Schaltspielen. Da Q1 an beiden sicherheitsbezogenen Stoppfunktionen beteiligt ist, folgt mit dem doppelten des oben angenommenen Wertes für n_{op} auf 42 240 eine $MTTF_D$ von 473 Jahren. Für den Frequenzumrichter T1 beträgt die $MTTF_D$ 10 Jahre. Insgesamt ergibt sich im Teilsystem Q1/T1 ein symmetrisierter $MTTF_D$-Wert

pro Kanal von 67,3 Jahren. Der Positionsschalter B1 weist eine begrenzte Betriebszeit von 4,7 Jahren auf. Ein rechtzeitiger Austausch wird empfohlen.

- ***MTTF*$_D$ (SF13.2):** Für den Positionsschalter B3 mit getrenntem Betätiger und den zwangsöffnenden Kontakten B3.1 und B3.2 ist für jeden Kontakt jeweils ein B_{10D}-Wert von 4 000 000 Zyklen angegeben. Bei 220 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 21120 Zyklen/Jahr und *MTTF*$_D$ beträgt 1893 Jahre. Für das Schütz Q1 entspricht bei induktiver Last (AC 3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen. Bei Annahme von 50 % gefahrbringender Ausfälle ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Da das Schütz Q1 an beiden sicherheitsbezogenen Stoppfunktionen (SF1 und SF2) beteiligt ist, folgt mit dem doppelten des angenommenen Wertes für n_{op} eine *MTTF*$_D$ von 473 Jahren. Für den Frequenzumrichter T1 beträgt die *MTTF*$_D$ 20 Jahre. Insgesamt ergibt sich im Teilsystem Q1/T1 ein symmetrisierter *MTTF*$_D$-Wert pro Kanal von 69 Jahre.
- ***MTTF*$_D$ (SF13.3):** Bei S1 handelt es sich um ein handelsübliches Not-Halt-Gerät nach DIN EN ISO 13850. Für das Not-Halt-Gerät gilt unabhängig von der Last, ein B_{10D}-Wert von 100 000 Schaltspielen für jeden Kontakt. Für n_{op} wird von drei Betätigungen im Jahr ausgegangen.
- ***DC*$_{avg}$:** *DC* = 99 % für B1 und B2 bzw. B3 beruht auf der Plausibilitätsüberwachung in K2 bzw. K3. Dies entspricht dem *DC*$_{avg}$ für das Teilsystem. *DC* = 99 % für das Schütz Q1 ergibt sich aus der Rücklesung der Kontaktstellung in den Sicherheitsschaltgeräten. Für den Frequenzumrichter T1 folgt *DC* = 60 % aus der Fehlererkennung durch den Prozess. Der Ausfall der Ansteuerung der Reglersperre des Umrichters T1 wird in der Anwendung erkannt. Zur Bestimmung der *DC* ist die bekannte Zyklenzahl von 42.240 als Prozessdiagnoserate (Testrate r_t) zugrunde gelegt worden. Bei Anforderungsrate r_d = 42.240 für die Sicherheitsfunktion führt dies zum Verhältnis r_t/r_d = 1. Dies entspricht einem *DC*-Wert von 60 % laut Norm Tabelle E.1 Anmerkung 3. Durch Mittelung ergibt sich damit für das Teilsystem Q1/T1 ein *DC*$_{avg}$ von 60,8 % („niedrig“). Eine ausreichende Testhäufigkeit des Not-Halt Gerätes ist gewährleistet (siehe Hinweise in den Abschnitten 8.2.14 und D.2.5.1).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Teilsystemen S1.1/S1.2, B2/B1, B3.1/B3.2 bzw. Q1/T2 (65, 70 bzw. 85 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10), in B2/B1 bewährte Bauteile (5), in Q1/T1 Diversität (20)
- **PL:** Die Teilsysteme B1/B2 und B3.1/B3.2 entsprechen Kategorie 4 mit hoher *MTTF*$_D$ und hoher *DC*$_{avg}$ (99 %). Damit ergibt sich jeweils eine mittlere Häufigkeit gefährlicher Ausfälle von $1{,}4 \cdot 10^{-9}$/Stunde und $1{,}2 \cdot 10^{-9}$/Stunde. Das Teilsystem Q1/T1 entspricht Kategorie 3 mit hoher *MTTF*$_D$ (67,3 Jahre) und niedrigem *DC*$_{avg}$ (60,8 %). Damit ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von $1{,}8 \cdot 10^{-7}$/Stunde für die Sicherheitsfunktionen SF13.1 und SF13.2. Für die Sicherheitsfunktion SF13.3 ergeben sich andere Werte für das Teilsystem Q1/T1. Aufgrund der geringen Anforderungsrate r_d der Not-Halt-Funktion (dreimal im Jahr) und einer Testrate r_t von 42.240 zu einem Verhältnis r_t/r_d = 14 080. Dies entspricht einem *DC*-Wert von 99 % laut Norm Tabelle E.1 Anmerkung 3 für den Umrichter T1.
- Für die Sicherheitsfunktion 13.1 ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von $1{,}9 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.
- Für die Sicherheitsfunktion 13.2 ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von $1{,}9 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.
- Für die Sicherheitsfunktion 13.3 ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von $2{,}1 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

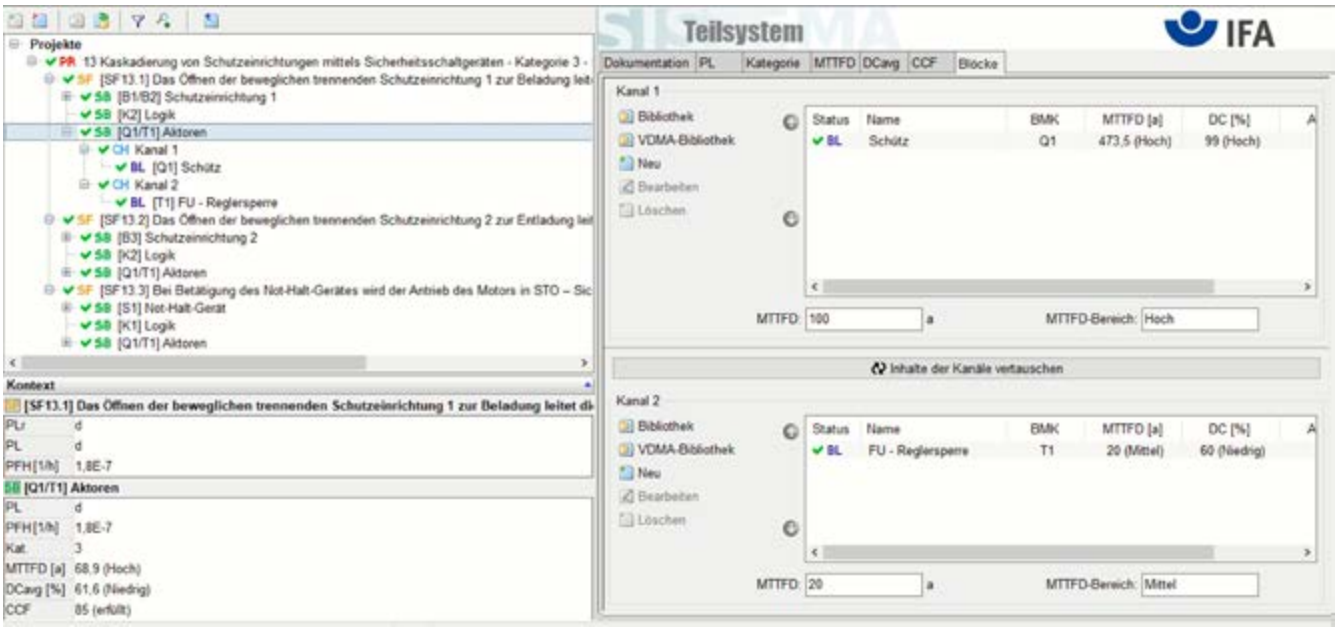


Abb. 11.28 PL-Bestimmung mithilfe von SISTEMA

11.2.14 Verriegelungseinrichtung mit Zuhaltung – Kategorie 3 – PL d (Beispiel 14)

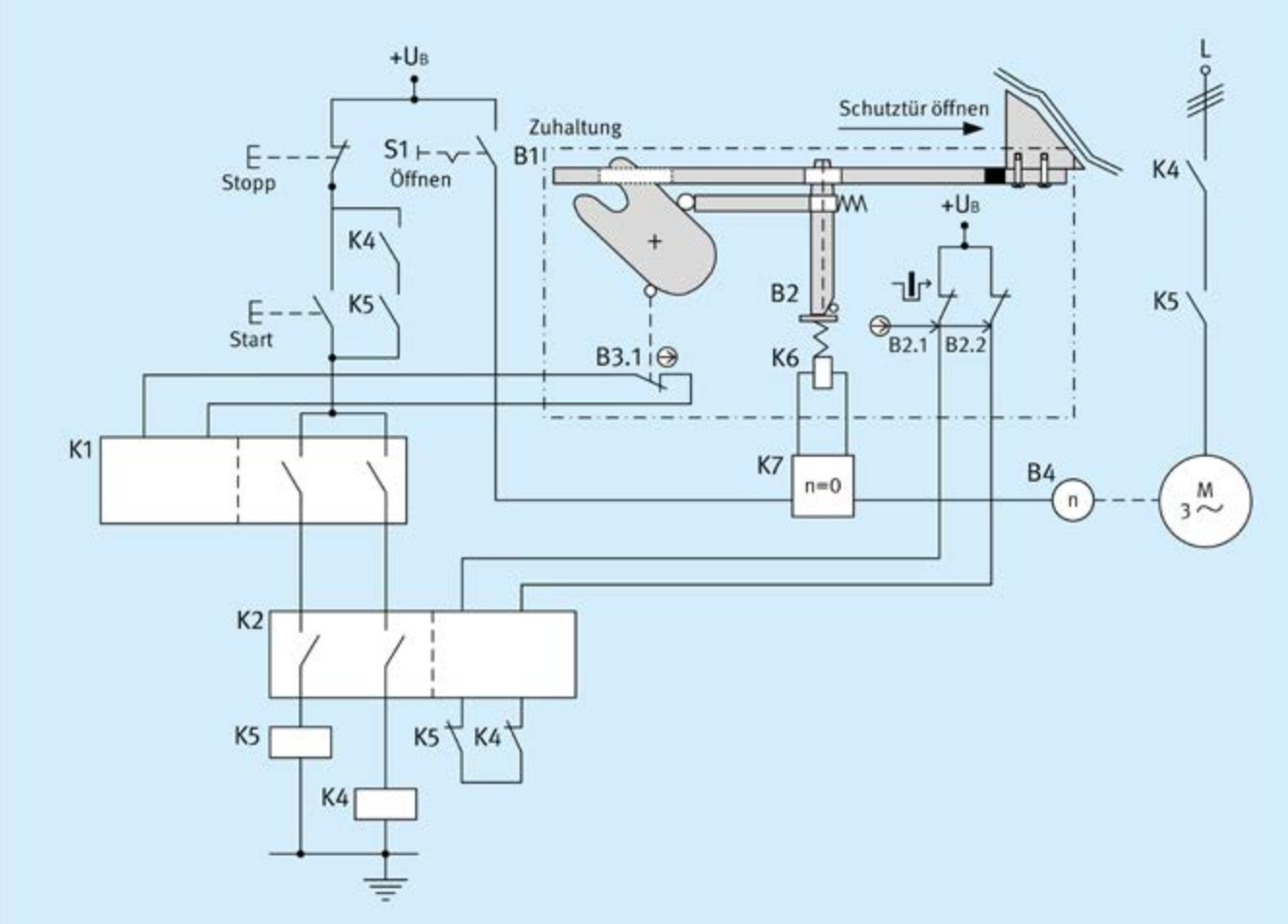


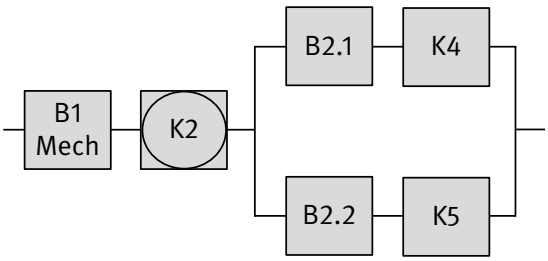
Abb. 11.29 Stellungsüberwachung einer verriegelten trennenden Schutzeinrichtung mit Zuhaltung

Sicherheitsfunktionen

- SF14.1: Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung verhindert.
- SF14.2: Ein Öffnen der Schutzeinrichtung ist nur möglich nach Erreichen des Stillstands des Motors.
- SF14.3: Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür.

Funktionsbeschreibung

- Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung so lange verhindert, bis die Bewegung zum Stillstand gekommen ist (Sicherheitsfunktion Zuhaltung). Die Tür wird durch einen federkraftbetätigten Bolzen (Sperrmittel) eines Hubmagneten zugehalten, der ein Herausziehen des Betätigers aus dem Schalterkopf verhindert, bis die Ansteuerung des Zuhaltemagneten erfolgt.
- Die Zuhaltung besitzt gemäß Herstellerangabe eine Fehlschließsicherung.
- Bei geöffneter Schutztür wird der unerwartete Anlauf des Motors zweikanalig durch die Sicherheitsfunktion Verriegelung verhindert (SF3).
- Der Bolzen des Sperrmittels wirkt direkt auf die zwangsöffnenden Kontakte B2.1 und B2.2, die an ein Sicherheitsschaltgerät K2 angeschlossen sind.
- Die gefahrbringende Bewegung kann nur bei geschlossener und zugehaltener Schutztür in Gang gesetzt werden, da die Freigaben von K1 und K2 in Reihe geschaltet sind.
- Mit Betätigen der Stopp-Taste fallen die Schütze K4 und K5 ab. Nach Stillstand des Motors kann die Zuhaltung durch Betätigen des rastenden Schalters S1 geöffnet werden (Sicherheitsfunktion Entsperren der Zuhaltung). Der Stillstand des Motors wird über eine zweikanalige Überwachung B4, K7 ermittelt.
- Das Entsperren der Zuhaltung führt nicht zu einem gefahrbringenden Zustand da die Tür weiterhin geschlossen bleibt. Beim Öffnen der Tür wird die gefahrbringende Bewegung durch die SF3 abgeschaltet. Der vollständigkeitshalber ist das Entsperren als Sicherheitsfunktion 2 in diesem Beispiel aufgenommen da ein unbemerktes Entsperren theoretisch zu einem Risiko führen könnte, wenn der Bediener in diesem Moment die Tür öffnen würde.



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 11 beschrieben, sind vorgesehen.
  - B1 ist eine elektromechanische Zuhaltung mit Fehlschließsicherung. Für die Mechanik der Zuhaltung einschließlich Bruch des Sperrmittels und des Betätigers kann ein Fehlerausschluss angenommen werden, wenn die folgenden Bedingungen erfüllt sind:
    - Anwendung entsprechend der Betriebsanleitung, insbesondere Montageanleitung und technische Daten (z. B. Betätigungsradius, Betätigungsgeschwindigkeit)
  - Verhinderung des Selbstlockerns
  - Die statischen Kräfte auf die Zuhaltung sind geringer als die im Datenblatt angegebene Zuhaltekraft.
  - Es treten keine dynamischen Kräfte auf, da die Bestromung des Entriegelungsmagneten bei geschlossener Schutztür erfolgt; siehe hierzu auch DGUV Information 203-079 „Auswahl und Anbringung von Verriegelungseinrichtungen“.
  - keine Verwendung als mechanischer Endanschlag
  - unlösbare Befestigung des Betätigers
  - regelmäßige Wartung
  - Formschluss nach Montage
  - ausreichende mechanische Festigkeit aller Träger- und Funktionselemente
    - Ein Absenken der Tür führt nicht dazu, dass der Betätiger außerhalb des vom Hersteller spezifizierten Bereichs eingesetzt wird.
  - Schäden, die durch vorhersehbare äußere Einflüsse (z. B. Eindringen von Schmutz, Staub und mechanische Erschütterung) entstehen könnten, werden durch die Art der Montage ferngehalten oder sind aufgrund der Einsatzbedingungen nicht zu erwarten.
- B2.1 und B2.2 sind Schaltelemente der Zuhaltung mit zwangsöffnenden Kontakten entsprechend DIN EN 60947-5-1 Anhang K. Für die Berechnung gibt der Hersteller einen B_{10D}-Wert an.
- B3.1 ist ein zwangsöffnender Kontakt entsprechend DIN EN 60947-5-1, Anhang K, und dient zur Überwachung der Türstellung.
- K4 und K5 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Sicherheitsschaltgeräte K1 und K2 erkennen Quer- und Erdschlüsse und erfüllen die Anforderungen der Kategorie 4, PL d der DIN EN ISO 13849-1.
- Die Stillstandsüberwachung besteht aus dem Sin-/Cos-Geber B4 und dem Stillstandswächter K7. Beide erfüllen jeweils die Anforderungen der Kategorie 3, PL e. B4 hat eine $PFH = 5{,}3 \cdot 10^{-9}$/Stunde und K7 hat eine $PFH = 5{,}8 \cdot 10^{-8}$/Stunde.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion SF14.1 besteht aus drei Teilsystemen. Im ersten Teilsystem der Kategorie 1 wird für die Mechanik der Zuhaltung B1 ein Fehlerausschluss angenommen. Hinweis: Bei Zuhaltungen mit „Fehlschließsicherung“ ist ein Fehlerausschluss nur entsprechend Angabe des Herstellers möglich. Als zweites gekapseltes Teilsystem ist das Sicherheitsschaltgerät der Kategorie 4 in der Sicherheitsfunktion aufgeführt. Zuletzt wird das Teilsystem der Kategorie 3 aus Sperrmittelüberwachung und Abschaltung zusammengefasst dargestellt.
- ***MTTF*$_D$ (SF14.1):** Für die Schaltelemente B2.1 und B2.2 gibt der Hersteller einen B_{10D}-Wert von jeweils 3 000 000 Zyklen an. Bei einer Betätigung alle 10 Minuten (an 200 Tagen und 16 Stunden) ist $n_{op} = 19\,200$ Zyklen/Jahr und $MTTF_D = 1562{,}5$ Jahre.
- Die Hilfsschütze K4 und K5 haben einen B_{10D}-Wert von 1 000 000 Zyklen. Bei einer Betätigung alle 10 Minuten an 200 Tagen und 16 Stunden) ist $n_{op} = 19\,200$ Zyklen/Jahr und $MTTF_D = 520{,}8$ Jahre.
- Für das Sicherheitsschaltgerät K1 und K2 gibt der Hersteller jeweils $PFH = 3{,}0 \cdot 10^{-9}$/Stunde an.
- ***DC*$_{avg}$:** $DC = 99\,\%$ für die Kontakte B2.1, B3.1 und B2.2 ergibt sich durch die direkte Überwachung in K2. $DC = 99\,\%$ für K4 und K5 begründet sich durch die direkte Überwachung in K1 bzw. K2 mittels zwangsgeführter Kontakte. Durch Mittelung ergibt sich damit ein DC_{avg} von 99 % („hoch“).

- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- **PL**: Für die Sicherheitsfunktion SF14.1 „Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung verhindert“ beträgt die mittlere Häufigkeit gefährlicher Ausfälle $PFH = 5{,}2 \cdot 10^{-8}$/Stunde. Dies entspricht PL e; da jedoch der Positionsschalter (B2) für die Sperrmittelüberwachung und die zugehörige Anfahrmechanik nur einmal vorhanden ist, wird der PL auf d beschränkt.
- Für die Sicherheitsfunktion SF14.2 „Entsperren der Zuhaltung: Ein Öffnen der Schutzeinrichtung ist nur möglich nach Erreichen des Stillstands des Motors“ wird die Ausfallhäufigkeit nur vom Sin-/Cos-Geber B4 und vom Stillstandswächter K7 bestimmt. Gemäß Herstellerangabe beträgt für den Sin/Cos-Geber B4 der $PFH = 5{,}3 \cdot 10^{-9}$/Stunde. Für den Stillstandswächter K7 wird eine $PFH = 5{,}8 \cdot 10^{-8}$/Stunde angegeben. Die PFH der SF14.2 beträgt $6{,}3 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.
- Für die Sicherheitsfunktion SF14.3 „Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür.“ wird die Ausfallhäufigkeit mittels SISTEMA bestimmt. Die PFH der SF14.3 beträgt $5{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Weiterführende Literatur

- DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen 203-079 (12/2015). Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2015. http://publikationen.dguv.de/dguv/pdf/10002/203-079.pdf
- Grundsätze für die Prüfung un d Zertifizierung von Verriegelungseinrichtungen mit Zuhaltung (GS-ET-19) (5/2015). Hrsg.: Fachbereich Energie Textil Elektro Medienerzeugnisse, Köln 2015. www.bgetem.de Webcode 12700341

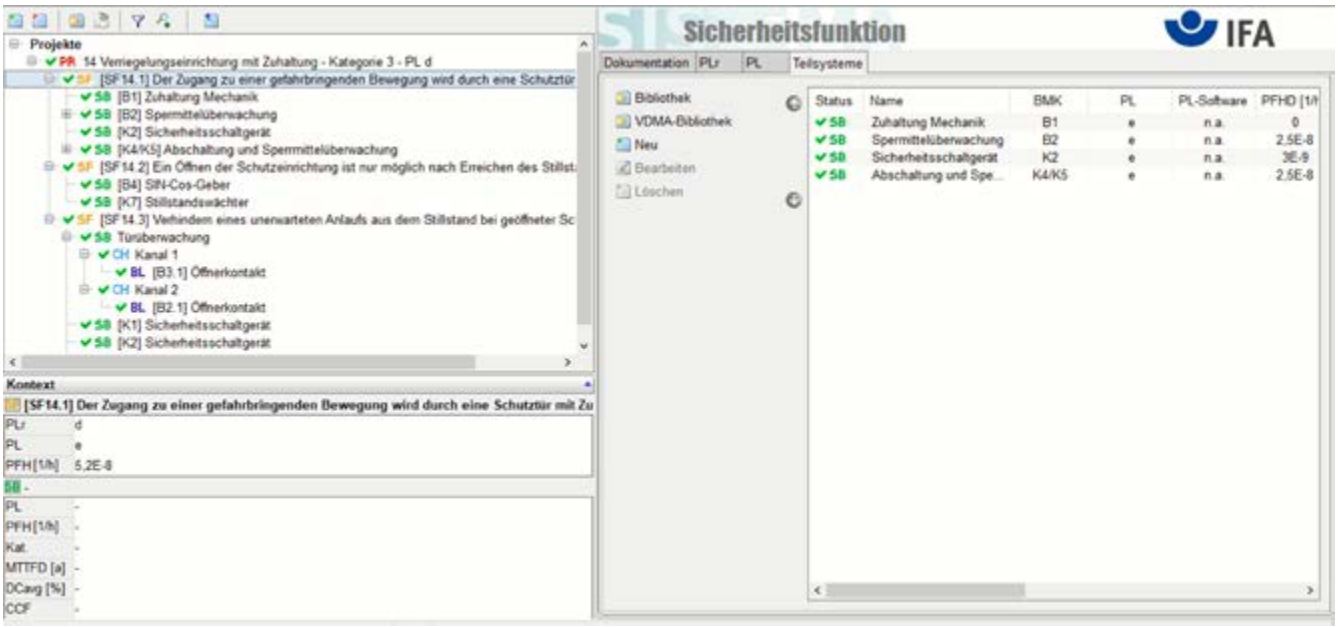


Abb. 11.30 PL-Bestimmung mithilfe von SISTEMA

11.2.15 Sicheres Stillsetzen eines SPS-gesteuerten Antriebs – Kategorie 3 – PL d (Beispiel 15)

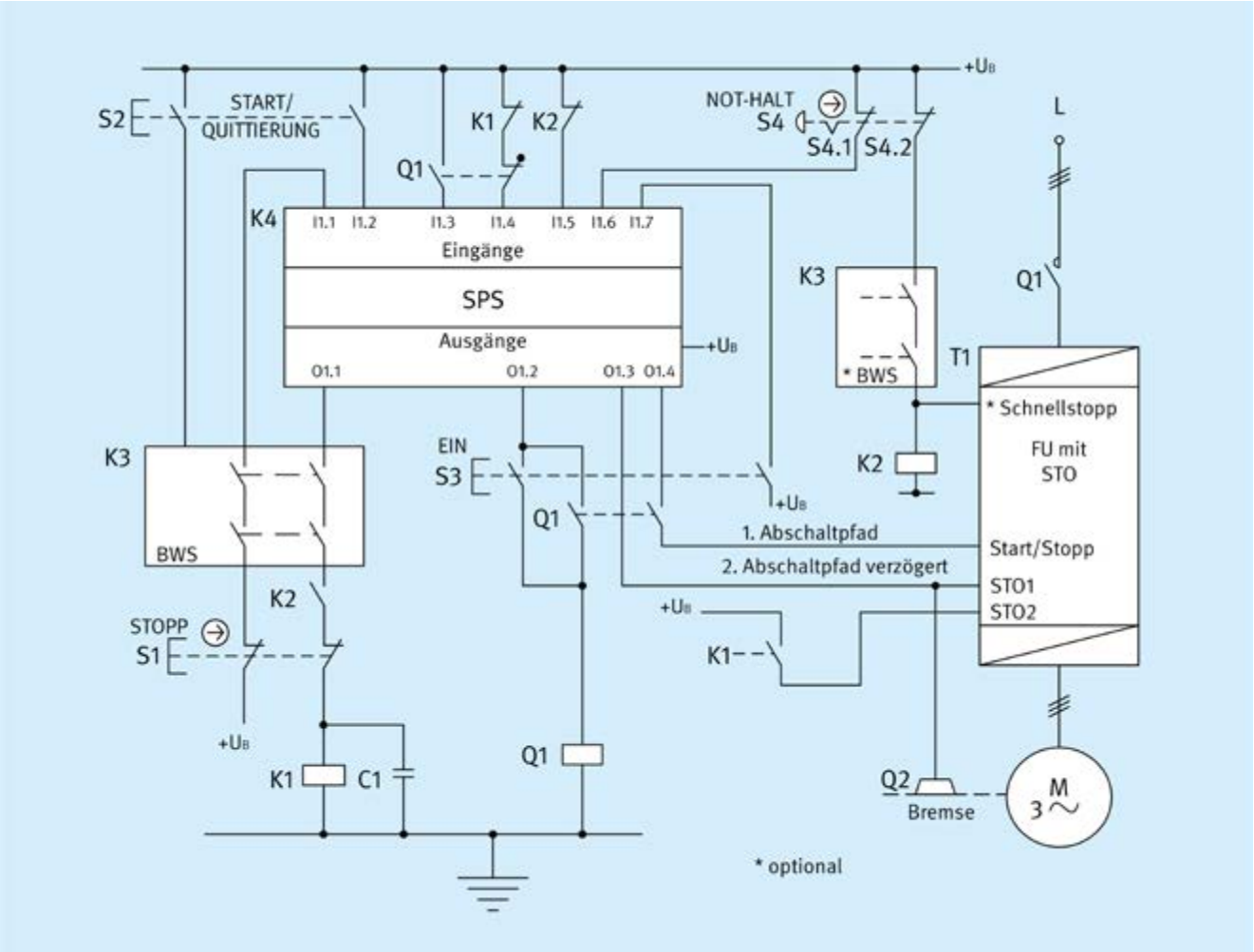


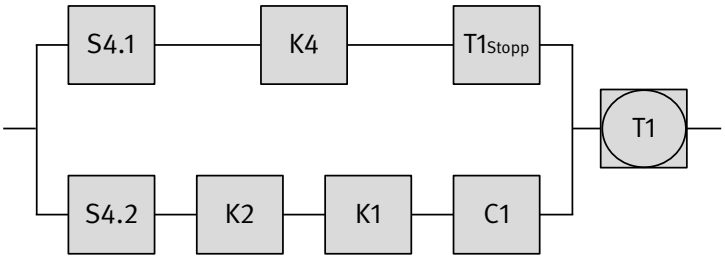
Abb. 11.31 Sicheres Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung (hier: BWS)

Sicherheitsfunktionen

- SF15.1: Sicherheitsbezogene Stoppfunktion: Nach einem Not-Halt-Befehl wird der Antrieb angehalten (SS1-t – Sicherer Stopp 1, STO wird zeitverzögert aktiviert). Diese Sicherheitsfunktion ist im sicherheitsgerichteten Blockdiagramm dargestellt.
- SF15.2: Sicherheitsbezogene Stoppfunktion: Nach dem Ansprechen einer Schutzeinrichtung wird der Antrieb angehalten (SS1-t – Sicherer Stopp 1, STO wird zeitverzögert aktiviert).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird redundant unterbrochen, falls entweder die Stopp-Taste S1 oder die Schutzeinrichtung K3 – im Schaltbild als berührungslos wirkende Schutzeinrichtung (BWS) dargestellt – aktiviert wird. Das Stillsetzen des Antriebs im Notfall erfolgt nach Betätigung des Not-Halt-Gerätes S4. In allen drei Fällen wird über den Ausgang O1.4 der SPS K4 durch Deaktivierung des Eingangs „Start/Stopp“ am Frequenzumrichter (FU) T1 der Stopp ausgelöst. Redundant dazu wird über das Entregen des Hilfsschützes K1 (abfallverzögert mithilfe des Kondensators C1) der Eingang „STO2“ an T1 deaktiviert. Über den Ausgang O1.3 der SPS K4 existiert ein weiterer Abschaltpfad auf den Eingang „STO1“ an T1, der auch die Bremse Q2 einfallen lässt. Der erste Abschaltpfad wird also über die SPS K4 unmittelbar realisiert, wohingegen der zweite Abschaltpfad verzögert kontaktbehaftet abschaltet. Die Zeitvorgaben für O1.3 im SPS-Programm und für K1 sind so gewählt, dass auch unter ungünstigen Betriebsbedingungen der Stillstand der Maschinenbewegung erreicht wird.
- Steht ein Eingang „Schnellstopp“ mit besonders kurzer Geschwindigkeitsabsteuerung am FU zur Verfügung, kann eine BWS optional – wie im Schaltbild gekennzeichnet – eingebunden werden. Diese Variante wird im Folgenden nicht weiter betrachtet.
- Bei einem einzelnen Versagen der SPS K4, der Umrichtereingänge „Start/Stopp“, „STO1“ oder „STO2“,



des abfallverzögerten Hilfsschützes K1 oder des Hilfsschützes K2 wird trotzdem das Stillsetzen des Antriebs sichergestellt, weil immer zwei voneinander unabhängige Abschaltpfade vorhanden sind. Das Nichtabfallen der Hilfsschütze K1 oder K2 wird wegen der vorhandenen Rückführung der zwangsgeführten Öffnerkontakte in die SPS-Eingänge I1.4 und I1.5 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 11 beschrieben, sind vorgesehen.
- Durch die Verwendung eines FU mit STO ist der Einsatz des Leistungsschützes Q1 zum Abschalten der Versorgungsspannung nicht unbedingt erforderlich. Der FU muss zum Antreiben und Bremsen geeignet sein.
- Für den Vergleich der Absteuerung der Eingänge „STO1/STO2“ im FU wird eine ausreichend große Zeitspanne gewählt, um die Varianz der Abfallverzögerung von K1 zu berücksichtigen.
- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Kontakte der Stopp-Taste S1 und des Not-Halt-Gerätes S4 sind zwangsöffnend ausgeführt entsprechend DIN EN 60947-5-1, Anhang K.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Für die Standardkomponente K4 und die Stoppfunktion des FU T1 ist die Einhaltung der SRESW-Anforderungen durch die Hersteller nicht bestätigt und kann durch den Integrator nicht nachträglich geleistet werden (nicht zugängliche Embedded-Software). Nach Abschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da das Teilsystem auf PL d mit Kategorie 3 begrenzt ist und die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Technologien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt. Die Programmierung der Software (SRASW) der Standardkomponente K4 erfolgt entsprechend Fall 2 (herabgestuft wegen Diversität) mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9. Die SRASW realisiert die erforderliche Fehlererkennung.
- T1 wird mittels softwarebasierter Parametrierung mit dem dafür vorgesehenen Parametrierungswerkzeug des Herstellers eingestellt. Die Anforderungen zur softwarebasierten manuellen Parametrierung nach Abschnitts 6.3 der Norm sind erfüllt.
- 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 Ausfallhäufigkeit nicht berücksichtigt. Diese Vorgehensweise setzt voraus, dass ein Austrudeln des Antriebs bei einem Versagen der Stoppfunktion und somit bei alleiniger Abschaltung über STO nicht mit einem verbleibenden inakzeptabel hohen Risiko verbunden ist. Die Beteiligung einer Bremse bei der Ausführung der Sicherheitsfunktion im Zusammenhang mit dem Einsatz eines FU ist im Beispiel 18 (Karusselltürsteuerung) beschrieben.
- Die BWS K3 erfüllt, z. B. als Lichtgitter, die Anforderungen für Typ 3 oder 4 nach DIN EN IEC 61496-1 und DIN EN IEC 61496-2 sowie korrespondierend für PL d oder e.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion SF 15.1 besteht aus zwei Teilsystemen der Kategorie 3.
- Es wird die Ausfallhäufigkeit PFH des sicheren Stillsetzens ausgelöst durch das Not-Halt-Gerät S4 bzw. durch die BWS berechnet. Die Funktion „Schnellstopp“ des FU und die Möglichkeit einer Abschaltung der Spannungsversorgung für den FU über Q1 werden bei der Berechnung der Ausfallhäufigkeit der Sicherheitsfunktion nicht berücksichtigt.
- Der FU T1 mit STO liegt als käufliches Sicherheitsbauteil vor, dessen Ausfallhäufigkeit am Ende der Berechnung addiert wird ($1{,}5 \cdot 10^{-8}$/Stunde). Die Stoppfunktion des FU wird im ersten Kanal des Blockdiagramms modelliert (T1Stopp). Der FU mit STO würde eigentlich im zweiten Kanal des Blockdiagramms modelliert. Ein Modell mit einem fertigen Sicherheitsbauteil inklusive PFH in nur einem Kanal kennt die Norm jedoch nicht. Deshalb wird der FU T1 mit seiner STO-Funktion als einzelnes Teilsystem betrachtet. Diese Betrachtung ist eine Abschätzung in die sichere Richtung.

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

- ***MTTF*$_D$:** Folgende *MTTF*$_D$-Werte liegen als Herstellerangaben vor: 46 Jahre für K4 und 100 Jahre für die Stoppfunktion T1Stopp des FU. Für S4.1 und S4.2 ergibt sich bei einem B_{10D}-Wert von jeweils 100 000 Zyklen und n_{op} = 12 Zyklen/Jahr eine *MTTF*$_D$ von 83 333 Jahren. Für K1 ergibt sich bei einem B_{10D}-Wert von 400 000 Zyklen 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 und täglichem Einschalten an 240 Arbeitstagen eine *MTTF*$_D$ von 16 667 Jahren. Der Kondensator C1 geht mit *MTTF*$_D$ = 45 662 Jahre in die Berechnung ein. Diese Werte ergeben eine symmetrisierte *MTTF*$_D$ des Kanals von 72 Jahren („hoch“).
- ***DC*$_{avg}$:** Fehlererkennung durch den Prozess führt auf DC = 60 % für T1Stopp und in Kombination mit internen Selbsttests auf DC = 60 % für K4. Testung des Zeitglieds bei spannungsfreiem FU führt auf DC = 99 % für K1. Für C1 führt die Testung des Zeitglieds bei spannungsfreiem FU in Kombination mit der Fehleraufdeckung durch Vergleich im FU bei Anforderung der Sicherheitsfunktion auf *DC* = 90 %. Für S4.1, S4.2 sowie K2 gilt *DC* = 99 % durch Plausibilitätstest in K4. Eine ausreichende Testhäufigkeit des Not-Halt-Gerätes ist gewährleistet (siehe Hinweise in den Abschnitten 8.2.14 und D.2.5.1). Die Mittelungsformel für *DC*$_{avg}$ ergibt 65 % („niedrig“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- **PL:** Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher MTTF$_D$ des Kanals (72 Jahre) und niedrigem DC$_{avg}$ (65 %). Zuzüglich des FU T1 ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls PFH von $1{,}7 \cdot 10^{-7}$/Stunde für SF15.1. Dies entspricht PL d.

Sicheres Stillsetzen ausgelöst durch die BWS K3:

- Die BWS K3 liegt als geprüftes Sicherheitsbauteil vor. Ihre Ausfallhäufigkeit PFH beträgt $3{,}0 \cdot 10^{-8}$/Stunde und wird am Ende der Berechnung addiert.
- Für die zweikanalige Struktur „SPS/Elektromechanik“ wird die Ausfallhäufigkeit mit den gleichen *MTTF*$_D$- und *DC*-Werten wie oben berechnet. Das Bauteil K2 ist an der Ausführung dieser Sicherheitsfunktion jedoch nicht beteiligt. Es ergeben sich folgende Werte: *MTTF*$_D$ des Kanals = 72 Jahre („hoch“) und *DC*$_{avg}$ = 65 % („niedrig“). Für Kategorie 3 ergibt dies eine mittlere Häufigkeit eines gefahrbringenden Ausfalls PFH von $1{,}6 \cdot 10^{-7}$/Stunde. Die Gesamtausfallhäufigkeit für SF15.2 wird durch Addition ermittelt und führt zu PFH = $2{,}0 \cdot 10^{-7}$/Stunde. Dies entspricht ebenfalls PL d.

Weiterführende Literatur

- *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld, R.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 4/2018. Hrsg.: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin 2018. https://publikationen.dguv.de/widgets/pdf/download/article/3500
- DIN EN IEC 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (6/2021). DIN Media, Berlin 2021
- DIN EN IEC 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, die aktive optoelektronische Schutzeinrichtungen (AOPD) verwenden (8/2021). DIN Media, Berlin 2021
- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (11/2017). DIN Media, Berlin 2017

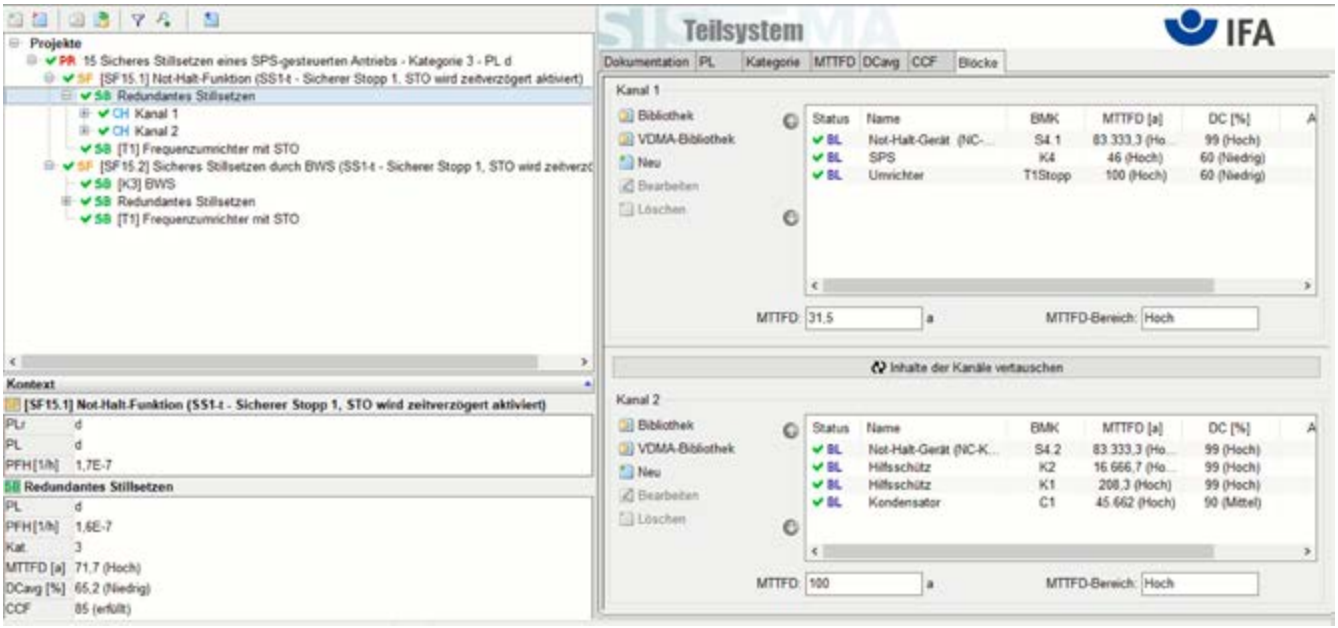


Abb. 11.32 PL-Bestimmung mithilfe von SISTEMA

11.2.16 Sicher begrenzte Geschwindigkeit – Kategorie 3 – PL d (Beispiel 16)

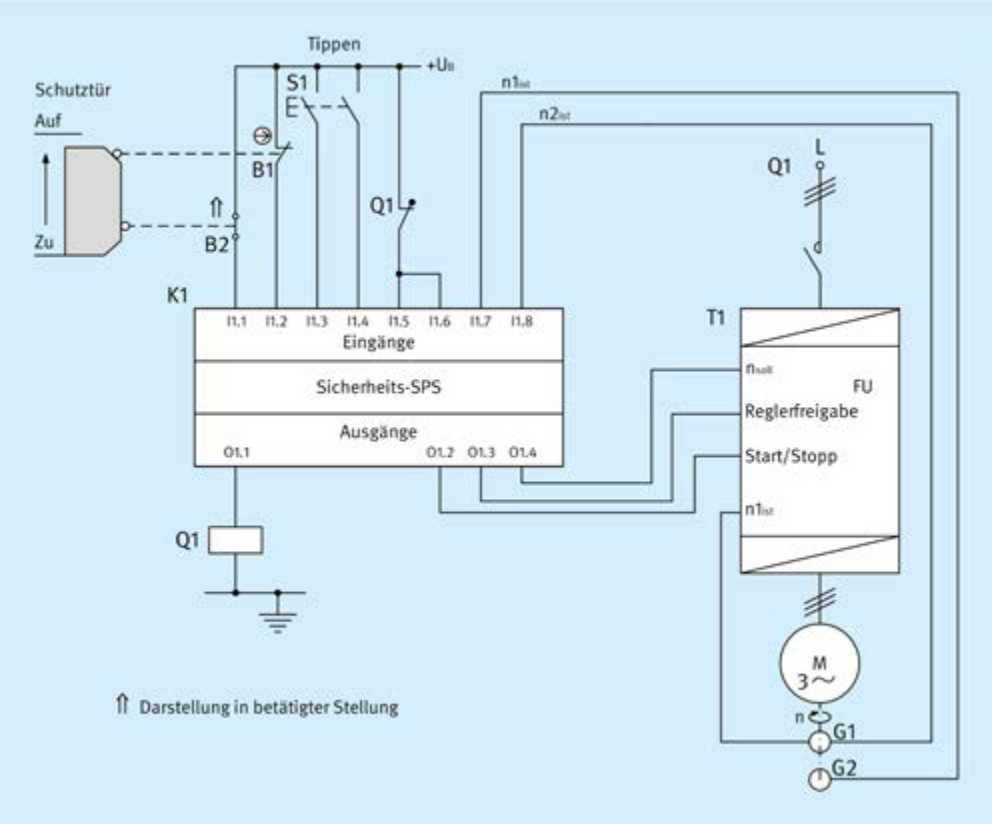


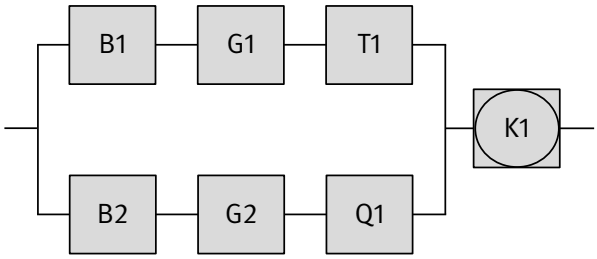
Abb. 11.33
Sicher begrenzte Geschwindigkeit bei geöffneter Schutztür, mit Soll-/Ist-Vergleich und Drehzahl-Grenzwertvorgabe innerhalb einer Sicherheits-SPS

Sicherheitsfunktion

- SF16.1: Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür wird das Überschreiten einer zulässigen Drehzahl verhindert.

Funktionsbeschreibung

- Dieses Beispiel zeigt die Realisierung der Sicherheitsfunktion SLS mit einem Frequenzumrichter ohne integrierte Sicherheitsfunktionen. Die Sicherheitsfunktion SLS wird z. B. für den Tippbetrieb im Rahmen von Serviceaufgaben genutzt.
- Eine gefahrbringende Bewegung wird bei geöffneter Schutztür sicher verhindert oder unterbrochen. Das Öffnen der Schutztür wird über zwei Positionsschalter B1 und B2 in Öffner-Schließer-Kombination erfasst. Bei betätigtem Taster S1 wird mithilfe der Sicherheits-SPS K1 eine Bewegung mit sicher begrenzter Geschwindigkeit (Tippbetrieb) ausgelöst. Beide Verarbeitungskanäle innerhalb der Sicherheits-SPS verarbeiten einen fest hinterlegten Sollgrenzwert. Die Überwachung der Istdrehzahl der begrenzten Geschwindigkeit an den Eingängen I1.7 und I1.8 von K1 erfolgt über zwei separate und diversitäre Drehgeber G1 und G2. Jeder Kanal der Sicherheits-SPS führt unabhängig den Soll-/Ist-Vergleich durch. Schlägt die über T1 geregelte Reduzierung der Drehzahl auf den begrenzten Wert fehl, so kann K1 über Sperrung des Start-/Stopp-Signals und der Reglerfreigabe am Frequenzumrichter einen Stillstand einleiten. Zusätzlich wird über das Netzschütz Q1 die Energieversorgung zu T1 nach Ablauf einer programmierten Zeit getrennt.
- Die zweikanalige Sicherheits-SPS K1 führt eine interne Fehlererkennung durch. Versagt ein Verarbeitungskanal, so erfolgt die Abwärtssteuerung des Frequenzumrichters T1 sowie des Netzschützes Q1 jeweils durch den anderen noch funktionierenden Verarbeitungskanal. Ein Versagen des Frequenzumrichters, das z. B. zum unerwarteten Anlaufen, zum Weiterlaufen oder zu einer Erhöhung der Drehzahl führen kann, wird über die getrennte Erfassung der Drehzahl durch die Drehgeber G1 und G2 in beiden Verarbeitungskanälen erkannt. Das Nichtabfallen des Netzschützes Q1 wird über den in beide Verarbeitungskanäle geführten Öffnerkontakt (Eingänge I1.5 und I1.6 von K1) bemerkt und führt sowohl zur Sperrung des Start-/Stopp-Signals als auch der Reglerfreigabe am Frequenzumrichter durch beide Verarbeitungskanäle.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 beschrieben, sind vorgesehen.
- Ein mechanisch stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter 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 IEC 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 „Sensorwelle löst sich von der Motorwelle“ (G1/G2) angenommen. Einzelheiten zur Möglichkeit eines Fehlerausschlusses geben z. B. DIN EN 61800-5-2, Tabelle D.8, bzw. DIN EN IEC 61800-5-3, Tabelle G.1.
- Die Drehgeber G1 und G2 erfüllen die Diversitätsanforderungen der CCF-Betrachtung.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Für die Standardkomponenten G1, G2 und T1 ist die Einhaltung der SRESW-Anforderungen durch die Hersteller nicht bestätigt und kann durch den Integrator nicht nachträglich geleistet werden (nicht zugängliche Embedded-Software). Nach Anschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da das Teilsystem auf PL d mit Kategorie 3 begrenzt ist und die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Technologien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt. Die Programmierung der Software (SRASW) von K1 erfolgt entsprechend Fall 3 mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9.
- T1 wird mittels softwarebasierter Parametrierung mit dem dafür vorgesehenen Parametrierungswerkzeug des Herstellers eingestellt. Die Anforderungen zur softwarebasierten manuellen Parametrierung nach Abschnitts 6.3 der Norm sind erfüllt.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Das SRP/CS wird in die beiden Teilsysteme Sensor/Aktor und SPS unterteilt. Für das Teilsystem SPS wird eine geprüfte, für Kategorie 3 PL d taugliche Sicherheits-SPS eingesetzt, deren Ausfallhäufigkeit $1{,}5 \cdot 10^{-7}$/Stunde am Ende der Berechnung für das Teilsystem Sensor/Aktor addiert wird. Zur Aufstellung des Blockdiagramms siehe auch Abbildung 7.5 und entsprechende Hinweise im zugehörigen Text. Nachfolgend wird die Ausfallhäufigkeit für das Teilsystem Sensor/Aktor berechnet.
- ***MTTF*$_D$:** Bei 240 Arbeitstagen, 8 Arbeitsstunden und einer Stunde Zykluszeit beträgt $n_{op} = 1920$ Zyklen/Jahr. Für den Positionsschalter B1 wird aufgrund der Zwangsöffnung ein B_{10D}-Wert von 20 000 000 Zyklen angenommen, die zugehörige $MTTF_D$ beträgt 104 166,7 Jahre. Für B2 wird aufgrund des definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) ein B_{10D}-Wert von 100 000 Zyklen für den durch Federkraft geöffneten Schließerkontakt angenommen (siehe auch Tabelle D.2) und damit eine $MTTF_D$ = 520 Jahre. Das Schütz Q1 mit B_{10D}-Wert von 400 000 Zyklen schaltet betriebsmäßig nur einmal täglich, entsprechend n_{op} = 240 Zyklen/Jahr und $MTTF_D$ = 16 667 Jahre. Folgende Herstellerangaben liegen vor: für T1 $MTTF_D$ = 100 Jahre, für G1 $MTTF_D$ = 190 Jahre und für G2 $MTTF_D$ = 130 Jahre. Diese Werte ergeben eine symmetrisierte $MTTF_D$ des Kanals von 84 Jahren („hoch“).
- ***DC*$_{avg}$:** Für die verwendeten Komponenten wird jeweils ein DC = 99 % angenommen. Dieser basiert für die Positionsschalter und die Drehgeber auf einem Kreuzvergleich von Eingangssignalen in K1. Für den Frequenzumrichter T1 erfolgt eine Drehzahlüberwachung über die zwei Drehgeber in der Sicherheits-SPS und eine Fehlererkennung durch den Prozess, für das Netzschütz Q1 erfolgt eine direkte Überwachung über die SPS. Diese Werte ergeben einen DC_{avg} von 99 % („hoch“).

- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- **PL:** Das Teilsystem Sensor/Aktor entspricht Kategorie 3 mit hoher $MTTF_D$ des Kanals (84 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls *PFH* von $3{,}0 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Der PL_r = d wird übertroffen, was bei erforderlicher zweikanaliger Ausführung der Hardware mit wenigen Bauteilen und der Verwendung von B_{10D}-Werten nach Norm, einem *DC* von „hoch“ sowie einer „moderaten“ Schalthäufigkeit nahezu immer der Fall sein wird.
- Die Gesamtausfallhäufigkeit für SF16.1 wird durch Addition der mittleren Häufigkeit gefahrbringender Ausfälle von K1 ($1{,}5 \cdot 10^{-7}$/Stunde) ermittelt und beträgt *PFH* = $1{,}8 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (11/2017). DIN Media, Berlin 2017
- DIN EN IEC 61800-5-3 (VDE 0160-105-3): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-3: Anforderungen an die Sicherheit von Encodern (Gebern) - Funktional, elektrisch und umwelttechnisch (Normentwurf) (7/2019). DIN Media, Berlin 2019
- IEC 61800-5-3: Adjustable speed electrical power drive systems – Part 5-3: Safety requirements – Functional, electrical and environmental requirements for encoders (3/2021). IEC Central Office, Switzerland, Geneva 2021
- DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Gemeinsame Anforderungen (6/2011). DIN Media, Berlin 2011

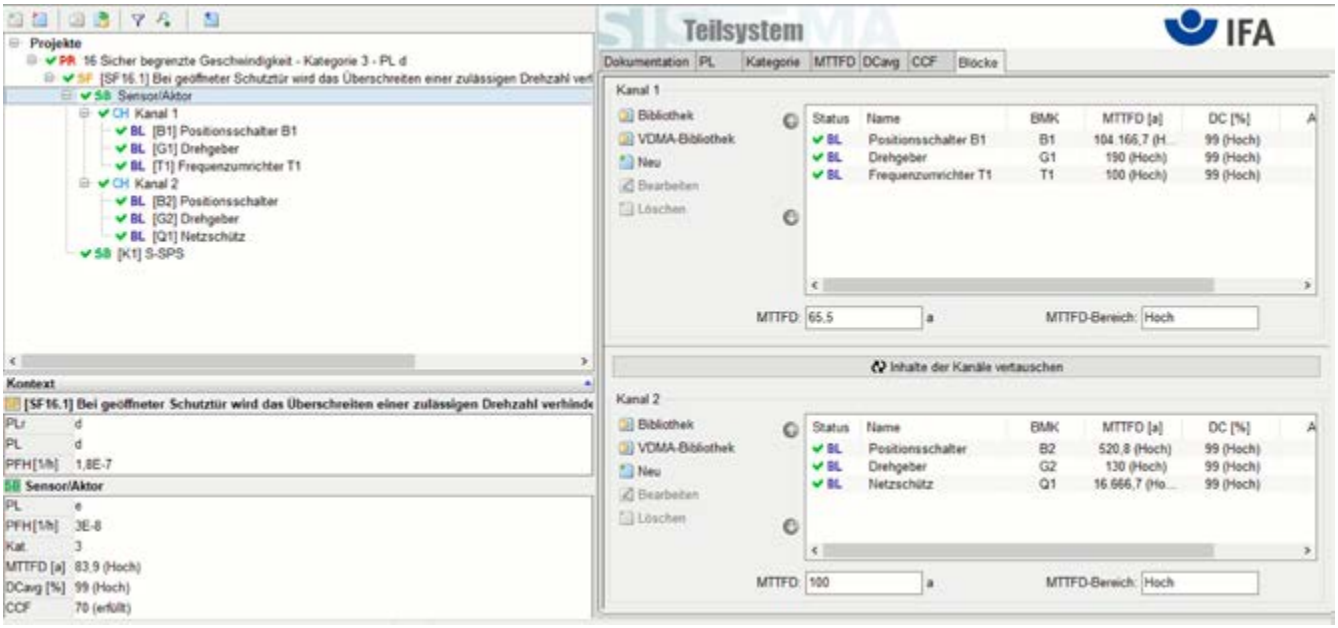


Abb. 11.34 PL-Bestimmung mithilfe von SISTEMA

11.2.17 Muting einer Schutzeinrichtung – Kategorie 3 – PL d (Beispiel 17)

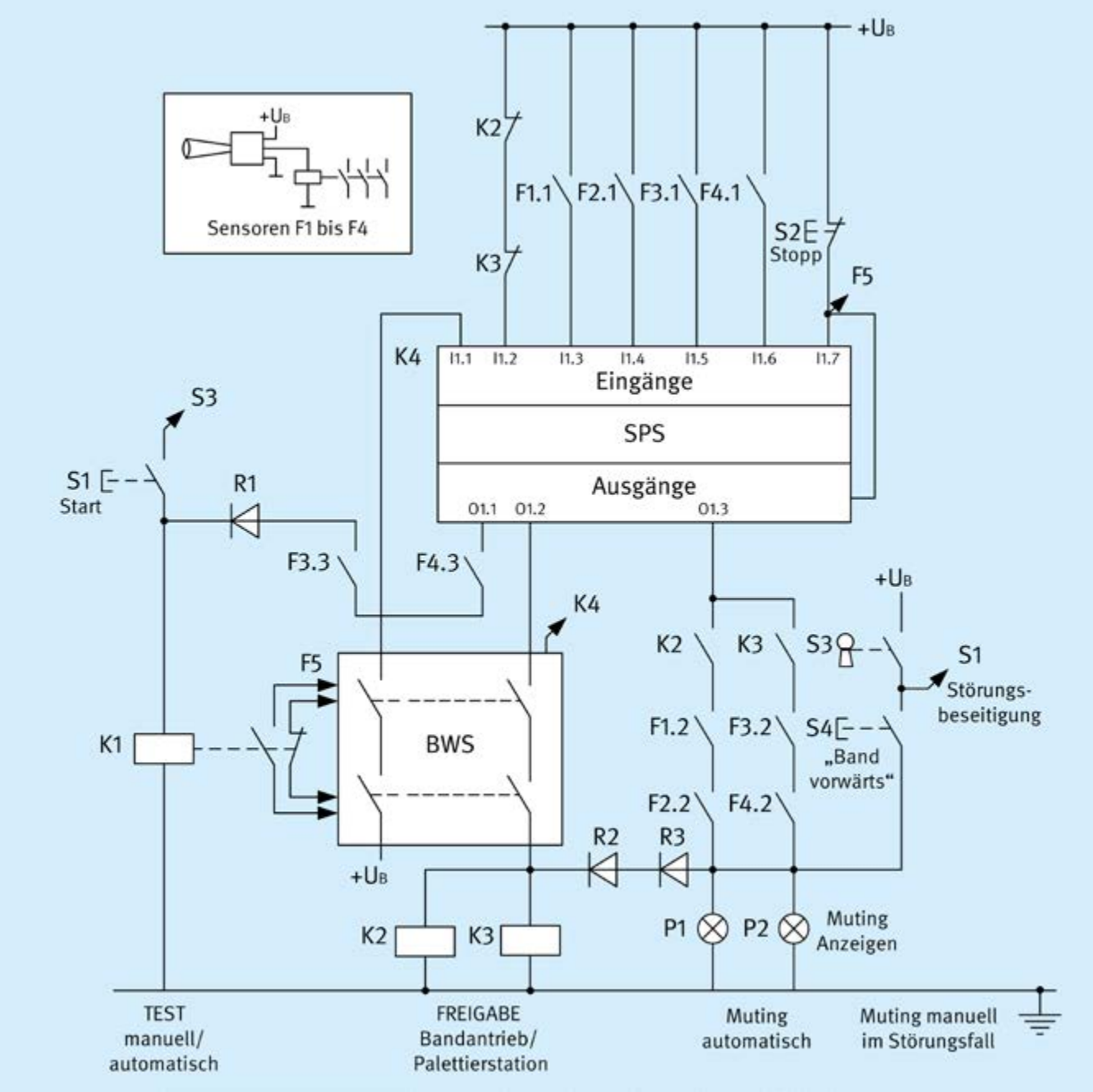


Abb. 11.35 Überbrückung einer Schutzeinrichtung am Auslauf einer SPS-gesteuerten Palettieranlage

Sicherheitsfunktion

- SF17.1: Mutingfunktion: Zeitlich begrenzte, prozessabhängige Überbrückung einer Schutzeinrichtung. Weitere Sicherheitsfunktionen wie 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 3 oder 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

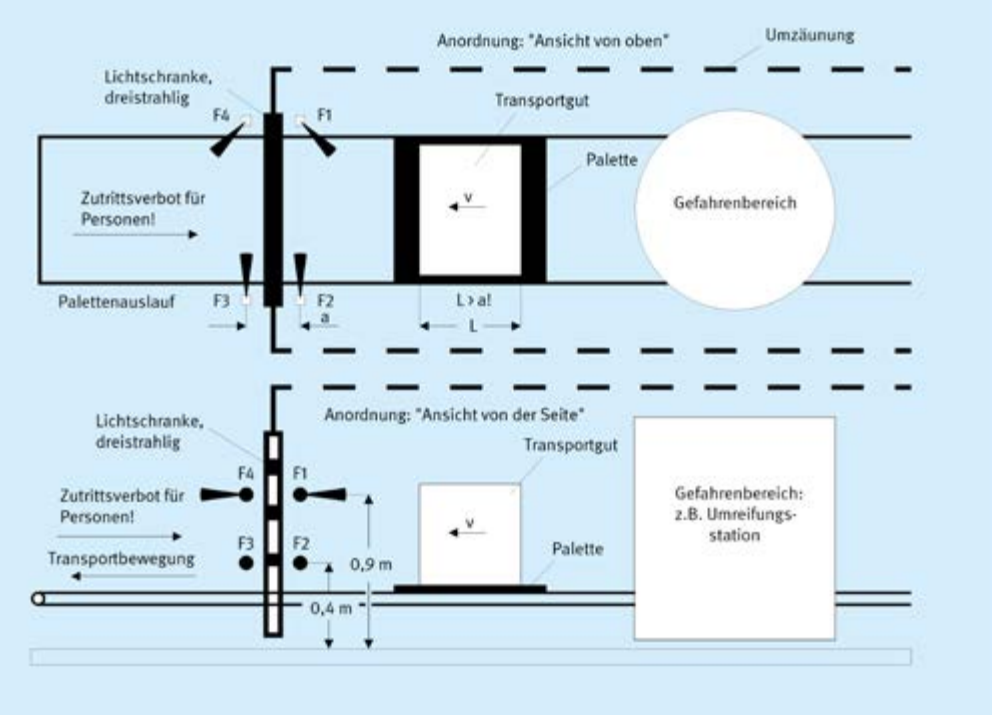
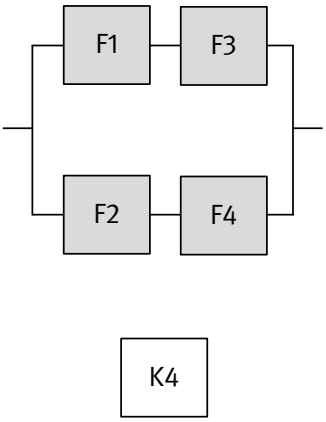


Abb. 11.36
Automatisch gesteuerte Palettierstation – Prinzip der Absicherung des Palettenauslaufs mit Lichtschranke und Anordnung der Überbrückungssensoren F1 bis F4

dem Betätigen und Loslassen des Starttasters S1. Voraussetzung für einen gültigen Startbefehl ist das Abgefallensein der Hilfsschütze K2 und K3 (abgefragt über Eingang I1.2) und die Aufhebung der Anlaufsperre (abgefragt über Eingang I1.1). Als Folge wird Ausgang O1.2 gesetzt.

- Zur Steuerung des Überbrückungsvorgangs sind vier Infrarot-Lichttaster F1 bis F4 (zur Anordnung siehe auch Abbildung 11.36) eingebunden. Über die Eingänge I1.3 bis I1.6 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 O1.3) 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.
- Bei Spannungsausfall mit anschließender Wiederkehr oder bei unterbrochener Lichtschranke F5 und nicht aktiver Überbrückungsfunktion werden die Hilfsschütze K2 und K3 entregt. Die jetzt nicht vorhandene Selbsthaltung verhindert deren Wiederanzug bei einem Wiederschließen der Überbrückungsstromkreise. Ein erneutes Ingangsetzen der Anlage kann nur über das Aufheben der Wiederanlaufsperre, d. h. durch willentliche Betätigung und Entlastung des Starttasters S1 erfolgen.
- Für das bestimmungsgemäße Ingangsetzen bzw. Wiederingangsetzen, z. B. nach einer Störung der Anlage, muss der Schlüsselschalter S3 betätigt werden. Mithilfe des Tipp-Tasters S4 kann im Störfall eine Palette aus dem Detektionsbereich der Lichtschranke und der Überbrückungssensoren herausfahren 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 Hilfsschütze K2 und K3 wird wegen der vorhandenen Rückführung der zwangsgeführten Öffnerkontakte in den SPS-Eingang I1.2 spätestens vor einem erneuten Ingangsetzen des Bandantriebs bzw.



der Palettieranlage aufgedeckt. Ein Versagen von K1 wird mit dem nächsten Auslass einer Palette aufgedeckt.

- Ein selbsttätiger unbeabsichtigter Anlauf des Bandantriebs bzw. der Palettieranlage bei einem Energieausfall mit anschließender Wiederkehr oder bei einem Versagen der Standard-SPS wird durch die Funktion der Anlauf- bzw. Wiederanlaufsperre verhindert. Die SPS kann die Wiederanlaufsperre nur direkt, nachdem die Palette die Lichtschranke passiert hat, also bei noch aktivierten Sensoren F3 und F4, aufheben.
- Das Versagen einzelner Überbrückungssensoren wird vom Programm der SPS entweder unmittelbar aufgedeckt (wegen Überwachung auf korrekten Ablauf von Aktivierung und Deaktivierung) oder macht sich während des Palettendurchlaufs betriebshemmend bemerkbar.
- Ein Versagen des Totmann-Tasters S4, der nur zur Störbeseitigung verwendet wird (Muting manuell), unterliegt einer unmittelbaren Erkennung durch die Bedienperson.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 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 den zwei Leuchtmeldern P1 und P2 angezeigt.
- Die Überbrückungssensoren F1 bis F4 sind Standardkomponenten ohne Software und in Elektronik ohne komplexe Bauteile wie Mikrocontroller, ASICs oder FPGAs aufgebaut.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Die Software (SRASW) von K4 dient ausschließlich zur Fehlererkennung für F1 bis F4 und ist somit nicht Teil der Realisierung der Sicherheitsfunktion. Es handelt sich wie in Abschnitt 9.11 empfohlen um eine qualitätsgesicherte Entwicklung. An die nicht zugängliche Embedded-Software von K4 werden keine Anforderungen gestellt.

Bemerkungen

- Beispiel für die Ermöglichung einer automatischen Materialabfuhr bei der Absicherung der Zugänge von Palettierern und Depalettierern, Umsetzstationen, Umreifungs- oder Umwickelungsmaschinen. Das gleiche Prinzip lässt sich für Zugänge mit Materialzufuhr verwenden.
- Beim Einsatz von Überbrückungssensoren, die komplexe Bauteile wie Mikrocontroller, ASICs oder FPGAs mit Software ohne Sicherheitsbewertung durch den Hersteller enthalten (d. h. die Anforderungen für sicherheitsbezogene Embedded-Software sind nicht erfüllt), müssen im angestrebten PL d in den beiden Kanälen Bauteile mit verschiedenen Technologien, Entwurfs- oder physikalischen Prinzipien zur Anwendung kommen.

- Nach DIN EN 415-4 kann vorausgesetzt werden, dass ein unbemerkter Zutritt von Personen durch Einlauf- bzw. Auslauföffnungen ausreichend sicher verhindert ist, wenn u. a. folgende Anforderungen eingehalten sind:
  - Verwendung einer zwei- bis dreistrahligen Lichtschranke unter Beachtung der erforderlichen Montagehöhen (bei offenem Zugang bzw. vorhandener Leerpalette im Zugang) oder
  - bei überbrückter Schutzfunktion der Lichtschranke durch die beladene Palette mit seitlichen Öffnungsweiten < 0,2 m sowie einsetzender Überbrückung durch die Palettenladung erst unmittelbar vor dem Unterbrechen der Lichtstrahlen (ohne größere zeitliche und geometrische Lücken).

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion wird von einem SRP/CS der Kategorie 3 realisiert.
- ***MTTF*$_D$:** Für den Sensorteil der Mutingsensoren F1 bis F4 wird jeweils eine $MTTF_D$ von 100 Jahren angenommen. Für die Ausgangsrelais von F1 bis F4 gilt ein B_{10D}-Wert von 2 000 000 Zyklen. Bei 300 Arbeitstagen, 16 Arbeitsstunden und 200 Sekunden Zykluszeit ist für diese Elemente n_{op} = 86 400 Zyklen/Jahr und $MTTF_D$ = 232 Jahre. Die $MTTF_D$ des Kanals ergibt sich zu 35 Jahren („hoch“).
- ***DC*$_{avg}$:** *DC* = 90 % für den Sensorteil der Mutingsensoren F1 bis F4 wird durch die SPS-Überwachung erreicht. Für die Ausgangsrelais der Mutingsensoren F1 bis F4 wird ein *DC* von 30 % abgeschätzt, da Ausfälle der Ausgangsrelais teilweise über die Mutingsequenz aufgedeckt werden, nicht aber ein einzelnes Versagen der zum Muting verwendeten Kontakte. Ein solches Versagen lässt sich über eine manuelle Überprüfung einzelner Sensoren mit Hilfe der Mutinganzeigen P1 und P2 erkennen. Der ermittelte DC_{avg}-Wert beträgt 72 % („niedrig“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL:** Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (35 Jahre) und niedrigem DC_{avg} (72 %). Für SF17.1 ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls *PFH* von 4,3 · 10^{-7}/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN EN 415-4: Sicherheit von Verpackungsmaschinen – Teil 4: Palettierer und Depalettierer (8/1997) und Berichtigung 1 (3/2003). DIN Media, Berlin 1997 und 2003
- DIN EN 415-10: Sicherheit von Verpackungsmaschinen – Teil 10: Allgemeine Anforderungen (7/2014). DIN Media, Berlin 2014
- DIN EN IEC 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (6/2021). DIN Media, Berlin 2021
- DIN EN IEC 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, die aktive optoelektronische Schutzeinrichtungen (AOPD) verwenden (8/2021). DIN Media, Berlin 2021
- DIN EN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zur Anwesenheitserkennung von Personen (3/2019). DIN Media, Berlin 2019
- DIN EN ISO 13855: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (10/2010). DIN Media, Berlin 2010

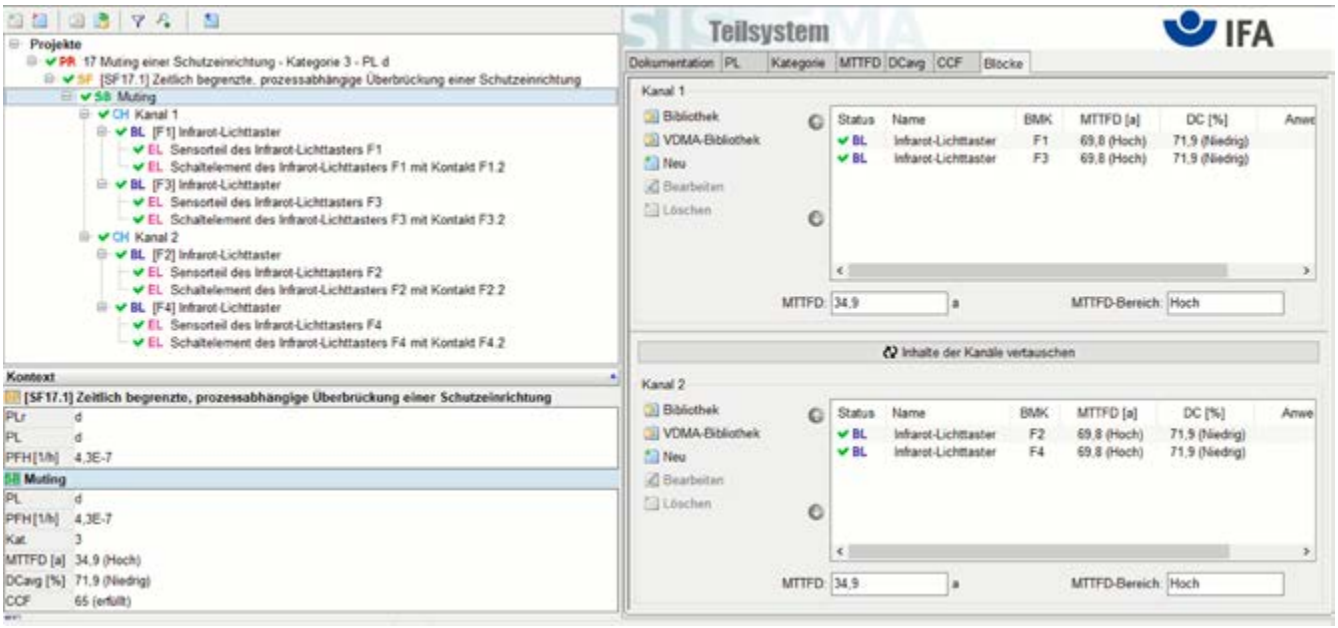


Abb. 11.37 PL-Bestimmung mithilfe von SISTEMA

11.2.18 Karusselltürsteuerung – Kategorie 3 – PL d (Beispiel 18)

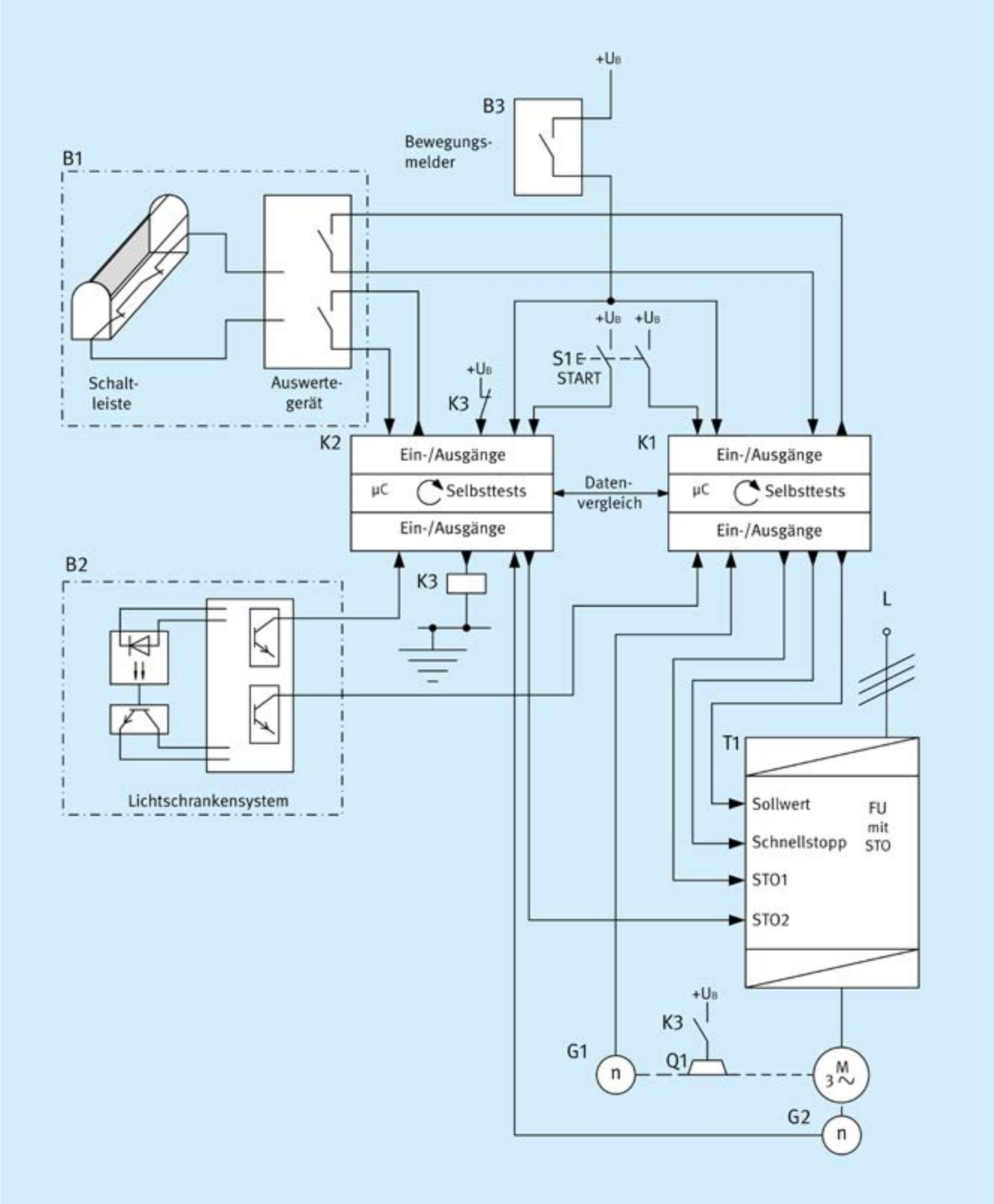
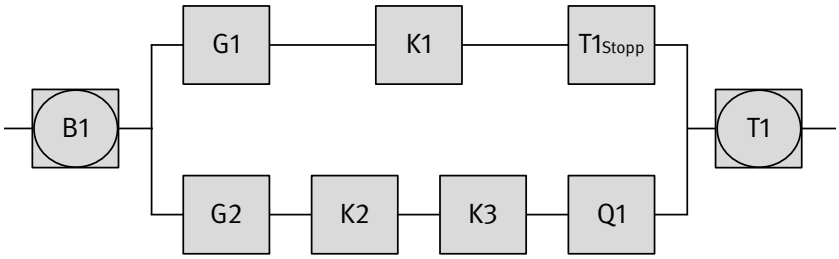


Abb. 11.38 Karusselltürsteuerung mit Mikrocontrollern



Sicherheitsfunktionen

- SF18.1: Sicherheitsbezogene Stoppfunktion: Bei Betätigung der Schaltleiste wird die Drehbewegung der Karusselltür stillgesetzt (SS1-r – Sicherer Stopp 1 mit Rampenüberwachung). Diese Sicherheitsfunktion ist im sicherheitsgerichteten Blockdiagramm dargestellt.
- SF18.2: Sicher begrenzte Geschwindigkeit (SLS): Bei Detektion einer Person oder eines Gegenstandes durch die Lichtschranke wird die Geschwindigkeit der Karusselltür reduziert und sicher begrenzt.

Funktionsbeschreibung

- Die Drehbewegung der Karusselltür wird erstmals nach dem Einschalten der Steuerung durch den Taster S1 eingeleitet. Im Normalbetrieb erfolgt die Anforderung zur Drehung über den an der Tür befindlichen Bewegungsmelder B3. Der Frequenzumrichter T1 wird gemeinsam durch die beiden Mikrocontroller K1 und K2 angesteuert. Jeder Mikrocontroller (µC) beinhaltet einen Mikroprozessor (CPU) als Recheneinheit sowie Arbeits- (RAM) und Festwertspeicher (ROM). K1 steuert die Funktionen der Sollwertvorgabe, von STO1 sowie des Schnellstopps (T1Stopp). Durch K2 wird STO2 angesteuert und die Bremse Q1 kann mithilfe des Hilfsschützes K3 gelöst werden. Die Drehgeber G1 und G2 übermitteln die Motordrehzahl an K1 bzw. K2. Die redundante Drehzahlüberwachung wird für beide Sicherheitsfunktionen SS1-r und SLS benötigt und dient auch zur Überwachung des Frequenzumrichters T1.
- Fehler in der Schaltleiste bzw. der Lichtschranke werden in den zugehörigen Auswertegeräten erkannt. Dies gilt auch für Fehler in den Auswertegeräten, die durch interne Überwachung erkannt werden. Fehler in den Komponenten der Mikrocontroller werden über Selbsttests bzw. durch Datenvergleich erkannt. Aufgedeckte Fehler führen, gesteuert über K1 und/oder K2, zur Stillsetzung der Türdrehbewegung durch T1 und/oder Q1. Zur Befreiung eingeschlossener Personen können die Türflügel von Hand geklappt werden.
- Durch redundante Verarbeitungskanäle führt ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktionen. Die Kombination unerkannter Fehler kann zum Verlust der Sicherheitsfunktionen führen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 beschrieben, sind vorgesehen.
- Die Schaltleiste dient der Absicherung von Quetsch-, Scher- und Einzugsstellen. Die Schaltleiste und das Auswertegerät werden als eine Einheit (B1) betrachtet. Das Teilsystem B1 erfüllt die Anforderungen nach DIN EN ISO 13856-2 in Kategorie 3 und nach DIN EN ISO 13849-1 für PL d. Fehler im Signalgeber der Schaltleiste bzw. in den Zuleitungen müssen ausgeschlossen oder über das Auswertegerät erkannt werden können (es können Schaltleisten, die nach dem Öffner- oder Schließer-Prinzip arbeiten, verwendet werden). Nach Entlastung einer zuvor betätigten Schaltleiste erfolgt ein automatischer zeitverzögerter Wiederanlauf der Drehbewegung. Die Schaltleiste verfügt über einen hinreichenden Verformungsweg und einen ausreichenden Wirkbereich.
- Die Lichtschranke dient der voreilenden, berührungslos wirkenden Absicherung von Gefahrstellen. Das Lichtschrankensystem B2 erfüllt die Anforderungen für Typ 4 nach DIN EN IEC 61496-1 und DIN EN IEC 61496-2 sowie für PL e nach DIN EN ISO 13849-1. Die nach der Detektion einer Person oder eines Gegenstandes durch die Lichtschranke eingenommene reduzierte, sicher begrenzte Geschwindigkeit wird nach einer voreingestellten Zeit wieder auf Normaldrehgeschwindigkeit erhöht. Die Zuleitungen zu Sender und Empfänger des Lichtschrankensystems sind getrennt oder geschützt verlegt.
- Während des ersten Anlaufs der Türdrehbewegung werden Einschalttests durchgeführt. Dabei werden unter anderem die Komponenten der Mikrocontroller (Mikroprozessor, Arbeits- und Festwertspeicher) getestet, Ein- und Ausgangstests durchgeführt sowie die Ansteuerung des Motors über den Frequenzumrichter überprüft (u. a. Test der Funktionen Schnellstopp sowie STO1/STO2). Ebenfalls findet ein regelmäßiger Bremsentest statt, bei dem der Frequenzumrichter gegen die eingefallene Bremse arbeiten muss.

- Im Rahmen des Datenvergleichs zwischen den beiden Controllern erfolgt der Austausch von Sollwerten und Zwischenergebnissen unter Einbeziehung der zyklisch durchgeführten Selbsttests.
- Durch die Verwendung eines Frequenzumrichters mit STO ist der Einsatz eines Schützes zum Abschalten der Versorgungsspannung nicht erforderlich. Der Frequenzumrichter ist zum Antreiben und gesteuerten Stillsetzen geeignet.
- K3 besitzt zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Die Schaltstellung des Öffnerkontaktes wird vom Mikrocontroller K2 zur Fehleraufdeckung überwacht.
- Bei dem Beispiel wird davon ausgegangen, dass zur Bremsung der Karusselltür die Regelung über den Frequenzumrichter T1 hinreichend ist. Nach Erreichen des Stillstandes wird zur Vermeidung des unerwarteten Anlaufes STO aktiviert. Bremszeit und Bremsweg werden von der Steuerung überwacht (Rampenüberwachung). Die Bremse Q1 im zweiten Kanal ist im Fehlerfall erforderlich, damit es nach einem Fehler, wenn T1 die Schnellstopp-Funktion T1Stopp nicht mehr ausführen kann, zu keiner Gefährdung kommen kann. Q1 arbeitet federkraftbetätigt nach dem Ruhestromprinzip.
- Die Drehgeber G1 und G2 erfüllen die Diversitätsanforderungen der CCF-Betrachtung.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Für die Standardkomponenten G1, G2 und die Stoppfunktion des FU T1 ist die Einhaltung der SRESW-Anforderungen durch die Hersteller nicht bestätigt und kann durch den Integrator nicht nachträglich geleistet werden (nicht zugängliche Embedded-Software). Nach Abschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da das Teilsystem auf PL d mit Kategorie 3 begrenzt ist und die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Technologien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt. Die Programmierung der Software (SRESW) von K1 und K2 erfolgt entsprechend den Maßnahmen des Falls 3 nach Tabelle N.3 der Norm und den Hinweisen in Kapitel 9. Die SRESW realisiert die Fehlererkennung.
- T1 wird mittels softwarebasierter Parametrierung mit dem dafür vorgesehenen Parametrierungswerkzeug des Herstellers eingestellt. Die Anforderungen zur softwarebasierten manuellen Parametrierung nach Abschnitts 6.3 der Norm sind erfüllt.
- Für die betrachteten Sicherheitsfunktionen wird ein Fehlerausschluss für den Fehler „Sensorwelle löst sich von der Motorwelle“ (G1/G2) angenommen. Einzelheiten zur Möglichkeit eines Fehlerausschlusses, siehe z. B. DIN EN 61800-5-2, Tabelle D.8 bzw. DIN EN IEC 61800-5-3, Tabelle G.1.

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 Ausfallhäufigkeit

Die detaillierte Berechnung der Ausfallhäufigkeit wird für die Sicherheitsfunktion SF18.1 „Sicherheitsbezogene Stoppfunktion (SS1-r)“, die auch im Blockdiagramm dargestellt ist, durchgeführt:

- **Kategorie**: Die Sicherheitsfunktion besteht aus drei Teilsystemen der Kategorie 3.
- Teilsystem 1: Da die Schaltleiste mit zugehörigem Auswertegerät als käufliches Sicherheitsbauteil vorliegt, wird deren Ausfallhäufigkeit am Ende der Berechnung addiert ($3{,}0 \cdot 10^{-7}$/Stunde).
- Teilsystem 2: Mikrocontrollersteuerung mit Drehgebern, Mikrocontrollern und Schnellstopp-Funktion T1Stopp im ersten Kanal des Blockdiagramms bzw. Hilfsschütz K3 und Bremse Q1 im zweiten Kanal des Blockdiagramms.
- Teilsystem 3: Der Frequenzumrichter T1 mit STO liegt ebenfalls als käufliches Sicherheitsbauteil vor, dessen Ausfallhäufigkeit am Ende der Berechnung addiert wird ($1{,}5 \cdot 10^{-8}$/Stunde).
- ***MTTF*$_D$ für Teilsystem 2:** Die sicherheitsrelevanten Bauteile von K1 und K2 einschließlich ihrer Peripherie werden nach Anwendung des „Parts Count“-Verfahrens mit einem Wert von 878 Jahren berücksichtigt. Für G1 fließt ein Wert von 190 Jahren und für G2 ein Wert von 130 Jahren in die Berechnung ein. Für T1Stopp wird ein Wert von 100 Jahren angesetzt. Für K3 wird ein B_{10D}-Wert von 400 000 Zyklen angesetzt. Bei einer Betätigung pro Tag ergeben sich n_{op} = 365 Zyklen/Jahr und eine $MTTF_D$ = 10 959 Jahre. Für Q1 wird ein B_{10D}-Wert von 1 000 000 Zyklen angesetzt, was zu einer $MTTF_D$ von 27 397 Jahren führt. Die Bremse Q1 ist nur im Fehlerfall erforderlich. Insgesamt ergibt sich eine symmetrisierte $MTTF_D$ des Kanals von 82 Jahren („hoch“) für die beiden Kanäle.
- ***DC*$_{avg}$:** Für die Mikrocontroller K1 und K2 ergibt sich aufgrund interner Selbsttests der Komponenten und Vergleich ein *DC* von 60 %. Für den Block T1Stopp resultiert aus der Rampenüberwachung ein *DC* von 99 %. G1 und G2 werden aufgrund des Vergleichs über K1 und K2 mit einem *DC* von 99 % bemessen. K3 wird entsprechend der direkten Überwachung eines zurückgelese-

nen zwangsgeführten Kontaktes mit einem $DC = 99$ % bemessen. Aufgrund der regelmäßig durchgeführten statischen Einschalttests wird für Q1 ein $DC = 30$ % angesetzt. Durch Mittelung ergibt sich damit ein DC_{avg} von 95 % („mittel“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- **PL:** Die Kombination der Steuerungselemente von Teilsystem 2 entspricht Kategorie 3 mit hoher $MTTF_D$ des Kanals (82 Jahre) und mittlerem DC_{avg} (95 %). Es ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls PFH von $4{,}2 \cdot 10^{-8}$/Stunde. Zuzüglich der Sensoreinheit B1 – bestehend aus Schaltleiste und Auswertegerät – und dem Frequenzumrichter T1 beträgt die mittlere Häufigkeit eines gefahrbringenden Ausfalls der Steuerung für diese Sicherheitsfunktion SF18.1 insgesamt $3{,}6 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Berechnung der Ausfallhäufigkeit für die Sicherheitsfunktion SF18.2 „Sicher begrenzte Geschwindigkeit (SLS)“
- **PL:** Für diese Berechnung wird die Sensoreinheit B1 aus der ersten Beispielberechnung durch das Lichtschrankensystem B2 mit einer Ausfallhäufigkeit PFH von $1{,}5 \cdot 10^{-9}$/Stunde ersetzt. Durch Addition ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion SF18.2 PFH von $5{,}8 \cdot 10^{-8}$/Stunde. Die Realisierung der Sicherheitsfunktion SLS entspricht PL d.

Weiterführende Literatur

- DIN EN ISO 13856-2: Sicherheit von Maschinen – Druckempfindliche Schutzeinrichtungen – Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltleisten und Schaltstangen (8/2013). DIN Media, Berlin 2013
- DIN EN 12978: Türen und Tore – Schutzeinrichtungen für kraftbetätigte Türen und Tore – Anforderungen und Prüfverfahren (10/2009). DIN Media, Berlin 2009
- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (3/2018). DIN Media, Berlin 2018
- DIN EN IEC 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (6/2021). DIN Media, Berlin 2021
- DIN EN IEC 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, die aktive optoelektronische Schutzeinrichtungen (AOPD) verwenden (8/2021). DIN Media, Berlin 2021
- DIN EN IEC 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (11/2017). DIN Media, Berlin 2017
- DIN EN IEC 61800-5-3 (VDE 0160-105-3): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-3: Anforderungen an die Sicherheit von Encodern (Gebern) – Funktional, elektrisch und umwelttechnisch (Normentwurf) (7/2019). DIN Media, Berlin 2019
- IEC 61500-5-3: Adjustable speed electrical power drive systems – Part 5-3: Safety requirements – Functional, electrical and environmental requirements for encoders (3/2021). IEC Central Office, Switzerland, Geneva 2021

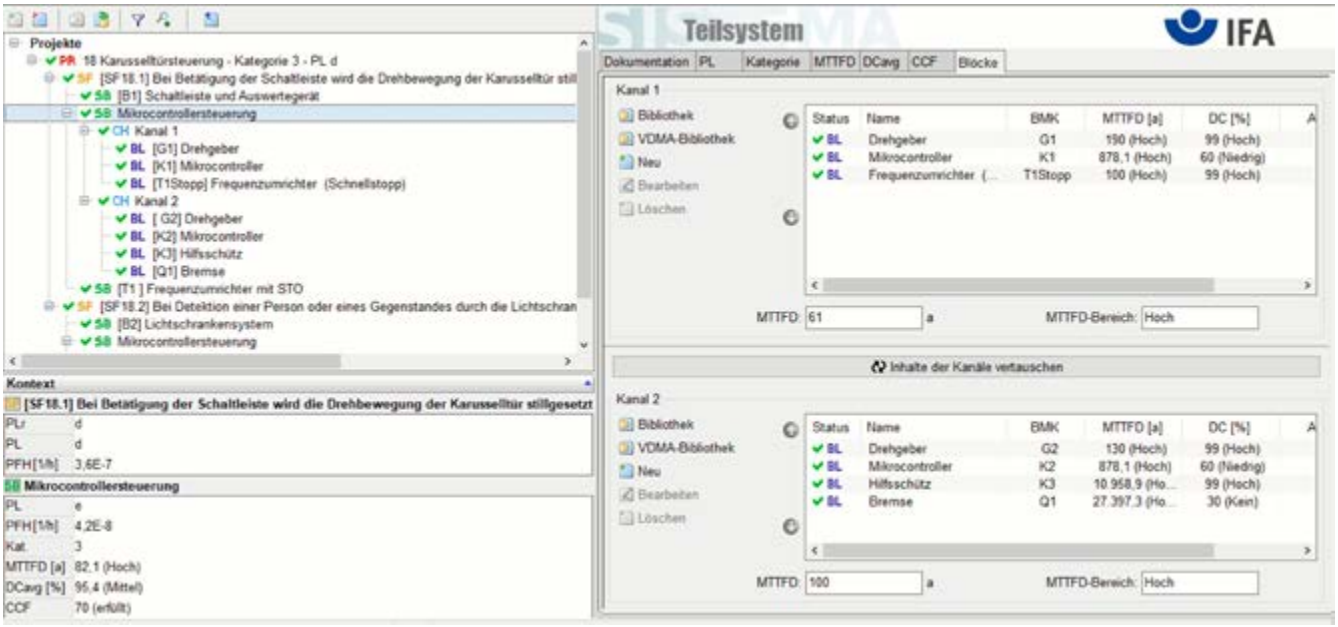


Abb. 11.39 PL-Bestimmung mithilfe von SISTEMA

11.2.19 Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine – Kategorie 3 - PL d bzw. c (Beispiel 19)

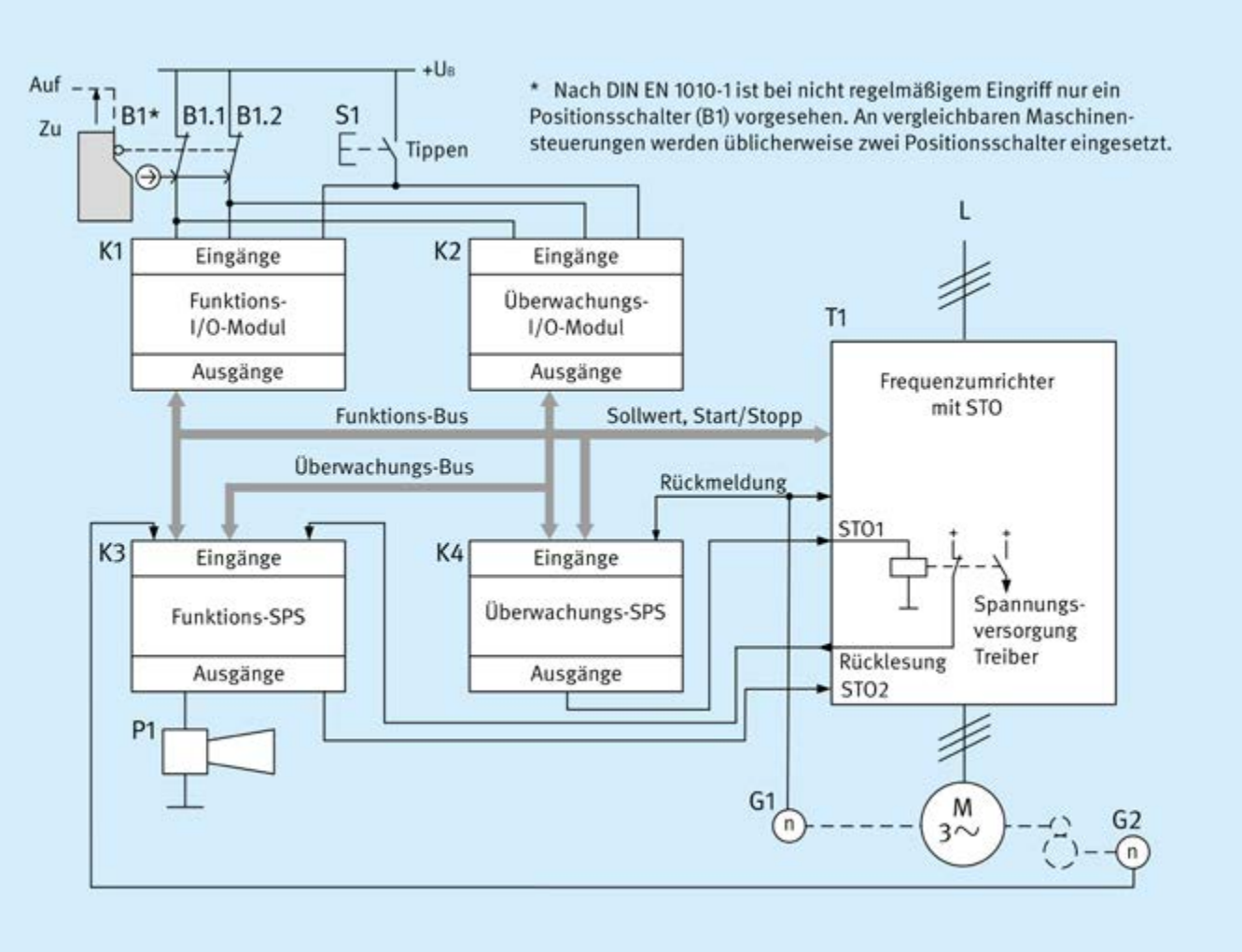
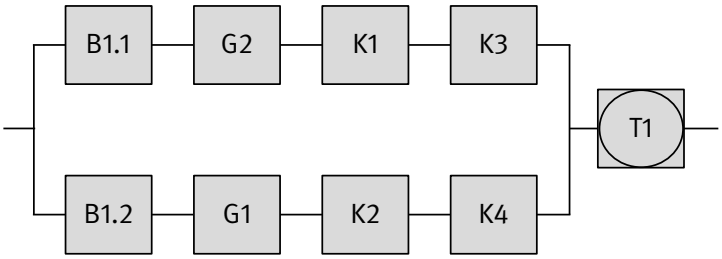


Abb. 11.40 Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine durch eine zweikanalige Rechnersteuerung

- SF19.1: Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Beim Öffnen der Schutztür soll der Antrieb anhalten (SS1-r – Sicherer Stopp 1, Überwachung Bremsrampe und STO nach Stillstand).
- SF19.2: Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür dürfen Maschinenbewegungen nur mit begrenzter Drehzahl erfolgen.
- SF19.3: Tippbetrieb: Bei geöffneter Schutztür sind Bewegungen nur während der Betätigung eines Tipptasters möglich.

Funktionsbeschreibung

- Das dezentrale Funktions-I/O-Modul K1 erfasst die Zustände des an der Schutzeinrichtung befestigten Positionsschalters mit Personenschutzfunktion B1 und des Tipptasters S1 und stellt diese auf dem Funktions-Bus als Information zur Verfügung. Diese Information wird durch die Funktions-SPS K3 ausgewertet und führt beim Öffnen der Schutztür zur Einleitung der Stoppfunktion am Frequenzumrichter T1. Dazu wird über den Funktions-Bus ein Signal zum schnellstmöglichen Stillsetzen gegeben. Redundant zu K1 und K3 arbeiten das Überwachungs-I/O-Modul K2 und die Überwachungs-SPS K4, die über einen eigenen Überwachungs-Bus kommunizieren. Die Bremsrampe wird in der Funktions-SPS K3 über den Geber G2 und in der Überwachungs-SPS K4 über den Geber G1 kontrolliert. Nach Stillstand oder im Falle eines erkannten Fehlers beim Stillsetzen wird durch K3 und K4 über die beiden STO-Eingänge STO1 und STO2 von T1 die integrierte Sicherheitsfunktion STO ausgelöst.
- Der offene Zustand der Schutzeinrichtung wird über B1, K1 und K2 wie oben beschrieben in K3 und K4 erfasst. K3 und K4 sorgen dann redundant zueinander mittels G2 bzw. G1 für eine Überwachung der spezifizierten begrenzten Geschwindigkeit (SLS). Falls diese überschritten wird, leiten K3 und K4 unabhängig voneinander wie oben beschrieben den SS1-r ein.



- Bei betätigtem B1 ist nur ein Tippbetrieb über S1 mit sicher begrenzter Geschwindigkeit erlaubt. Das Loslassen von S1 wird über K1 und K2 redundant in K3 und K4 erfasst und führt, wie oben für die sicherheitsbezogene Stoppfunktion und SLS beschrieben, zum Sicheren Stopp 1 des Antriebs (SS1-r).
- Entsprechend DIN EN 1010-1:2011, Abschnitt 5.2.11 ist ein einziger Positionsschalter B1 ausreichend. Die meisten Fehler in S1 werden durch einen besonderen Betätigungsablauf, der einen Signalwechsel (Dynamisierung) erzwingt, aufgedeckt und beherrscht: Nach erstmaliger Betätigung von S1 erfolgt eine akustische Warnung (Signalgeber P1), erst nach Loslassen und erneutem Betätigen das verzögerte Anlaufen des Antriebs.
- Fehler in K1 und K2 werden durch Zustandsvergleich in K4 erkannt. K4 überwacht auch K3 durch Mithören der Eingangs- und Ausgangsinformationen. Ein Teil der Fehler in K3 wird zusätzlich durch Fehler im Prozess offenbart. In K4 finden Selbsttests statt (z. B. zeitliche Programmlaufüberwachung durch internen Watchdog). Außerdem benutzt K3 K4 zur regelmäßigen Anwahl von STO1 und überwacht das Rücklesesignal von T1.
- Der Frequenzumrichter T1 bildet mit dem Sin/Cos-Geber G1 ein Regelsystem, in dem Fehler durch den hochsynchronen Produktionsprozess offenbart werden (Fehldruck, Papierriss). Die Gebersignale von G1 auf der Motorwelle werden auch in K4 eingelesen und in T1 auf Plausibilität der Sin/Cos-Information ($Sin^2 + Cos^2 = 1$) überwacht. Redundant dazu werden die Signale eines diversitären Gebers G2 auf der Maschinenwelle ausgewertet. Obwohl beide Geber nicht auf derselben Welle sitzen, können ihre in K4 bzw. K3 eingelesenen und in Papiergeschwindigkeiten umgerechneten Werte in K4 miteinander verglichen werden und führen so zu einer Fehlererkennung für G1 und G2. Fehlererkennung für STO1 in T1 erfolgt durch ein bereitgestelltes Rücklesesignal, das in K3 ausgewertet wird. Die korrekte Abarbeitung von STO2 wird durch T1-interne Testmaßnahmen überwacht, die im Fehlerfall einen Stillstand einleiten.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 beschrieben, sind vorgesehen.
- Die Öffner von B1 entsprechen DIN EN 60947-5-1, Anhang K; B1 ist in Übereinstimmung mit der DGUV Information 203-079 „Auswahl und Anbringung von Verriegelungseinrichtungen“ installiert. Maßnahmen zur Verhinderung der Lageänderung und der vernünftigerweise vorhersehbaren Manipulation sind realisiert (siehe DIN EN 14119). Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.
- S1 entspricht DIN EN 60947-5-1, sodass der Kurzschluss von benachbarten Kontakten, die voneinander isoliert sind, ausgeschlossen werden kann. Trotz Anlaufwarnung und Dynamisierung kann S1 während des Tippbetriebs hängen bleiben. Zusätzlich muss nach DIN EN 1010-2 in Reichweite der Bedienperson ein Not-Halt-Gerät installiert sein.
- Für die Anschlussleitungen von S1 müssen die Bedingungen eines Fehlerausschlusses für Leitungskurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4, eingehalten werden. Fehler in den Anschlussleitungen von B1 werden durch eine Überwachung in K4 erkannt.
- Die Drehgeber G1 und G2, die I/O-Module K1 und K2 sowie die SPS K3 und K4 erfüllen die Diversitätsanforderungen der CCF-Betrachtung. G1 ist in den Regelkreis eingebunden (Gewinnung der Kommutierung). Der diversitäre Geber G2 dient zur Fehlererkennung.
- T1 besitzt eine integrierte Sicherheitsfunktion STO, die alle Anforderungen für Kategorie 3 und PL d erfüllt. Die erforderliche Fehlererkennung wird durch ein bereitgestelltes und extern überwachtes Rücklesesignal für STO1 und interne Überwachungsmaßnahmen für STO2 erreicht. T1 wird mittels softwarebasierter manueller Parametrierung mit dem dafür vorgesehenen Parametrierungswerkzeug des Herstellers eingestellt. Die Anforderungen zur softwarebasierten manuellen Parametrierung nach Abschnitts 6.3 der Norm sind erfüllt.
- Der Einsatz der Bussysteme (Funktions-Bus, Überwachungs-Bus) erfolgt entsprechend den Hinweisen aus Abschnitt 8.2.18.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software**: Für die Standardkomponenten K1 bis K4, G1 und G2 ist die Einhaltung der SRESW-Anforderungen durch die Hersteller nicht bestätigt und kann durch den

Integrator nicht nachträglich erfolgen (nicht zugängliche Embedded-Software). Nach Abschnitt 7.3.2 der Norm ist der Verzicht auf den Nachweis der SRESW-Anforderungen zulässig, da das Teilsystem auf PL d mit Kategorie 3 begrenzt ist und die Diversitätsanforderungen der CCF-Betrachtung durch Anwendung unterschiedlicher Technologien erfüllt werden. Die weiteren Hinweise in Abschnitt 9.10 werden berücksichtigt. Die Programmierung der Software (SRASW) von K3 und K4 erfolgt entsprechend Fall 2 (herabgestuft wegen Diversität) mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der Norm und den Hinweisen in Kapitel 9.

Bemerkungen

- Dieses Beispiel beschreibt die Absicherung von Einzugsstellen an Rotationsdruckmaschinen. Die Anwendung der DIN EN 1010-1 erfordert bei Maschinen ohne betriebsmäßig regelmäßigen Eingriff in den Gefahrenbereich nur einen Positionsschalter für die Stellungsüberwachung der trennenden Schutzeinrichtung. Das Kriterium der Fehlertoleranz für Kategorie 3 wird bei vergleichbaren Maschinensteuerungen üblicherweise durch die Verwendung von zwei Positionsschaltern erfüllt.
- Für den Tippbetrieb unter der Voraussetzung bereits gewährleisteter sicher begrenzter Geschwindigkeit kann unter bestimmten Bedingungen von der Möglichkeit zur Vermeidung der Gefährdung ausgegangen werden. Siehe zur Risikobeurteilung auch Beispiel 4 in Anhang A.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktionen SF19.1 und SF19.2 bestehen jeweils aus einem zweikanaligen Teilsystem der Kategorie 3, gefolgt vom gekapselten Teilsystem T1 (Kategorie 3, PL d). Bei SF19.3 kommt S1 als weiteres Teilsystem der Kategorie 2 hinzu.
- Die drei Sicherheitsfunktionen unterscheiden sich nur in der Sensorebene. B1, G1/G2 und S1 werden daher separat beschrieben.
- ***MTTF*$_D$ und *DC*$_{avg}$ von B1**: Die beiden zwangsöffnenden Kontakte von B1 sind in die nachfolgende Kategorie-3-Struktur eingebunden. Pro Kontakt wird ein B_{10D}-Wert von 20 000 000 Zyklen angenommen. Bei wöchentlich 10-facher Betätigung ist n_{op} = 520 Zyklen/Jahr und $MTTF_D$ = 384 615 Jahre. Unter den besonderen Anforderungen der DIN EN 1010-1 an B1 (siehe konstruktive Merkmale), wird ein DC_{avg} von 60 % (Kreuzvergleich von Eingangssignalen ohne dynamischen Test, seltener Signalwechsel durch die Anwendung) unterstellt.
- ***MTTF*$_D$ und *DC* von G1/G2**: G1 und G2 sind ebenfalls in je einen Kanal der nachfolgenden Kategorie-3-Struktur eingebunden. Sie gehen mit 30 Jahren $MTTF_D$ pro Kanal, 90 % DC für G2 durch Plausibilitätsprüfung und 99 % *DC* für G1 durch Überwachung auf $Sin^2 + Cos^2 = 1$, Plausibilitätsprüfung und Fehlererkennung im Prozess in die Bestimmung der PFH ein.
- **Teilsystem S1**: S1 besitzt einen B_{10D}-Wert von 100 000 Zyklen. Bei wöchentlich 10-facher (doppelter) Betätigung ist n_{op} = 1040 Zyklen/Jahr und $MTTF_D$ = 962 Jahre. Wegen erzwungenen Signalwechsels (Dynamisierung) wird S1 als ein Kategorie-2-Teilsystem modelliert und ein *DC* von 60 % angenommen (ein Hängenbleiben nach wiederholtem Tippen wird aber nicht erkannt). Die Testung erfolgt in K1 und K3, deren Ausfallhäufigkeit bereits in das nachfolgende Kategorie-3-Teilsystem eingeht und daher nicht zusätzlich im Testkanal berücksichtigt werden muss. Um keine Fehlermeldung in SISTEMA zu provozieren, wird im Testkanal ein $MTTF_D$-Wert von 100 Jahren eingesetzt. Da die Testung unmittelbar bei der Anforderung der Sicherheitsfunktion erfolgt, ist eine ausreichende Testhäufigkeit gegeben. S1 erreicht damit als separates Teilsystem eine mittlere Häufigkeit gefährlicher Ausfälle von $5{,}3 \cdot 10^{-7}$/Stunde.
- ***MTTF*$_D$ und *DC*$_{avg}$ von K1 bis K4:** K1 und K3 sowie K2 und K4 gehen in zwei Kanälen eines Kategorie-3-Teilsystems in alle drei betrachteten Sicherheitsfunktionen ein. Hinsichtlich $MTTF_D$ werden 100 Jahre für K1 und K2, 50 Jahre für K4 und 30 Jahre für K3 in Rechnung gestellt. *DC* = 99 % für K1 und K2 ergibt sich durch den direkten Vergleich der bereitgestellten Zustandsinformationen in K4. *DC* = 99 % für K3 gründet sich auf die parallele Verarbeitung aller sicherheitsrelevanten Informationen in K4 und den dortigen direkten Vergleich mit den von K3 gebildeten Zwischenergebnissen und Ausgangssignalen. Die in K4 umgesetzten Selbsttests plus partielle Überwachung durch die von K3 zurückgelesene Anwahl von STO1 führen für K4 auf einen *DC* von 60 %.
- **CCF**: Das zweikanalige Teilsystem der Kategorie 3 und das Teilsystem S1 verwenden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **Teilsystem T1**: T1 geht mit seiner integrierten Sicherheitsfunktion STO als gekapseltes Teilsystem mit Kategorie 3, PL d und einer *PFH* von $1{,}5 \cdot 10^{-10}$/Stunde ein.
- **PL (SF19.1 und SF 19.2):** Die sicherheitsbezogene Stoppfunktion und die sicher begrenzte Geschwindigkeit werden durch ein durchgängiges Kategorie-3-Teilsystem aus B1.1/B1.2, G2/G1 und K1 bis K4 realisiert, das mit T1 als gekapseltem Kategorie-3-Teilsystem kombiniert wird. Für das erste Teilsystem ergibt sich mit einer mittleren $MTTF_D$ pro Kanal von 14,5 Jahren und mittlerem DC_{avg} von 91 % eine *PFH* von $7{,}1 \cdot 10^{-7}$/Stunde. Durch Kombination mit T1 (PFH = $1{,}5 \cdot 10^{-10}$/Stunde) ergibt sich für beide Sicherheitsfunktionen eine PFH von $7{,}1 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- **PL (SF19.3):** Der Tippbetrieb wird durch eine Kombination des Kategorie-2-Teilsystems S1 (*PFH* = 5,3 · 10^{-7}/Stunde) mit den beiden Kategorie-3-Teilsystemen aus T1 (*PFH* = 1,5 · 10^{-10}/Stunde) und G2/G1 mit K1 bis K4 umgesetzt. Das zweite Kategorie-3-Teilsystem erreicht mit einer mittleren $MTTF_D$ pro Kanal von 14,5 Jahren und mittlerem DC_{avg} von 91 % eine *PFH* von 7,1 · 10^{-7}/Stunde. Die Kombination der drei Teilsysteme ergibt eine *PFH* von 1,2 · 10^{-6}/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Gemeinsame Anforderungen (11/2006). DIN Media, Berlin 2011
- DIN EN 1010-2: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 2: Druck- und Lackiermaschinen einschließlich Maschinen der Druckvorstufe (11/2006). DIN Media, Berlin 2011
- Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitungsmaschinen – Mechanik. Bestell-Nr. MB050. Hrsg.: Berufsgenossenschaft Energie Textil Elektro Medienerzeugnisse, Köln 2023 https://medien.bgetem.de/medienportal?suchtext=MB050
- *Werner C., Zilligen H., Köhler, B. Apfeld, R.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 4/2018. Hrsg.: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin 2018. https://publikationen.dguv.de/Webcode: p012737
- DIN EN IEC 61800-5-3 (Entwurf): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-3: Anforderungen an die Sicherheit von Encodern (Gebern) – Funktional, elektrisch und umwelttechnisch (IEC 22G/383/CD:2018). DIN Media, Berlin (2019)
- IEC 61800-5-3: Adjustable speed electrical power drive systems – Part 5-3: Safety requirements – Functional, electrical and environmental requirements for encoders. VDE-Verlag, Genf (2021)
- DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015. https://publikationen.dguv.de/Webcode:p203079

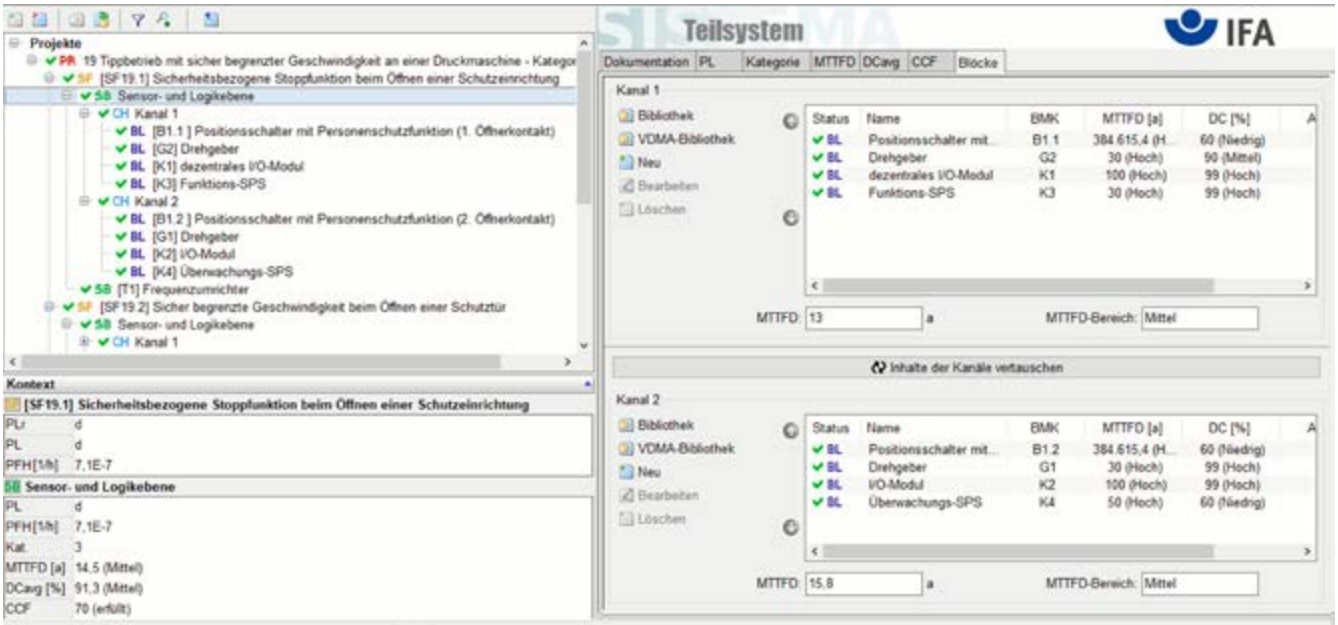


Abb. 11.41 PL-Bestimmung mithilfe von SISTEMA

11.2.20 Pneumatische Ventilsteuerung (Teilsystem) – Kategorie 3 – PL e (Beispiel 20)

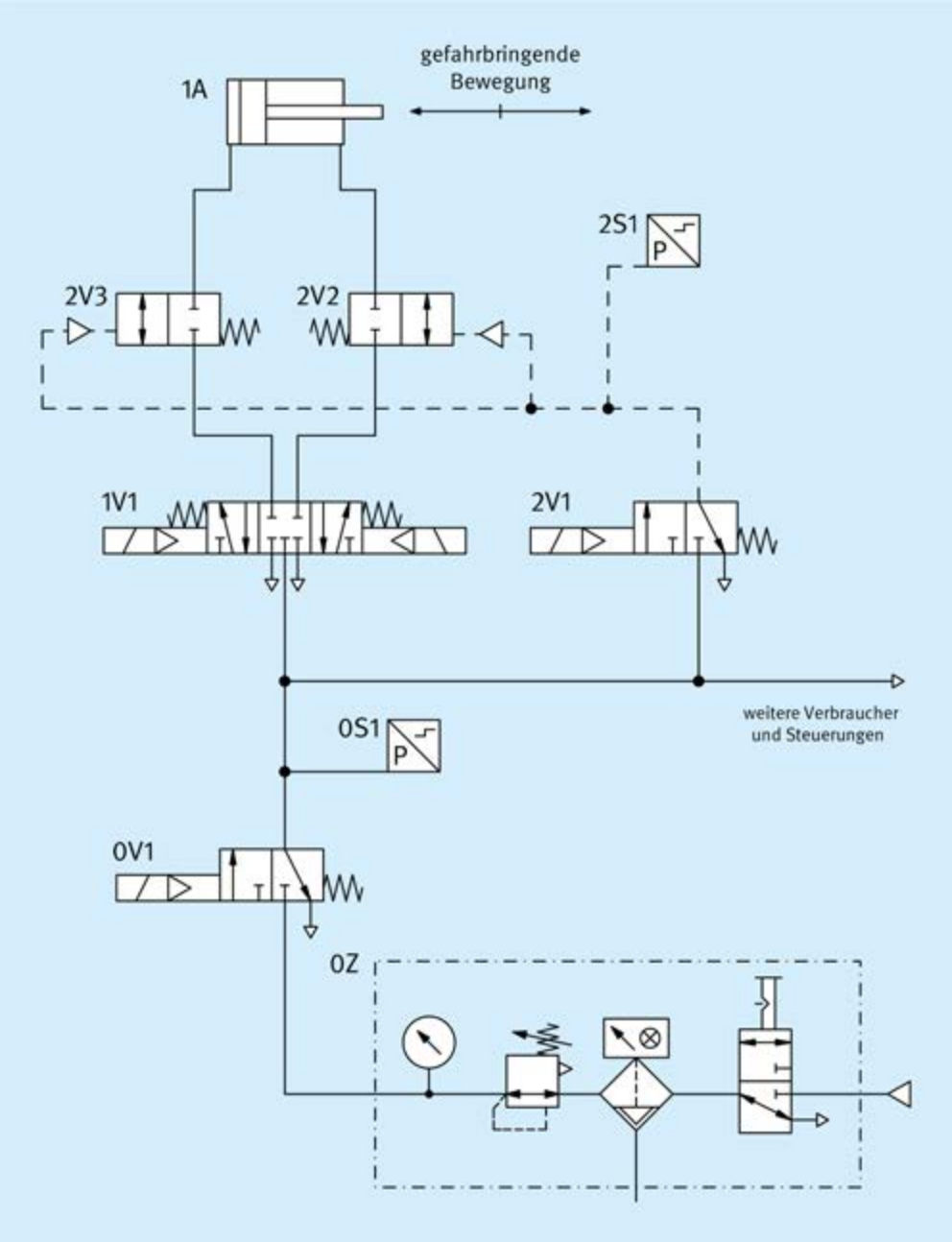


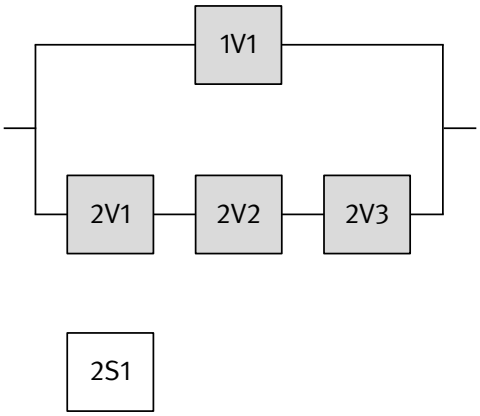
Abb. 11.42
Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- SF20.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktion SSC.
- Hier ist nur der pneumatische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden redundant durch Wegeventile gesteuert. Ein Stillsetzen kann entweder durch das Wegeventil 1V1 oder durch die Wegeventile 2V2 und 2V3 erfolgen. Letztere werden durch das Steuerventil 2V1 angesteuert.
- Der alleinige Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- Alle Wegeventile werden zyklisch im Prozess angesteuert.
- Die Funktion des Steuerventils 2V1 wird durch einen Druckschalter 2S1 überwacht. An den nicht überwachten Ventilen werden einige Fehler im Arbeitsprozess erkannt. Die Ventile 2V2 und 2V3 sollten eine Stellungsüberwachung aufweisen oder – da diese noch



nicht Stand der Technik ist – es muss eine regelmäßige Überprüfung der Funktion durchgeführt werden. Eine Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen. Nähere Informationen zur Realisierung fehlererkennender Maßnahmen finden sich in der Praxishilfe „Sicherheits-Teilfunktionen nach VDMA-Einheitsblatt 24584 – Beispiele zweikanaliger elektro-pneumatischer Steuerungen“.
- 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.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das pneumatische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Die Signalverarbeitung der Drucküberwachung 2S1 erfolgt beispielsweise in einer einkanaligen SPS außerhalb der Funktionskanäle (nicht dargestellt). Die Programmierung der Software (SRASW) realisiert die erforderliche Fehlererkennung für 2V1. Es wird durch ein herstellerinternes Verfahren sichergestellt, dass die zur Fehlererkennung erforderliche SRASW auch tatsächlich in die SPS implementiert ist.
- An die nicht zugängliche Embedded-Software in der einkanaligen SPS zur Diagnose außerhalb der Funktionskanäle werden keine Anforderungen gestellt.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 3.
- ***MTTF*$_D$:** Für die Ventile 1V1, 2V1, 2V2 und 2V3 werden B_{10D}-Werte von 20 000 000 Zyklen angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 20 Sekunden Zykluszeit ist n_{op} = 691 200 Zyklen/Jahr. Damit beträgt die $MTTF_D$ für 1V1, 2V1, 2V2 und 2V3 289 Jahre. Nach Kürzen beider Kanäle auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_D$-Wert pro Kanal von 98 Jahren („hoch“).
- ***DC*$_{avg}$:** DC = 99 % für 2V1 ergibt sich aus der Drucküberwachung des Steuersignals für die Sperrventile. DC = 60 % für 1V1 ergibt sich aus der Fehlererkennung über den Prozess bei zyklischer Ansteuerung (Prozessdiagnoserate sehr viel größer als die Anforderungsrate der Sicherheitsfunktion) und DC = 60 % für 2V2 bzw. 2V3 aus der regelmäßigen Überprüfung der Funktion. Durch Mittelung folgt damit ein DC_{avg} von 70 % („niedrig“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL**: Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_D$ (100 Jahre) und niedrigem DC_{avg} (70%). Für SF20.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $8{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022.
- *Uppenkamp, J*: Sicherheits-Teilfunktionen nach VDMA-Einheitsblatt 24584 – Beispiele zweikanaliger elektropneumatischer Steuerungen. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2020. https://www.dguv.de/medien/ifa/de/pra/hydraulik_pneumatik/beispiele_teilsicherheitsfunktionen.pdf

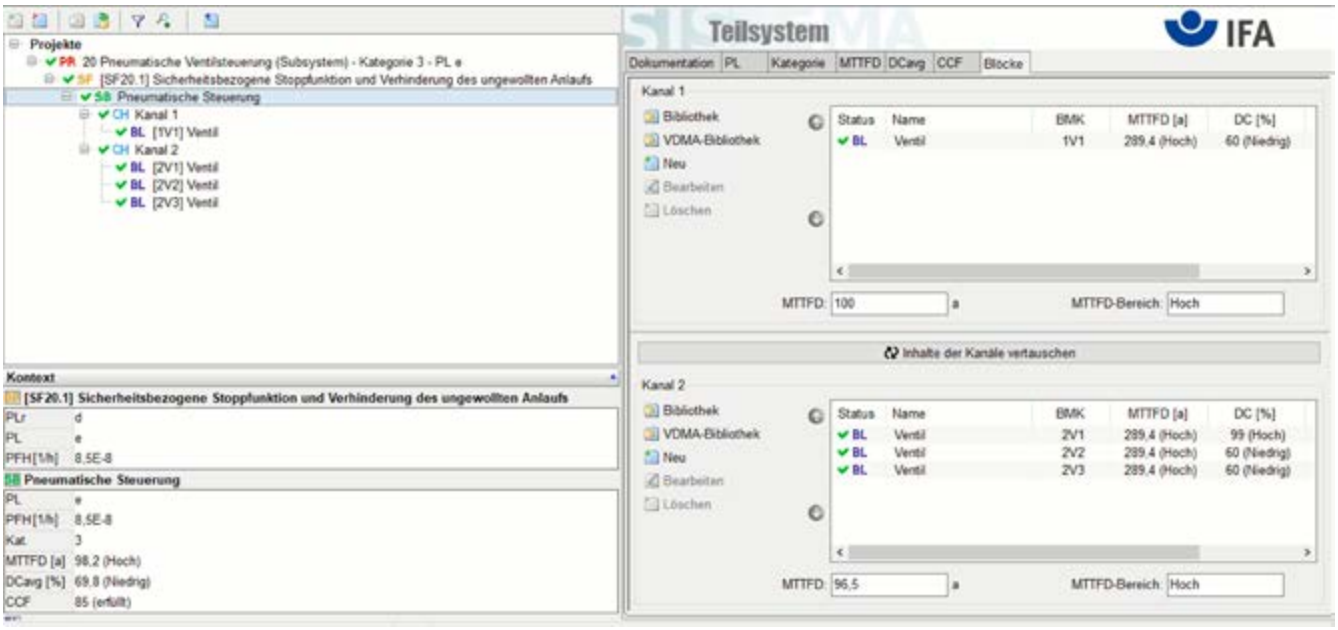


Abb. 11.43 PL-Bestimmung mithilfe von SISTEMA

11.2.21 Hydraulische Ventilsteuerung (Teilsystem) – Kategorie 3 – PL e (Beispiel 21)

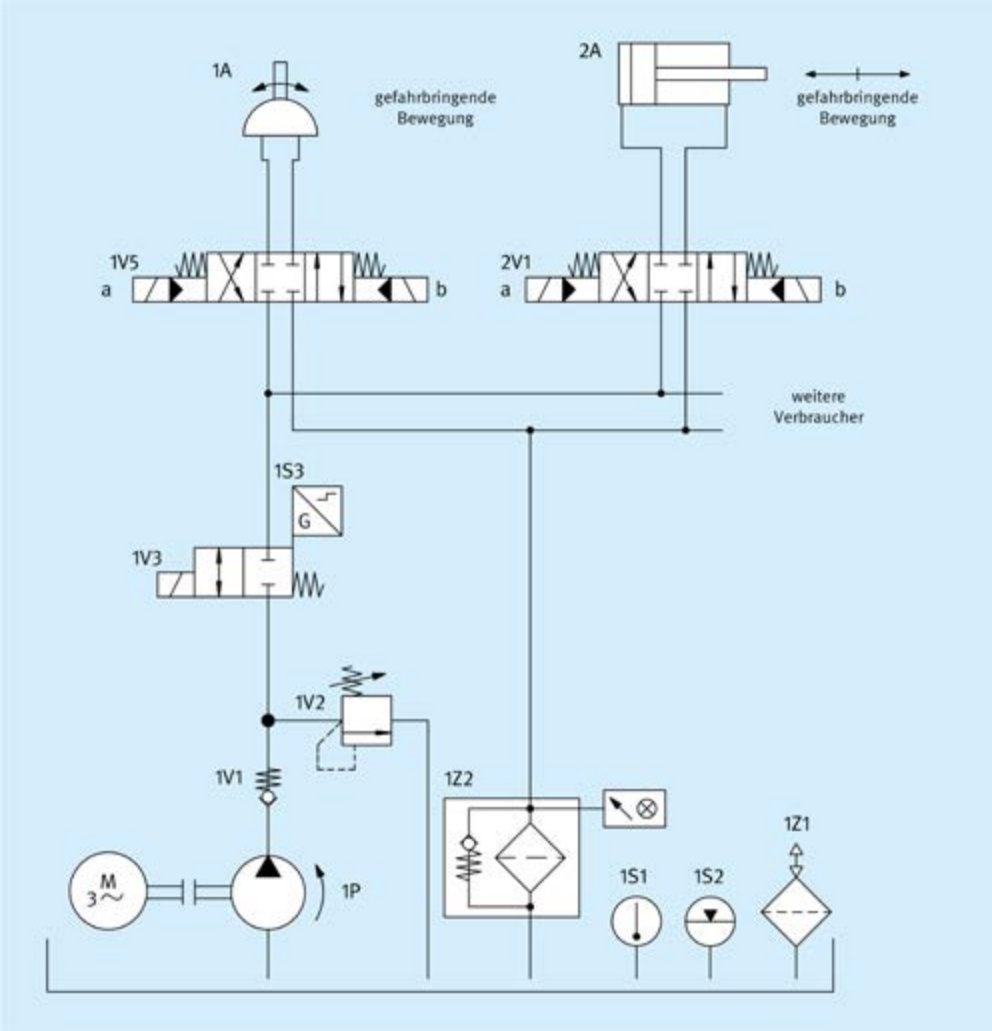


Abb. 11.44
Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

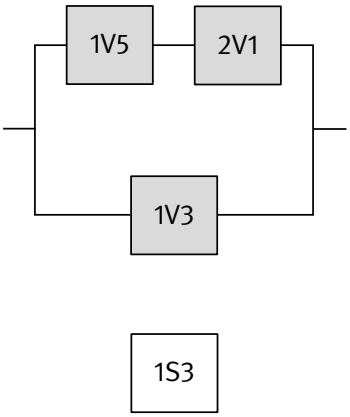
- SF21.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage.
- Hier ist nur der hydraulische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme 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.



- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das hydraulische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Die Signalverarbeitung der elektrischen Stellungsüberwachung 1S3 erfolgt beispielsweise in einer einkanaligen SPS außerhalb der Funktionskanäle (nicht dargestellt). Die Programmierung der Software (SRASW) realisiert die erforderliche Fehlererkennung für 1V3. Es wird durch ein herstellerinternes Verfahren sichergestellt, dass die zur Fehlererkennung erforderliche SRASW auch tatsächlich in die SPS implementiert ist.

An die nicht zugängliche Embedded-Software in der einkanaligen SPS zur Diagnose außerhalb der Funktionskanäle werden keine Anforderungen gestellt

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 3.
- ***MTTF*$_D$:** Für die Wegeventile 1V3, 1V5 und 2V1 wird eine *MTTF*$_D$ von 150 Jahren angenommen [H]. Nach Kürzen des zweiten Kanals (1V3) auf 100 Jahre ergibt sich ein symmetrisierter *MTTF*$_D$-Wert von 88 Jahren („hoch“).
- ***DC*$_{avg}$:** *DC* = 99 % für 1V3 beruht auf der direkten Überwachung des Schaltzustandes durch 1S3. *DC* = 60 % für die Wegeventile 1V5 bzw. 2V1 beruht auf der indirekten Überwachung durch den Prozess bei zyklischer Ansteuerung (Prozessdiagnoserate sehr viel größer als die Anforderungsrate der Sicherheitsfunktion). Durch Mittelung ergibt sich damit ein *DC*$_{avg}$ von 73 % („niedrig“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL**: Die Kombination der hydraulischen Steuerungselemente entspricht Kategorie 3 mit hoher *MTTF*$_D$ (88 Jahre) und niedrigem *DC*$_{avg}$ (73 %). Für SF21.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $9{,}4 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022

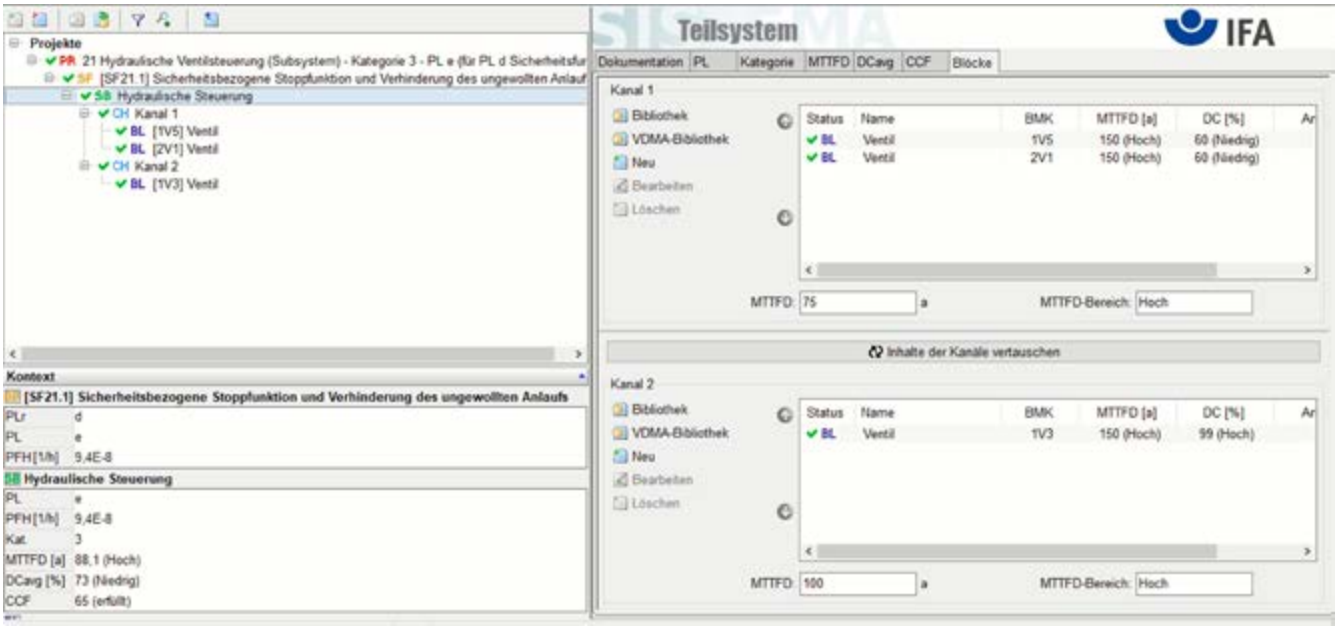


Abb. 11.45 PL-Bestimmung mithilfe von SISTEMA

11.2.22 Kaskadierung von Not-Halt-Geräten mittels Sicherheitsschaltgerät– Kategorie 3 – PL e (Beispiel 22)

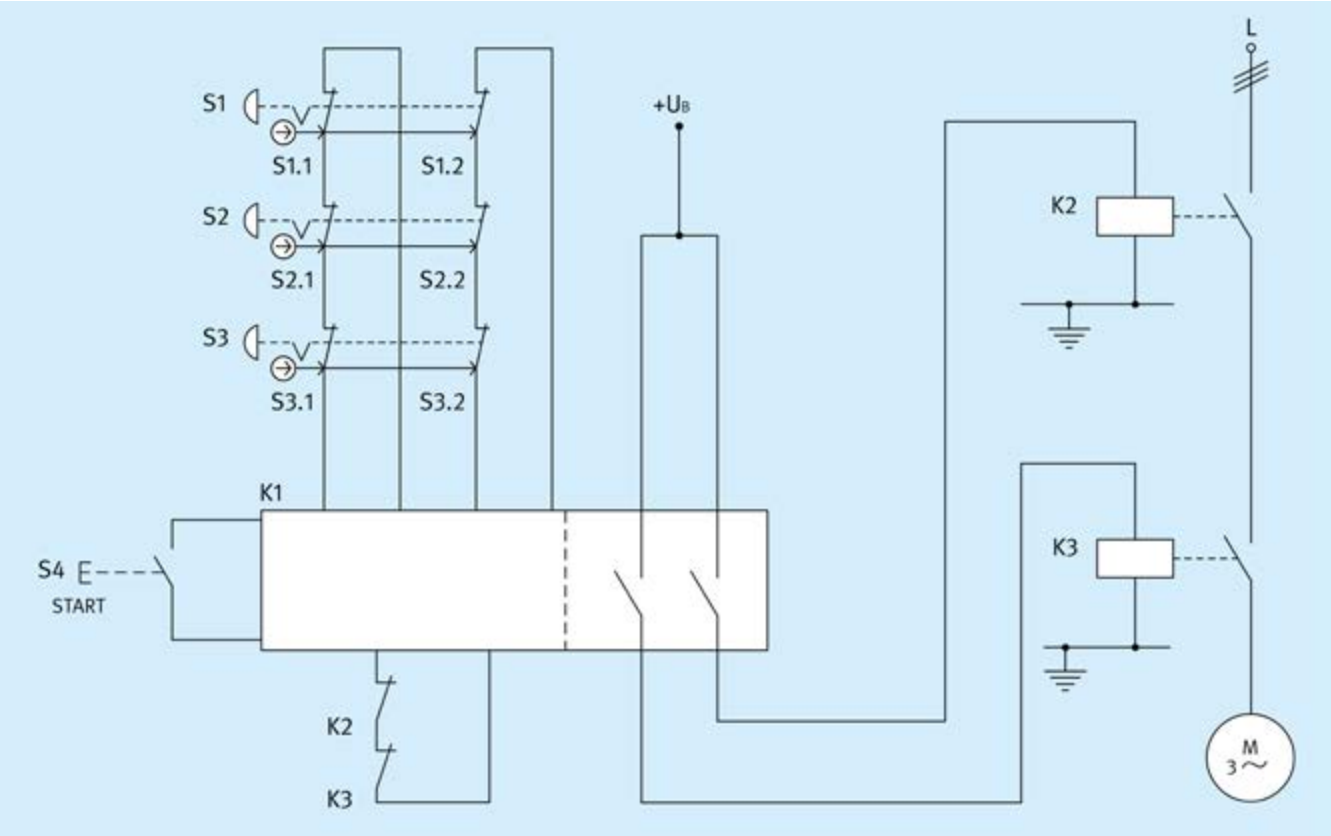


Abb. 11.46 Kaskadierung von Not-Halt-Geräten mittels Sicherheitsschaltgerät (Not-Halt-Funktion, STO)

Sicherheitsfunktion

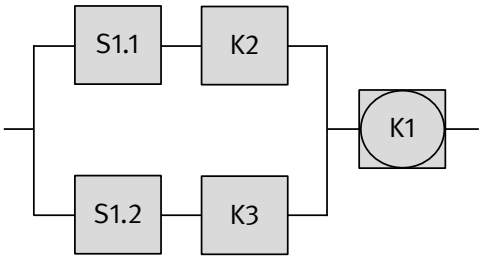
- SF22.1: Durch Betätigung des Not-Halt-Gerätes S1, S2 oder S3 wird die Energie zum Motor sicher abgeschaltet (STO).

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden durch Betätigung eines Not-Halt-Gerätes unterbrochen bzw. verhindert. Entsprechend Beispiel 3 in Abschnitt 6.3.2 löst jedes Not-Halt-Gerät eine eigene Sicherheitsfunktion aus. Stellvertretend wird im Folgenden nur S1 betrachtet. Die Sicherheitsfunktion für die beiden anderen Not-Halt-Geräte S2 und S3 ist identisch ausgeführt und führt in der Bewertung zu den gleichen Ergebnissen. Die Auswertung der in Reihe geschalteten Not-Halt-Geräte erfolgt in einem Sicherheitsschaltgerät K1, das zwei redundante Hilfsschütze K2 und K3 ansteuert.
- Die Not-Halt-Geräte S1, S2 und S3 werden zur Fehlererkennung redundant in das Sicherheitsschaltgerät K1 eingelesen. Das Schaltgerät verfügt über einen Kreuzvergleich von Eingangssignalen ohne dynamischen Test. Die Häufigkeit des Signalwechsels beeinfluss den Diagnosedeckungsgrad für die in Reihe liegenden Not-Halt-Geräte.
- Durch organisatorische Maßnahmen wird sichergestellt, dass jedes Not-Halt-Gerät mindestens einmal pro Jahr betätigt wird, zusätzlich wird eine tatsächliche Auslösung der Not-Halt-Funktion pro Jahr angenommen.
- Es wird nicht unterstellt, dass mehr als ein Not-Halt-Gerät gleichzeitig betätigt wird.
- 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.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung) und CCF-Maßnahmen, wie in den ersten Abschnitten von Kapitel 11 beschrieben, sind vorgesehen.
- Bei den Not-Halt-Geräten S1, S2 und S3 handelt es sich um Schaltgeräte mit zwangsöffnenden Kontakten entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Schaltgeräten sind geschützt verlegt.
- Das Sicherheitsschaltgerät K1 erfüllt alle Anforderungen für Kategorie 4, PL e und PFH = $2{,}3 \cdot 10^{-9}$/Stunde.
- K2 und K3 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.



- Das Teilsystems wird in geeigneten Umgebungsbedingungen eingesetzt. Dies beinhaltet die Mindestanforderungen der Kategorie B. Die elektromagnetische Störfestigkeit, mechanischen Bedingungen wie Schock-, Vibrations-, und Temperaturfestigkeit der eingesetzten Komponenten sind eingehalten.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Bemerkung

- Die Not-Halt-Funktion ist eine ergänzende Schutzmaßnahme nach DIN EN ISO 12100:2011

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus zwei Teilsystemen der Kategorie 3.
- ***MTTF*$_D$:** Bei S1, S2 und S3 handelt es sich um identische handelsübliche Not-Halt-Geräte nach DIN EN ISO 13850. Bei der zweikanaligen Modellierung wird für jeden Kontakt eines Not-Halt-Gerätes jeweils ein B_{10D} von 100 000 Schaltspielen angesetzt. Die Ausfallhäufigkeit des Sicherheitsschaltgerätes K1 wird am Ende der Berechnung addiert. Für die Hilfsschütze K2 und K3 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1000 000 Schaltspielen. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10D}-Wert durch Verdoppelung des B_{10}-Wertes. Bei jährlich zwölf Anforderungen der Not-Halt-Funktion und 24 Startbefehlen ist n_{op} = 36 Zyklen/Jahr und $MTTF_D$ beträgt 555 555 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 durch einen Kreuzvergleich von Ausgangssignalen ohne dynamischen Test. Der *DC* beruht auf der Testung und Querschlusserkennung durch das Sicherheitsschaltgerät K1. Für die *DC* der Kontakte S1.1 und S1.2 ist im Sicherheitsschaltgerät die Maßnahme des Kreuzvergleich von Eingangssignalen ohne dynamischen Test eingestellt. Der prozentuale Anteil des *DC*-Werts ist aufgrund der Testrate r_t von 1/Jahr und einmal jährliche Not-Halt-Funktion auf 90 % anzusetzen (siehe Tabelle E.1 Anmerkung 4 der Norm). Dies führt für beide Teilsysteme zu einer DC_{avg} von 90 % („mittel“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), bewährte Bauteile (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL:** Für das erste Teilsystem bestehend aus Not-Halt-Gerät und Hilfsschützen ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle PFH von $4{,}3 \cdot 10^{-8}$/Stunde.
- Nach Hinzufügen des zweiten Teilsystems K1 beträgt für SF22.1 die mittlere Häufigkeit gefährlicher Ausfälle 4,5 10^{-8}/Stunde. Dies entspricht PL e.

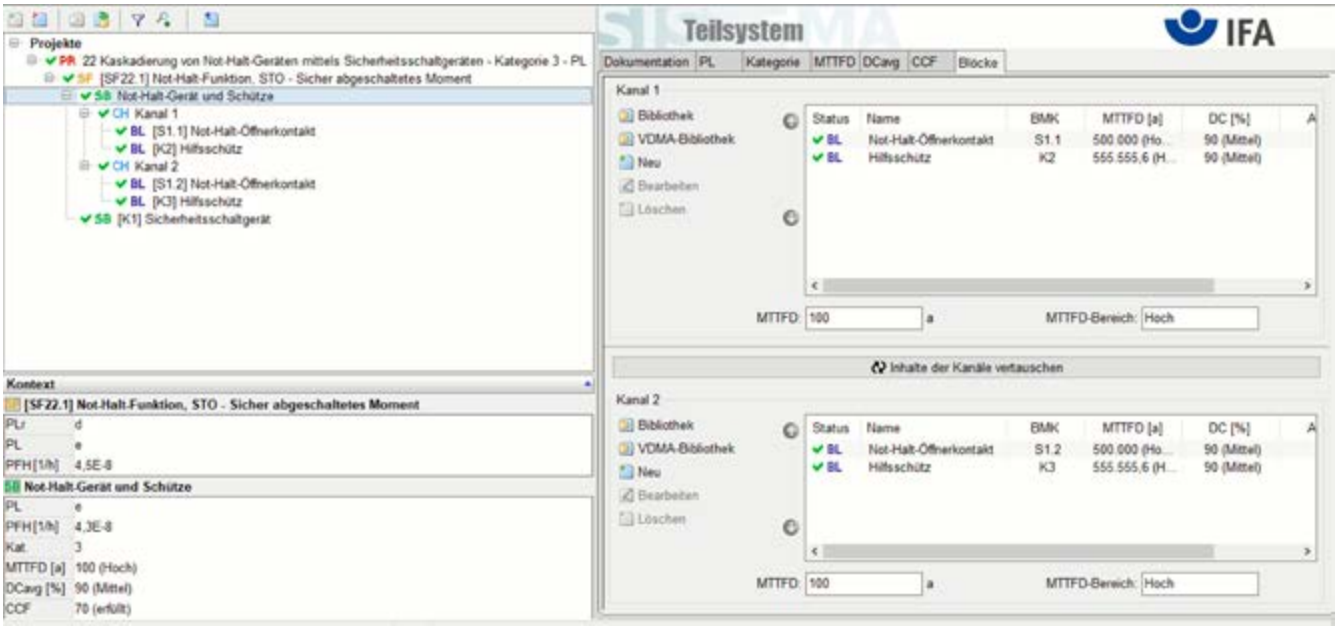


Abb. 11.47 PL-Bestimmung mithilfe von SISTEMA

11.2.23 Pneumatische Ventilsteuerung (Teilsystem) – Kategorie 4 – PL e (Beispiel 23)

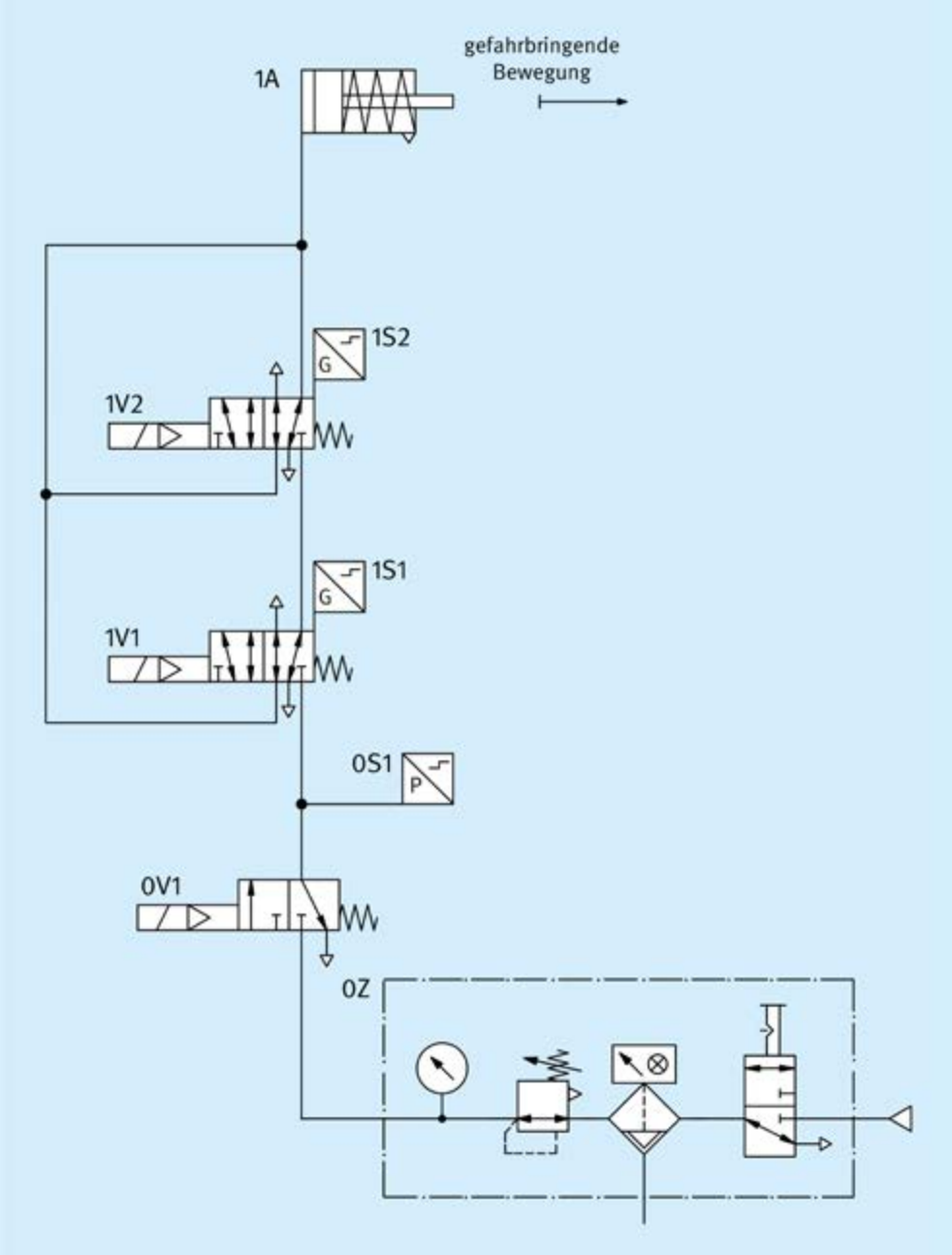


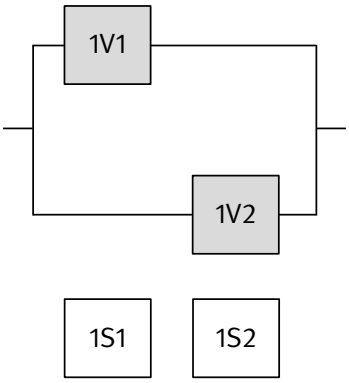
Abb. 11.48
Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- SF23.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktion SDE.
- Hier ist nur der pneumatische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme hinzuzufügen.

Funktionsbeschreibung

- Eine gefahrbringende Bewegung des Zylinders wird redundant durch die Ventile 1V1 und 1V2 gesteuert. Ein Stillsetzen der Bewegung kann entweder durch das Wegeventil 1V1 oder 1V2 erfolgen.
- Der alleinige Ausfall eines der beiden Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- Nach Wegnahme mindestens eines Steuersignals wird die Kolbenseite des Zylinders entlüftet.
- Der einzelne Fehler eines Ventils wird bei Wegnahme der Ansteuerung durch die integrierte Stellungsüberwachung erkannt; nach einem Fehler wird das Einleiten der nächsten gefahrbringenden Bewegung verhindert.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- 1V1 und 1V2 sind Wegeventile mit ausreichend positiver Überdeckung, Federrückstellung sowie elektrischer Stellungsüberwachung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme der Steuersignale erreicht.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das pneumatische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Die Signalverarbeitung der elektrischen Stellungsüberwachung 1S1 und 1S2 erfolgt beispielsweise in einer einkanaligen SPS außerhalb der Funktionskanäle (nicht dargestellt). Die Programmierung der Software (SRASW) realisiert die erforderliche Fehlererkennung für 1V1 und 1V2. Es wird durch ein herstellerinternes Verfahren sichergestellt, dass die zur Fehlererkennung erforderliche SRASW auch tatsächlich in die SPS implementiert ist. An die nicht zugängliche Embedded-Software in der einkanaligen SPS zur Diagnose außerhalb der Funktionskanäle werden keine Anforderungen gestellt.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 4.
- ***MTTF*$_D$:** Für die Wegeventile wird ein B_{10D}-Wert von 20 000 000 Zyklen angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 20 Sekunden Zykluszeit ist n_{op} = 691 200 Zyklen/Jahr und $MTTF_D$ = 289 Jahre („hoch“). Dies ist gleichzeitig der $MTTF_D$-Wert pro Kanal.
- ***DC*$_{avg}$:** DC = 99 % für 1V1 und 1V2 ergibt sich aus der direkten Überwachung der Schaltzustände. Damit ergibt sich ein DC_{avg} von ebenfalls 99 % („hoch“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL**: Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_D$ (289 Jahre) und hohem DC_{avg} (99 %). Für SF23.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $8{,}1 \cdot 10^{-9}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022.

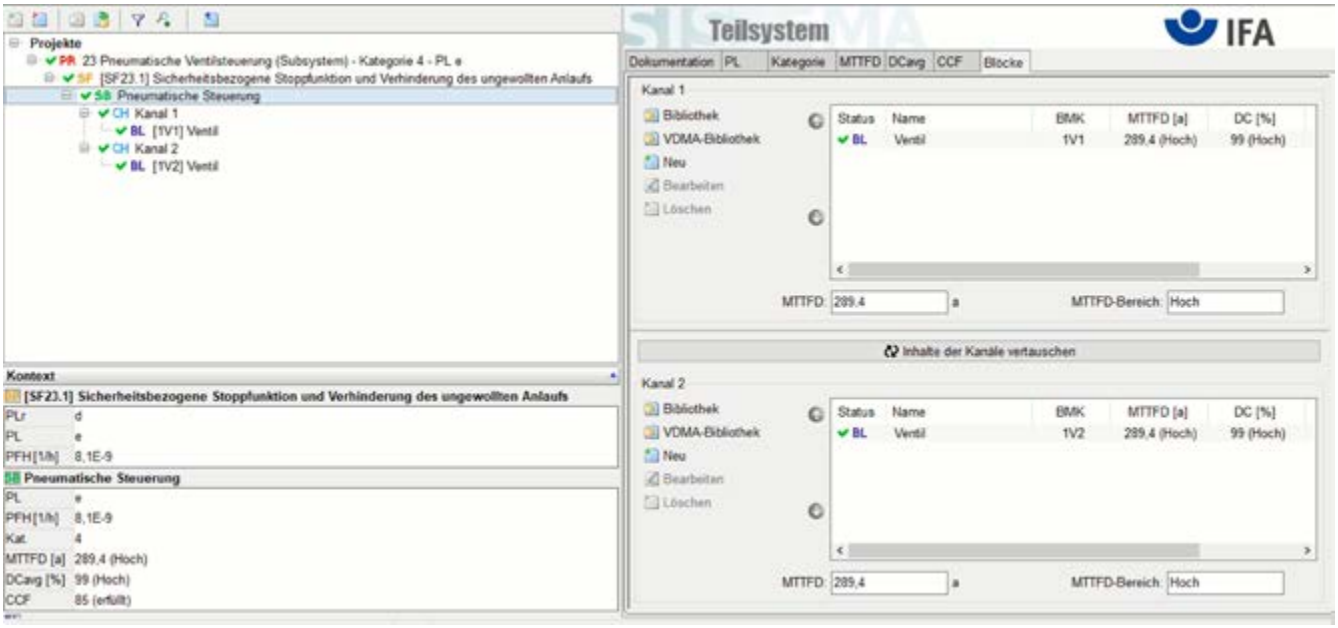


Abb. 11.49 PL-Bestimmung mithilfe von SISTEMA

11.2.24 Hydraulische Ventilsteuerung (Teilsystem) – Kategorie 4 – PL e (Beispiel 24)

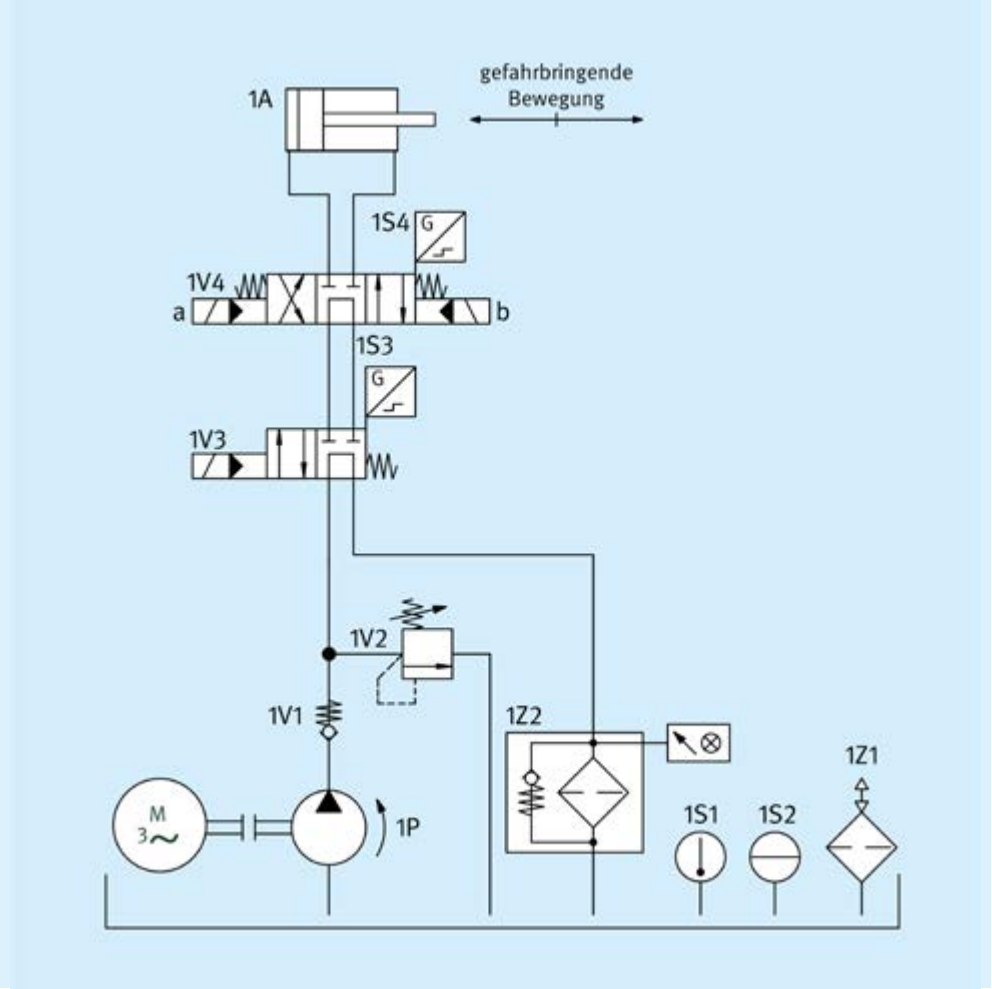


Abb. 11.50
Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

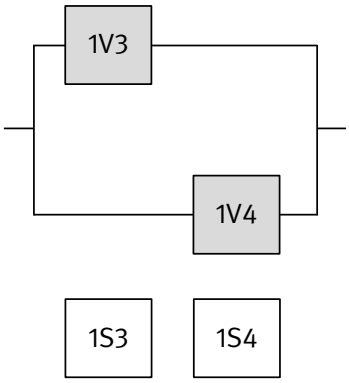
- SF24.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktion SSC.
- Hier ist nur der hydraulische Steuerungsteil als Teilsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme 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 in Ruhestellung eine Sperrstellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung sowie eine elektrische Stellungsüberwachung.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das hydraulische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Die Signalverarbeitung der elektrischen Stellungsüberwachung 1S3 und 1S4 erfolgt beispielsweise in einer einkanaligen SPS außerhalb der Funktionskanäle (nicht dargestellt). Die Programmierung der Software (SRASW) realisiert die erforderliche Fehlererkennung für 1V3 und 1V4. Es wird durch ein herstellerinternes Verfahren sichergestellt, dass die zur Fehlererkennung erforderliche SRASW auch tatsächlich in die SPS implementiert ist. An die nicht zugängliche



Embedded-Software in der einkanaligen SPS zur Diagnose außerhalb der Funktionskanäle werden keine Anforderungen gestellt.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 4.
- ***MTTF*$_D$:** Für die Wegeventile 1V3 und 1V4 wird eine *MTTF*$_D$ von 150 Jahren angenommen.
- ***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“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL**: Die Kombination der hydraulischen Steuerungselemente entspricht Kategorie 4 mit hoher *MTTF*$_D$ und hohem *DC*$_{avg}$ (99 %). Für SF24.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von 1,6 · 10^{-8}/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Teilsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022

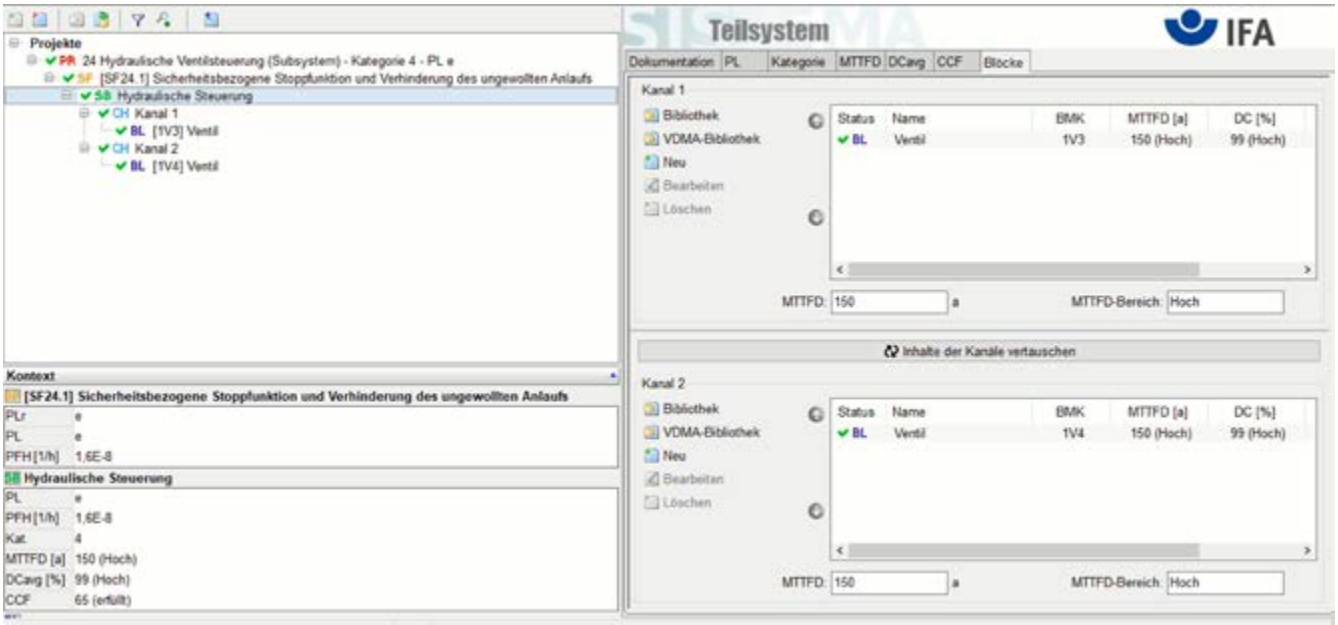


Abb. 11.51 PL-Bestimmung mithilfe von SISTEMA

11.2.25 Elektrohydraulische Pressensteuerung – Kategorie 4 – PL e (Beispiel 25)

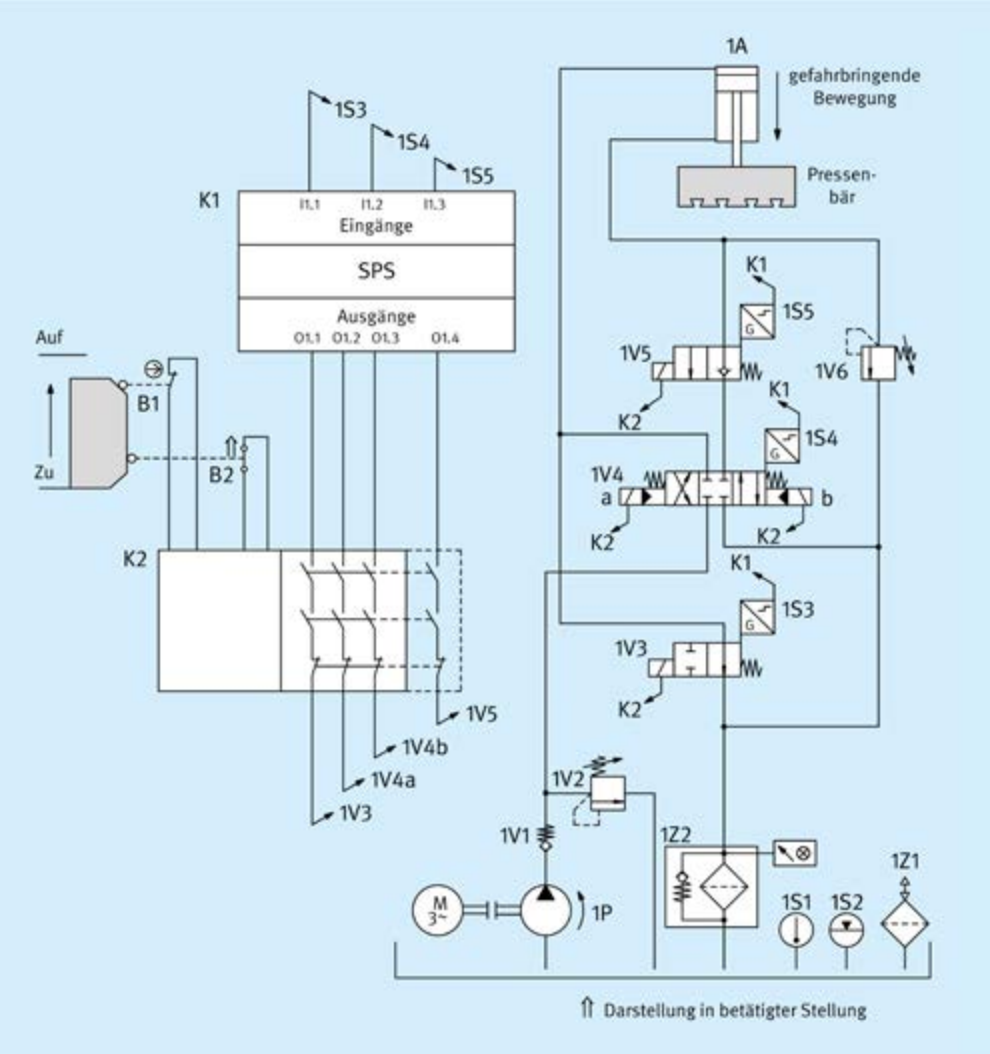


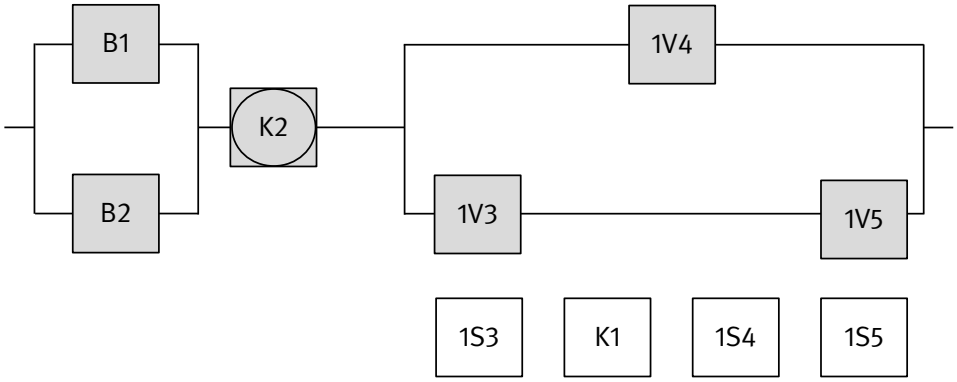
Abb. 11.52
Pressensteuerung, elektrische Überwachung einer beweglichen trennenden Schutzeinrichtung mit hydraulischem Stillsetzen der gefahrbringenden Bewegung

Sicherheitsfunktion

- SF25.1: Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktion SSC.

Funktionsbeschreibung

- Der Gefahrenbereich ist mittels einer verriegelten trennenden Schutzeinrichtung gesichert, deren Stellung von zwei Positionsschaltern B1 und B2 in Öffner-Schließer-Kombination erfasst wird. Die Signale der Positionsschalter werden in ein handelsübliches Sicherheitsschaltgerät K2 eingelesen, das in die Ansteuersignale der elektrischen Vorsteuerung K1 (herkömmliche SPS) für die hydraulischen Aktoren eingeschleift ist. Gefahrbringende Bewegungen oder Zustände werden aktorseitig durch drei Wegeventile (1V3, 1V4 und 1V5) gesteuert. Bei Anforderung der Sicherheitsfunktion werden alle Ventile durch K2 stromlos geschaltet und gehen aufgrund der vorhandenen Rückstellfedern in die Sperr-Mittelstellung (1V4), in die Sperr-Stellung (1V5) und entlasten zum Tank (1V3). Dabei wird der Ölrückfluss von der Kolbenunterseite des Zylinders zum Tank durch die Ventile 1V4 und 1V5 gleichzeitig abgesperrt. Bei dem Ventil 1V5 handelt es sich um ein Sitzventil, das aufgrund seiner Konstruktion den Volumenstrom leckagefrei absperrt. Ventil 1V4, das auch die Bewegungsrichtung des Zylinders steuert, ist ein Wegeventil in Schieberbauweise, das auch in der Sperr-Mittelstellung eine gewisse Leckage aufweist. Obwohl das Ventil 1V3 nur mittelbar an der Stoppfunktion beteiligt ist, kann es die Sicherheitsfunktion in gefährlicher Weise beeinträchtigen. Würden 1V3 und 1V4 gleichzeitig hängen bleiben, so würde auf der Kolbenoberseite Druck aufgebaut, während die Kolbenunterseite durch 1V5 abgesperrt bleibt. Wegen der Druckübersetzung im Zylinder würde dann das Druckbegrenzungsventil 1V6 öffnen und der Pressenbär absinken.



- Der Ausfall eines Ventils führt nicht zum Verlust der Sicherheitsfunktion. Alle Ventile werden zyklisch angesteuert.
- An allen Ventilen ist jeweils eine Stellungsabfrage 1S3, 1S4 bzw. 1S5 zur Fehlererkennung vorgesehen. Der Ausfall jedes der drei Ventile wird in der 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 11 beschrieben, sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Das Sicherheitsschaltgerät K2 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Zuleitungen zu den Positionsschaltern sind getrennt oder geschützt verlegt.
- Die Ventile 1V3, 1V4 und 1V5 haben eine Sperr-Mittelstellung bzw. Sperr-Stellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung und sind stellungsüberwacht.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Das Druckbegrenzungsventil 1V6 zum Schutz des Zylinders 1A und der darunter liegenden Bauteile gegen „Druckübersetzerwirkung“ erfüllt die Anforderungen der DIN EN ISO 16092-3, Abs. 5.2.3.3.

- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt werden (siehe Anhang L der Norm).
- **Software:** Für K1 wird eine handelsübliche SPS ohne Sicherheitsfunktionen verwendet. Die Programmierung der Software (SRASW) von K1 außerhalb der Funktionskanäle realisiert die erforderliche Fehlererkennung für 1V3, 1V4 und 1V5. Es wird durch ein herstellerinternes Verfahren sichergestellt, dass die zur Fehlererkennung erforderliche SRASW auch tatsächlich in K1 implementiert ist.
- An die nicht zugängliche Embedded-Software in K1 zur Diagnose außerhalb der Funktionskanäle werden keine Anforderungen gestellt.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion besteht aus drei Teilsystemen der Kategorie 4. Elektromechanik und Hydraulik werden getrennt zu jeweils einem Teilsystem der Kategorie 4 zusammengefasst, deren Ausfallhäufigkeit im Folgenden berechnet wird. K2 wird als gekapseltes Teilsystem mit einer Ausfallhäufigkeit von $2{,}3 \cdot 10^{-9}$/Stunde addiert.
- ***MTTF*$_D$:** Für den Positionsschalter B1 wird aufgrund der Zwangsöffnung ein B_{10D}-Wert von 20 000 000 Schaltspielen angenommen. Für den elektrischen Schließerkontakt von Positionsschalter B2 beträgt B_{10D} = 1 000 000 Schaltspiele. 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 5 707 Jahre für B1 bzw. 285 Jahre für B2. Für die Ventile 1V3, 1V4 und 1V5 wird jeweils eine $MTTF_D$ von 150 Jahren angenommen. Dies ergibt einen $MTTF_D$-Wert pro Kanal von 100 bzw. 88 Jahren („hoch“) für beide Teilsysteme.
- ***DC*$_{avg}$:** *DC* = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung beider Schaltzustände in K2. Der *DC* von 99 % für alle Ventile beruht auf der direkten Überwachung der Schaltzustände durch die SPS K1. Dies ergibt einen DC_{avg} von 99 % („hoch“) für beide Teilsysteme.

- **CCF**: Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte) für beide Teilsysteme: Trennung (15), bewährte Bauteile (5), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL**: Der elektromechanische und der hydraulische Teil der Steuerung entsprechen Kategorie 4 mit hoher $MTTF_D$ und hohem DC_{avg} (99 %). Damit ergibt sich die mittlere Häufigkeit gefahrbringender Ausfälle von $1{,}3 \cdot 10^{-9}$/Stunde und $2{,}1 \cdot 10^{-8}$/Stunde. Für die komplette Sicherheitsfunktion SF25.1 ergibt sich durch Addition inklusive K2 eine mittlere Häufigkeit gefährlicher Ausfälle von $2{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

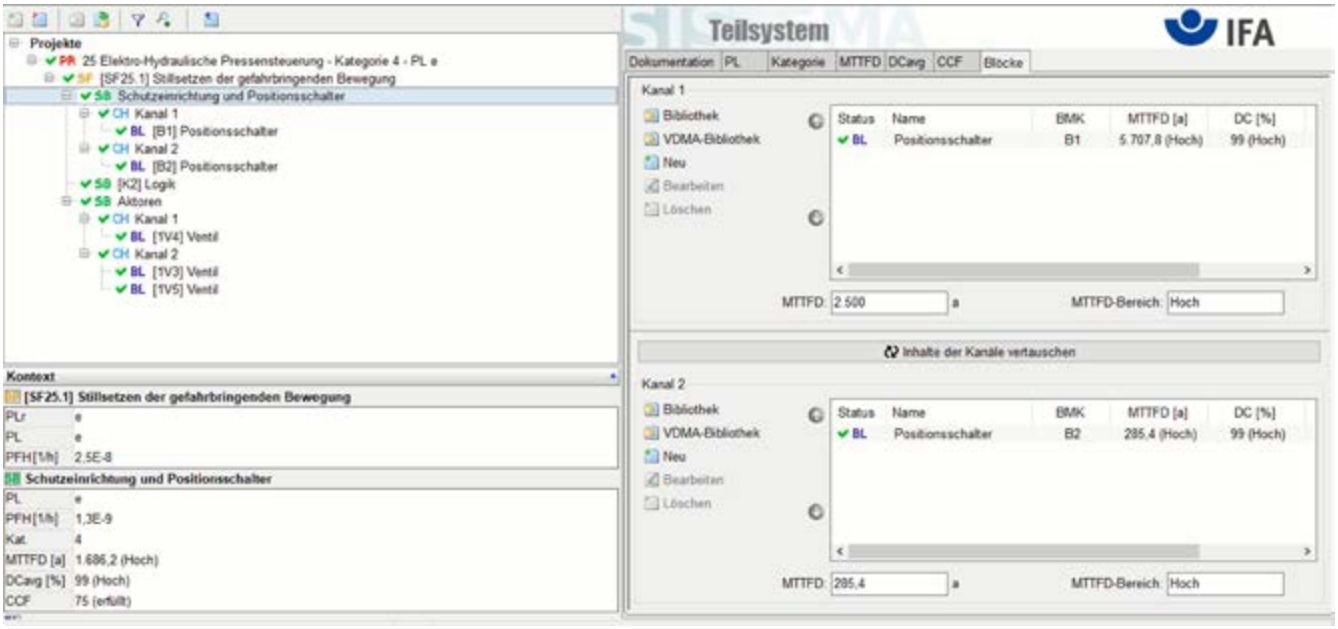


Abb. 11.53 PL-Bestimmung mithilfe von SISTEMA

11.2.26 Stellungsüberwachung einer verriegelten trennenden Schutzeinrichtung – Kategorie 4 – PL e (Beispiel 26)

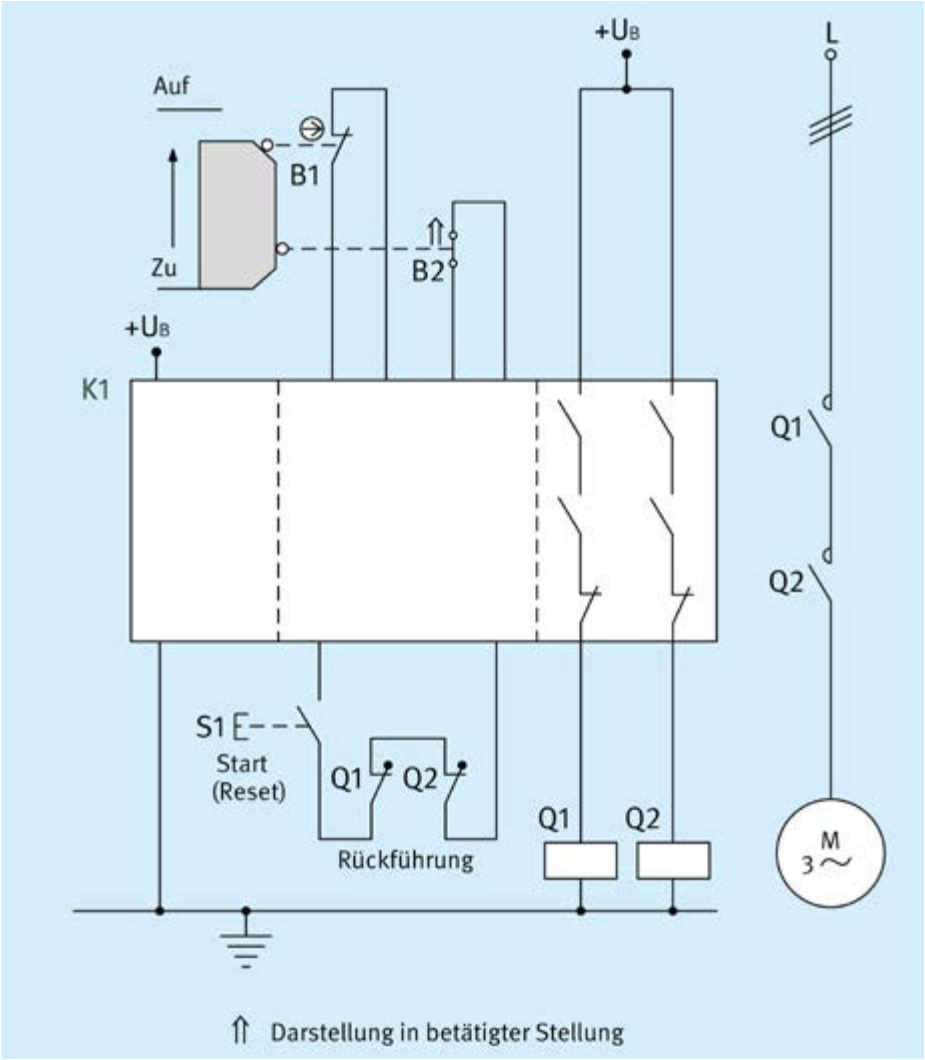


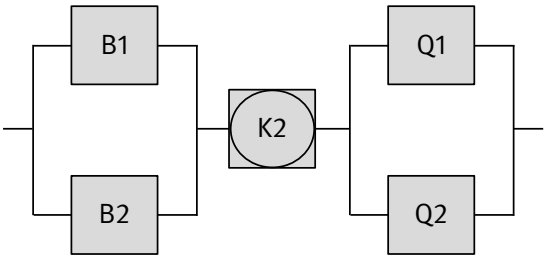
Abb. 11.54
Stellungsüberwachung einer verriegelten trennenden Schutzeinrichtung mittels Sicherheitsschaltgerät

Sicherheitsfunktion

- SF26.1: Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der verriegelten trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion Sicher abgeschaltetes Moment (STO) ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt durch eine verriegelte trennende Schutzeinrichtung (Schutzgitter). Das Öffnen des Schutzgitters wird durch zwei Positionsschalter B1/B2 in Öffner-Schließer-Kombination erfasst und in einem Sicherheitsschaltgerät K1 ausgewertet. Dieses steuert zwei Leistungsschütze Q1 und Q2 an, durch deren Abfallen gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert werden.
- Die Positionsschalter B1/B2 werden zur Fehlererkennung in K1 überwacht und auf Plausibilität geprüft. Fehler in den Schützen Q1 und Q2 werden durch eine Anlauftestung in K1 erkannt. Hierzu sind Spiegelkontakte (Öffner) der Schütze in den Rückführkreis von K1 eingebunden. Ein Start-Befehl ist nur erfolgreich, wenn Q1 und Q2 zuvor abgefallen waren. Eine Anlauftestung durch Öffnen und Schließen der Schutzeinrichtung ist nicht erforderlich.
- Die Sicherheitsfunktion bleibt auch beim Auftreten einzelner Fehler erhalten. Diese werden während des Betriebs oder beim Betätigen (Öffnen und Schließen) der Schutzeinrichtung aufgedeckt.
- 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 11 beschrieben, sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtungen zur Betätigung der Positionsschalter ist sichergestellt.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern B1 und B2 sind getrennt oder geschützt verlegt.
- Das Sicherheitsschaltgerät K1 erfüllt alle Anforderungen an Kategorie 4 und PL e.
- Die Schütze Q1 und Q2 besitzen Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt werden (siehe Anhang L der Norm).
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Bemerkung

- Kategorie 4 wird nur eingehalten, wenn nicht mehrere Schutzeinrichtungen mit mechanischen Positionsschalter hintereinandergeschaltet werden (keine Kaskadierung), da ansonsten die Fehlererkennung in den Schaltern eingeschränkt ist (siehe Anhang E).

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion lässt sich in drei Teilsysteme aufteilen, wie im sicherheitsbezogenen Blockdiagramm gezeigt. Die Ausfallhäufigkeit des handelsüblichen Sicherheitsschaltgerätes K1 wird am Ende der Berechnung addiert ($2{,}3 \cdot 10^{-9}$/Stunde, geeignet für PL e). Für die übrigen Teilsysteme wird die Ausfallhäufigkeit im Folgenden berechnet.
- ***MTTF*$_D$:** Für den Positionsschalter B1 (zwangsöffnend) beträgt der B_{10D} 20 000 000 Schaltspiele. Für den Positionsschalter B2 (Schließerkontakt) beträgt B_{10D} 100 000 Schaltspiele. Bei 365 Arbeitstagen, 16 Arbeitsstunden und einer Stunde Zykluszeit ist für diese Komponenten n_{op} = 5 840 Zyklen/Jahr und die symmetrisierte $MTTF_D$ beträgt 1674 Jahre für B1 und B2.
  Für die Schütze Q1 und Q2 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen. 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 (gekürzt auf 2 500 Jahre) pro Kanal. Der Positionsschalter B2 weist eine begrenzte Betriebszeit von 17,1 Jahren auf. Ein rechtzeitiger Austausch wird empfohlen.
- ***DC*$_{avg}$:** *DC* = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in K1. *DC* = 99 % für die Schütze Q1 und Q2 ergibt sich aus der regelmäßigen Überwachung der Spiegelkontakte durch K1 bei jedem Start. Die genannten *DC*-Werte entsprechen dem DC_{avg} für das jeweilige Teilsystem.
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Teilsystemen B1/B2 und Q1/Q2 (85 bzw. 70 Punkte): Trennung (15), bewährte Bauteile (5 nur Q1/Q2), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL:** Die Teilsysteme B1/B2 und Q1/Q2 entsprechen jeweils Kategorie 4 mit hoher $MTTF_D$ (1674 und 2500 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von $1{,}4 \cdot 10^{-9}$/Stunde (B1/B2) und $9{,}1 \cdot 10^{-10}$/Stunde (Q1/Q2). Nach Hinzufügen des Teilsystems K1 beträgt die mittlere Häufigkeit gefährlicher Ausfälle für die gesamte Sicherheitsfunktion SF26.1 beträgt $4{,}6 \cdot 10^{-9}$/Stunde. Dies entspricht PL e.

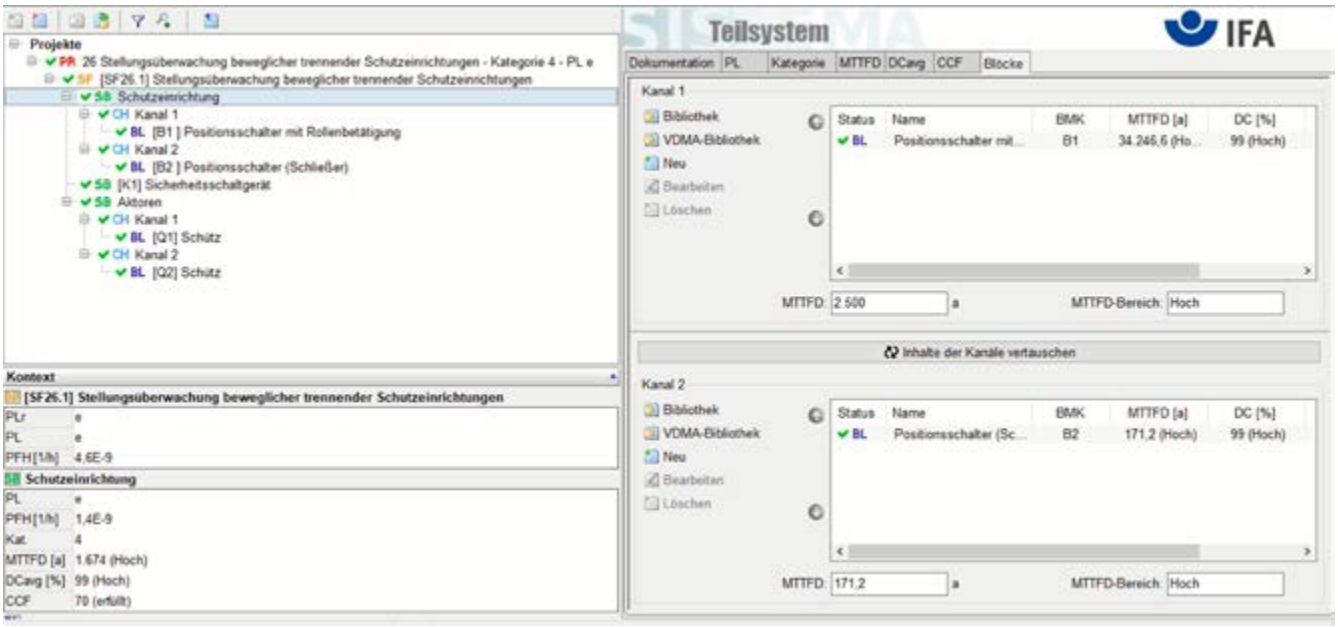


Abb. 11.55 PL-Bestimmung mithilfe von SISTEMA

11.2.27 Zweihandschaltung – Kategorie 4 – PL e (Beispiel 27)

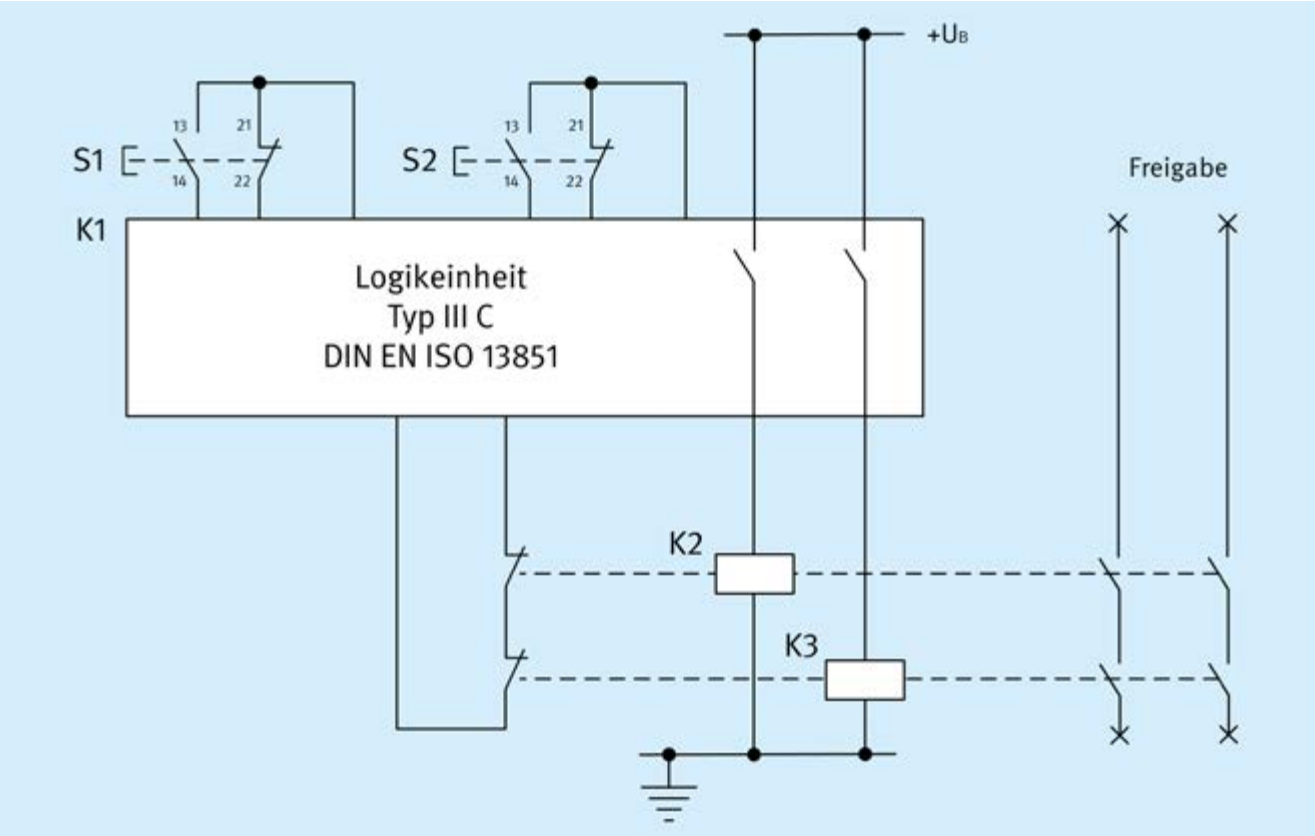


Abb. 11.56 Zweihandschaltung, Signalverarbeitung durch eine Logikeinheit mit nachgeschalteten Hilfsschützen

Sicherheitsfunktion

- SF27.1: Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung: Beim Loslassen mindestens eines der beiden Taster S1/S2 wird die Freigabe aufgehoben und solange blockiert, bis beide Taster entlastet und erneut synchron betätigt werden.

Funktionsbeschreibung

- Die Logikeinheit K1 überwacht die Betätigung der Stellteile (Taster) S1 und S2. Nur wenn beide aus dem entlasteten Zustand synchron (d. h. innerhalb einer festgelegten Zeitvorgabe von maximal 500 ms gemäß DIN EN ISO 13851) betätigt werden, ziehen die Hilfsschütze K2 und K3 an und die Freigabe erfolgt. Beim Loslassen mindestens eines der Taster S1/S2 heben K2/K3 die Freigabe auf.
- Durch K2 und K3 erfolgt eine Kontaktvervielfachung/Lastanpassung. Die eigentliche Verhinderung der gefahrbringenden Bewegung, z. B. durch Trennung der elektrischen oder hydraulischen Energie, ist anwendungsabhängig und hier nicht dargestellt.
- Störungen im Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschiedenen Kontakten (Öffner-Schließer-Kombination) in S1/S2 weitestgehend erkannt. Nach der Recommendation for Use (RfU) CNB/M/11.033 Rev 09 können mechanische Fehler der Stellteile ausgeschlossen werden, wenn diese DIN EN 60947-5-1 entsprechen.
- Fehler in S1/S2 und in K2/K3 (mit Öffnerkontakten im Rückführkreis) werden in K1 erkannt und führen zum dauerhaften Abschalten über K2 und K3. Alle Einzelfehler werden bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt.
- Eine häufige Betätigung der elektromechanischen Elemente sorgt für eine ausreichend hohe Testrate (Dynamisierung).

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in Abschnitt 8.1 beschrieben, sind vorgesehen.
- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1. Daher können nach RfU CNB/M/11.033 Rev 09 mechanische Fehler ausgeschlossen werden.
- Fehler in den Anschlussleitungen von S1 und S2 werden in der Logikeinheit erkannt. Wäre dies nicht möglich, so müssten die Bedingungen für einen Fehlerausschluss für Leitungskurzschlüsse nach DIN EN ISO 13849-2,

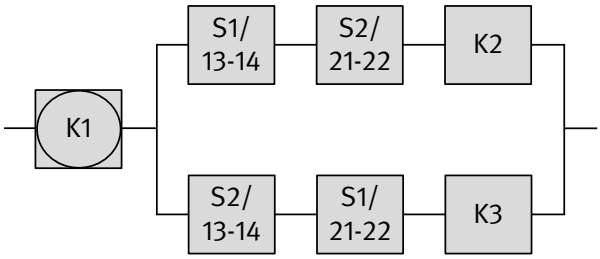


Tabelle D.4, eingehalten werden. Wegen der geringen Ströme werden Taster mit Goldauflage empfohlen.

- Zum Anbau der Taster und zu Maßnahmen zur Vermeidung von versehentlicher Betätigung und von Umgehen siehe DIN EN ISO 13851, Abschnitte 7 und 8. Der Sicherheitsabstand zum Gefährdungsbereich muss ausreichend groß sein.
- Die Logikeinheit K1 entspricht Typ III C gemäß DIN EN ISO 13851 mit Selbstüberwachung und Erkennung interner Fehler. K1 ist ein geprüftes Sicherheitsbauteil für den Einsatz in Kategorie 4 und PL e.
- Die Hilfsschütze K2 und K3 besitzen zur Rücklesung zwangsgeführte Öffnerkontakte entsprechend DIN EN 60947-5-1, Anhang L.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Bemerkung

- Das dargestellte Beispiel eignet sich für die Anwendung z. B. an mechanischen Pressen (DIN EN ISO 16092-1 und DIN EN ISO 16092-2).

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion wird von zwei Teilsystemen der Kategorie 4 ausgeführt.
- K1 wird als Teilsystem mit einer Ausfallhäufigkeit von $3{,}0 \cdot 10^{-9}$/Stunde betrachtet. Der übrige Steuerungsteil wird zu einem Teilsystem der Kategorie 4 zusammengefasst, dessen Ausfallhäufigkeit im Folgenden berechnet wird.
- Da S1 und S2 unabhängig voneinander beim Loslassen eine Abschaltung auslösen müssen, sind sie logisch in Reihe geschaltet. Dazu wurde je ein Schließerkontakt 13-14 und ein Öffnerkontakt 21-22 einem Steuerungskanal zugeordnet. Das sicherheitsgerichtete Blockdiagramm unterscheidet sich hier deutlich vom funktionalen Schaltplan. Wenn Zuverlässigkeitsdaten nur für die Taster insgesamt (Betätigungsmechanik plus Öffner- und Schließerkontakt) verfügbar sind, können die Ausfallwerte der Taster als Abschätzung zur sicheren Seite für die Ausfallwerte der Kontakte (plus Betätigungsmechanik) herangezogen werden.
- ***MTTF*$_D$:** Für S1 und S2 werden wegen des durch K1 erzeugten definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) B_{10D}-Werte von je 2 000 000 Schaltspielen angenommen. Bei 240 Arbeitstagen, 8 Arbeitsstunden und 30 Sekunden Zykluszeit ist für diese Komponenten n_{op} = 230 400 Zyklen/Jahr und pro Kontakt $MTTF_D$ = 86,8 Jahre. Da K2 und K3 ebenfalls Steuerströme schalten, gelten für K2 und K3 B_{10D}-Werte von je 20 000 000 Zyklen und daraus resultierende $MTTF_D$-Werte von 868 Jahren. Bei höheren Anforderungen (längere Arbeitszeit oder kürzere Zykluszeit) sind unter Umständen für K2/K3 höhere, durch den Hersteller abgesicherte B_{10D}-Werte erforderlich. Insgesamt ergibt sich ein $MTTF_D$-Wert pro Kanal von 41 Jahren („hoch“).
- ***DC*$_{avg}$:** *DC* = 99 % für S1 und S2 ergibt sich durch die direkte Überwachung mithilfe der Öffner-Schließer-Kombinationen in K1. *DC* = 99 % für K2 und K3 gründet sich auf dem Rücklesen der zwangsgeführten Öffnerkontakte im Rückführkreis von K1. Die hohe Betätigungsdynamik in der Anwendung führt zu einer häufigen Testung (siehe Abschnitt 8.2.14). Durch Mittelung ergibt sich damit ein DC_{avg} von 99 % („hoch“).
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).
- **PL:** Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_D$ pro Kanal (41 Jahre) und hohem DC_{avg} (99 %). Für die Kombination von S1, S2, K2 und K3 ergibt sich eine mittlere Häufigkeit gefährlicher Ausfälle von $6{,}7 \cdot 10^{-8}$/Stunde. Wird ein Wert von $3{,}0 \cdot 10^{-9}$/Stunde für K1 hinzuaddiert, so ergibt sich für SF27.1 eine mittlere Häufigkeit gefährlicher Ausfälle von $7{,}0 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Unter Umständen ist zur Komplettierung der Sicherheitsfunktion zusätzlich die Ausfallhäufigkeit nachgeordneter Leistungselemente zu addieren.
- Die Gebrauchsdauer der verschleißbehafteten Elemente S1 und S2 endet nach Ablauf von T_{10D} = 8 Jahren. Danach verliert die *PFH*-Berechnung ihre Grundlage. Ein rechtzeitiger Austausch wird empfohlen.

Weiterführende Literatur

- DIN EN ISO 13851: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte und Gestaltungsleitsätze (11/2019). DIN Media, Berlin 2019
- Vertical Recommendation for Use Sheets (RfUs) – Status on November 2023, Number CNB/M/11.033 Rev 09, S. 144, Hrsg.: European Co-Ordination of Notified Bodies Machinery Directive 2006/42/EC + Amendment, 2023. https://ec.europa.eu/docsroom/documents/57275

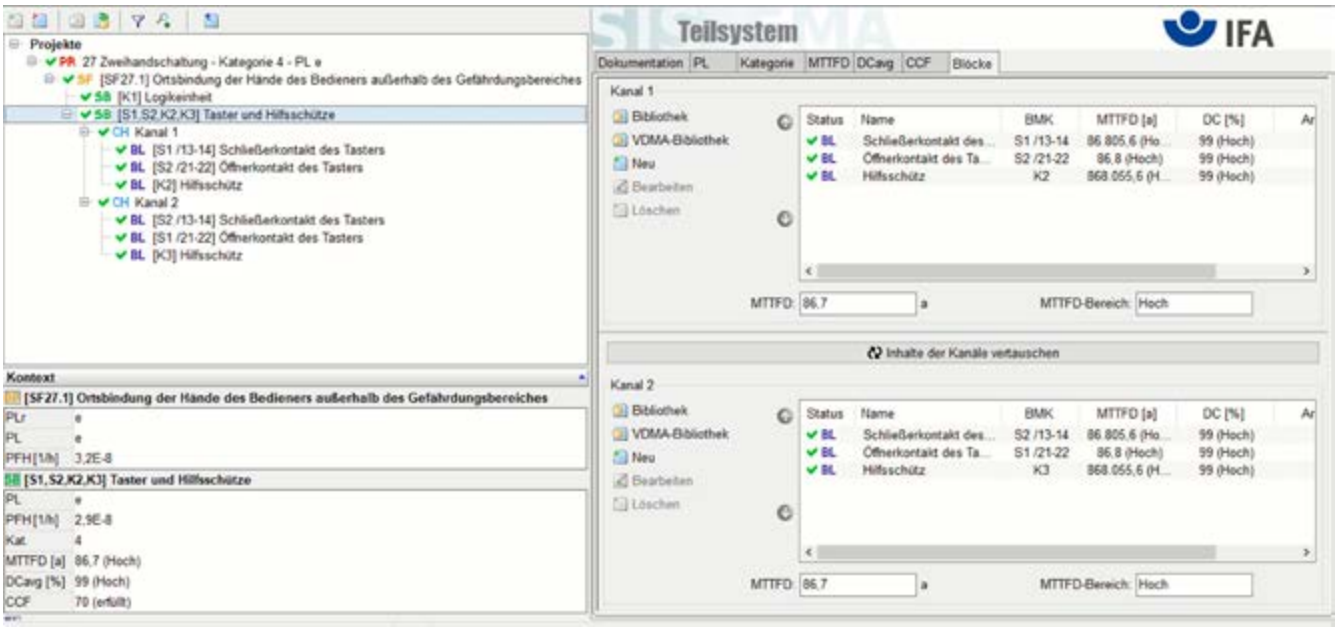


Abb. 11.57 PL-Bestimmung mithilfe von SISTEMA

11.2.28 Planschneidemaschine mit programmierbarer elektronischer Logiksteuerung – Kategorie 4 – PL e (Beispiel 28)

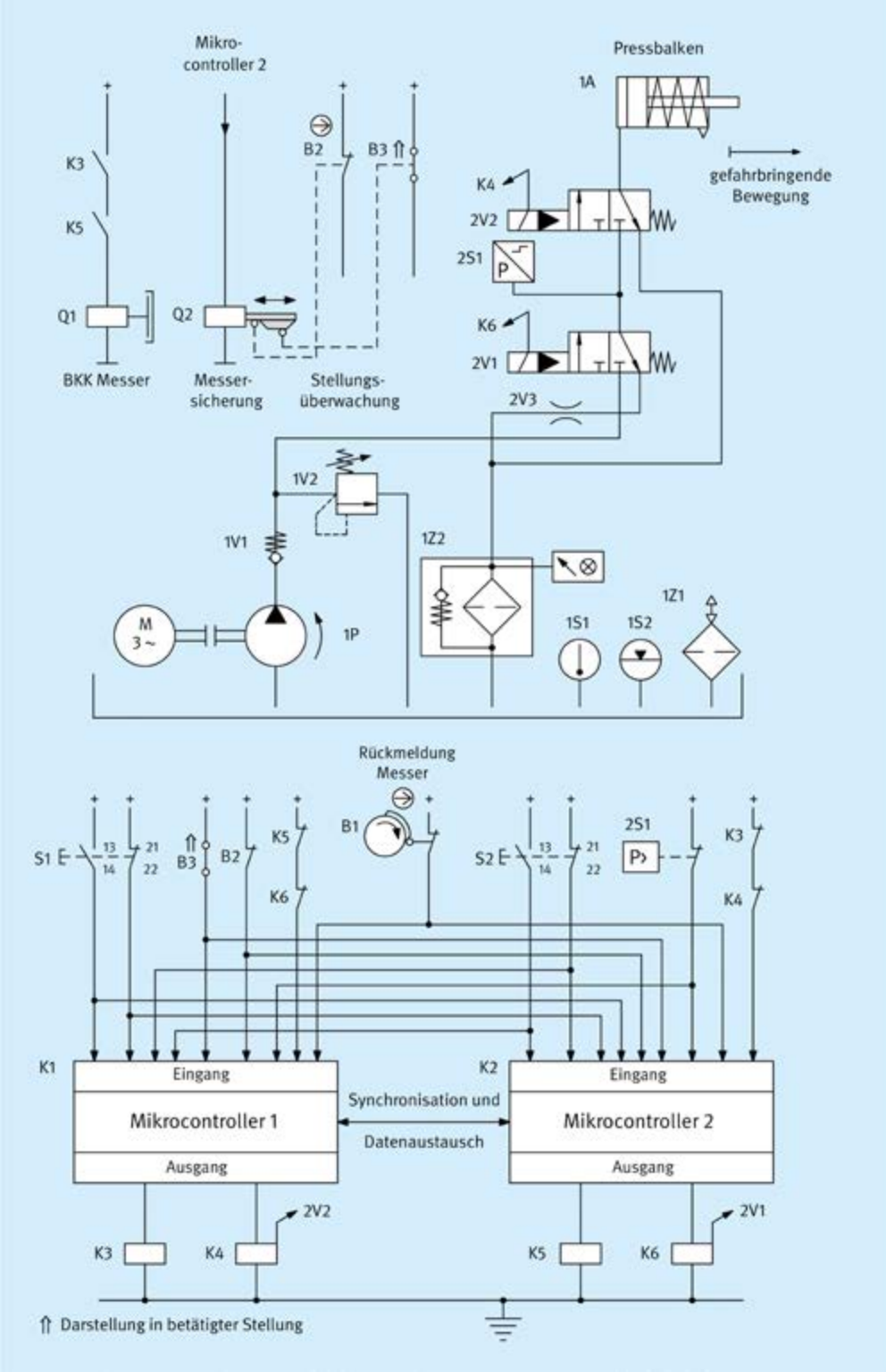


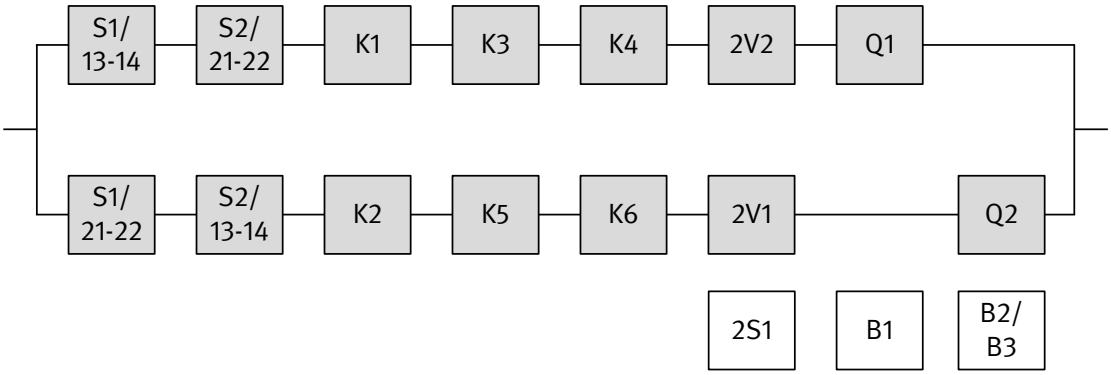
Abb. 11.58
Ansteuerung eines elektrischen Messerantriebs und eines hydraulischen Pressbalkens

Sicherheitsfunktion

- SF28.1: Ortsbindung der Hände einer einzelnen Bedienperson außerhalb des Gefährdungsbereiches während der Press- und Schneidbewegung: Beim Loslassen mindestens eines der beiden Taster S1/S2 wird die Freigabe aufgehoben und so lange blockiert, bis beide Taster entlastet und erneut synchron betätigt werden.

Funktionsbeschreibung

- Die Betätigung der Zweihandschaltung (ZHS) S1 und S2 startet die gefahrbringenden Bewegungen (Bearbeitungszyklus) des Pressbalkens (Hydraulik) 1A und des Messers (Elektromechanik). Wird während eines Zyklus auch nur ein Taster S1 oder S2 losgelassen oder erfolgt ein Signalwechsel in der Peripherie der Maschine



(z. B. Lichtgitter, im Schaltbild nicht dargestellt) nicht wie durch die Steuerung erwartet, stoppt der Zyklus und die Maschine verbleibt in diesem sicheren Zustand. Das Messer und der Pressbalken stellen wegen ihrer unmittelbaren räumlichen Nähe zueinander eine gemeinsame Gefahrstelle dar; die Gefährdung wiederholt sich zyklisch. Nicht explizit dargestellt ist der Antrieb des Messers durch einen Exzenterantrieb, dessen Energie aus einer kontinuierlich laufenden Schwungmasse entnommen wird. Der Pressbalken wird linear durch eine Hydraulik angetrieben, deren Pumpe an den Antrieb der Schwungmasse gebunden ist.

- Mit Betätigen 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 ISO 13851, 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 S1/S2 werden durch Verwendung von zwei prinzipverschiedenen Kontakten (Öffner-Schließer-Kombination) erkannt. Nach der Recommendation for Use (RfU) CNB/M/11.033 Rev 09 können mechanische Fehler der Stellteile ausgeschlossen werden, wenn diese DIN EN 60947-5-1 entsprechen.
- Fehler 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. Ein Ausfall des Ventils 2V2 oder ein Hängenbleiben im offenen Zustand wird durch eine stark verzögerte Rückzuggeschwindigkeit des Hydraulikzylinders bemerkt. Ein Ausfall des Ventils 2V1 oder ein Hängenbleiben im offenen Zustand wird unmittelbar durch die Überwachung des Signalwechsels des Druckschalters 2S1 bemerkt. Denn dann würde ein Druck signalisiert, obwohl kein Druck anstehen dürfte. Durch geeignete Auswertung des Drucksignals und der Druckabfallzeit erfolgt dies auch steuerungstechnisch. 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 (z.B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 11 beschrieben, sind vorgesehen.
- Die Taster S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1. Daher können nach RfU CNB/M/11.033 Rev 09 mechanische Fehler ausgeschlossen werden.
- 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.

- 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.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über den Pfad D oder alternativ den Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt (siehe Anhang L der Norm) werden.
- **Software:** Die Programmierung der Software (SRESW) von K1 und K2 (homogen redundante Rechnerstruktur) erfolgt entsprechend den Anforderungen der DIN EN 61508-3:2011, Abschnitt 7 für SIL 3.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** 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 Ausfallhäufigkeit 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 Zyklen/Jahr. Für S1 und S2 liegt die Herstellerangabe B_{10D} = 2 000 000 Zyklen vor. Damit ergibt sich für S1 und S2 eine $MTTF_D$ = 173 Jahre. Für die Mikrocontroller einschließlich ihrer Peripherie wird nach SN 29500-2 eine $MTTF_D$ von 878 Jahren angegeben. Für die Hilfsschütze K3 bis K6 gilt bei geringer Last B_{10D} = 20 000 000 Zyklen und damit $MTTF_D$ = 1736 Jahre. Für die BKK Q1 wird die $MTTF_D$ von 607 Jahre aus B_{10D} = 7 000 000 Zyklen 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. Diese Werte ergeben eine $MTTF_D$ des 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 (Prozessdiagnoserate sehr viel größer als die Anforderungsrate der Sicherheitsfunktion). *DC* = 90 % für K1/K2 folgt aus Selbsttests durch Software und dynamischem Kreuzvergleich von Daten mit zeitlicher Erwartungshaltung. *DC* = 99 % für K3 bis K6 ergibt sich durch Plausibilitätsprüfung über zwangsgeführte Kontakte. Für 2V1/2V2 ist der *DC* = 99 % wegen indirekter und direkter Überwachung durch elektrische Drucküberwachung bei häufigem Signalwechsel. Ein Verschleiß der Kupplung führt zu einem geänderten Schnittverhalten. Dieses Verhalten wird messtechnisch erfasst und daher für Q1 ein *DC* = 99 % angenommen. Ein Ausfall von Q2 wird infolge der zyklischen Betätigung und der Überwachungselemente B1 und B3 sofort bemerkt. Damit wird ein *DC* = 99 % begründet. Diese Werte ergeben einen DC_{avg} von 98,5 % (im Toleranzbereich von „hoch“).
- **CCF:** Ausreichende Maßnahmen gegen Fehler gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebung (25 + 10).
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für die verschleißbehafteten Taster S1 und S2 folgende Bewertung. Die Gebrauchsdauer der verschleißbehafteten Taster S1 und S2 endet nach Ablauf von T_{10D} = 17 Jahren. Danach verliert die PFH-Berechnung ihre Grundlage. Ein rechtzeitiger Austausch wird empfohlen.
- **PL:** Für die SF28.1 ergibt sich eine mittlere Häufigkeit eines gefahrbringenden Ausfalls *PFH* von $6{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Weiterführende Literatur

- DIN EN 1010-3: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 3: Schneidemaschinen (6/2010). DIN Media, Berlin 2010
- DIN EN ISO 13851: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte und Gestaltungsleitsätze (11/2019). DIN Media, Berlin 2019
- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (3/2018). DIN Media, Berlin 2018
- Vertical Recommendation for Use Sheets (RfUs) – Status on November 2023, Number CNB/M/11.033 Rev 09, S. 144, Hrsg.: European Co-Ordination of Notified Bodies Machinery Directive 2006/42/EC + Amendment, 2023. https://ec.europa.eu/docsroom/documents/57275

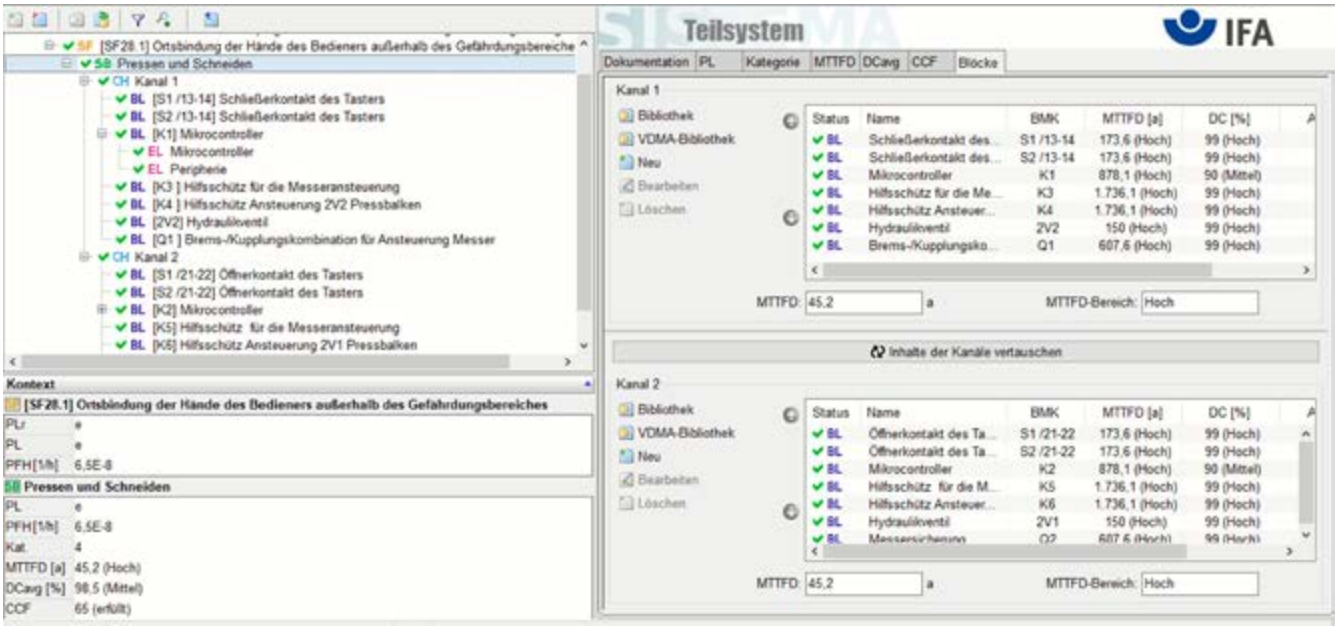


Abb. 11.59 PL-Bestimmung mithilfe von SISTEMA

11.2.29 Hydraulische Ventilsteuerung (Teilsystem) – Kategorie 1 – PL c (Beispiel 29)

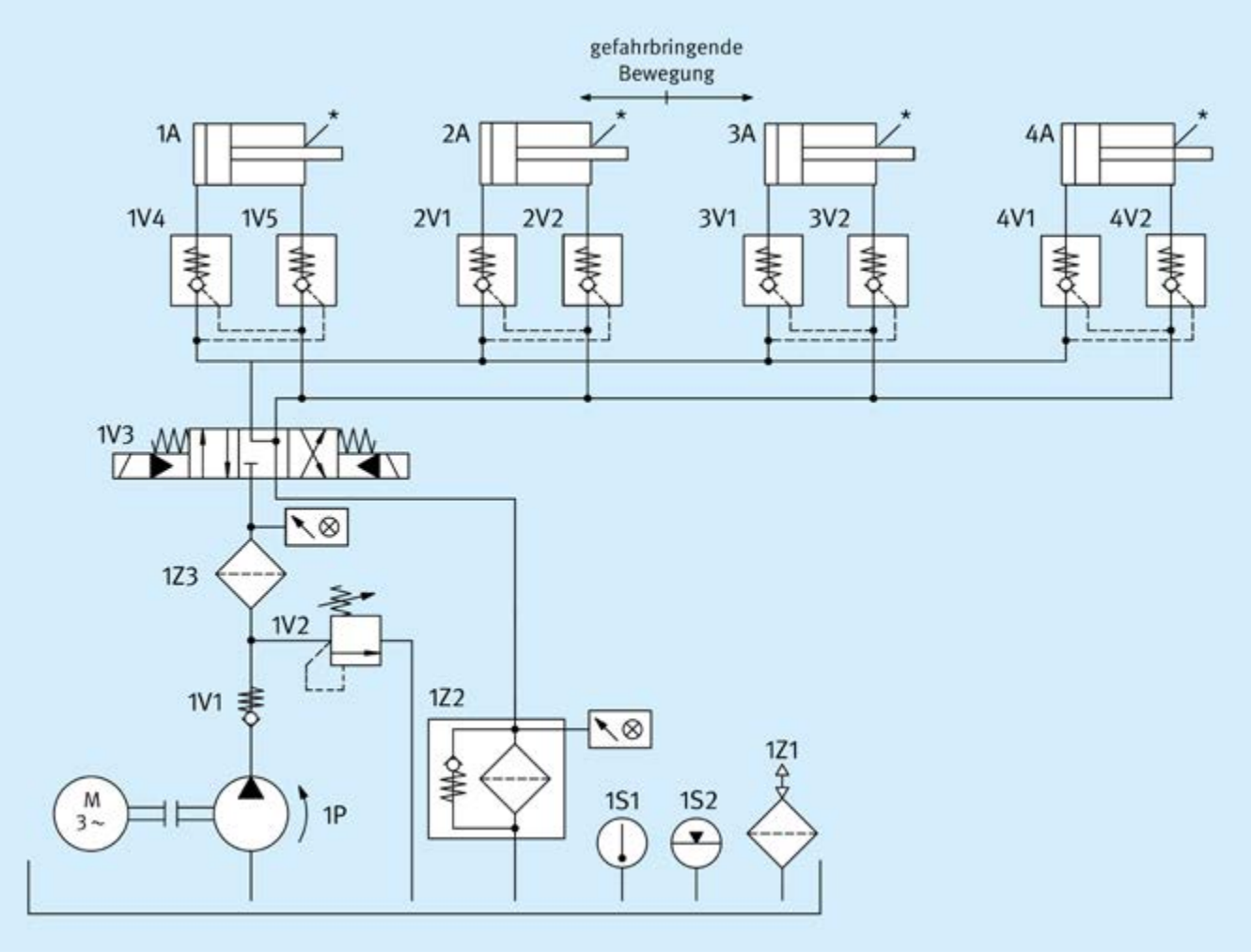


Abb. 11.60 Hydraulische Ventile zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

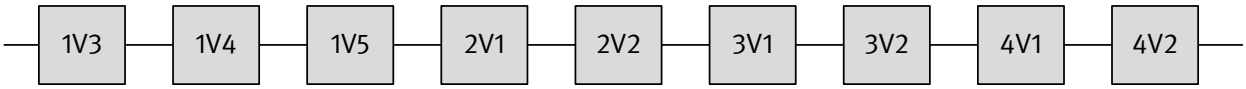
- SF29.1: Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des unerwarteten Anlaufs aus der Ruhelage, realisiert durch die Sicherheits-Teilfunktion SSC.
- In diesem Beispiel ist nur der hydraulische Steuerungsteil als Teilsystem dargestellt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z. B. Schutzeinrichtungen und elektrische Logik) als Teilsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch vier Aktoren 1A bis 4A ausgeführt. Ein Stillsetzen der Bewegungen erfolgt über das sicherheitstechnisch bewährte Wegeventil 1V3 in Verbindung mit den sicherheitstechnisch bewährten entsperrbaren Rückschlagventilen.
- Der Ausfall des Wegeventils oder eines der entsperrbaren Rückschlagventile kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit der Ventile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V3 handelt es sich um ein Wegeventil mit ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- Bei den Ventilen 1V4, 1V5, 2V1, 2V2, 3V1, 3V2, 4V1 und 4V2 handelt es sich um entsperrbare Rückschlagventile.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.



- Die Bestätigung für das Wegeventil und die entsperrbaren Rückschlagventile als sicherheitstechnisch bewährtes Bauteil erfolgt durch den Hersteller/Anwender.
- Als gezielte Maßnahmen zur Erhöhung der Zuverlässigkeit der Ventile sind ein Druckfilter 1Z3 vor dem Wegeventil und geeignete Maßnahmen gegen Schmutzeinzug durch die Kolbenstange am Zylinder (z. B. wirksamer Abstreifer an den Kolbenstangen, siehe * in Abbildung 8.7.2) vorgesehen.
- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit wurden in diesem Beispiel nicht bewertet. Die Bewertung erfolgt, wenn das hydraulische Teilsystem in die vollständige Sicherheitsfunktion integriert wird.
- **Software:** Dieses Beispiel enthält keine zu bewertende Software.

Berechnung der Ausfallhäufigkeit

- **Kategorie:** Die Sicherheitsfunktion besteht aus einem Teilsystem der Kategorie 1.
- ***MTTF*$_D$:** Für das Wegeventil und die entsperrbaren Rückschlagventile wird jeweils eine *MTTF*$_D$ von 600 Jahren angenommen, da die Schaltspielzahl der Ventile für diese Anwendung zwischen 250 000 und 500 000 pro Jahr (n_{op}) liegt.
- ***DC*$_{avg}$** und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) sind in Kategorie 1 nicht relevant.
- **PL**: Der hydraulische Teil der Steuerung entspricht Kategorie 1 mit hoher *MTTF*$_D$ (66,7 Jahre). Für SF29.1 ergibt sich eine mittlere Häufigkeit gefahrbringender Ausfälle von $1{,}7 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (6/2022). DIN Media, Berlin 2022

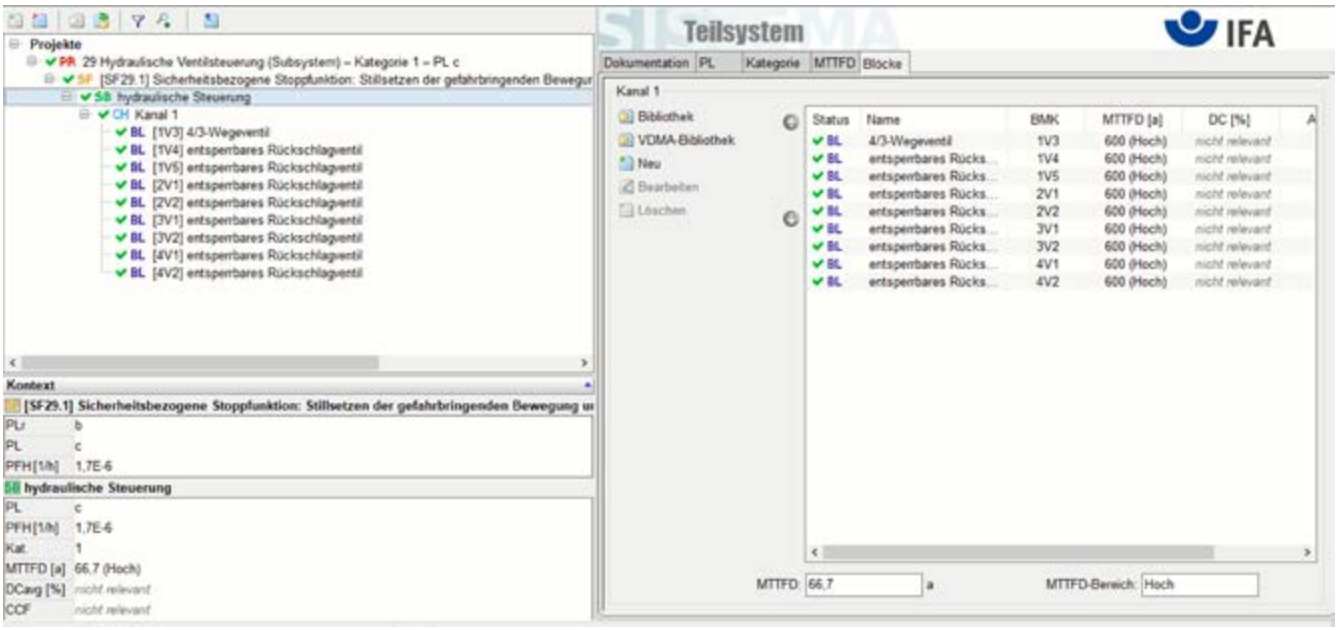


Abb. 11.61 PL-Bestimmung mithilfe von SISTEMA

11.2.30 Manuelle Rückstellung an einer Roboterzelle einer Fertigungslinie – Kategorie 2 – PL d (Beispiel 30)

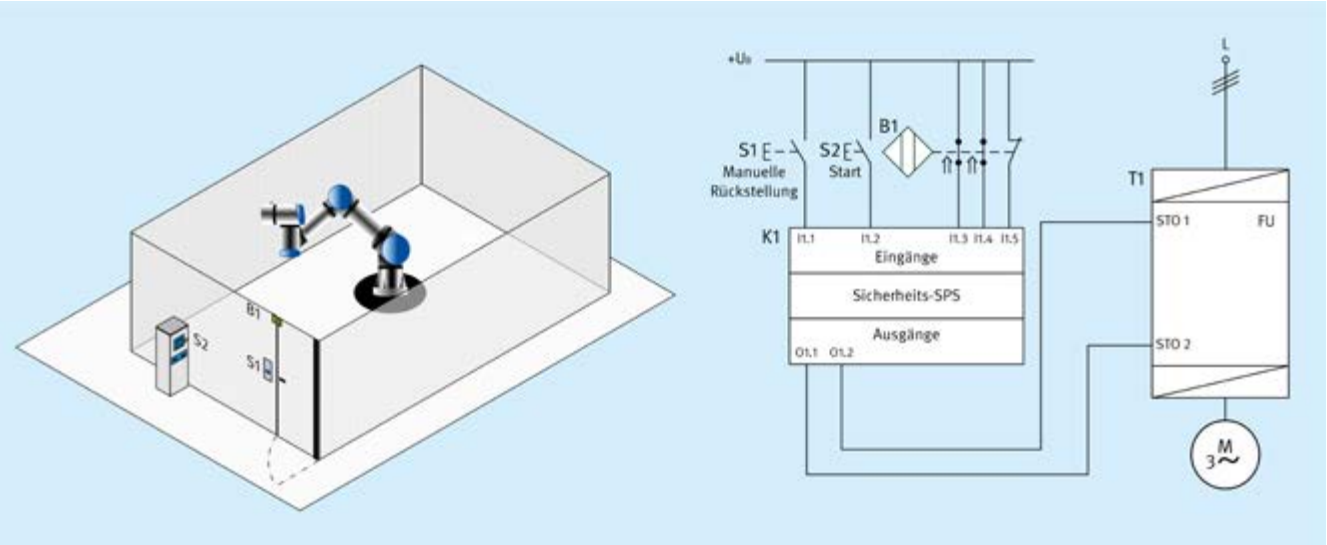


Abb. 11.62 Prinzipschaltbild zur manuellen Rückstellfunktion an einer Roboterzelle einer Fertigungslinie

Sicherheitsfunktionen

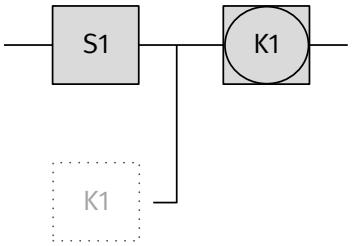
- SF30.1: Manuelle Rückstellfunktion: Das Betätigen des Befehlsgebers zur manuellen Rückstellung S1 setzt die sicherheitsbezogene Stoppfunktion, eingeleitet durch das Öffnen der beweglichen trennenden Schutzeinrichtung B1, zurück und ermöglich ein erneutes In-Gang-Setzen der Fertigungslinie
- Zugehörige Sicherheitsfunktion: Verhindern des unerwarteten Anlaufs der Fertigungslinie bei geöffneter Schutzeinrichtung B1 sowie bei fehlender manueller Rückstellung. Diese zugehörige Sicherheitsfunktion wird hier vollständigkeitshalber aufgeführt, jedoch nicht weiter betrachtet.

Funktionsbeschreibung

- Nach einem ausgelösten Stopp des Frequenzumrichters T1 durch Betätigung der Verriegelungseinrichtung B1 an der beweglichen trennenden Schutzeinrichtung (Öffnen der Tür zur Roboterzelle), verlässt die Bedienperson den hintertretbaren Roboterarbeitsbereich und schließt die Zutrittstür. Nun muss die manuelle Rückstellfunktion mittels Rückstelleinrichtung (S1) erfolgen, bevor das erneute In-Gang-Setzen der Produktion über einen separaten Start-Taster (S2) möglich ist.
- Zur Vereinfachung wird in diesem Beispiel zur manuellen Rückstellfunktion nur eine Zutrittstür der Roboterzelle dargestellt. Die Rückstelleinrichtung S1 befindet sich an einer Stelle außerhalb des Gefährdungsbereichs, mit Einsicht auf die Gefahrenstellen der Roboterzelle.

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 11 beschrieben, sind vorgesehen.
- Fehler in den Anschlussleitungen von S1, S2 und K1 dürfen sich nicht gefahrbringend 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.
- Die elektromechanische Rückstelleinrichtung S1 besteht aus einem Schließerkontakt. Der Taster ist nach DIN EN IEC 60947-5-1 gebaut und für industrielle Umgebungen geeignet. Der normativ geforderte überwachte Signalwechsel schließt das Drücken und Loslassen des Tasters ein. Eine gültige Betätigungssequenz ist bei Einhaltung der zeitlichen Begrenzung (mindestens 0,2 Sekunden bis maximal 3 Sekunden) gegeben.
- Bei der Sicherheits-SPS K1 handelt es sich um ein Sicherheitsbauteil mit PFH = $2{,}2 \cdot 10^{-8}$/Stunde, dass die Anforderungen der Kategorie 3 erfüllt und für den Einsatz in Sicherheitsfunktionen bis PL e geeignet ist.
- Das Kategorie 2 Teilsystem besteht aus der elektromechanischen Rückstelleinrichtung S1 im Funktionskanal und einem Testkanal, der in der Sicherheits-SPS K1 realisiert ist. Die Rückstelleinrichtung wird dazu in der Sicherheits-SPS eingelesen und auf einen Flankenwechsel (steigende gefolgt von einer fallenden Flanke innerhalb des vorgegebenen Zeitfensters) überwacht. Gemäß den Mindestanforderungen der Kategorie 2 können relevante äußere Einflüsse, wie mechanische



Schwingungen, elektromagnetische Störungen (EMI), Unterbrechungen oder Störungen der Energieversorgung, keinen negativen Einfluss auf das Teilsystem ausüben. Das Teilsystem ist für den Einsatz in der vorgesehenen Umgebung geeignet.

- **EMI:** Die Anforderungen an die elektromagnetische Störfestigkeit kann in diesem Beispiel über Pfad D oder alternativ Pfad C und die Umsetzung von Maßnahmen auf Systemebene erfüllt werden (siehe Anhang L der Norm).
- **Software:** Die Programmierung der sicherheitsrelevanten Applikations-Software (SRASW) von K1 erfolgt entsprechend Fall 3 mit Maßnahmen nach Tabelle N.2 (bei LVL) bzw. Tabelle N.3 (bei FVL) der DIN EN ISO 13849-1 und den Hinweisen in Kapitel 9.

Bemerkungen

- Die Rückstellung ist als manuelle, beabsichtige und eigenständige Handlung ausgeführt. Sie wird auch als Quittierung der Sicherheitsfunktion bezeichnet. Eine Detaillierte Beschreibung der Funktion ist in Abschnitt D.2.5.7 dieses Reports zu finden.
- Die manuelle Rückstellfunktion ist in der Norm im Abschnitt 5.2.2.3 als mögliche Sicherheitsfunktion definiert. Es gibt darüber hinaus einige Produktnormen, die auch auf die Sicherheitsfunktion der manuellen Rückstellfunktion eingehen. Der erforderliche PL_r für diese Sicherheitsfunktion kann von der zugehörigen Sicherheitsfunktion abweichen.
- Die manuelle Rückstellfunktion bestätigt, dass sich in dem hintertretbaren Bereich (Roboterzelle) keine Person aufhält. Sollte vom Betätigungsstandort der manuellen Rückstellfunktion aus der Gefährdungsbereich nicht vollständig einsehbar sein, muss ein weiterer Standort definiert werden oder eine andere vergleichbare technische Lösung angewendet werden, um die Einsehbarkeit zu gewährleisten.
- Das Betätigen der Rückstelleinrichtung aus dem Gefahrenbereich der Roboterzelle ist durch die konstruktive Gestaltung unterbunden.
- Eine manuelle Rückstellfunktion kann allein keine ausreichende Risikominderung an einer Maschine realisieren.
- In einzelnen Branchen ist ggf. eine Anlaufwarnung vor dem Start der Maschine oder Anlage vorgesehen.

Berechnung der Ausfallhäufigkeit

- **Kategorie**: Die Sicherheitsfunktion wird durch zwei Teilsysteme realisiert. Das erste Teilsystem ist als Kategorie 2 ausgeführt und besteht im Funktionskanal aus der Rückstelleinrichtung S1. Im Testkanal wird die Sicherheits-SPS nur gestrichelt dargestellt, weil sie als gekapseltes Teilsystem bereits in der Sicherheitsfunktion aufgeführt ist. Dies stellt eine Ausnahme dar und weicht von der vorgesehenen Architektur der Kategorie 2 ab. In SISTEMA wird dies als gelbe Meldung angezeigt und muss bestätigt werden. Im zweiten Teilsystem befindet sich nur die Sicherheits-SPS als gekapseltes Kategorie 3 Teilsystem.
- ***$MTTF_D$*:** Die Rückstelleinrichtung ist mit einem Schließerkontakt S1 aufgeführt, der einen B_{10D}-Wert von 100 000 Zyklen hat. Mit einer Betätigungsfrequenz von 60 Minuten an 240 Tagen im Zweischichtbetrieb (16 Stunden) ergibt dies n_{op} = 3 840 Zyklen/Jahr und eine $MTTF_D$ = 260 Jahre, die auf 100 Jahre gekappt wird. Im Testkanal wird mit dem Kehrwert der *PFH* der Sicherheits-SPS K1 eine $MTTF_D$ = 5 188 Jahre berechnet.
- ***DC_{avg}*:** Die implementierte Überwachungsmaßnahme in K1 besteht aus der Flankenauswertung mit vorgegebenem Zeitfenster. Dadurch werden die meisten auftretenden Fehler der Rückstelleinrichtung erkannt. Ein Nicht-Öffnen des Schließerkontaktes wird beispielweise durch die zeitliche Überwachung auf der „fallenden Flanke“ erkannt. Ein Nicht-Schließen des Schließers (z. B. bei mechanischem Abbruch) würde ebenfalls keinen sicherheitsrelevanten Fehler darstellen, da in diesem Fall die Maschine nicht wieder gestartet werden kann (Fehlererkennung im Prozess da die Maschine nicht anläuft). Eine Diskrepanz beim zeitlichen Abstand der Flanken, Störimpulse oder Verfälschungen der Eingangssignalsignale werden aufgedeckt. Diese Maßnahmen bewirken eine *DC* von 99 %. Aufgrund der gewählten Kategorie 2 wird rechnerisch die *DC* auf 90 % begrenzt.
- **CCF:** Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10).

- **PL**: Die PFH der Sicherheitsfunktion setzt sich aus zwei Teilsystemen zusammen. Das erste Teilsystem wird als Kategorie 2 aus S1 mit 260 Jahren $MTTF_D$ im Funktionskanal und K1 mit 5188 Jahren $MTTF_D$ im Testkanal gebildet. Durch die *DC* von 90 % ergibt sich dafür eine PFH von $2{,}3 \cdot 10^{-7}$/Stunde. Nach Hinzurechnen der PFH von $2{,}2 \cdot 10^{-8}$/Stunde für das gekapselte Teilsystem K1 beträgt die *PFH* der Sicherheitsfunktion „Manuelle Rückstellung“ insgesamt $2{,}5 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DGUV Information „Manuelle Rückstelleinrichtung der Rückstellfunktion nach DIN EN ISO 13849-1“, Ausgabe 02/2015. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015. https://www.dguv.de/medien/fb-holzundmetall/publikationen-dokumente/infoblaetter/infobl_deutsch/067_rueckstellfunktion.pdf

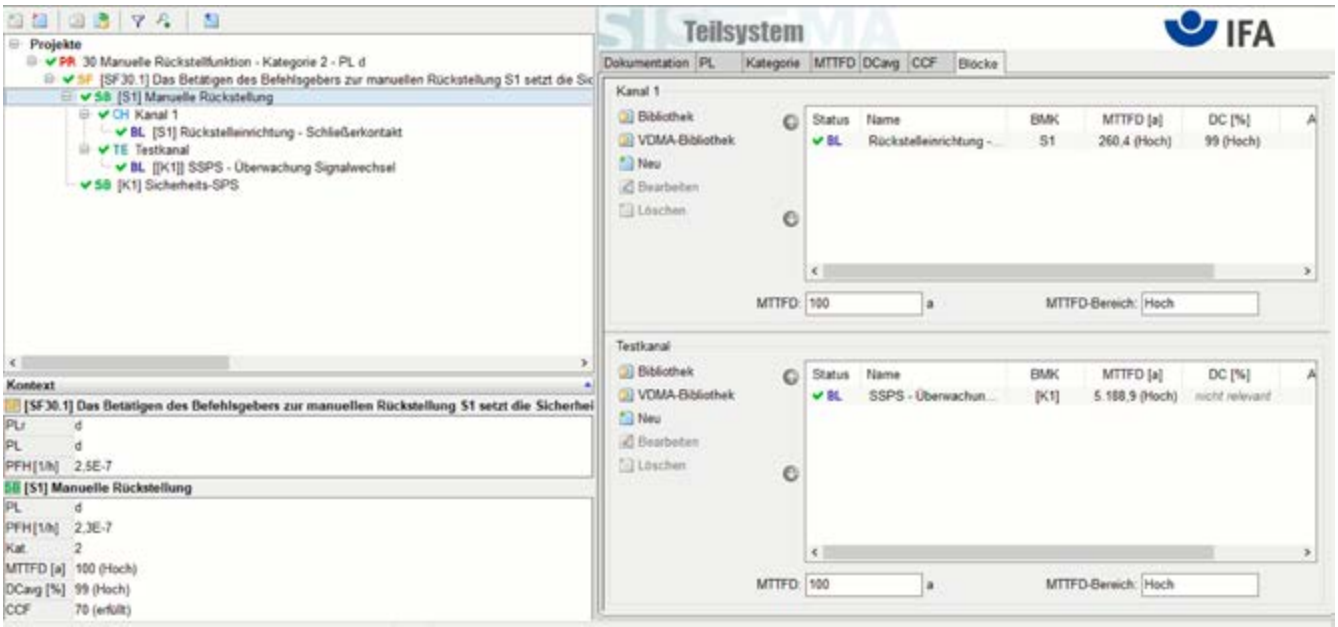


Abb. 11.63 PL-Bestimmung mithilfe von SISTEMA

12 Literatur

[1] Richtlinie 98/37/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen. ABl. EG (1998) Nr. L 207, S. 1–46; geänd. Richtlinie 98/79/ EG, ABl. EG (1998) Nr. L 331, S. 1–37. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042

[2] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17.Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). ABl. EU (2006) Nr. L 157, S. 24–86. http://eur-lex.europa.eu/

[3] Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates. ABl. EG (2023) L 165. https://eur-lex.europa.eu/search.html?scope=EURLEX&text=2023%2F1230&lang=en&type=quick&qid=1706200078838

[4] Leitfaden für die Anwendung der Maschinenrichtlinie 2006/42/EG, Auflage 2.2 – Oktober 2019. Hrsg.: Europäische Kommission, Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU. https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsschutz/leitfaden-fuer-anwendung-maschinenrichtlinie-2006-42-eg.html

[5] DIN EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (3/2011). DIN Media, Berlin 2011

[6] DIN ISO/TR 14121-2: Sicherheit von Maschinen – Risikobeurteilung – Teil 2: Praktische Anleitung und Verfahrensbeispiele (2/2013). DIN Media, Berlin 2013

[7] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (12/2023). DIN Media, Berlin 2023

[8] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (2/2013). DIN Media, Berlin 2013

[9] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1 bis Teil 7 (2/2011). DIN Media, Berlin 2011

[10] DIN EN IEC 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (2/2023). DIN Media, Berlin 2023

[11] Vierte Ausgabe der DIN EN ISO 13849-1, Die wesentlichen Neuerungen aus 2023 im Überblick. Hrsg.: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin 2023. https://publikationen.dguv.de Webcode: p022401

[12] *Apfeld R.; Zilligen H.; Köhler B.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 4/2018. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2018. https://publikationen.dguv.de Webcode: p012737

[13] *Huelke, M.; Becker, N.; Eggeling, M.:* Sicherheitsbezogene Anwendungssoftware von Maschinen – Die Matrixmethode des IFA. IFA Report 2/2016. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2016. https://publikationen.dguv.de Webcode: p012452

[14] *Bömer, T.; Büllesbach, K.-H.; Hauke, M.; Otto, S.; Werner, C.*: Praxisgerechte Umsetzung der Anforderungen für sicherheitsbezogenen Embedded-Software nach DIN EN ISO 13849-1. IFA Report 1/2020. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2020. https://publikationen.dguv.de Webcode: p021463

[15] Software-Assistent SISTEMA: Bewertung von sicherheitsbezogenen Maschinensteuerungen nach DIN EN ISO 13849. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin. https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-sistema

[16] SISTEMA-Kochbücher. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin. https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-sistema/sistema-kochbuecher

[17] *Schaefer, M.; Hauke, M.*: Performance Level Calculator – PLC. 5. Aufl. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI), Frankfurt a. M.; Verband Deutscher Maschinen- und Anlagenbau (VDMA), Frankfurt a. M., 2015. https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/performance-level-calculator

[18] Software-Assistent SOFTEMA: Projektierung und Dokumentation sicherheitsbezogener Anwendersoftware an Maschinen (SRASW). Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin. https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-softema

[19] SOFTEMA-Kochbücher. Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2022. https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-softema/softema-kochbuecher

[20] Übersicht über die Prüfgrundsätze des DGUV Test. Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin. https://www.dguv.de/dguv-test/prod-pruef-zert/pruefgrundsaetze-erfahrung/pruefgrundsaetze

[21] SISTEMA-Kochbuch 6: Definition von Sicherheitsfunktionen – Was ist wichtig? Version 1.1 (DE). Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2015. https://www.dguv.de/medien/ifa/de/pra/softwa/sistema/kochbuch/sistema_kochbuch_6_de.pdf

[22] Summary list of titles and references of harmonised standards under Directive 2006/42/EC on Machinery. Hrsg.: European Commission. https://ec.europa.eu/docsroom/documents/61614

[23] IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2. Aufl. 2003. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin. Erich Schmidt, Berlin 2003 – Losebl.-Ausg. www.ifa-handbuchdigital.de

[24] DIN EN 61800-5-2: Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (11/2017). DIN Media, Berlin 2017

[25] VDMA Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme (8/2016). DIN Media, Berlin 2016

[26] *Apfeld, R.; Schaefer, M.*: Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachmesse und Kongress SPS/IPC DRIVES, 23.–25. November 2010, Nürnberg – Vortrag.

[27] DIN EN 60204-1; VDE 0113-1:2019-06: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (6/2019). DIN Media, Berlin 2019

[28] DIN EN ISO 13850:2016-05: Sicherheit von Maschinen – Not-Halt-Funktion – Gestaltungsleitsätze (5/2016). DIN Media, Berlin 2016

[29] DIN EN 1010-3: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 3: Schneidemaschinen (6/2010). DIN Media, Berlin 2010

[30] Das SISTEMA-Kochbuch 4: „Wenn die vorgesehenen Architekturen nicht passen“ Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2012. https://www.dguv.de/medien/ifa/de/pra/softwa/sistema/kochbuch/sistema_kochbuch_4_v2_de.pdf

[31] *Apfeld, R.; Huelke, M.; Lüken, K.; Schaefer, M.* et al.: Manipulation von Schutzeinrichtungen an Maschinen. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006. https://publikationen.dguv.de Webcode: p010131 www.stopp-manipulation.org

[32] DGUV Information 209-068/069 (bisher: BGI/GUV-I 5048-1/2): Ergonomische Maschinengestaltung, Checkliste, Auswertungsbogen und Informationen (02.2018). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Sankt Augustin 2018. https://publikationen.dguv.de Webcode: p209068

[33] DGUV Information 215-450, Softwareergonomie April 2021, Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin April 2021. www.dguv.de/publikationen, Webcode p215450

[34] VDI/VDE 3850: Gebrauchstaugliche Gestaltung von Benutzungsschnittstellen für technische Anlagen. Blatt 1: Konzepte, Prinzipien und grundsätzliche Empfehlungen (04.14). Blatt 2: Interaktionsgeräte für Bildschirme (01.17). Blatt 3: Merkmale, Gestaltung und Einsatzmöglichkeiten von Benutzungsschnittstellen mit Touchscreens (11.15). DIN Media, Berlin 2014/2015/2017.

[35] DGUV Test Information 06: Kann mit einer Standard-SPS PL c erreicht werden? Stand: 06/2022. www.dguv.de/publikationen/, Webcode p022178

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

[37] SISTEMA-Kochbuch 1: „Vom Schaltbild zum Performance Level – Quantifizierung von Sicherheitsfunktionen mit SISTEMA“ Version 2.0 (DE) Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2020. https://publikationen.dguv.de Webcode: p012452

[38] DIN EN ISO 14119: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (3/2014). DIN Media, Berlin 2014

[39] Vertical Recommendation for Use Sheets (RfUs) – Status on November 2023, Number CNB/M/11.050/R/E Rev 05, S. 151. Hrsg.: European Co-Ordination of Notified Bodies Machinery Directive 2006/42/EC + Amendment, 2023. https://ec.europa.eu/docsroom/documents/57275

[40] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (2/2011). DIN Media, Berlin 2011

[41] Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten (GS-ET-26). Hrsg.: Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2014. https://www.dguv.de/dguv-test/aktuelles/details-aktuelles_81926.jsp

[42] DIN EN IEC 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile (2/2022). DIN Media, Berlin 2022

[43] *Reinert, D.; Schaefe*

[44] *r, M.:* Sichere Bussysteme für die Automation. Hüthig, Heidelberg 2001

[45] SN 29500: Ausfallraten Bauelemente, Erwartungswerte. Hrsg.: Siemens AG, CT TIM Regulation & Standardization. München 2004–2016

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

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

[48] DIN EN 61508-3: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (2/2011). DIN Media, Berlin 2011

[49] *Friedrich, J.; Kuhrmann, M.; Sihling, M.; Hammerschall, U.*: Das V-Modell XT für Projektleiter und QS-Verantwortliche kompakt und übersichtlich. Springer, Berlin 2009

[50] DIN EN 61131-3: Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (6/2014). DIN Media, Berlin 2014

[51] MISRA C:2023. Guidelines for the use of the C language in critical systems. www.misra.org.uk/product/misra-c2023/

[52] DIN EN 61508-7: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen (2/2011). DIN Media, Berlin 2011

[53] Leitfaden Software-Ergonomie; Gestaltung von Bedienoberflächen. VDMA Verlag, Frankfurt a. M. 2004

[54] DIN EN ISO 9241-11: Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte (11/2018). DIN Media, Berlin 2017

[55] DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Gemeinsame Anforderungen (6/2011). DIN Media, Berlin 2011

[56] DIN EN ISO 13851: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte und Gestaltungsleitsätze (11/2019). DIN Media, Berlin 2019

[57] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (3/2018). DIN Media, Berlin 2018

[58] DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (2/2011). DIN Media, Berlin 2011

[59] DIN EN 61131-6: Speicherprogrammierbare Steuerungen – Teil 6: Funktionale Sicherheit (10/2013). DIN Media, Berlin 2013

[60] DIN EN ISO 9001: Qualitätsmanagementsysteme – Anforderungen (11.15). DIN Media, Berlin 2015

[61] *Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.* et al.: Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849. IFA Report 2/2017. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2017. https://publikationen.dguv.de Webcode: p012455

[62] DIN EN ISO 4413: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile (4/2011). DIN Media, Berlin 2011

[63] DIN EN ISO 4414: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile (4/2011). DIN Media, Berlin 2011

[64] DIN EN 1037: Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf (11/2008). DIN Media, Berlin 2008

[65] ISO 1219-1: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 1: Graphische Symbole für konventionelle und datentechnische Anwendungen (6/2012). DIN Media, Berlin 2012

[66] ISO 1219-2: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 2: Schaltpläne (9/2012). DIN Media, Berlin 2012

[67] ISO 8573-1: Druckluft – Teil 1: Verunreinigungen und Reinheitsklassen (4/2010). DIN Media, Berlin 2010

Anhang A

Beispiele zur Risikobeurteilung

Änderung gegenüber dem IFA Report 2/2017

- Definition der Sicherheitsfunktionen erweitert
- Einschätzung der Häufigkeit und Expositionsdauer detaillierter dargestellt
- Berücksichtigung Unfallgeschehen ergänzt

Beispiel 1

Schließkantensicherung

In Abbildung A.1 ist die Risikobeurteilung für die Sicherheitsfunktion

- SF1 Unterbrechung der Schließbewegung und Reversieren bei Erkennung eines Hindernisses

einer Schließkantensicherung[1] dargestellt. Mit der Bewegung kraftbetätigter Fenster-, Tür- und Torflügel (siehe Abbildung A.1) ist in der Regel die Bildung von Quetsch- und Scherstellen verbunden. Diese Gefahrstellen bestehen im Allgemeinen nur dann, wenn sich der Flügel seinen Endstellungen nähert. Verletzungen von Personen an derartigen Gefahrstellen lassen sich z. B. durch Schließkantensicherungen vermeiden. Schließkantensicherungen, z. B. Schaltleisten, werden auf die Schließkanten der Flügel gesetzt. Bei Erkennung eines Hindernisses wird die Schließbewegung unterbrochen und eine rückläufige Bewegung eingeleitet.

Quetsch- und Scherstellen können an kraftbetätigten Fenster-, Tür- und Torflügeln Ursache für schwere, unter Umständen tödliche Verletzungen sein, sodass als Schadensausmaß S2 angenommen werden muss. Personen halten sich im Bereich der zeitlich begrenzt auftretenden Quetsch- und Scherstellen nur selten (Häufigkeit geringer als einmal alle 15 Minuten) und auch nur für kurze Zeit (Expositionsdauer insgesamt geringer als 1/20 der gesamten Betriebsdauer) auf (F1). Normalerweise erkennen Personen die Gefährdung und haben die Möglichkeit und den Platz, sich aus dem vom langsam bewegten Flügel gebildeten Gefahrenbereich zu entfernen (P1); damit ergibt sich ein erforderlicher Performance Level PL_r = c. Dieses Ergebnis wird durch die Produktnorm DIN EN 12453:2022 bestätigt.

Das Normungsgremium hatte offensichtlich keine Veranlassung, aufgrund des Unfallgeschehens hiervon abzuweichen. Wie man diese Sicherheitsfunktion realisieren kann, ist im Beispiel 13 in [A1] beschrieben.

Bei Schnelllauftoren ist es kaum möglich, sich rechtzeitig aus dem Gefahrenbereich zu entfernen. Durch die Einschätzung P2 anstatt P1 ergibt sich daher für diese Produkte ein erforderlicher Performance Level PL_r = d.

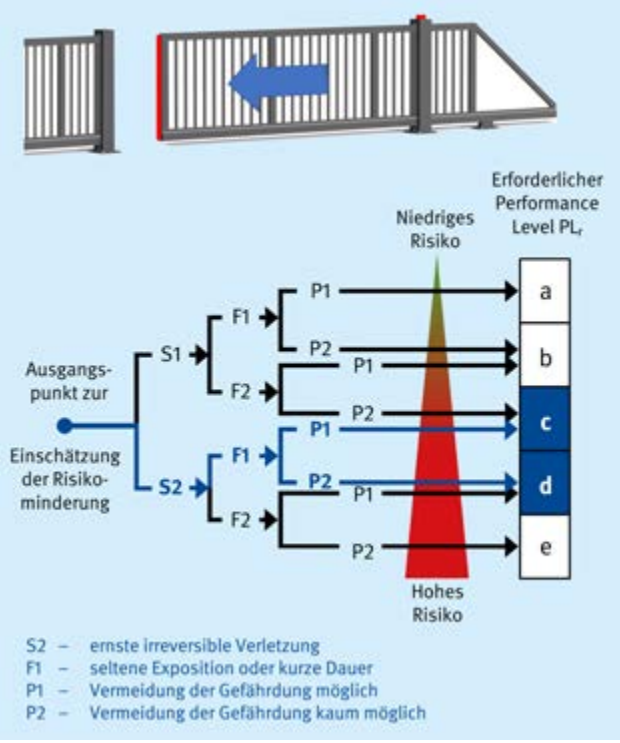


Abb. A.1 Risikobeurteilung für die Schließkantensicherung an kraftbetätigten Fenstern, Türen und Toren

[1] Da die eingesetzten Schaltleisten Sicherheitsbauteile nach der Maschinenrichtlinie sind, werden auch Schließkantensicherungen nach dieser Richtlinie bewertet.

Beispiel 2

Fahrerloses Transportfahrzeug

An fahrerlosen Transportfahrzeugen wird für den Auffahrschutz die Sicherheitsfunktion

- SF1 Stillsetzen des Transportfahrzeugs bei Annäherung an ein Hindernis

eingesetzt. Da sich ein fahrerloses Transportfahrzeug unter Umständen mit tonnenschwerer Last bewegt, ist eine schwere irreversible Verletzung bei einer Kollision mit dem Fahrzeug, wenn sie bei voller Geschwindigkeit stattfindet, wahrscheinlich (S2). Die Fahrwege des Fahrzeugs sind für Personen frei zugänglich; deshalb muss mit einem relativ häufigen Aufenthalt von Personen im Gefahrenbereich (Häufigkeit höher als einmal alle 15 Minuten) gerechnet werden (F2). Da das Fahrzeug mit recht niedriger Geschwindigkeit fährt (in der Regel 3 bis 5 km/h), hat eine Person beim Herannahen eines solchen Fahrzeugs meist die Möglichkeit, die Gefährdung wahrzunehmen und eine Kollision zu vermeiden. Zudem fahren die Fahrzeuge in der Regel in größeren Hallen oder Bereichen, wo genügend Platz zum Ausweichen vorhanden ist (P1). Für SF1 ergibt sich damit ein erforderlicher Performance Level PL_r = d (Abbildung A.2). Dieses Ergebnis wird durch die Produktnorm DIN EN ISO 3691-4:2020 bestätigt. Das Normungsgremium hatte offensichtlich keine Veranlassung, aufgrund des Unfallgeschehens hiervon abzuweichen.

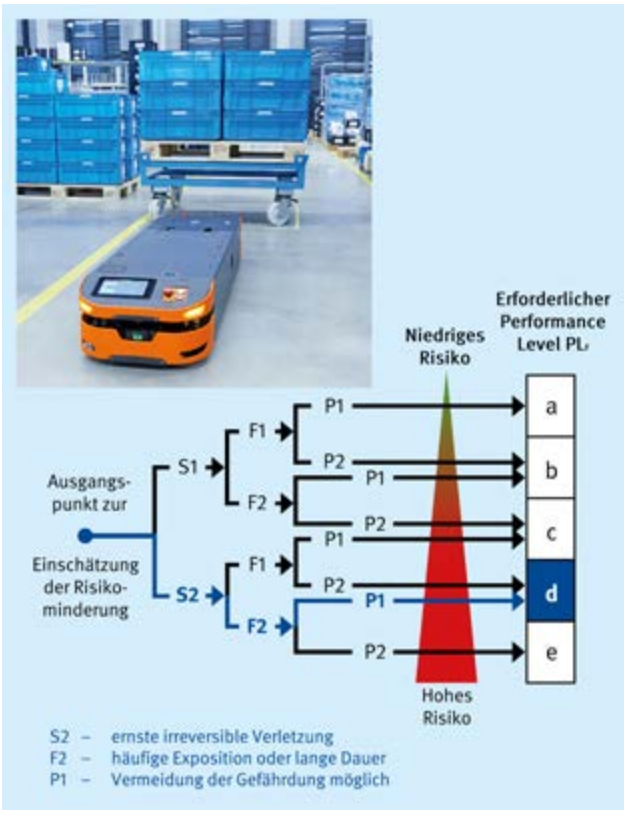


Abb. A.2 Risikobeurteilung für den Auffahrschutz an einem fahrerlosen Flurförderzeug

Beispiel 3

Webmaschine

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

- SF1 Bei Eingreifen in den Gefahrenbereich Verhinderung eines unerwarteten Anlaufs durch Sicher abgeschaltetes Moment (Safe Torque Off, STO) aller Antriebe

eingesetzt. Bei einem Maschinenanlauf kann es zu Fingerquetschungen und -brüchen kommen (S2). Die Häufigkeit der Gefährdungsexposition kann mit selten (geringer als einmal alle 15 Minuten) bezeichnet werden. Die gesamte Expositionsdauer ist geringer als 1/20 der gesamten Betriebsdauer (F1). Befinden sich die Hände der Bedienperson bereits im Gefahrenbereich, während es zu einem unerwarteten Anlauf kommt, ist diese Bewegung so schnell, dass ein Ausweichen kaum möglich ist. Zudem ist die plötzlich auftretende Gefährdung für das Bedienpersonal nicht im Vorhinein zu erkennen (P2). Damit ergibt sich für SF1 ein erforderlicher Performance Level PL_r = d (Abbildung A.3). Dieses Ergebnis wird durch die Produktnorm DIN EN ISO 11111-6:2016 bestätigt. Das Normungsgremium hatte offensichtlich keine Veranlassung, aufgrund des Unfallgeschehens hiervon abzuweichen.

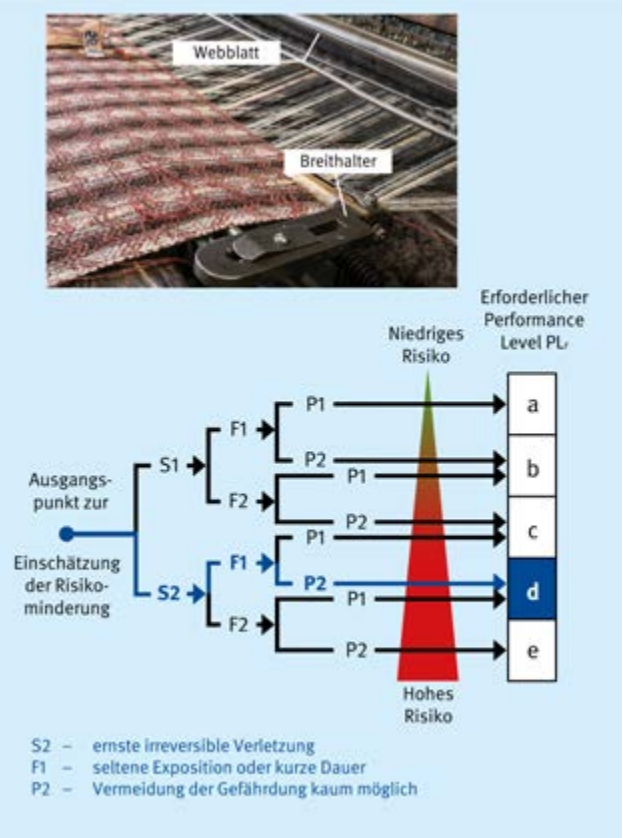


Abb. A.3 Risikobeurteilung für SF1 an einer Webmaschine

Beispiel 4

Rotationsdruckmaschine

In einer Rollenrotationsdruckmaschine wird eine Papierbahn durch eine Vielzahl von rotierenden 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.
- SF2 – Bei geöffneter Schutztür dürfen Maschinenbewegungen nur mit begrenzten Drehzahlen erfolgen.
- SF3 – Bei geöffneter Schutztür sind Bewegungen nur während der Betätigung eines Tipptasters möglich.

Ein Einzug zwischen den Zylindern führt zu schweren Verletzungen (S2). Da Tätigkeiten im Gefahrenbereich nur zu Wartungsarbeiten anfallen, kann die Häufigkeit der Gefährdungsexposition mit selten (geringer als einmal alle 15 Minuten) bezeichnet werden, die gesamte Expositionsdauer ist geringer als 1/20 der gesamten Betriebsdauer (F1). Die Möglichkeit, der gefahrbringenden Bewegung auszuweichen, ist bei Produktionsgeschwindigkeiten nicht gegeben (P2). Für die Sicherheitsfunktionen SF1 und SF2 ergibt sich daher ein erforderlicher Performance Level PL_r = d (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). Je nach Anwendungsfall sind die möglichen Maschinenbewegungen für die Bedienperson überschaubar und sie kann den gefahrbringenden Bewegungen ausweichen (P1) oder ein Ausweichen kann nicht realistisch angenommen werden (P2). Für SF3 kann daher ein erforderlicher Performance Level PL_r = c oder PL_r = d ausreichend sein (siehe Abbildung A.4). Die für diese Maschine zutreffende Produktnorm DIN EN 1010-1:2011 unterscheidet zwischen verschiedenen Anwendungsfällen und legt für Sicherheitsfunktion SF3 bei Justierungen und Einstellungen und vorhandener sicher begrenzter Geschwindigkeit einen PL_r von b fest.

Wie man die hier beschriebenen Sicherheitsfunktionen realisieren kann, ist in Kapitel 11 im Beispiel 19 beschrieben.

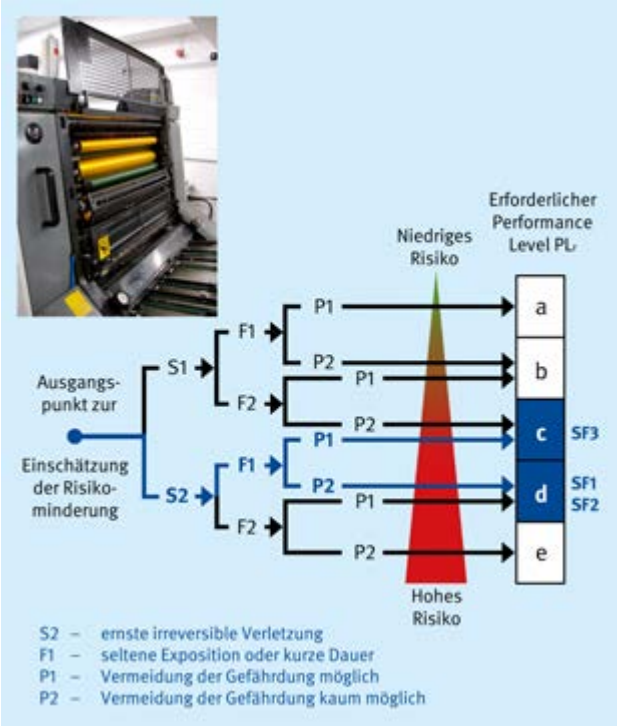


Abb. A.4 Risikobeurteilung für Sicherheitsfunktionen an einer Rotationsdruckmaschine

Literatur

[A1] *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld, R.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 4/2018. Hrsg.: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2018. https://publikationen.dguv.de Webcode: p012737

Anhang B

Sicherheitsbezogenes Blockdiagramm und FMEA

Änderung gegenüber dem IFA Report 2/2017

- Schreibung von *PFH* (früher: PFH_D) und Definition dieser Größe an die neue Normversion angepasst (Ersetzung von Wahrscheinlichkeit durch Häufigkeit)
- Aktualisierte Darstellung der Anwendung der Größe RDF (Anteil gefahrbringender Ausfälle), die neu in die Norm aufgenommenen wurde
- Aktualisierung der Angaben im Abschnitt „Literatur“

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* (Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde, engl.: average frequency of a dangerous failure per hour) oder direkt die PL-Eignung in quantitativer Hinsicht bestimmt werden kann. Zwei wichtige Schritte auf diesem Weg sind das sicherheitsbezogene Blockdiagramm und die funktionsblockweise durchgeführte Ausfalleffektanalyse FMEA (Failure Mode and Effects Analysis)[1].

B.1 Zweck und Erstellung eines sicherheitsbezogenen Blockdiagramms

Das Ergebnis der unter sicherheitstechnischem Blickwinkel erfolgenden Analyse der Systemstruktur wird zweckmäßig in Form eines Blockdiagramms dargestellt, das man als „sicherheitsbezogenes Blockdiagramm“ bezeichnen kann. Im Diagramm soll zum Ausdruck kommen, ob die Sicherheitsfunktion ganz oder teilweise ein- oder mehrkanalig ausgeführt wird und welche Diagnosemöglichkeiten bestehen, um interne Bauelementausfälle zu erkennen. Weil unter dem hier interessierenden Aspekt der Quantifizierung von Ausfallwahrscheinlichkeiten die Diagnose ein Kompensationsmittel für Bauelementausfälle ist, wird in diesem Anhang anstelle des sonst üblichen Begriffs „Fehlererkennung“ der Ausdruck „Ausfallerkennung“ verwendet.

In der Maschinensicherheit akzeptiert man meistens, dass infolge eines Steuerungsausfalls anstelle der Ausführung der ursprünglich vorgesehenen Sicherheitsfunktion eine Ersatzreaktion erfolgt, die einen sicheren Zustand herbeiführt, z. B. die Betriebshemmung mit energielosen Ausgängen (Abschaltsystem, engl.: 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 9 und 10 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 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 Ausfäl-

[1] Die hier beschriebene FMEA betrachtet auch die Erkennung von Ausfällen (Diagnose) und kann deswegen auch als FMEDA (Failure Mode, Effects and Diagnostics Analysis) bezeichnet werden.

len eine schädliche Wirkung auf die Sicherheitsfunktion, ihre Ersatzfunktion oder Diagnosefunktionen ausgehen kann. Beispielsweise muss bei Bauteilen zur Sicherstellung der elektromagnetischen Verträglichkeit (EMI) 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 angeordnete Teilschaltungen – also Schaltungen, die nacheinander verschiedene Schritte der Signalverarbeitung ausführen – zu einem Funktionsblock zusammengefasst werden. Bei anders angeordneten Blöcken sollte die Zusammenfassung sinnvollerweise nur so weit gehen, dass Redundanzen wie 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. Spannungsversorgungen, 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 EMI). 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 dem 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 eines Teils der 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“, engl.: Safe Torque Off, STO). Der Mikrocontroller und die nachgeschaltete Antriebssteuerung führen neben der Sicherheitsfunktion verschiedene andere Maschinenfunktionen aus, die hier nicht betrachtet werden, weil sie keine Sicherheitsfunktionen sind. Obwohl in diesem Beispiel die Sicherheitsfunktion allein mit elektrotechnischen Mitteln realisiert wird, gelten die beschriebenen Prinzipien für das sicherheitsbezogene Blockdiagramm und die FMEA technologieübergreifend.

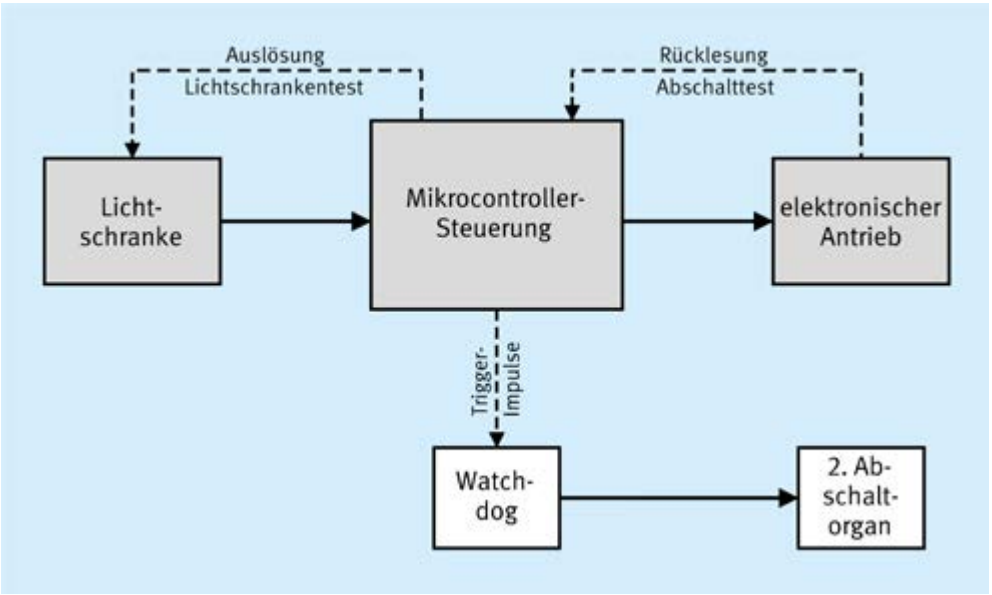


Abb. B.1
Beispiel für das sicherheitsbezogene Blockdiagramm einer einkanaligen Maschinensteuerung in Kategorie 2

Im sicherheitsbezogenen Blockdiagramm erscheinen nur Funktionsblöcke, die mit der Sicherheitsfunktion „Sicher abgeschaltetes Moment“ im Zusammenhang stehen, jedoch keine Bedien- und Anzeigeorgane für andere Maschinenfunktionen. Eventuell kann von einigen Bauelementen dieser Schaltungsteile im Fehlerfall eine die Sicherheitsfunktion störende Rückwirkung ausgehen. Nur dann sind diese Bauelemente denjenigen Funktionsblöcken zuzurechnen, die sie zum Ausfall bringen können.

Oft wird das sicherheitsbezogene Blockdiagramm wie im vorgestellten Beispiel die Gestalt einer der „vorgesehenen Architekturen“ nach der Norm DIN EN ISO 13849-1, Abschnitt 6.1.3.2 (Abschnitt 8.2.3 bis 8.2.7 dieses Reports) haben. Dann kann das in Abschnitt 6.1.8 der Norm dargestellte Verfahren (ergänzt durch die Anhänge B, C, D, E, F, I und K der Norm) zur quantitativen Bestimmung des PL 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 *Goble* [B1] und *Signoret* et al. [B2].

B.2 Zweck und Eigenart einer FMEA für die Quantifizierung

Für den quantitativen Nachweis des PL muss die mittlere Häufigkeit eines gefahrbringenden 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 6.1.3.2.2 bis 6.1.3.2.6 der DIN EN ISO 13849-1 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 [B3].

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.

B.2.1 Ausführung einer FMEA für die Quantifizierung

Im Folgenden wird die prinzipielle Vorgehensweise bei einer Quantifizierungs-FMEA am Beispiel des Funktionsblocks „Lichtschranke“ aus Abbildung B.2 demonstriert. Zu diesem Zweck wurde die Schaltung bewusst einfach gehalten. Nur die gestrichelt eingerahmten Bauelemente gehören zum Funktionsblock. Die Elemente S1 und P2 sind eine Ersatzschaltung für die reale Einbindung des Funktionsblocks innerhalb des Systems nach Abbildung B.1. Solange der Fototransistor K1 Licht von der Infrarot-LED P1 empfängt, hält er den Transistor K2 gesperrt, wodurch der Transistor K3 leitet und an Anschluss X1.2 eine positive Ausgangsspannung ansteht, die mit dem Voltmeter P2 messbar ist. Wird der Lichtstrahl unterbrochen, so sperrt K1, K2 wird leitend und K3 schaltet die Ausgangspannung ab. Der Test des Funktionsblocks „Lichtschranke“, den die Mikrocontroller-Steuerung aus Abbildung B.1 programmgesteuert durchführt, kann mit dem Taster S1 und dem Voltmeter P2 simuliert werden: Die Lichtquelle P1 wird kurzzeitig ausgeschaltet und dabei wird geprüft, ob die Ausgangsspannung ordnungsgemäß auf null Volt absinkt. Den signalverarbeitenden Elementen des Funktionsblocks „Lichtschranke“ (K1 bis K3, R2 bis R9, C1) wird dabei dasselbe Verhalten abverlangt wie bei einer „echten“ Anforderung der Sicherheitsfunktion durch Unterbrechen des Lichtstrahls. Dieser Test wird im Folgenden als „Test 1“ bezeichnet.

B.2.2 Gefährliche Ausfallrichtung eines Funktionsblocks

Als erster Schritt muss die gefährliche Ausfallrichtung des Funktionsblocks bestimmt werden. Im Allgemeinen können nicht nur einzelne Bauelemente, sondern in der Folge auch ein ganzer Funktionsblock auf verschiedene Weise ausfallen. Als „gefährliche“ Ausfallrichtung eines Funktionsblocks gelten diejenigen Arten des Ausfalls, die aus sicherheitstechnischer Sicht ungünstig sind. Manche Ausfälle lassen das ganze System direkt gefährlich ausfallen, sodass es weder die ursprüngliche Sicherheitsfunktion noch eine sicherheitsgerichtete Ersatzaktion ausführen kann. Andere Ausfälle erhöhen die Wahrscheinlichkeit, dass dies geschieht, indem jetzt eine geringere Zahl weiterer Ausfälle ausreicht, um das System gefährlich aus-

fallen zu lassen. Gibt es für den ausfallenden Funktionsblock keine Redundanz, also keinen zweiten Kanal, der seine Funktion ersetzen kann, und wird nicht durch Diagnose hinreichend schnell eine Aktion ausgeführt, die einen sicheren Zustand erzeugt, so führt der gefährliche Ausfall des Funktionsblocks zum gefährlichen Ausfall des Systems. Aber auch, wenn wegen vorhandener Redundanz oder einer schnellen Ausfallreaktion anderer Schaltungsteile keine der möglichen Ausfallarten des infrage stehenden Funktionsblocks einen gefährlichen Systemausfall verursacht, kann und muss seine „gefährliche" Ausfallrichtung festgestellt werden. Es ist diejenige Ausfallrichtung, die dazu führt, dass der Funktionsblock seinen vorgesehenen Beitrag zu einem sicheren Systemverhalten nicht mehr leistet. Mitunter müssen auch mehrere Ausfallarten, die durch unterschiedliches, aber gleichermaßen schädliches Blockverhalten gekennzeichnet sind, berücksichtigt werden (z. B. dauerhaftes Einschalten und Schwingung am Ausgang). Es ist daher am einfachsten, die gefährliche Ausfallrichtung durch den Verlust der sicherheitstechnisch geforderten Funktion des Funktionsblocks zu beschreiben. Diagnosemöglichkeiten werden erst später berücksichtigt und bleiben bei diesem Schritt zunächst außer Acht. Beim vorliegenden Beispiel (Lichtschranke, Abbildung B.2) soll die Ausgangsspannung des Funktionsblocks auf null abfallen, solange der Fototransistor K1 kein Licht von der LED P1 empfängt, denn darin besteht der Beitrag dieses Sicherheitsblocks zur Ausführung der Sicherheitsfunktion „Sicher abgeschaltetes Moment bei unterbrochenem Lichtstrahl".

Somit kann die gefährliche Ausfallrichtung des Funktionsblocks beschrieben werden als „Anliegen einer Ausgangsspannung größer als Null bei Nichtbeleuchtung des Fototransistors K1".

B.2.3 Bauelementausfallraten

Verschiedene Datenquellen kommen für Bauelementausfallraten infrage. Beispiele mit Ausfallraten für elektronische Bauelemente sind SN 29500 [B4], Telcordia SR-332 [B5] und HDBK-217Plus [B6]. Alle diese Quellen bieten 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 6.1.8, gehen von der zeitlichen Konstanz der Ausfallraten aus, was eine Idealisierung darstellt. Durch entsprechende Dimensionierung und notfalls vorbeugenden Austausch kann erreicht werden, dass die Bauelemente während der Gebrauchsdauer T_M (Mission Time) noch nicht in die Verschleißphase mit stark ansteigender Ausfallrate geraten.

Als schnell verfügbare Quelle für zumeist konservativ (pessimistisch) abgeschätzte Ausfallraten bietet sich DIN EN ISO 13849-1, Anhang C an. Hier wird insbesondere ein Weg gewiesen, auf dem für zyklisch arbeitende elektromechanische, fluidtechnische und mechanische Einzelkomponenten Ausfallraten aus den sogenannten B_{10D}-Werten (siehe Tabelle D.2. dieses Reports) abgeleitet werden können.

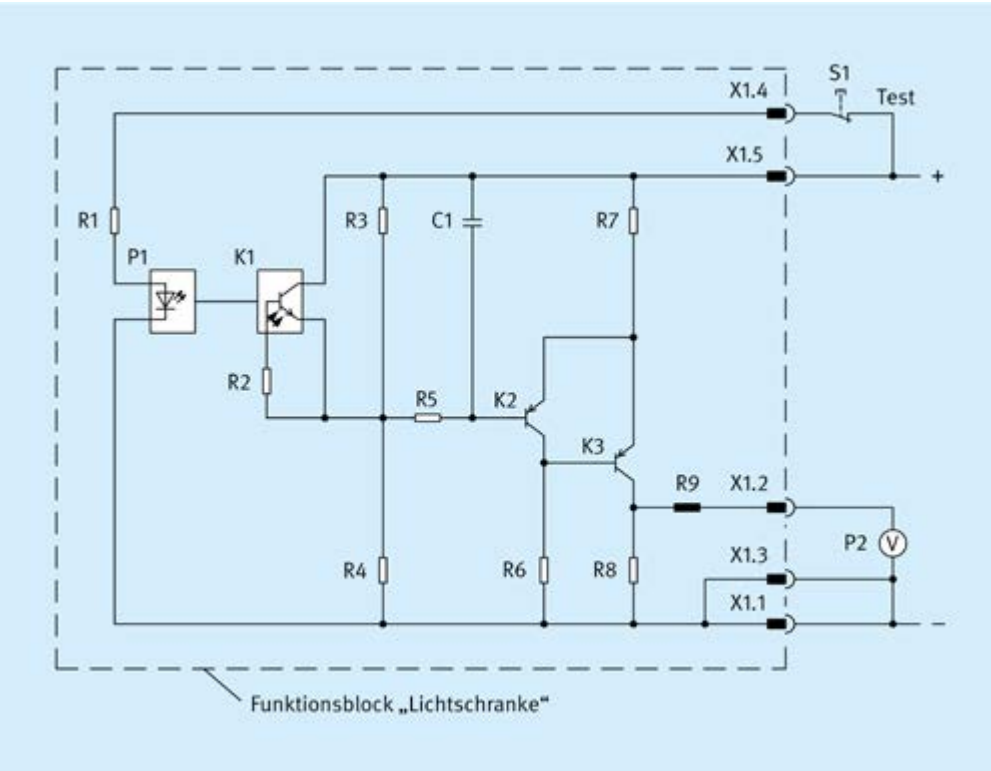


Abb. B.2
Angenommene Schaltung (einfaches Beispiel) des Funktionsblocks „Lichtschranke" aus dem sicherheitsbezogenen Blockdiagramm nach Abbildung B.1

Bezeichnung des Funktionsblocks:	Lichtschranke
Gefährliche Ausfallrichtung des Funktionsblocks:	Anstehen einer Ausgangsspannung größer als Null bei Nichtbeleuchtung des Fototransistors K1
Datenquelle für Ausfallraten:	XYZ-Datenbank

Referenz-bezeich-nung	Bauelement-Art	Relev. Bauelem.-Temp. (°C)	Basis-Ausfall-Rate (FIT)	Tempe-ratur-faktor	Ausf.anteil in sichere Richtung	Ausf.anteil in gefährl. Richtung	erk.bar durch Test Nr.	*DC*	λ (FIT)	λ_S (FIT)	λ_D (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)	Anm.
R1	Chip-Widerstand MS	55	0,5	1,20	1	0	–	–	0,60	0,60	0,00	0,00	0,00	
R2	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	1)
R3	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R4	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R5	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R6	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R7	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R8	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R9	HF-Spule SMD	50	1,8	1,12	1	0	–	–	2,02	2,02	0,00	0,00	0,00	
C1	Chip-Kond. keram.	50	1,1	1,60	0	1	1	0,5	1,76	0,00	1,76	0,88	0,88	2)
P1	Infrarot-LED	60	2,5	2,24	1	0	–	–	5,60	5,60	0,00	0,00	0,00	
K1	Fototransistor	60	3,4	1,80	0,5	0,5	1	1	6,12	3,06	3,06	3,06	0,00	
K2	Transistor SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
K3	Transistor SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
X1	Steckverb. 5-polig	50	1,5	1,00	0,5	0,5	1	1	1,50	0,75	0,75	0,75	0,00	3)
–	Leiterpl. mit 36 Lötst.	50	1,8	1,00	0,5	0,5	1	0,9172	1,80	0,90	0,90	0,83	0,07	4)
								Summen:	**31,23**	**19,71**	**11,52**	**10,57**	**0,95**	

$MTTF_D$ (a): **9905,9** *DC* (%): **91,72**

Anmerkungen:

1) Bei Unterbrechung und hoher Umgebungstemperatur fließt durch K1 unter Umständen ein zu hoher Dunkelstrom.
2) Bei Unterbrechung wird die Schaltung gegenüber EM-Störungen empfindlich; Erkennbarkeit nicht gesichert.
3) Kurzschlüsse innerhalb von X1 können einen Ausfall in die gefährliche Richtung verursachen.
4) Aufteilung DD/DU wie die durchschnittliche Aufteilung von allen übrigen Elementen.

Abb. B.3 Sinnvolle Ausführungsform einer FMEA-Tabelle für den Funktionsblock „Lichtschranke“ aus Abbildung B.2

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 etc.) gilt. Auch die Eigenerwärmung ist zu berücksichtigen. Gängige Datenquellen, z. B. [B4] bis [B6], 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 IEC 61709 [B7]. Dieselben Formeln sind auch in SN 29500 enthalten.

B.2.4 Erstellung einer funktionsblockweisen FMEA für Quantifizierungszwecke

Bei der FMEA werden die Bauelemente des Funktionsblocks zunächst einzeln bewertet und daraus die Komplettbewertung des Blocks abgeleitet. Dies geschieht zweckmäßig in Form einer Tabelle, die diesen Prozess und zugleich das Ergebnis dokumentiert. Die FMEA kann mit unterschiedlichem Exaktheitsanspruch ausgeführt werden, was sich in verschieden hohem Aufwand für die Erstellung der dazugehörigen Tabellen widerspiegelt. Eine mögliche Ausführung ist beispielsweise in [B8], Anhang C beschrieben. Verbindliche Vorschriften existieren nicht. Die in Abbildung B.3 vorgestellte Variante stellt einen Kompromiss zwischen hohem Akkuratheitsanspruch und Aufwand einerseits sowie allzu starker Vereinfachung andererseits dar und nimmt Rücksicht auf die Genauigkeit und die Verfügbarkeit der verwendeten Daten. Die dort verwendeten Zahlen sind angenommene Beispielwerte.

Die Bauelemente des Funktionsblocks werden zeilenweise aufgelistet und mit ihren Ausfallraten versehen. Die übliche Einheit der Ausfallrate ist „FIT“ (Failures In Time); 1 FIT = 10^{-9}/h. Als einziger Gewichtsfaktor für die Basisausfallrate erscheint hier der Temperaturfaktor, der mithilfe von IEC 61709 ermittelt werden kann. Das in dieser Norm dargestellt Verfahren wird auch von SN 29500 verwendet. 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 für Prozessoren und Leistungshalbleiter zutreffen kann, 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, sichere Richtung) und λ_D (dangerous, gefährliche Richtung) aufgeteilt, wozu u. a. die „gefährliche Ausfallrichtung“ des Funktionsblocks bekannt sein muss (siehe oben). Nach der „reinen Lehre“ muss dies in zwei Schritten geschehen:

Die Gesamtausfallrate wird zuerst auf die verschiedenen Ausfallarten (z. B. Unterbrechung, Kurzschluss, Drift, Funktionsänderung) verteilt. Angaben zur Ausfallartenverteilung für verschiedene Bauelemente findet man z. B. in IEC 61709. Auch in kommerzieller FMEDA-Software sind typischerweise Ausfallartenverteilungen hinterlegt. Die Angaben in den verschiedenen Quellen sind nicht einheitlich. Ein unnötiger Wechsel der Quelle für die Ausfallartenverteilung von Bauteil zu Bauteil ist nicht akzeptabel.

Im zweiten Schritt werden die auf jede Ausfallart entfallenden Ausfallratenanteile λ_S oder λ_D zugewiesen, je nachdem, ob die betreffende Ausfallart den Funktionsblock in dessen sichere oder gefährliche Richtung ausfallen lässt. Das unveränderte Weiterfunktionieren wird dabei wie ein Ausfall in die sichere Richtung gewertet.

In Abbildung B.3 wird ein vereinfachter pragmatischer Weg dargestellt, der ohne eine bestimmte Quelle für Ausfallartenverteilungen auskommt und bei dem nur geprüft wird, welcher der drei folgenden Fälle bei einem Bauelement vorliegt:

a) Alle Ausfallarten führen zum Ausfall des Funktionsblocks in dessen sichere Richtung oder haben keine Auswirkung auf sein Verhalten.
b) Es gibt mindestens eine Ausfallart, die den Funktionsblock in dessen sichere Richtung ausfallen lässt, und mindestens eine Ausfallart, die ihn in seine gefährliche Richtung ausfallen lässt.
c) Alle Ausfallarten führen zum Ausfall des Funktionsblocks in dessen gefährliche Richtung.

Im Fall a) wird die komplette Ausfallrate λ der Ausfallrate λ_S in die sichere Richtung zugewiesen (Beispiel: Infrarot-LED P1). Entsprechend wird im Fall c) die gesamte Ausfallrate λ der Ausfallrate λ_D in die gefährliche Richtung zugerechnet (Beispiel: Kondensator C1). Im Fall b) weist man die Gesamtausfallrate λ je zur Hälfte λ_S und λ_D zu (Beispiel: Transistor K2).

Die vereinfachte Vorgehensweise im Fall b) ist normalerweise bei Bauelementen mit einem kleinen Beitrag zur Gesamtausfallrate des Funktionsblocks gerechtfertigt, wenn dieser viele solche Elemente enthält. Einzelne Bauelemente mit einem überdurchschnittlichen Beitrag zur Gesamtausfallrate des Funktionsblocks sind ggf. geson-

dert zu betrachten. Bei komplexen integrierten Schaltungen wie Prozessoren kann ebenfalls eine 50-zu-50-%-Aufteilung der Ausfallrate auf λ_S und λ_D vorgenommen werden. Dasselbe gilt für Lötstellen/Leiterplatten. Vorsicht ist geboten bei diskreten oder niedrig integrierten Bauelementen mit relativ hoher Ausfallrate. Trägt z. B. ein Schütz oder ein Leistungshalbleiter wesentlich zur Gesamtausfallrate des Funktionsblocks bei, so ist im Zweifelsfall von einem überwiegenden Ausfall in die gefährliche Richtung auszugehen. Dies gilt umso mehr, wenn es sich um die den Ausgangsstrom schaltenden Elemente von Sicherheitsausgängen handelt.

Bei Bauelementen zur Ertüchtigung der Schaltung gegenüber Störeinflüssen – z. B. elektromagnetischen Störungen oder hoher Umgebungstemperatur – ist zur Bewertung des Funktionsblockverhaltens eine Unterscheidung zwischen zwei möglichen Fällen sinnvoll. Ist das Auftreten der Störphänomene lediglich „möglich“ und dient die Schaltungsmaßnahme im Wesentlichen zur Erhöhung der Geräteverfügbarkeit unter (seltenen) ungünstigen Bedingungen, so muss bei der Beurteilung des Funktionsblockverhaltens beim Bauelementeausfall das gleichzeitige Vorliegen des „Störphänomens“ nicht angenommen werden. Sieht jedoch die vorgesehene Betriebsweise des Gerätes die gelegentliche bis ständige Präsenz der Störung vor oder legt die typische Betriebsweise dies nahe (z. B. Einbau in der Reichweite bekannter elektromagnetischer Störquellen oder heißer Einbauort), so muss die Bewertung des Bauelementausfalls die Anwesenheit der Störbeaufschlagung berücksichtigen. Das gilt auch für die Beurteilung der Ausfallerkennbarkeit bei diesen Bauelementen durch Diagnosemaßnahmen.

Bei verschleißbehafteten Bauelementen wird meistens eine zeitkonstante Ersatz-Ausfallrate in die gefährliche Richtung verwendet, die mithilfe der Gleichung (C.5) aus DIN EN ISO 13849-1, Anhang C.4.3 berechnet wird. Hierfür wird der Kennwert B_{10D} benötigt, der die Anzahl der Schaltspiele bis zum Ausfall in die gefährliche Richtung angibt. Idealerweise stammt der B_{10D}-Wert vom Hersteller des Bauelements, der zugleich angibt, welche Ausfallrichtung dabei als die gefährliche angenommen wurde (z. B. Nichtöffnen von Schaltkontakten). Denn prinzipiell kann eine Ausfallrichtung nur im Hinblick auf eine bestimmte Applikation als gefährlich bzw. ungefährlich bewertet werden. Oftmals ist vom Hersteller nur ein B_{10}-Wert (Anzahl der Schaltspiele bis zu irgendeinem Ausfall) verfügbar. Für diesen Fall erlaubt DIN EN ISO 13849-1 in Anhang C.4.2 die Berechnung des B_{10D}-Wertes mit der Gleichung C.4, d. h. mit $B_{10D} = B_{10}/RDF$, wobei *RDF* der Anteil der gefährlichen Ausfälle an der Gesamtheit der Ausfälle ist („Ratio of Dangerous Failure“). Auch die Norm folgt in Anhang C.4.2, Fußnote 1, mit $RDF = 0{,}5$ diesem Ansatz. Diese Berechnungsmethode beruht jedoch auf vereinfachenden Annahmen, die von den tatsächlichen Verhältnissen bei den hier betrachteten Verschleißteilen deutlich abweichen können. Daher sollte B_{10D} auf das Zweifache des Wertes von B_{10} begrenzt werden, wenn B_{10D} mittels des Quotienten B_{10}/RDF ermittelt wird. Durch den Zusammenhang aus Gleichung (C.3) in DIN EN ISO 13849-1, Anhang C.4.2 hat die B_{10D}-Ermittlung auch Konsequenzen für die zulässige Bauteil-Betriebszeit T_{10D} und somit eventuell auch für zu spezifizierende Bauteil-Austauschintervalle. Bei *RDF*-Werten von unter 0,5 sieht die Norm jedoch eine Begrenzung von T_{10D} auf das Zweifache des Wertes von T_{10} vor.

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 (Diagnostic Coverage, *DC*) 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. Bei zu Testzwecken abgeschalteter LED P1 detektiert der Test also eine Ausgangsspannung von > 0. Daher wird diesen Elementen der bauelementbezogene *DC*-Wert von „1“ zuerkannt. Anders ist dies beim Kondensator C1, der zur Unterdrückung von regelmäßig,

aber nicht ständig vorkommenden elektromagnetischen Störungen dient (Annahme bei diesem Beispiel). Driftausfälle (begrenzte Kapazitätsänderungen) sind unkritisch, aber ein Kurzschluss führt dazu, dass der Ausgang (Anschluss X1.2) nicht abgeschaltet werden kann (gefährliche Ausfallrichtung des Funktionsblocks). Ein Kurzschluss von C1 wird durch Test 1 erkannt. Bei Unterbrechung von C1 pflanzt sich die elektromagnetische Störung über K2 und K3 bis zum Ausgang des Funktionsblocks fort. Dabei ist unklar, wie die nachfolgende Schaltung dieses hochfrequente Wechselsignal interpretiert und ob das Störphänomen auch während des Tests vorliegt. Ungünstigstenfalls verhindert die nicht unterdrückte Störung, dass das mit Störungen überlagerte Ausgangssignal bei nicht beleuchtetem Fototransistor K1 von der nachfolgenden Schaltung als Anforderung der Sicherheitsfunktion interpretiert wird (= gefährlicher Ausfall des Funktionsblocks „Lichtschranke“). Wenn die Störung zum Testzeitpunkt nicht vorliegt, kann Test 1 die Kondensatorunterbrechung nicht erkennen. Da keine verlässliche Ausfallartenverteilung für den Kondensator bekannt ist, wird – unter Vernachlässigung der unkritischen Driftausfälle – angenommen, dass Kurzschlüsse und Unterbrechungen je 50 % der Ausfälle ausmachen. Beide Ausfallarten führen zum gefährlichen Funktionsblockausfall. Sicher erkennbar sind jedoch nur die Kondensatorkurzschlüsse, d. h. die (geschätzte) Hälfte aller gefährlichen Kondensatorausfälle. Somit wird der bauelementbezogene Diagnosedeckungsgrad mit 50 % bzw. 0,5 abgeschätzt.

Die Leiterplatte mit den Lötstellen kann Kurzschlüsse und Unterbrechungen an verschiedenen Stellen in die Schaltung einbringen. Der in Abbildung B.3 realisierte pragmatische Ansatz zur Abschätzung des *DC*-Wertes für Lötstellen und Leiterplatte besteht darin, ihnen jenen mittleren *DC*-Wert zuzuweisen, der sich für alle übrigen Bauelemente des Funktionsblocks aus der Gleichung $DC = \Sigma \lambda_{DD} / \Sigma \lambda_D$ ergibt. So wirkt sich das Einbeziehen von Leiterplatte und Lötstellen nicht auf den *DC*-Wert aus, der für den kompletten Funktionsblock berechnet wird.

In jeder Tabellenzeile, d. h. für jedes Bauelement gilt:

λ = Temperaturfaktor · Basisausfallrate (ggf. mit weiteren Korrekturfaktoren, s.o.)

λ_S = Ausfallanteil in die sichere Richtung · λ

λ_D = Ausfallanteil in die gefährliche Richtung · λ

$\lambda_{DD} = DC \cdot \lambda_D$

$\lambda_{DU} = (1 - DC) \cdot \lambda_D$

Für diese λ-Werte werden in der Tabelle Spaltensummen gebildet. Aus dem Summenwert λ_D bzw. aus den Summenwerten λ_D und λ_{DD} ergeben sich die $MTTF_D$, d. h. die mittlere Zeit bis zum gefährlichen Ausfall des Funktionsblocks, sowie der *DC* des Funktionsblocks:

$MTTF_D = 1/\lambda_D$

$DC = \lambda_{DD}/\lambda_D$

Um den PL bei einer der vorgesehenen Architekturen nach Abschnitt 8.2.3 bis 8.2.7 zu bestimmen, werden als Eingangsgrößen nur die Werte von $MTTF_D$ und *DC* benötigt. Im vorliegenden Beispiel ergeben sich ein $MTTF_D$-Wert von 9 905,9 Jahren und ein *DC* von 91,72 %. Wird ein anderes Quantifizierungsverfahren angewendet, können auch Werte wie λ_{DD} bzw. λ_{DU} aus der FMEA-Tabelle Verwendung finden.

B.3 „Parts Count“-Verfahren

Zur Arbeits- und Zeitersparnis kann anstelle einer FMEA ein einfacheres Verfahren angewandt werden. Verzichtet man auf die detaillierte Analyse des Schaltungsverhaltens bei den verschiedenen Ausfallarten der einzelnen Bauelemente, gelangt man zum sogenannten „Parts Count“-Verfahren (vgl. Anhang D dieses Reports). Es stammt ursprünglich aus dem MIL-Handbook 217F (Nachfolgepublikation siehe HDBK-217Plus) 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

[B1] *Goble, W. M.*: Control Systems Safety Evaluation & Reliability. 3rd ed. Hrsg.: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010. https://www.isa.org

[B2] *Signoret, J.-P., Leroy, A.*: Reliability Assessment of Safety and Production Systems. Springer Nature Switzerland, Cham 2021

[B3] DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (11/2006). DIN Media, Berlin 2006

[B4] SN 29500: Ausfallraten Bauelemente, Erwartungswerte. Hrsg.: Siemens AG, CT TIM Regulation & Standardization, München 2004–2016. (Bestellanfragen an michaela.pabst@siemens.com oder thomas.haizmann@siemens.com)

[B5] Telcordia SR-332: Reliability Prediction Procedure for Electronic Equipment, Issue 4, March 2016. Ericsson Information Superstore. https://telecom-info.njdepot.ericsson.net/

[B6] HDBK-217Plus: 2015, Notice 1, Reliability Prediction Models. Quanterion Solutions Incorporated, Utica, New York 2017

[B7] IEC 61709: Elektrische Bauelemente – Zuverlässigkeit – Referenzbedingungen für Ausfallraten und Beanspruchungsmodelle zur Umrechnung, Edition 3.0 (02.17). IEC, Genf, Schweiz

[B8] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (02.11). DIN Media, Berlin 2011

Anhang C

Fehlerlisten, Fehlerausschlüsse und Sicherheitsprinzipien

C.1 Fehlerlisten

Die bei der Validierung von SRP/CS bzw. Teilsystemen anzunehmenden Fehler und mögliche Fehlerausschlüsse für mechanische, pneumatische, hydraulische und elektrische Bauteile finden sich in DIN EN ISO 13849-2 [C1], Anhang A bis D in sogenannten Fehlerlisten. In einzelnen Produktnormen, z. B. DIN EN 61800-5-2 [C2] und DIN EN 61496-1 [C3], sind ebenfalls Fehlerlisten oder Ergänzungen zu den genannten Fehlerlisten vorhanden. Der Beitrag 340 220 im IFA-Handbuch [C4] erläutert Hintergründe und das Zustandekommen der Fehlerlisten.

C.2 Fehlerausschlüsse

Ohne die Annahme von Fehlerausschlüssen sind sichere Steuerungen manchmal nicht mit vertretbarem Aufwand zu realisieren. Gründe für einen Fehlerausschluss können insbesondere die physikalische Unmöglichkeit einer bestimmten Fehlerart oder die technische Unwahrscheinlichkeit des Auftretens eines Fehlers sein sowie allgemein anerkannte technische Erfahrungen (siehe auch Abschnitt 6.1.10.3 der DIN EN ISO 13849-1). Fehlerausschlüsse sind auch für neu entworfene Komponenten oder Bauelemente grundsätzlich möglich. Oft gilt ein Fehlerausschluss nicht für alle möglichen Fehler eines Bauteils. Jeder einzelne Fehlerausschluss muss in der technischen Dokumentation genau begründet werden. Es bleibt die Notwendigkeit von Maßnahmen gegen systematische Ausfälle. Ein Fehlerausschluss muss unter allen anzunehmenden Umgebungsbedingungen gültig sein und darf auch nicht alleinige Begründung für einen PL e sein. DIN EN ISO 13849-2 beschreibt für einzelne Bauelemente mögliche Fehlerausschlüsse, soweit sie als zulässig erachtet werden. Angaben in den folgenden Beispielen sind, wo erforderlich, im Sinne üblicher Praxis aktualisiert.

C.2.1 Beispiele für Fehlerausschlüsse an Bauteilen

C.2.1.1 Bauteile der Fluidtechnik

Für pneumatische und hydraulische Bauteile sind häufig vergleichbare Fehlerausschlüsse formuliert. Jedoch sind auch fluidspezifische Fehlerausschlüsse vorhanden. Beispiel für gemeinsame Fehlerausschlüsse an fluidischen Bauteilen:

- Wegeventile
  Die Fehlerannahme „Nichtschalten oder nicht vollständiges Schalten“ kann unter folgenden Voraussetzungen ausgeschlossen werden: Zwangsläufige mechanische Betätigung der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist. Bei hydraulischen Wegeventilen kann für ein Patronensitzventil spezieller Bauart (siehe Anmerkungen in DIN EN ISO 13849-2, Tabelle C.3) bezogen auf das Nichtöffnen ein Fehlerausschluss formuliert werden, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert.

C.2.1.2 Elektrische Bauteile

- Optokoppler
  Die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs“ kann unter folgenden Voraussetzungen ausgeschlossen werden:
  – Der Optokoppler ist entsprechend Überspannungskategorie III nach IEC 60664-1 gebaut.
  – Bei der Verwendung einer SELV/PELV-Spannungsversorgung ist Verschmutzungsgrad 2 bzw. Überspannungskategorie II ausreichend.
  – Ein interner Fehler des Optokopplers darf nicht zu einem übermäßigen Temperaturanstieg seiner Isolierwerkstoffe führen.

- Leiterplatte/bestückte Leiterplatte
  Die Fehlerannahme „Kurzschluss zwischen benachbarten Leiterbahnen/Kontaktstellen“ kann nach Norm ausgeschlossen werden, sofern folgende Voraussetzungen zutreffen:
  – Als Basismaterial wird mindestens EP GC nach IEC 60893-1 verwendet.
  – Luft- und Kriechstrecken werden nach IEC 60664-5 (für Strecken von mehr als 2 mm nach IEC 60664-1) bemessen mit Verschmutzungsgrad 2 bzw. Überspannungskategorie III. Wenn die Versorgung beider Leiterbahnen über ein SELV/PELV-Netzgerät erfolgt, muss die Mindeststrecke 0,1 mm betragen; zudem gilt Verschmutzungsgrad 2 bzw. Überspannungskategorie II.
  – Die bestückte Leiterplatte ist in einem Gehäuse eingebaut, das einen Schutz von mindestens IP54 gibt und die Leiterseite(n) ist/sind 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 Luft- und Kriechstrecken verringern.

Werden bleifreie Lötverfahren und Produkte angewendet, können elektrische Kurzschlüsse durch die Bildung von Zinnwhiskern vorkommen. Zinnwhisker bilden sich hauptsächlich bei Oberflächen mit reiner, glänzender Zinnbeschichtung. Die nadelähnlichen Überstände können eine Länge von mehr als 1 mm erreichen (Anmerkung: in DIN EN ISO 13849-2 wird ein Wert von mehreren hundert µm genannt) und elektrische Kurzschlüsse verursachen. Die vorherrschende Theorie lautet, dass Whisker durch Druckbelastung verursacht werden, die sich beim Verzinnen aufbaut. Diese Möglichkeit sollte beurteilt werden, insbesondere wenn ein Fehlerausschluss an einem Bauteil angewendet wird, z. B. Fehlerausschluss eines Kurzschlusses.

Wenn das Risiko der Zinnwhisker-Bildung als hoch eingeschätzt wird, ist ein Fehlerausschluss für einen Kurzschluss zwischen Anschlüssen von Bauteilen auf einer Leiterplatte trotz Einhaltung der oben aufgeführten Voraussetzungen nicht möglich. Whisker an Leiterbahnen von Leiterplatten wurden bisher nicht festgestellt. Die Leiterbahnen bestehen üblicherweise aus Kupfer ohne Zinnbeschichtung. Die Literaturhinweise [C5, C6] können zur Beurteilung des Phänomens hilfreich sein.

- Leitungen/Kabel
  Die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Leitern“ kann ausgeschlossen werden, wenn die Leiter
  - dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt (z. B. durch Kabelkanal, Panzerrohr),
  - in unterschiedlichen Mantelleitungen verlegt oder innerhalb eines elektrischen Einbauraumes verlegt oder
  - einzeln durch eine Erdverbindung geschützt sind.

  Für diesen Fehlerausschluss ist es erforderlich, dass sowohl die Leitungen als auch der Einbauraum den jeweiligen Anforderungen der DIN EN 60204-1 entsprechen.

- Elektromechanische Positionsschalter, Handschalter
  Die Fehlerannahme „Nichtöffnen von Kontakten“ kann unter folgender Voraussetzung ausgeschlossen werden:
  - Kontakte nach IEC 60947-5-1: 2003, Anhang K (aktualisierte Ausgabe 2016), öffnen sich.
  - Es ist anzumerken, dass dieser Fehlerausschluss nur für den elektrischen Teil des Schalters gilt (es handelt sich um einen Fehlerausschluss aus der Fehlerliste zur Elektrik). Anhang D.2.5 enthält detaillierte Ausführungen zu den Themen Fehlerausschluss und Modellierung von elektromechanischen Bauteilen.

C.3 Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien werden in den Tabellen A.1, B.1, C.1 und D.1 der informativen Anhänge der DIN EN ISO 13849-2:2013 behandelt.

C.3.1 Allgemein für alle Technologien

- Anwendung geeigneter Werkstoffe und angemessener Herstellungsverfahren
  Werkstoffe, Herstellungs- und Behandlungsverfahren werden unter Berücksichtigung von Einsatz und Beanspruchungen ausgewählt.

- Richtige Dimensionierung und Formgebung aller Bauteile
  Alle Bauteile werden so ausgewählt, dass sie den erwarteten Betriebsbedingungen genügen. Wichtige Kriterien sind z. B. Schaltvermögen, Schalthäufigkeit, Spannungsfestigkeit, Druckhöhe, dynamisches Druckverhalten, Volumenstrom, Temperatur und Viskosität der Druckflüssigkeit, Art und Zustand der Druckflüssigkeit bzw. der Druckluft.

- Alle Bauteile sind gegen Umgebungsbedingungen und relevante äußere Einflüsse beständig
  Die SRP/CS sind so ausgelegt, dass sie ihre Funktionen auch unter für die Anwendung üblichen äußeren Einflüssen ausführen können. Wichtige Kriterien sind z. B. mechanische Einflüsse, klimatische Einflüsse, Dichtigkeit des Gehäuses und EMI-Störfestigkeit.

- Prinzip der Energietrennung (Ruhestromprinzip)
  Der sichere Zustand wird durch Wegnahme des Steuersignals (elektrische Spannung, Druck), also durch Energieabschaltung, erreicht. Wichtige Kriterien sind z. B. sicherer Zustand bei Energieunterbrechung oder wirksame Federrückstellung bei Ventilen in der Fluidtechnik.

- Schutz gegen unerwarteten Anlauf
  Der unerwartete Anlauf, z. B. verursacht durch gespeicherte Energie oder nach Wiederherstellung der Energieversorgung, wird vermieden.

C.3.2 Beispiele für grundlegende Sicherheitsprinzipien in der Fluidtechnik

- Druckbegrenzung
  Der Anstieg des Drucks in einem System oder in Teilsystemen über ein festgelegtes Niveau hinaus wird in der Regel durch ein oder mehrere Druckbegrenzungsventile verhindert. In der Pneumatik werden dazu vorwiegend Druckregelventile mit Sekundärentlüftung eingesetzt.

- Maßnahmen zur Vermeidung von Verunreinigungen des Druckmediums
  Die für die verwendeten Bauteile erforderliche Reinheitsklasse des Druckmediums wird durch eine geeignete Einrichtung, meist ein Filter, erreicht. In der Pneumatik ist auch eine entsprechende Entwässerung erforderlich.

C.3.3 Beispiele für grundlegende Sicherheitsprinzipien in der Elektrik

- Richtige Schutzleiterverbindung
  Eine Seite des Steuerstromkreises, eine Klemme jedes elektromagnetisch betätigten Geräts oder eine Klemme anderer elektrischer Geräte ist mit einem Schutzleiter verbunden. Diese Seite des Geräts wird also nicht benutzt, um z. B. die Abschaltung einer gefahrbringenden Bewegung herbeizuführen. Ein Fehler durch Masseschluss kann daher nicht dazu führen, dass ein Abschaltpfad (unbemerkt) ausfällt.

- Unterdrückung von Spannungsspitzen
  Eine Einrichtung zur Unterdrückung von Spannungsspitzen (RC-Glied, Diode, Varistor) wird parallel zur Last (nicht parallel zu den Kontakten) geschaltet.

C.3.4 Beispiele für grundlegende Sicherheitsprinzipien in der Rechnertechnik/Software

DIN EN ISO 13849-2 beschreibt keine grundlegenden Sicherheitsprinzipien für den Einsatz von programmierbaren Systemen bzw. Software. Als solche können jedoch die sogenannten Basismaßnahmen für SRESW und SRASW nach den Abschnitten 7.3.1 und 7.4 der Norm verstanden werden (siehe hierzu auch Kapitel 9 in diesem Report). 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 „getriggerten“ Watchdogs, der die SRP/CS bei fehlerhaftem Programmablauf in einen definierten sicheren Zustand bringen können muss.

C.4 Bewährte Sicherheitsprinzipien

Die Tabellen A.2, B.2, C.2 und D.2 der informativen Anhänge der DIN EN ISO 13849-2:2013 behandeln bewährte Sicherheitsprinzipien. Ziel der Anwendung bewährter Sicherheitsprinzipien ist es, kritische Fehler oder Ausfälle zu minimieren oder auszuschließen und so die Häufigkeit von Fehlern oder Ausfällen, die die Sicherheitsfunktion beeinflussen, zu vermindern.

C.4.1 Allgemein für alle Technologien bewährte Sicherheitsprinzipien

- Überdimensionierung/Sicherheitsfaktor
  Alle Betriebsmittel werden unter Nennwert beansprucht. Ziel ist es, die Ausfallhäufigkeit 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 ein zwangläufiges Öffnen eines verschweißten Kontaktes bewirkt.

- Begrenzung elektrischer und/oder mechanischer Parameter
  Kraft-, Weg-, Zeit-, Strom-, Drehzahl- oder Geschwindigkeitsbegrenzungen werden durch elektrische, mechanische oder fluidtechnische Einrichtungen auf zulässige Werte reduziert. Ziel ist die Risikominderung durch verbesserte Gefahrenabwehr.

C.4.2 Beispiele für bewährte Sicherheitsprinzipien in der Fluidtechnik

- Gesicherte Position
  Das bewegliche Element eines Bauteils wird mechanisch in einer möglichen Position gehalten (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Kraft notwendig.

- Anwendung bewährter Federn
  DIN EN ISO 13849-2 führt in Tabelle A.2 detaillierte Anforderungen zu bewährten Federn auf.

C.4.3 Beispiele für bewährte Sicherheitsprinzipien in der Elektrik

- Begrenzung elektrischer Parameter
  Begrenzung von Spannung, Strom, Energie oder Frequenz zum Vermeiden eines unsicheren Zustands

- Vermeidung undefinierter Zustände
  Undefinierte Zustände im SRP/CS sind zu vermeiden. Das SRP/CS ist so zu konstruieren, dass sein Zustand während des üblichen Betriebs und unter allen zu erwartenden Betriebsbedingungen vorherbestimmt werden kann, z. B. durch Verwendung von Bauteilen mit definiertem Ansprechverhalten (Schaltschwellen, Hysterese) und mit definierter zeitlicher Abfolge.

- Trennung von Nicht-Sicherheitsfunktionen und Sicherheitsfunktionen
  Um unvorhergesehene Einflüsse auf Sicherheitsfunktionen auszuschließen, werden diese von Nicht-Sicherheitsfunktionen getrennt realisiert.

C.4.4 Beispiele für bewährte Sicherheitsprinzipien in der Rechnertechnik/Software

DIN EN ISO 13849-2 beschreibt keine bewährten Sicherheitsprinzipien für den Einsatz von programmierbaren Systemen bzw. Software. Als solche können jedoch die sogenannten zusätzlichen Maßnahmen für SRESW und SRASW nach den Abschnitten 7.3.1 und 7.4 der Norm verstanden werden (siehe hierzu auch Kapitel 9). Ein weiteres bewährtes Sicherheitsprinzip ist die Fehleraufdeckung in komplexen Bauelementen wie Mikrocontrollern durch Selbsttests. Tabelle E.1 der Norm zur Abschätzung des Diagnosedeckungsgrades listet solche Selbsttests wie Speichertests oder CPU-Tests. Informationen zur Realisierung solcher Tests enthält auch BGIA-Report 7/2006 [C7]. Abhängig von der Anwendung können auch „Fehlererkennung durch den Prozess“ und „Fehlererkennung durch Vergleich zwischen Kanälen“ als bewährte Sicherheitsprinzipien gelten.

C.5 Bewährte Bauteile

Bewährte Bauteile für Mechanik und Elektrik werden in Tabellen A.3 und D.3 der informativen Anhänge der DIN EN ISO 13849-2:2013 behandelt. Ziel der Verwendung bewährter Bauteile ist es, kritische Fehler oder Ausfälle zu minimieren oder auszuschließen und so die Häufigkeit von Fehlern oder Ausfällen, die die Sicherheitsfunktion beeinflussen, zu vermindern. Als allgemeine Kriterien für ein bewährtes Bauteil gelten gemäß Abschnitt 6.1.11 von DIN EN ISO 13849-1, dass das Bauteil

a) in der Vergangenheit weit verbreitet mit dokumentierten erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet wurde,
b) in ISO 13849-2:2012, Anhang A bis Anhang D aufgeführt ist oder
c) 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) dürfen im Sinne der Norm nicht als bewährt betrachtet werden. Die Einstufung als bewährtes Bauteil hängt auch von der Anwendung ab: In manchen Anwendungen kann ein Bauteil als bewährt gelten, wohingegen dies in anderen Anwendungen, z. B. aufgrund der Umgebungseinflüsse, ausgeschlossen werden muss.

C.5.1 Beispiel für ein bewährtes Bauteil in der Mechanik

- Feder
  Eine Feder gilt als bewährtes Bauteil, wenn die Angaben zu bewährten Sicherheitsprinzipien für die Anwendung bewährter Federn in DIN EN ISO 13849-2:2013, Tabelle A.2 eingehalten und weiterhin die technischen Festlegungen für Federstähle nach ISO 4960 [C8] berücksichtigt werden.

C.5.2 Beispiele für bewährte Bauteile in der Fluidtechnik

DIN EN ISO 13849-2 benennt für die Fluidtechnik keine bewährten Bauteile. Die Eigenschaft, bewährt zu sein, hängt insbesondere von der speziellen Anwendung sowie von der Einhaltung der Anforderungen zu bewährten Bauteilen der Kategorie 1 und Anforderungen aus den Normen DIN EN 4413 [C9] und DIN EN 4414 [C10] ab.

Sicherheitstechnisch bewährte Bauteile können z. B. sein
- Wegeventile, Sperrventile und Druckventile.

C.5.3 Beispiele für bewährte Bauteile in der Elektrik

- Sicherung
  Eine Sicherung ist eine Überstromschutzeinrichtung, die einen Stromkreis bei zu hoher Stromstärke, z. B. infolge eines Isolationsfehlers, unterbricht (Prinzip der Energietrennung). Zu unterscheiden sind Schmelzsicherungen sowie ersatzweise Leitungsschutzschalter. Sicherungen haben sich seit Jahrzehnten als Überstromschutzeinrichtungen bewährt. Für Sicherungen existieren umfangreiche Bestimmungen [C11; C12]. Versagensfälle von Sicherungen sind bei bestimmungsge-

mäßem 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 [C13]. Den Geräten gemeinsam ist die Ausrüstung mit zwangsöffnenden Hilfsstromschaltern zur Energieunterbrechung nach Anhang K in DIN EN 60947-5-1 [C14]. Zwei Arten von Hilfsstromschaltern mit Zwangsöffnung werden unterschieden:
  – Typ 1: Mit nur einem Schaltglied, das als zwangsöffnender Kontakt ausgeführt ist.
  – Typ 2: Mit einem oder mehreren Öffnern und möglicherweise mit einem oder mehreren Schließern und/oder einem oder mehreren Wechslern. Alle Öffnerkontakte einschließlich der Öffnerteile der Wechsler müssen zwangläufig öffnende Schaltglieder haben.

  Zu weiteren Details, insbesondere zur Modellierung von Not-Halt-Geräten, siehe Anhang D.2.5.4.

- Schalter mit zwangläufigem Betätigungsmodus (direkt öffnend)
  Diese besondere Art der Schalter wird als Tastschalter, Positionsschalter und als Wahlschalter mit Nockenbetätigung, z. B. zur Anwahl von Betriebsarten, auf dem Markt angeboten. Die Schalter haben sich seit Jahrzehnten bewährt. Ihnen zugrunde liegt das bewährte Sicherheitsprinzip des zwangläufigen Betätigungsmodus durch zwangsöffnende Kontakte. Als bewährtes Bauteil muss der Schalter den Anforderungen der DIN EN 60947-5-1, Anhang K entsprechen.

Literatur

[C1] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (2/2013). DIN Media, Berlin 2013

[C2] DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (11/2017). DIN Media, Berlin 2017

[C3] DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (6/2021). DIN Media, Berlin 2021

[C4] *Bömer, T.; Grigulewitsch, W.; Kühlem, W.; Meffert, K.; Reuß, G.*: Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Kennzahl 340 220. In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Lfg. 1/16, VI/2016. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.ifa-handbuchdigital.de/340220

[C5] Measuring whisker growth on tin and tin alloy surface finishes, JESD22-A121A. Hrsg.: JEDEC Solid State Technology Association, Arlington, USA 2008

[C6] Environmental acceptance requirements for tin whisker susceptibility of tin and tin alloy surface finishes, JESD201A. Hrsg.: JEDEC Solid State Technology Association, Arlington, USA 2008

[C7] *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. https://www.dguv.de/medien/ifa/de/pub/rep/pdf/rep05/biar0706/report7_2006.pdf

[C8] ISO 4960: Kaltband aus unlegierten Stählen mit Kohlenstoffgehalten über 0,25 % (7/2019). DIN Media, Berlin 2019

[C9] DIN EN ISO 4413: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile (4/2011). DIN Media, Berlin 2011

[C10] DIN EN ISO 4414: Fluidtechnik – Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile (4/2011). DIN Media, Berlin 2011

[C11] DIN EN 60269-1: Niederspannungssicherungen – Teil 1: Allgemeine Anforderungen (5/2015). DIN Media, Berlin 2015

[C12] DIN EN 60127-1: Geräteschutzsicherungen – Teil 1: Begriffe für die Geräteschutzsicherungen und allgemeine Anforderungen an G-Sicherungseinsätze (12/2015). DIN Media, Berlin 2015

[C13] DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt-Funktion – Gestaltungsleitsätze (5/2016). DIN Media, Berlin 2016

[C14] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (3/2018). DIN Media, Berlin 2018

Anhang D

Mean Time to Dangerous Failure ($MTTF_D$)

Änderung gegenüber dem IFA Report 2/2017

- In D.1.3 Hinweise zu Felddaten als alternative $MTTF_D$-Datenquelle hinzugefügt
- In D.2.4.1 Erläuterungen zur Umrechnung von B_{10} in B_{10D} sowie T_{10} in T_{10D} mittels RDF (Anteil gefahrbringender Ausfälle) ergänzt
- Erläuterungen in D.2.4.1 und D.2.4.2 zur $MTTF_D$-Näherung für Verschleißbauteile überarbeitet, einschließlich Abbildung D.3 und des neuen Kastens D.1
- Neue Abschnitte D.2.5.7 (Drucktaster für die manuelle Rückstellung) und D.2.5.8 (Drucktaster für Zweihandschaltungen) hinzugefügt
- Literaturhinweise aktualisiert

D.1 Was bedeutet „$MTTF_D$“?

Die mittlere Zeit bis zum gefahrbringenden Ausfall (Mean Time to Dangerous Failure, $MTTF_D$) ist ein Maß für die Zuverlässigkeit der in einer Steuerung verwendeten Bauteile und fließt als einer von mehreren Parametern in die Bestimmung des Performance Levels (PL) ein. Die von DIN EN ISO 13849-1 verwendete Definition der $MTTF_D$ als „Mittlere Dauer bis zum gefahrbringenden Ausfall“ beinhaltet mehrere Aspekte:

- $MTTF_D$ 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 Funktionskanäle die Sicherheitsfunktion aus (Redundanz), so spricht man auch von einem „gefahrbringenden Ausfall“, wenn nur ein einzelner Funktionskanal betroffen ist.

D.1.1 Badewannenkurve und konstante Ausfallrate

Eine übliche Form der Beschreibung von Bauteilzuverlässigkeiten ist die Angabe von Ausfallraten, abgekürzt λ (nur auf gefahrbringende Ausfälle bezogen entsprechend λ_D), mit der gebräuchlichen Einheit FIT (Failures In Time, d. h. Anzahl der Ausfälle pro intaktem Bauteil in 10^9 Bauteilstunden, 1 FIT = 10^{-9}/h). Diese Ausfallrate beschreibt zu einem bestimmten Zeitpunkt die Rate, mit der der vorgefundene funktionsfähige Anteil der Bauteile gerade ausfällt. Das heißt, die absolute Zahl der Ausfälle je Zeiteinheit wird durch die Anzahl der zum jeweiligen Zeitpunkt noch ausfallfreien Bauteile geteilt. Das Ausfallverhalten vieler Arten von Bauteilen stellt sich in Abhängigkeit von der Zeit als mehr oder weniger ausgeprägte „Badewannenkurve“ dar [D1] (siehe **Abbildung D.1**).

Oft fallen am Anfang der Gebrauchsdauer verstärkt Bauteile aus. Dies sind Frühausfälle, die aber nur für kurze Zeit dominieren. Nach einer gewissen Zeit des Betriebs steigen bei vielen Bauteilen die Ausfälle wieder an. Im mittleren Bereich der üblichen Gebrauchsdauer ist insbesondere bei elektronischen Bauelementen oft eine zeitkonstante Ausfallrate zu beobachten. Dieser Bereich 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

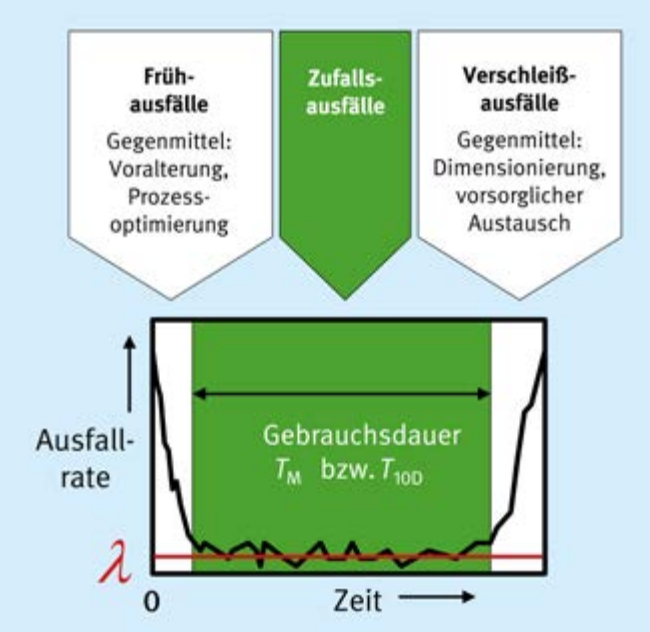


Abb.D.1 „Badewannenkurve“ der Ausfallrate

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 zeitkonstanten 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*), der dem Kehrwert der Ausfallrate entspricht. Bezogen allein auf die gefahrbringenden Ausfälle bedeutet dies:

$$MTTF_D = \frac{1}{\lambda_D} \qquad \text{(D.1)}$$

Hierbei verweist der Index D für „dangerous“ darauf, dass Ausfälle in die gefahrbringende Richtung gemeint sind.

Bei konstanter Ausfallrate ist also die Angabe der $MTTF_D$ der Angabe einer Ausfallrate gleichwertig, sie ist jedoch viel illustrativer. Während die praktische Bedeutung eines FIT-Wertes wenig anschaulich ist, vermittelt die Angabe eines zeitlichen Erwartungswertes in Jahren eher eine Vorstellung von der Bauelementgüte. **Abbildung D.2** zeigt den zeitlichen Verlauf der Wahrscheinlichkeit eines gefahrbringenden Ausfalls 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. Der anfangs steile und dann abflachende Anstieg der Ausfallwahrscheinlichkeit ergibt sich durch die mit der Zeit abnehmenden Zahl funktionsfähiger Bauteile, die noch ausfallen können. Dieser Verlauf bringt es mit sich, dass bis zum Zeitpunkt $MTTF_D$, der mittleren Zeit bis zum gefährlichen Ausfall, bereits mehr als 50 % der gefährlichen Ausfälle stattfinden.

Das vereinfachte Quantifizierungsverfahren nach DIN EN ISO 13849-1 unterstellt eine übliche Gebrauchsdauer von maximal 20 Jahren für Bauteile in Sicherheitssteuerungen im Maschinenbau. Vor diesem Hintergrund und bei Kenntnis des zeitlichen Verlaufs der Ausfallrate (Abbildung D.1) wird verständlich, dass die Angabe eines $MTTF_D$-Wertes nur als illustrative Kennzeichnung für das Zuverlässigkeitsniveau innerhalb der Gebrauchsdauer verstanden werden sollte und weder eine Garantie für eine ausfallfreie Zeit vor Erreichen der $MTTF_D$ noch eine exakte Vorhersage für den Ausfallzeitpunkt eines Einzelbauteils bietet. Ist der Verschleißbereich erreicht, ändert sich das Ausfallverhalten grundlegend und kann nicht mehr sinnvoll durch eine konstante Ausfallrate beschrieben werden.

D.1.2 Klasseneinteilung und Begrenzung

Wenn kein Fehlerausschluss begründet werden kann, ist für jedes sicherheitsrelevante Bauteil die Kenntnis

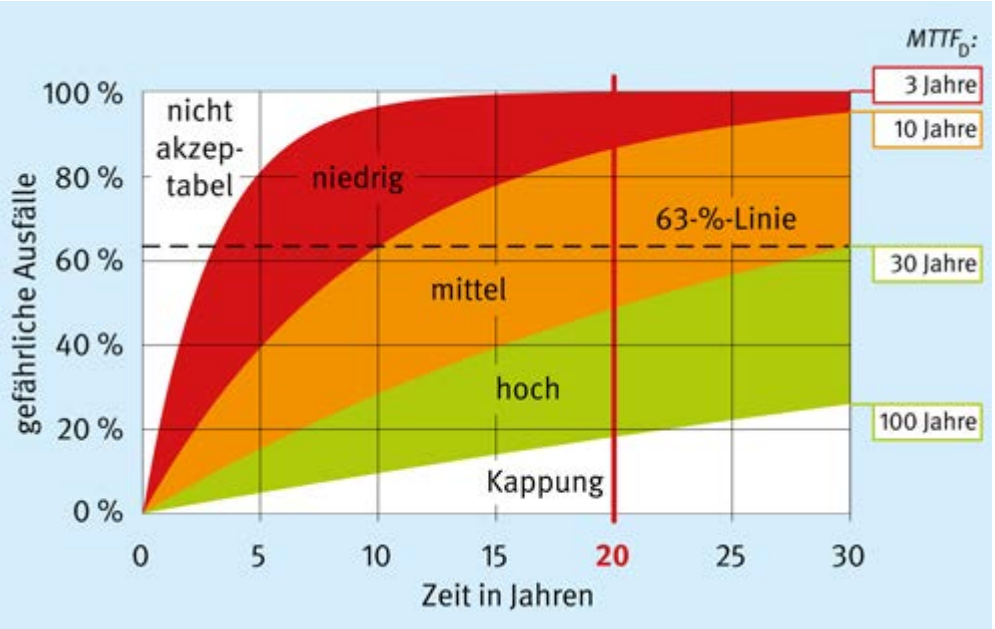


Abb. D.2
Illustration der $MTTF_D$

einer $MTTF_D$, notfalls eines Schätzwertes dafür, Voraussetzung für die nachfolgenden Schritte. Sie führen zunächst auf Block- und dann auf Kanalebene zur sogenannten $MTTF_D$ jedes Kanals. Für die Kanalebene sieht DIN EN ISO 13849-1 die Einteilung in drei $MTTF_D$-Klassen vor (**Tabelle D.1**). Diese Klassen sollen kleine Unterschiede in den errechneten $MTTF_D$-Werten nivellieren, die ohnehin innerhalb der statistischen Unsicherheit untergehen. Des Weiteren wird damit eine gleichartige Behandlung wie bei den anderen Parametern (fünf Kategorien, vier *DC*-Stufen) erreicht und ebenso die notwendige Vereinfachung für die Darstellung im Säulendiagramm.

Tabelle D.1 Klasseneinteilung der $MTTF_D$ für Kanäle, die die Sicherheitsfunktion ausführen

Bezeichnung der $MTTF_D$ für jeden Kanal	Bereich der $MTTF_D$ für jeden Kanal
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre

Gewünschte Nebeneffekte dieser Klassenbildung sind die Zurückweisung von $MTTF_D$-Werten jedes Kanals < 3 Jahre und die Beschränkung höherer $MTTF_D$-Werte jedes Kanals auf maximal 100 Jahre (in Kategorie 4 wird diese Beschränkung auf 2500 Jahre angehoben; auch diese Werte sind der Klasse „hoch“ zuzuordnen). Abbildung D.2 macht deutlich, dass bei einer $MTTF_D$ von drei Jahren schon nach einem Jahr fast 30 % gefahrbringende Ausfälle zu erwarten sind, was für eine Sicherheitssteuerung inakzeptabel ist. Am anderen Ende des Spektrums erscheint ein statistisch abgesicherter Nachweis einer Zuverlässigkeit, die mehr als 100 Jahren $MTTF_D$ entspricht, sehr fragwürdig. (In Kategorie 4 ist dies akzeptabel, da die anderen Einflussparameter für die Zuverlässigkeit wie Redundanz und Fehlererkennung schon ein hohes Niveau haben.) Außerdem bleibt selbst bei beliebig hohen $MTTF_D$-Werten eine Restwahrscheinlichkeit für einen gefahrbringenden Ausfall innerhalb der Gebrauchsdauer, der darüber hinaus auch aus anderen Gründen auftreten kann (z. B. durch Fehlanwendung). Daher wird die Absicherung hoher Performance Level allein durch Verwendung hoch zuverlässiger Bauteile ohne entsprechende Redundanz und Fehlererkennung als nicht angemessen betrachtet. 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 Berechnung der Ausfallhäufigkeit möglich wäre. Die Rückstufung höherer $MTTF_D$-Werte auf den Maximalwert von 100 bzw. 2500 Jahren findet erst auf Kanalebene statt, d. h. für einzelne Bauteile können deutlich höhere $MTTF_D$-Werte in die Berechnung einfließen.

D.1.3 Woher kommen die Daten?

Ein mögliches Problem für die Normanwendung sind fehlende $MTTF_D$-Angaben für im SRP/CS verwendete Bauteile [D2]. Grundsätzlich schlägt die Norm in Abschnitt 6.1.4 eine Hierarchie von Datenquellen vor:

- An erster Stelle stehen Herstellerangaben, die am verlässlichsten die Ausfallhäufigkeit beschreiben. Üblicherweise nennt der Bauteilhersteller im Datenblatt und seinen Anwendungshinweisen auch die dabei zu berücksichtigenden Voraussetzungen und Grenzen. Gibt ein Hersteller dezidiert eine $MTTF_D$ bzw. eine Ausfallrate λ_D an, so ist diese an eine bestimmte Ausfallart geknüpft. Der Bauteilanwender kann diese Angabe jeweils dann verwenden, wenn die genannte Ausfallart auch in seiner Anwendung die gefährliche Ausfallrichtung darstellt.
- An zweiter Stelle folgen dann typische Zahlenwerte, die nach dem Verfahren guter ingenieurmäßiger Praxis erfahrungsgemäß erreicht werden. Sie sind in der Norm in Anhang C selbst gelistet. Diese sind zur sicheren Seite hin abgeschätzt und an die Erfüllung der grundlegenden und (ab Kategorie 1) bewährten Sicherheitsprinzipien geknüpft (Details dazu folgen in D.2.5).
- An dritter Stelle wird seit der vierten Normausgabe eine weitere Möglichkeit genannt, die herangezogen werden kann, wenn die beiden vorher genannten Optionen nicht nutzbar sind. Verlässliche Felddaten für identische Bauteilanwendungen aus vergleichbaren Umgebungen können als Datenquelle dienen, wenn sie mit ausreichender statistischer Sicherheit gewonnen wurden. Die Norm gibt an dieser Stelle einen Hinweis auf Abschnitt B.5.4 der DIN EN 61508-7, die unter dem Stichwort „Felderfahrung“ strenge Bedingungen an den statistischen Nachweis anführt.
- An letzter Stelle kann schließlich ein sehr konservativ abgeschätzter Ersatzwert von zehn Jahren angesetzt werden. 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, ist diese letzte Option von geringer praktischer Relevanz.

Vor diesem Hintergrund sind die in der Norm selbst gelisteten $MTTF_D$-Werte nach dem Verfahren guter ingenieurmäßiger Praxis von besonderer Bedeutung. Dies gilt zumindest noch so lange, bis die Angabe von $MTTF_D$-Werten vonseiten der Hersteller zur Selbstverständlichkeit wird – auch für Bauteile, die nicht von vornherein für die Verwendung in SRP/CS entwickelt wurden.

D.2 Unterschiede der Technologien

Das Ausfallverhalten von Bauteilen hängt naturgemäß sehr stark von der eingesetzten Technologie ab, da die „Badewannencharakteristik“ und die Bedeutung von Verschleißeffekten unterschiedlich stark ausgeprägt sein können. Bei mechanischen und hydraulischen Komponenten, die von der Konstruktion und der Anwendung auf hohe Zuverlässigkeit und geringen Verschleiß optimiert werden, kann von einer sehr hohen $MTTF_D$ ausgegangen werden. Hier spielen Zufallsausfälle (der Bereich konstanter Ausfallrate) und Verschleißausfälle eine geringere Rolle. Bei den meisten elektronischen Komponenten hingegen ist das Ausfallverhalten innerhalb der typischen Einsatzdauer vergleichsweise preisgünstiger industrieller Komponenten normalerweise sehr gut durch eine konstante Ausfallrate beschrieben, da der Verschleißbereich nur bei verschärften Einsatzbedingungen außerhalb der spezifizierten Grenzen erreicht wird. Ein solcher Betrieb widerspricht jedoch den bei allen Kategorien einzuhaltenden grundlegenden Sicherheitsprinzipien. 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 Ausfallrate. Allen diesen technologieabhängigen Besonderheiten muss bei der Bestimmung des $MTTF_D$-Wertes Rechnung getragen werden, sodass die Norm hier unterschiedliche Herangehensweisen vorschlägt.

D.2.1 $MTTF_D$ mechanischer Steuerungskomponenten

Der Ansatz konstanter Ausfallraten ist für mechanische Steuerungskomponenten leider wenig geeignet. Andererseits enthält fast jede Sicherheitsfunktion zumindest im Bereich der Sensoren oder Aktoren mechanische Steuerungselemente, die z. B. Bewegungen oder Kräfte übertragen, um eine Information weiterzugeben oder um eine gefahrbringende Bewegung stillzusetzen. 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 effizienteste Methode, um die Zuverlässigkeit der mechanischen Komponenten zu berücksichtigen [D3]. Zu diesen Voraussetzungen gehört u. a. die ausreichende Widerstandsfähigkeit gegenüber den zu erwartenden Umwelteinflüssen, d. h. die Gültigkeit eines Fehlerausschlusses hängt immer von der gewählten Applikation ab. Eine andere Voraussetzung ist z. B. ausreichende Überdimensionierung, die sicherstellt, dass die mechanischen Komponenten nur im Bereich der Dauerfestigkeit belastet werden. Falls ein Fehlerausschluss nicht möglich ist, bietet eventuell die Anwendung des in D.2.5 beschriebenen Verfahrens guter ingenieurmäßiger Praxis die Möglichkeit, einen $MTTF_D$-Wert abzuschätzen.

D.2.2 BIA-Report 6/2004 „Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen“

Bei hydraulischen Anlagen ist als „sicherheitsbezogener Teil der Steuerung“ insbesondere der Ventilbereich zu betrachten. Dabei müssen speziell jene Ventile bei der Berechnung der *PFH* berücksichtigt werden, die direkt oder über weitere Elemente gefahrbringende Bewegungen oder Zustände steuern. 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 Überbeanspruchung, ungünstige Einsatzbedingungen oder fehlende Wartung – also Ursachen, die durch Nichteinhaltung der in allen Kategorien geforderten grundlegenden Sicherheitsprinzipien entstanden sind. Um die Lebensdauer hydraulischer Ventile unter realen, nicht durchweg perfekten Bedingungen besser abschätzen zu können, initiierte das IFA (damals noch BGIA) eine Diplomarbeit zu diesem Thema, deren Ergebnisse als BIA-Report 6/2004 „Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen“ [D4] vorliegen. Da es sich bei Ventilen, die Steuerungsaufgaben übernehmen, in der Mehrzahl um Wegeventile in Schieberbauweise handelt, wurden die $MTTF_D$-Werte für „hydraulische Bauteile“ stellvertretend für die Mehrzahl der Anwendungsfälle überwiegend an solchen Ventilen ermittelt. Die wichtigsten Ergebnisse dieser Untersuchung werden im Folgenden kurz vorgestellt:

Die Grundlage für die Abschätzung eines $MTTF_D$-Wertes bilden in erster Linie die Ausfallraten von hydraulischen Wege-Schieberventilen, die im Rahmen einer Untersuchung in den Instandhaltungsabteilungen zweier großer Hydraulikanwender ermittelt wurden (im Folgenden Anwender A und B genannt). Dies erfolgte durch Auswertung von EDV-Daten (Neubeschaffungsmengen von hydraulischen Wegeventilen in Schieberbauweise und Reparaturberichten) und Mitwirkung bei Instandhaltungsarbeiten. Zusätzlich zu den Ausfalldaten der Ventile wurden die Einsatzbedingungen berücksichtigt. Somit ist die Vergleichbarkeit der bei den jeweiligen Hydraulikanwendern ermittelten $MTTF_D$-Werte gegeben. Zur Absicherung und Bestätigung dieser Daten wurden darüber hinaus durch eine Umfrage unter Ventilherstellern zusätzliche Ausfalldaten gesammelt. Bei Anwender A wurden die Ausfallraten der Wegeventile in der Instandhaltungsabteilung der Getriebefertigung erfasst. Verfügbar waren die Daten aller ausgefallenen Wegeventile über einen Zeitraum von 38 Monaten, in dem es 143 Ausfälle von Wegeventilen gab. In den Maschinen der Getriebefertigung, größtenteils Werkzeugmaschinen, waren ungefähr 8 050 Wegeventile unterschiedlichen Alters im Einsatz. Wenn in dieser Zeitspanne eine konstante Ausfallrate unterstellt wird, lässt sich aus den Daten für Anwender A eine $MTTF_D$ von 178 Jahren als Kehrwert der Ausfallrate errechnen. Bei

diesem Anwender wurden die Einsatzbedingungen an den Hydraulikanlagen weitgehend nach den Vorgaben der Hersteller eingehalten. Da es sich vorwiegend um neue Fertigungsstraßen handelte, erfolgte eine zustandsorientierte Instandhaltung.

Bei Anwender B wurden die Ausfalldaten für die Wegeventile ebenfalls in der Instandhaltungsabteilung der Getriebefertigung aufgenommen. Hier waren ungefähr 25 000 Wegeventile unterschiedlichen Alters im Einsatz. Verfügbar waren die Daten aller ausgefallenen Wegeventile in einem Zeitraum von vier Jahren (2000 bis 2003). Im Gegensatz zum Anwender A waren hier die Ausfalldaten für jedes Jahr einzeln abrufbar. Somit war es möglich, eine $MTTF_D$ für jedes einzelne Jahr zu bestimmen. Dabei stieg die $MTTF_D$ von 195 Jahren im Jahr 2000 auf 300 in 2003. Es zeigte sich ein signifikanter Zusammenhang zwischen Ventilausfällen und Einsatz- bzw. Umgebungsbedingungen, denn Anwender B hatte seine Instandhaltungsmaßnahmen und Einsatzbedingungen im Laufe der Jahre kontinuierlich verbessert. Des Weiteren wurden gegenüber Anwender A die Einsatzbedingungen durch zusätzliche Maßnahmen verbessert, z. B. Überwachung der Öltemperatur, größere meist außerhalb der Maschine untergebrachte Öltanks, feinere Rücklauffilter sowie Abzugsanlagen zur Minderung der Verunreinigungen in der Umgebungsluft. Die Untersuchung zeigte, dass die zylindrischen Führungen der Bauteile in Ventilen, z. B. Steuerschieber, in Verbindung mit Art, Qualität und Verschmutzungsgrad der eingesetzten Druckflüssigkeit sowie Auslegung, Material und Ausführung der Zentrier-/Rückstellfeder einen wesentlichen Einfluss auf die zu erwartende Lebensdauer hydraulischer Wege-Schieberventile haben. Dabei wurde ein deutlicher Zusammenhang zwischen Qualität der Einsatzbedingungen und der erreichten Lebensdauer bis zum Ausfall über einen definierten Betrachtungszeitraum festgestellt.

D.2.3 $MTTF_D$ hydraulischer Steuerungskomponenten

Aufgrund der Ergebnisse der oben genannten Untersuchung wird in DIN EN ISO 13849-1 für hydraulische Bauteile unter bestimmten Voraussetzungen eine $MTTF_D$ von 150 bis 1200 Jahren vorgeschlagen. Zwar wurden schwerpunktmäßig Ventile in Schieberbauweise untersucht, aufgrund des ähnlichen Ausfallverhaltens lässt sich die ermittelte $MTTF_D$ aber als gute Abschätzung für alle sicherheitsrelevanten hydraulischen Ventile verwenden. Voraussetzung hierfür ist allerdings die Einhaltung der in DIN EN ISO 13849-2 aufgeführten, auf hydraulische Ventile bezogenen grundlegenden und bewährten Sicherheitsprinzipien bei Konstruktion und Herstellung. Weiterhin müssen die ebenfalls in DIN EN ISO 13849-2 aufgeführten anwendungsbezogenen grundlegenden und bewährten Sicherheitsprinzipien vom Ventilhersteller genannt (Herstellervorgaben, Einsatzbedingungen) und in der Praxis eingehalten werden.

Anhang C.2, Tabelle C.1 der DIN EN ISO 13849-2 nennt die grundlegenden Sicherheitsprinzipien für hydraulische Systeme. Zu den wichtigsten Prinzipien gehören die Anwendung geeigneter Werkstoffe und Herstellungsverfahren sowie das Prinzip der Energietrennung, Druckbegrenzung, Schutz gegen unerwarteten Anlauf und Betrieb im geeigneten Temperaturbereich (weitere Erläuterungen siehe Anhang C).

Anhang C.3, Tabelle C.2 der DIN EN ISO 13849-2 listet bewährte Sicherheitsprinzipien für hydraulische Systeme auf. Die wichtigsten Prinzipien umfassen Überdimensionierung/Sicherheitsfaktoren, Begrenzung/Verringerung der Geschwindigkeit durch einen Widerstand zum Erreichen eines definierten Volumenstroms, Begrenzung/Verringerung der Kraft, einen geeigneten Bereich für die Betriebsbedingungen, Überwachung des Zustands des Druckmediums, Verwendung bewährter Federn und eine ausreichend große positive Überdeckung in Schieberventilen (weitere Erläuterungen siehe ebenfalls Anhang C).

Die Erfahrung mit der Anwendung der zweiten Edition der Norm hat gezeigt, dass für Hydraulikventile auch die Betätigungshäufigkeit n_{op} (Anzahl der jährlichen Betätigungen, siehe Abschnitt D.2.4) ein für die Zuverlässigkeit relevanter Parameter ist. Daher werden in der dritten Edition der Norm im Rahmen des Verfahrens guter ingenieurmäßiger Praxis (siehe Abschnitt D.2.5) abhängig von n_{op} abgestufte $MTTF_D$-Werte für Hydraulikventile zwischen 150 und 1200 Jahren angegeben (siehe Tabelle D.2).

Auch wenn die Norm unter diesen Voraussetzungen $MTTF_D$-Werte für hydraulische Ventile angibt, sollte jeder Hersteller von Ventilen für seine Bauteile möglichst eigene Ausfallzahlen ermitteln und eine eigene $MTTF_D$ angeben.

D.2.4 $MTTF_D$ pneumatischer und elektromechanischer Steuerungskomponenten

Bei häufig betätigter Pneumatik und Mechanik wird die Lebensdauer bzw. die Zuverlässigkeit der Komponenten vornehmlich vom Verschleißverhalten der bewegten Elemente und deren Führungselementen bestimmt. Bei häufig betätigter Elektromechanik begrenzt der Kontaktverschleiß, abhängig von der Schaltlast, die Lebensdauer.

Bei Ventilen, die meistens komplexe Einheiten mit vielen beweglichen Elementen (z. B. Schieber, Stößel, Federn in Vorsteuerstufe und Hauptstufe) darstellen, können auch die Umgebungsbedingungen während des Betriebs die Lebensdauer stark beeinflussen. Hier sind insbesondere zu nennen:

- Qualität und Zustand des Druckmediums (Druckluft),
- Verträglichkeit von Dichtungen mit den Schmierstoffen,
- Umgebungstemperatur,
- Kontakt mit schädlichen Substanzen, z. B. mit Stäuben, Gasen, Flüssigkeiten.

Auf die Einhaltung der vom Hersteller der Komponenten spezifizierten Anforderungen ist unbedingt zu achten, damit die bei der Ermittlung der Steuerungskategorie zugrunde gelegten Annahmen bezüglich des Ausfallverhaltens der Komponente zutreffend sind.

Bei den elektromechanischen Schützen unterscheidet man zwischen Hilfsschützen und Leistungsschützen. Hilfsschütze werden zur Realisierung logischer Verknüpfungen und zur Ansteuerung von Leistungsschützen eingesetzt. Für das Schalten größerer Leistungen wie von Motoren > 3 kW werden üblicherweise Leistungsschütze eingesetzt. Für Hilfsschütze gelten die Bestimmungen aus DIN EN IEC 60947-5-1 und für Leistungsschütze aus DIN EN IEC 60947-4-1.

Für die Auswahl und den Einsatz ist eine Reihe von Kriterien zu beachten. Dies sind insbesondere:
- Netz- und Betriebsbedingungen,
- Schaltaufgaben und -bedingungen,
- Schalthäufigkeit und Lebensdauer,
- Schutz vor Überstrom und Übertemperatur,
- Schutz vor Überspannungen,
- ggf. vorgeschriebene Einbaulage,
- spezielle Einsatzbedingungen, z. B Betrieb in aggressiver Umgebungsluft.

Die Hersteller geben in speziellen Handbüchern umfassende Hinweise zur Auswahl und Projektierung.

Im Rahmen der Quantifizierung nach DIN EN ISO 13849 wird an dieser Stelle kurz auf die Auswahlkriterien zur Lebensdauer eingegangen. Man unterscheidet zwischen der mechanischen und der elektrischen Lebensdauer. Die mechanische Lebensdauer eines Schützes wird durch die Schaltspielzahl ausgedrückt, die das Schütz ohne Belastung der Strombahnen erreicht. Sie hängt vom Verschleiß der mechanisch bewegten Teile ab.

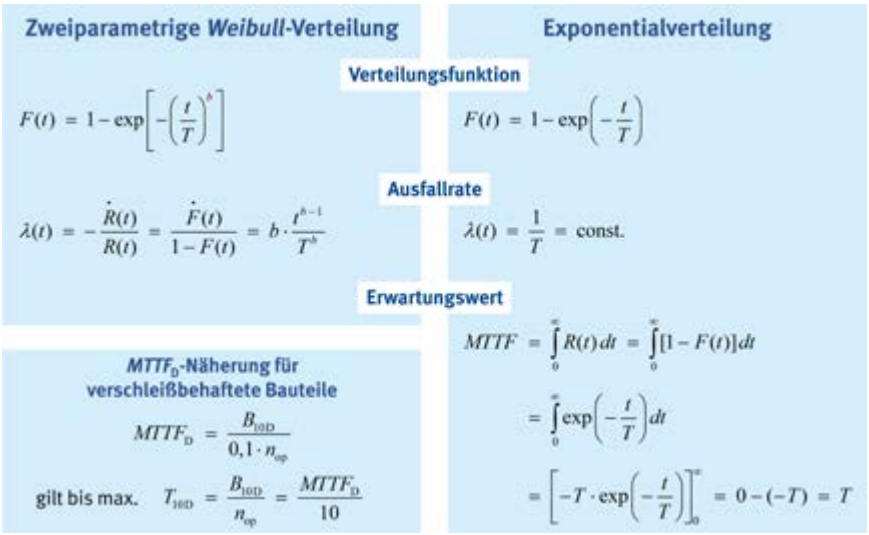
Die elektrische Lebensdauer eines Schaltgeräts wird durch die Anzahl der Schaltspiele festgelegt, nach der die elektrischen Schaltkontakte abgenutzt sind. Die elektrischen Schaltkontakte werden beim Schalten unter Last sowohl beim Einschalt- als auch beim Ausschaltvorgang beansprucht. Der dabei auftretende Kontaktabbrand verursacht den Verschleiß der Schaltstücke. Er ist abhängig von Spannung, Strom, Last (z. B. induktiv) und Zeit. Bei vollständigem Kontaktabbrand kommt es in der Regel zu einem Verschweißen der Kontakte. Dies muss in sicherheitsrelevanten Anwendungen ab Steuerungskategorie 2 detektiert werden, um gefahrbringende Zustände durch das Nichtöffnen zu verhindern. Für die Detektion sind Schütze mit zwangsgeführten Kontakten bei Hilfsschützen oder sogenannten Spiegelkontakten bei Leistungsschützen einzusetzen. Hierzu sind die Angaben des Herstellers zu beachten.

Die mechanische Lebensdauer und die elektrische Lebensdauer der Schaltstücke werden von den Herstellern separat ermittelt. Üblich ist die Angabe der Lebensdauer in Form des sogenannten B_{10}-Wertes, der die mittlere Schaltspielzahl bis zum Ausfall von 10 % der Einheiten angibt. Bezieht sich die Angabe auf Ausfälle in die gefährliche Richtung (zumeist das Nichtöffnen der Kontakte), so lautet die Bezeichnung B_{10D}. Die in einer Applikation tatsächlich erreichte Lebensdauer eines Schützes, die auch Gerätelebensdauer genannt wird, ist der kleinere der beiden Werte mechanische Lebensdauer und elektrische Lebensdauer, wobei die letztere von der Größe und Art der Schaltlast (deren Wechselstromwiderstand) abhängig ist. Oft ist die elektrische Lebensdauer deutlich kleiner als die mechanische und somit maßgeblich.

Die in Tabelle D.2 (Seite 251) dieses Reports angegebenen sogenannten B_{10D}-Werte (siehe Abschnitt D.2.4.1) für die Gerätelebensdauer sind als Anhaltswerte zu sehen. Es sind bevorzugt die Angaben des Herstellers zu verwenden. Gibt ein Hersteller selbst keinen B_{10D}-Wert an, wohl aber Werte (Anzahl Schaltzyklen) für die mechanische und die elektrische Lebensdauer, so kann der kleinere dieser Werte als Schätzwert für den B_{10}-Wert angenommen werden. Durch Verdoppelung kann daraus der B_{10D}-Wert ermittelt werden (siehe Abschnitt D.2.4.1).

Sind die folgenden Merkmale erfüllt, so kann der $MTTF_D$-Wert für ein einzelnes pneumatisches, elektromechanisches oder mechanisches Bauteil nach den weiter unten aufgeführten Formeln abgeschätzt werden:
- Der Hersteller des Bauteils bestätigt die Verwendung grundlegender Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabelle B.1 oder Tabelle D.1 für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller eines Bauteils, das in einer Steuerung der Kategorie 1, 2, 3 oder 4 verwendet werden soll, bestätigt die Verwendung bewährter Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabellen B.2 oder D.2 für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für die SRP/CS-Konstruktion und die Anwendung fest. Der SRP/CS-Konstrukteur erfüllt die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabellen B.1 oder D.1 für die Implementierung und den Betrieb des Bauteils und informiert den Anwender über seine Verantwortung, die von ihm umzusetzenden Sicherheitsprinzipien zu erfüllen. Bei den Kategorien 1, 2, 3 und 4 gilt dieselbe Verpflichtung auch hinsichtlich der Einhaltung der bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013, Tabellen B.2 oder D.2 und dies wiederum bei Implementierung und Betrieb des Bauteils.

Kasten D.1



Kenngrößen der Weibull-Verteilung mit Formfaktor b und charakteristischer Lebensdauer *T* im Vergleich zur Exponentialverteilung (b = 1), mit Verteilungsfunktion $F(t)$, Zuverlässigkeitsfunktion $R(t) = 1 - F(t)$, Ausfallrate $\lambda(t)$ und Erwartungswert der ausfallfreien Zeit *MTTF*; links unten ist die $MTTF_D$-Näherung für verschleißbehaftete Bauteile und ihre Gültigkeitsgrenze T_{10D} angegeben.

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 die maßgeblichen Einflussparameter festgelegt werden. Dies können zurückgelegte Strecken für Pneumatikzylinder, Betätigungshäufigkeiten für Ventile oder elektromechanische Bauteile und Lastwechsel bei mechanischen Komponenten sein. Üblicherweise wird die Zuverlässigkeit für pneumatische oder elektromechanische Bauteile im Labor bestimmt.

D.2.4.1 Bestimmung des Lebensdauerkennwertes B_{10D}

Mit im Labor oder eventuell auch bei Felduntersuchungen ermittelten Werten kann die Ausfallhäufigkeit verschleißbehafteter Bauteile z. B. mithilfe der *Weibull*-Statistik bestimmt werden [D5, D6]. Die in **Kasten D.1** beschriebene und in **Abbildung D.3** dargestellte zweiparametrige *Weibull*-Verteilungsfunktion ist flexibler als die Exponentialverteilung, die sie als Spezialfall (b = 1, $T = 1/\lambda$) enthält. Ein Ansteigen der Ausfallrate bei Erreichen der Verschleißphase (rot unterlegter Bereich rechts von T_{10D}) lässt sich durch b-Parameter > 1 gut beschreiben. Der *T*-Parameter beschreibt die charakteristische Lebensdauer, bei der 63,2 % der betrachteten Bauteile ausgefallen sind (außerhalb des in Abbildung D.3 dargestellten Bereichs). Während im Kasten D.1 die Kenngrößen der beiden Verteilungen allgemein gegenübergestellt werden (Verteilungsfunktion F(t), Zuverlässigkeitsfunktion $R(t) = 1 - F(t)$, Ausfallrate $\lambda(t)$ und Erwartungswert der ausfallfreien Zeit *MTTF*), werden im Folgenden und in Abbildung D.3 nur gefahrbringende Ausfälle betrachtet. Dies wird durch den Index D bei den Verteilungsfunktionen sowie bei der Zeit T_{10D} und den Ausfallraten λ_D ausgedrückt. Als Methode zur Bestimmung der *Weibull*-Parameter können je nach Testverfahren verschiedene Methoden angewendet werden. Dies umfasst auch unvollständige Daten, wenn also z. B. nicht schadhafte Teile berücksichtigt werden sollen. Als Ergebnis können aus den Testdaten die Parameter b und *T* ermittelt werden. Dafür ist Software auf dem Markt erhältlich, die die statistische Analyse der Testdaten unterstützt. Aus den ermittelten Kennwerten lässt sich dann die nominale Lebensdauer T_{10} bestimmen, bei der 10 % der betrachteten Bauteile ausgefallen sind (ablesbar am Kreuzungspunkt der beiden roten Linien im oberen Teil von Abbildung D.3, hier bezogen auf gefährliche Ausfälle).

Bei pneumatischen und elektromechanischen Bauteilen werden Lebensdauern statt in der Dimension „Zeit“ meist als Anzahl der Schaltspiele in der Pseudo-Einheit „Zyklen“ angegeben. Die Umrechnung von Lebensdauern in Schaltspiele erfolgt durch Multiplikation mit der mittleren Anzahl jährlicher Betätigungen n_{op} (in Zyklen je Jahr, siehe Kasten D.1 und Abschnitt D.2.4.2). Der B_{10D}-Wert in Zyklen entspricht dabei dem T_{10D}-Wert auf Zeitbasis. Wie aus der nominalen Lebensdauer B_{10} bzw. B_{10D} ein $MTTF_D$-Wert ermittelt werden kann, wird im Abschnitt D.2.4.2 beschrieben.

Die sicherheitstechnischen Zuverlässigkeitskennwerte für fluidtechnische und elektromechanische Komponenten sind den Herstellerangaben für diese Bauteile zu entnehmen. Für die Ermittlung der Zuverlässigkeit von pneumatischen Komponenten kann die Norm ISO 19973 „Pneumatik – Bewertung der Zuverlässigkeit von Bauteilen durch Prüfung“ zugrunde gelegt werden. Diese Norm besteht zurzeit aus fünf Teilen:

- Teil 1: Allgemeine Verfahren,
- Teil 2: Ventile,
- Teil 3: Zylinder mit Kolbenstange,
- Teil 4: Druckregelventile,
- Teil 5: Rückschlagventile, Wechselventile (ODER-Ventile), Zweidruckventile (UND-Ventile), einstellbare Drosselrückschlagventile, Schnellentlüftungsventile.

Bei Pneumatikventilen wird die Lebensdauer (B_{10}-Wert) in Zyklen bis zum Ausfall angegeben. Die nominale Lebensdauer B_{10} (in einigen Literaturangaben auch t_{10}) ist die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der 10 % der betrachteten Menge ausgefallen sind. Da das Ausfallkriterium „Verfügbarkeit“ bei Ventilen auch nicht sicherheitsrelevante Ausfälle umfasst (z. B. Leckage über dem definiertem Schwellwert), ist für Sicherheitsfunktionen der B_{10D}-Wert relevant (mittlere Schaltspielzahl, nach der 10 % der Bauteile gefahrbringend ausgefallen sind; D im Index steht für „dangerous“). In Anhang C.4.2 der Norm, Fußnote 1 wurde zugelassen, dass bei unbekanntem Anteil der gefahrbringenden Ausfälle an den Gesamtausfällen als B_{10D}-Wert der ermittelte Wert für die nominale Lebensdauer (B_{10}) multipliziert mit zwei verwendet werden darf. Dem liegt die Abschätzung zu Grunde, dass 50 % der Ausfälle in die gefahrbringende Richtung gehen. Hat der Bauteilhersteller jedoch den Anteil gefahrbringender Ausfälle (Ratio of Dangerous Failures, *RDF*) z. B. durch entsprechende Labor- oder Felduntersuchungen bestimmt, dann kann dieser Faktor zur Umrechnung genutzt werden:

$$B_{10D} = \frac{B_{10}}{RDF} \qquad \text{(D.2)}$$

Bei *RDF*-Werten unter 50 % kann sich der B_{10D}-Wert im Vergleich zu B_{10} deutlich erhöhen, woraus sich hohe $MTTF_D$-Werte ergeben können (siehe Kasten D.1 und Abschnitt D.2.4.2). Damit einher gehen durch die in Gleichung (D.4) beschriebene Umrechnung mittels n_{op} auch sehr hohe Gebrauchsdauern T_{10D}. Die Norm begrenzt in ihrem Anhang C.4.2 allerdings die zulässige Gebrauchsdauer – unabhängig vom nach Gleichung D.2 ermittelten B_{10D}-Wert – auf einen T_{10D}-Wert, der maximal dem doppelten T_{10}-Wert entspricht.

Der B_{10}-Wert und ggf. der *RDF*-Wert werden üblicherweise im Labor ermittelt. Dabei werden mindestens sieben Ventile von unterschiedlichen Produktionszeitpunkten einer Langzeitbelastung ausgesetzt. Die maximale Schaltfrequenz für die Langzeitbelastung wird über den Druckaufbau (Erreichen von 90 % des Prüfdruckes) und den Druckabbau (Erreichen von 10 % des Prüfdruckes) in einem angeschlossenen, nach Anschlussquerschnitten definierten Volumen ermittelt. Für eine Bewertung der Prüfergebnisse sollten mindestens fünf von sieben Ventilen ausgefallen sein. Als Verfahren zur Bestimmung der *Weibull*-Parameter werden in ISO 19973-1 beispielhaft die Verfahren „Maximum Likelihood“ und „Rank Regression“ genannt.

Näherungsweise gilt, dass bei einer geringen Anzahl von Prüflingen, z. B. sieben Ventilen, der Erstausfall den B_{10}-Wert bestimmt bzw. die bis zum Zeitpunkt des Erstausfalls erreichten Zyklen ungefähr dem B_{10}-Wert entsprechen. Ist der Erstausfall gefahrbringend, entspricht diese Schaltspielzahl ungefähr dem B_{10D}-Wert.

Tabelle B.3 in DIN EN ISO 13849-2 listet die möglichen und damit zu betrachtenden Ausfallarten von Pneumatikventilen auf und gibt dabei auch Hinweise auf mögliche Fehlerausschlüsse und die dafür geltenden Bedingungen. Abhängig von der Applikation können insbesondere folgende Ausfallarten gefahrbringend sein:

- 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.

Bei B_{10D}- oder *RDF*-Angaben des Herstellers ist zu beachten, welche Ausfallarten der Hersteller als gefahrbringend eingestuft hat. Gehören hierzu nicht alle Ausfallarten, die in der betrachteten Applikation gefahrbringend sind, so kann die B_{10D}- oder *RDF*-Angabe des Herstellers nicht verwendet werden. Im Hinblick auf das Zusammenspiel von Bauteil und Applikation sollte dann eine vorsichtige Abschätzung der benötigten Werte vorgenommen werden.

D.2.4.2 Umrechnung von B_{10D} in $MTTF_D$

Die Norm erwartet für das vereinfachte Verfahren zur Abschätzung des PL für ein Teilsystem die Angabe eines $MTTF_D$-Wertes zur Berücksichtigung zufälliger Bauteilausfälle. Für elektromechanische und pneumatische Bauteile liegen aber typischerweise B_{10D}-Werte vor, die noch in $MTTF_D$-Werte umgerechnet werden müssen. Dazu bietet die Norm eine Näherungsformel an, die an bestimmte Voraussetzungen geknüpft ist:

$$MTTF_D = \frac{T_{10D}}{0{,}1} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} \qquad \text{(D.3)}$$

Diese Näherung basiert auf einer Umformung in zwei Schritten. Zunächst wird der in der Pseudoeinheit „Zyklen“ angegebene B_{10D}-Wert in einen T_{10D}-Wert umgerechnet. Dabei handelt es sich um die Zeit, bei der 10 % der betrachteten Bauteile gefährlich ausgefallen sind:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \qquad \text{(D.4)}$$

Als Umrechnungsfaktor dient dabei die mittlere Anzahl jährlicher Betätigungen n_{op} (in Zyklen je Jahr) auf der Grundlage folgender Parameter, die für die zu erwartende Anwendung (ggf. als Worst case-Ansatz) zu schätzen sind:

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

Aus diesen Parametern (einschließlich ihrer zugehörigen Einheiten) kann n_{op} (in Zyklen je Jahr) folgendermaßen ermittelt werden:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{Zyklus}} \cdot 3\,600\,\frac{s}{h} \qquad \text{(D.5)}$$

Der zweite Schritt der in Gleichung (D.3) verborgenen Näherung besteht in der Annahme einer zeitkonstanten „Ersatz-Ausfallrate“ für das eigentliche, von Verschleiß geprägte Ausfallverhalten. Diese Näherung funktioniert allerdings in ausreichender Güte nur bis zum Erreichen des $T_{10\,D}$-Wertes (der in „Zyklen“ dem $B_{10\,D}$-Wert entspricht).

Dieser Teil der Näherung wird in Abbildung D.3 illustriert. Im oberen Teil ist dazu die prozentuale Wahrscheinlichkeit für den gefährlichen Bauteilausfall abhängig von der Betriebszeit t dargestellt. Diese Wahrscheinlichkeit entspricht bei Beobachtung von vielen Bauteilen dem Anteil der zum Zeitpunkt t gefährlich ausgefallenen Exemplare. Im unteren Teil ist die zugehörige Ausfallrate, d. h. die aktuelle Rate der gefährlichen Ausfälle, abhängig von der Betriebszeit t abgebildet. Die durchgezogene Kurve im oberen Teil stellt die ursprüngliche *Weibull*-Verteilung $F_{D\,WBL}(t)$ mit einem angenommenen Formfaktor von b = 3 dar. Im Spezialfall b = 1 geht die *Weibull*-Verteilung in eine Exponentialverteilung über, die durch eine zeitkonstante Ausfallrate gekennzeichnet ist. Die gestrichelte Linie gehört zu jener speziellen Exponentialverteilung $F_{D\,EXP}(t)$ mit zeitkonstanter „Ersatz-Ausfallrate“, die die ursprüngliche *Weibull*-Verteilung im Punkt ($t = T_{10\,D}$; $F_D = 10\,\%$) schneidet. Beide Verteilungen erreichen also nach Ablauf von $T_{10\,D}$ den Punkt, an dem 10 % der betrachteten Bauteile gefährlich ausgefallen sind. Im oberen Teil von Abbildung D.3 lässt sich erkennen, dass die Wahrscheinlichkeit eines gefährlichen Ausfalls vor Erreichen der Verschleißphase sehr gering ist und bis $T_{10\,D}$ unterhalb der Ersatz-Exponentialverteilung verläuft – es handelt sich hier also um eine Abschätzung zur sicheren Seite. Es ist auch zu erkennen, dass die Begrenzung der Einsatzdauer auf $T_{10\,D}$ sehr wichtig ist: Oberhalb steigt die Wahrscheinlichkeit gefährlicher Ausfälle mit der Zeit gegenüber der exponentiellen Ersatzfunktion deutlich an. Die Gültigkeit der Näherung auf Basis der zeitkonstanten Ersatz-Ausfallrate kann verlängert werden, indem das betroffene Bauteil bei Erreichen des T_{10D}-Wertes vorsorglich erneuert wird.

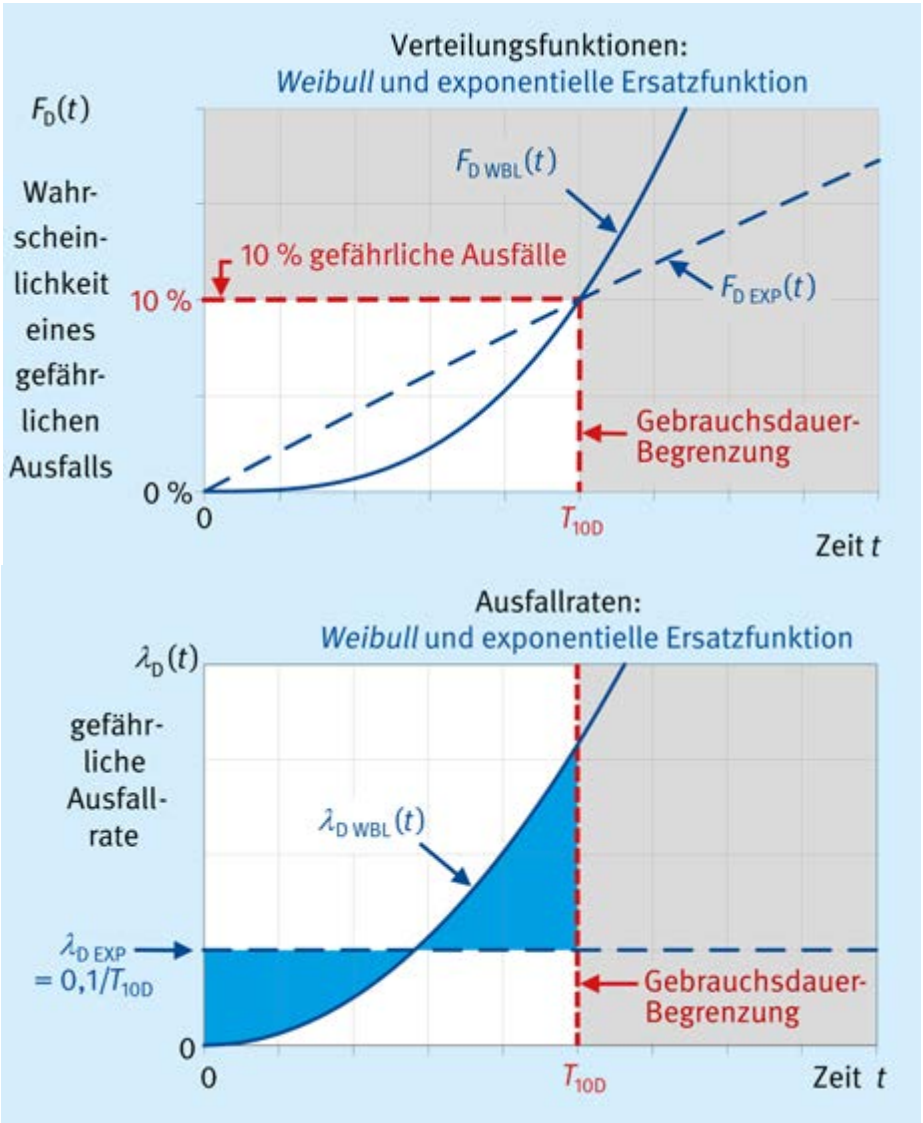


Abb.D.3
Illustration der Ermittlung einer zeitkonstanten Ersatzausfallrate $\lambda_{D\,EXP}$ auf Basis einer Ersatz-Exponentialverteilung $F_{D\,EXP}(t)$, wenn ursprünglich eine *Weibull*-Verteilung $F_{D\,WBL}(t)$ mit der zeitveränderlichen Ausfallrate $\lambda_{D\,WBL}(t)$ vorliegt

Im unteren Teil von Abbildung D.3 wird deutlich, dass die gewählte zeitkonstante „Ersatz-Ausfallrate“ $\lambda_{D\,EXP}$, die auf der Exponentialverteilung beruht, ungefähr dem Mittelwert der real zu erwartenden Ausfallrate $\lambda_{D\,WBL}(t)$ bis zum Zeitpunkt $T_{10\,D}$ entspricht. Jenseits von $T_{10\,D}$ ergeben sich jedoch durch das Eintreten in die Verschleißphase starke Abweichungen.

Doch wie ergibt sich aus diesen Bedingungen die Gleichung (D.3) für die genäherte Ersatz-$MTTF_D$? Ausgangspunkt ist die Bedingung $F_{D\,EXP}(T_{10\,D}) = 1 - \exp(-\lambda_{D\,EXP} \cdot T_{10\,D}) = 10\,\%$ für die die Näherung bildende Exponentialverteilung, wobei $\lambda_{D\,EXP}$ die erwähnte „Ersatz-Ausfallrate“ darstellt. Die Umformung dieser Gleichung führt auf $\lambda_{D\,EXP} = -\ln(0{,}9)/T_{10\,D}$. Da $-\ln(0{,}9)$ in guter Näherung 0,1 entspricht und für die Exponentialverteilung mit konstanter Ausfallrate $MTTF_D = 1/\lambda_D$ gilt (siehe Kasten D.1), folgt schließlich $MTTF_D \approx T_{10D}/0{,}1$.

D.2.5 Verfahren guter ingenieurmäßiger Praxis

Sind keine Herstellerangaben für die Zuverlässigkeit von Bauteilen verfügbar, schlägt die Norm als erste Alternative vor, dort gelistete typische Werte zu verwenden. Als Unterstützung liefert sie in ihrer Tabelle C.1 für mechanische, hydraulische und pneumatische Komponenten sowie für häufig in der Praxis eingesetzte elektromechanische Sicherheitsbauteile „typische Werte“ mit. Diese Werte sind als $MTTF_D$- oder $B_{10\,D}$-Werte in **Tabelle D.2** aufgeführt.

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

	Grundlegende und bewährte Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013	Andere relevante Normen	Typische Werte: $MTTF_D$ (Jahre) B_{10D} (Zyklen)
Mechanische Bauteile	Tabellen A.1 und A.2	—	$MTTF_D$ = 150 Jahre
Hydraulische Bauteile mit n_{op} ≥ 1 000 000 Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 150 Jahre
Hydraulische Bauteile mit 500 000 Zyklen pro Jahr ≤ n_{op} < 1 000 000 Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 300 Jahre
Hydraulische Bauteile mit 250 000 Zyklen pro Jahr ≤ n_{op} < 500 000 Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 600 Jahre
Hydraulische Bauteile mit n_{op} < 250 000 Zyklen pro Jahr	Tabellen C.1 und C.2	DIN EN ISO 4413	$MTTF_D$ = 1 200 Jahre
Pneumatische Bauteile	Tabellen B.1 und B.2	DIN EN ISO 4414	B_{10D} = 20 000 000 Zyklen
Relais und Hilfsschütze mit geringer Last	Tabellen D.1 und D.2	DIN EN 61810-1/-2/-3 DIN EN 60947-4-1 DIN EN 60947-5-1	B_{10D} = 20 000 000 Zyklen
Relais und Hilfsschütze mit nominaler Last	Tabellen D.1 und D.2	DIN EN 61810-1/-2/-3 DIN EN 60947-4-1 DIN EN 60947-5-1	B_{10D} = 400 000 Zyklen
Näherungsschalter mit geringer Last	Tabellen D.1 und D.2	DIN EN 60947-5-3 DIN EN ISO 14119	B_{10D} = 20 000 000 Zyklen
Näherungsschalter mit nominaler Last	Tabellen D.1 und D.2	DIN EN 60947-5-3 DIN EN ISO 14119	B_{10D} = 400 000 Zyklen
Schütze mit geringer Last	Tabellen D.1 und D.2	DIN EN 60947-4-1	B_{10D} = 20 000 000 Zyklen
Schütze mit nominaler Last	Tabellen D.1 und D.2	DIN EN 60947-4-1	B_{10D} = 1 300 000 Zyklen
Positionsschalter [a]	Tabellen D.1 und D.2	DIN EN 60947-5-1 DIN EN ISO 14119	B_{10D} = 20 000 000 Zyklen
Positionsschalter (mit separatem Betätiger, Zuhaltung) [a]	Tabellen D.1 und D.2	DIN EN 60947-5-1 DIN EN ISO 14119	B_{10D} = 2 000 000 Zyklen
Not-Halt-Geräte [a]	Tabellen D.1 und D.2	DIN EN 60947-5-5 DIN EN ISO 13850	B_{10D} = 100 000 Zyklen
Druck-Taster (z. B. Zustimmungsschalter) [a]	Tabellen D.1 und D.2	DIN EN 60947-5-1 DIN EN 60947-5-8	B_{10D} = 100 000 Zyklen

a) falls Fehlerausschluss für Zwangsöffnung möglich ist.

Der $B_{10\,D}$-Wert, den der Bauteilhersteller durch Prüfung ermittelt, gibt die mittlere Anzahl von Zyklen an, bei der 10 % der Bauteile gefahrbringend ausgefallen sind. Mithilfe dieses Wertes ist es möglich, den $MTTF_D$-Wert abzuschätzen. Die Verwendung der Werte aus Tabelle D.2 ist allerdings an verschiedene Voraussetzungen gebunden:

- Der Hersteller des Bauteils bestätigt die Verwendung von grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013 oder der entsprechenden Norm (siehe Tabelle D.2) für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller eines Bauteils, das in einer Steuerung der Kategorie 1, 2, 3 oder 4 verwendet werden soll, bestätigt die Verwendung bewährter Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013 oder der entsprechenden Norm (siehe Tabelle D.2) für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den SRP/CS-Konstrukteur und den Anwender fest und informiert diese über ihre Verantwortung, die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013 für die Implementierung und den Betrieb des Bauteils zu erfüllen.
- Der SPR/CS-Konstrukteur und der Anwender erfüllen die grundlegenden und/oder bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2013 für die Implementierung und den Betrieb des Bauteils.

Mit der Umsetzung dieser Anforderungen soll sichergestellt werden, dass die Anwendung grundlegender und bewährter Sicherheitsprinzipien von der Herstellung über die Implementierung bis zum laufenden Betrieb des Bauteils gewährleistet ist. Auch die Schnittstelle zwischen Hersteller, SRP/CS-Konstrukteur und Anwender bzw. Betreiber der Maschine ist klar definiert: Der Hersteller muss die Berücksichtigung der Sicherheitsprinzipien bei der Konstruktion verbindlich bestätigen und alle relevanten Informationen zu Einsatz- und Betriebsbedingungen zur Verfügung stellen. Der SRP/CS-Konstrukteur und der Anwender bzw. Betreiber der Maschine ihrerseits sind für die Einhaltung aller Sicherheitsprinzipien verantwortlich, die Implementierung und Betrieb des Bauteils betreffen. Unter diesen Voraussetzungen kann bei der Berechnung der $MTTF_D$, ggf. über $B_{10\,D}$, 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 $B_{10\,D}$-Werte für elektromechanische Bauteile genannt, die nach dem ebenfalls oben vorgestellten Verfahren mit der durchschnittlichen Anzahl jährlicher Betätigungen n_{op} in einen $MTTF_D$-Wert umgerechnet werden können.

Alle Werte in der Tabelle beziehen sich nur auf gefahrbringende Ausfälle, was durch den Index „D“ ausgedrückt ist. Hier wurde unterstellt, dass nur die Hälfte aller Ausfälle gefahrbringend ist. Seit der dritten Ausgabe der Norm wurde für „Schütze mit nominaler Last“ allerdings von dieser Regel abgewichen und der in der Produktnorm DIN EN 60947-4-1 [D6], Tabelle K.2 angegebene Anteil gefahrbringender Ausfälle (75 % Öffnungsfehler oder Kurzschluss) für die Umrechnung genutzt. Dies führte auf einen gegenüber der zweiten Ausgabe der Norm reduzierten $B_{10\,D}$-Wert von 1 300 000 Zyklen (vorher 2 000 000 Zyklen). Die hier angegebenen Werte können also durchaus optimistischer aussehen als Datenblattangaben von Herstellern, die sich im Sinne der Verfügbarkeit auf alle Fehlerarten beziehen, die den Funktionsablauf beeinträchtigen können. Bei einigen elektromechanischen Bauteilen, beispielsweise Relais, Hilfsschützen und Schützen, geht die elektrische Belastung der Kontakte stark in den $B_{10\,D}$-Wert ein, was durch vielfältige Beobachtungen aus der Praxis bestätigt wird. Bei geringer elektrischer Last (typischerweise ohmscher Last) – DIN EN ISO 13849-1 spricht hier von bis zu 20 % des Bemessungswertes – ergeben sich deutlich bessere Werte. Hier wurde dann die mechanische statt der elektrischen Lebensdauer unterstellt (siehe Abschnitt D.2.4). Je nach Art (ohmsch oder induktiv) und Größe der Last können auch $B_{10\,D}$-Zwischenwerte der hier genannten Extreme abgeleitet werden. Bei den in der Tabelle aufgeführten Positionsschaltern, Zuhaltungen, Not-Halt-Geräten und Tastern, beispielsweise Zustimmungsschaltern, wird für den elektrischen Teil meist das Sicherheitsprinzip der Zwangsöffnung vorausgesetzt. Zwischen der zweiten und dritten Ausgabe der Norm haben sich für diese Bauteile im Rahmen des Verfahrens der guten ingenieurmäßigen Praxis einige Änderungen ergeben, die sich aus der Erfahrung mit der praktischen Anwendung ergaben. Daher wird dieses Thema in den folgenden Abschnitten D.2.5.1 bis D.2.5.8 separat ausführlich erläutert.

Naturgemäß handelt es sich bei diesen Ansätzen um starke Vereinfachungen der komplexen realen Zusammenhänge. So kann z. B. 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 sowie der elektrischen Bauteileigenschaften an die zu erwartende Belastung gehören.

D.2.5.1 Modellierung von elektromechanischen Bauteilen (Positionsschalter, Zuhaltungen, Not-Halt-Geräte, Zustimmungsschalter und Drucktaster)

In der praktischen Anwendung der Norm hat sich gezeigt, dass immer wieder Unsicherheit bei der Modellierung elektromechanischer Bauteile besteht. Dies zeigt sich auch darin, dass beide Teile der Norm hier teilweise eine unterschiedliche Sprache sprechen: Während im ersten Teil im Rahmen des Verfahrens guter ingenieurmäßiger Praxis (siehe Tabelle D.2) ein Ansatz über B_{10D}-Werte gewählt wird, kümmert sich der zweite Teil um mögliche Fehlerausschlüsse. Hier kommt erschwerend hinzu, dass eine eindeutige Trennung zwischen mechanischem und elektrischem Teil für viele dieser Bauteile kaum möglich ist. Daher werden im Folgenden zunächst allgemein die Anforderungen und Hinweise aus beiden Normteilen vorgestellt, um dann für die verschiedenen elektromechanischen Bauteile eine pragmatische Modellierung vorzuschlagen, die sich hauptsächlich am Teil 1 der Norm orientiert. Teil 2 ist alternativ ebenfalls anwendbar. Die praktische Umsetzung scheitert aber oft daran, dass ein kompletter Fehlerausschluss für den mechanischen und elektrischen Teil eine Bestätigung des Herstellers z. B. im Datenblatt erfordert oder die genaue Kenntnis der Einsatzbedingungen voraussetzt. Beide Voraussetzungen sind in der Praxis oft nicht gegeben.

Was sagt die Norm? – Elektromechanische Bauteile nach Teil 1 der Norm

DIN EN ISO 13849-1 schlägt mit dem oben eingeführten Verfahren guter ingenieurmäßiger Praxis vor, dass unter den nachfolgenden Voraussetzungen die in Tabelle D.2 genannten typischen B_{10D}-Werte für Positionsschalter, Zuhaltungen, Not-Halt-Geräte, Zustimmungsschalter und Drucktaster angenommen werden dürfen:

- Verwendung von grundlegenden und bewährten Sicherheitsprinzipien bei Konstruktion, Anwendung und Betrieb des Bauteils (siehe Tabellen D.1 und D.2 in DIN EN ISO 13849-2) und
- Möglichkeit des Fehlerausschlusses für Zwangsöffnung (dies erfordert nach Tabelle D.8 in DIN EN ISO 13849-2 Kontakte nach DIN EN 60947-5-1, Anhang K, in den Prinzipschaltbildern gekennzeichnet durch ⊖).

Herstellerangaben sind gegenüber den typischen Werten nach Norm natürlich immer zu bevorzugen. Zur Modellierung wird in der Norm in Tabelle C.1, Anmerkung 3 darauf hingewiesen, dass die Bauteile „*als Teilsystem der Kategorie 1 oder Kategorie 3/4 abgeschätzt werden* [können]*, je nach Anzahl der elektrischen Ausgangskontakte und der Fehlererkennung im nachgeordneten Teilsystem. Jedes Kontaktelement (einschließlich der mechanischen Betätigung) kann als ein Kanal mit entsprechendem B_{10D}-Wert betrachtet werden.*“

Obwohl dieser Hinweis sich formal nur auf Not-Halt-Geräte und Zustimmungsschalter bezieht, kann das dort genannte Prinzip auch auf andere elektromechanische Bauteile übertragen werden.

Dass die ein- oder zweikanalige Modellierung von der Anzahl der elektrischen Ausgangskontakte bestimmt wird, obwohl für zwangsöffnende Kontaktelemente ja ein Fehlerausschluss für Zwangsöffnung angenommen werden kann, erscheint zunächst unstimmig. Durch den Hinweis, dass der B_{10D}-Wert jedes Kanals für das Kontaktelement einschließlich der mechanischen Betätigung gelten soll, wird jedoch klar, dass es sich hier um einen Kunstgriff handelt, der das komplexe Zusammenspiel von mechanischen und elektrischen Elementen in den genannten elektromechanischen Bauteilen auf möglichst einfache Weise darstellen soll. Hier standen nicht die Details der elektromechanischen Konstruktion im Vordergrund, sondern ein möglichst simples Kochrezept:

- Ein elektromechanisches Bauteil mit einem zwangsöffnenden Kontaktelement, das die oben genannten Voraussetzungen erfüllt, kann als Teil eines Kategorie-1-Teilsystems modelliert werden. Im Funktionskanal enthält das Teilsystem einen Block mit dem entsprechenden B_{10D}-Wert.
- Ein elektromechanisches Bauteil mit (mindestens) zwei zwangsöffnenden Kontaktelementen, das die oben genannten Voraussetzungen erfüllt, kann je nach der Fehlererkennung im nachgeordneten Teilsystem als Bestandteil eines Kategorie-3- oder -4-Teilsystems modelliert werden. In den beiden Funktionskanälen enthält das Teilsystem je einen Block mit dem entsprechenden B_{10D}-Wert.

DIN EN ISO 13849-1 ergänzt über den allgemeinen Fall hinausgehend ebenfalls in Tabelle C.1, Anmerkung 3: „*In einigen Fällen* [kann es] *möglich sein, dass der Maschinenhersteller einen Fehlerausschluss nach DIN EN ISO 13849-2, Tabelle D.8, unter Berücksichtigung der jeweiligen Anwendungs- und Umgebungsbedingungen des Gerätes anwenden kann.*“ Die Formulierung des Fehlerausschlusses für ein elektromechanisches Bauteil ist dabei einerseits Sache des Bauteilherstellers, denn nur er kennt die Details der mechanischen Konstruktion. Andererseits muss man bei der Anwendung prüfen, ob ein Fehlerausschluss unter Berücksichtigung von Umgebungs-, Betriebs- und Anwendungsaspekten zulässig ist. Dies sind Sonderfälle, in denen der Maschinenhersteller in Rücksprache mit dem Bauteilhersteller individuell für spezifische Applikationen bestimmte Fehler ausschließt.

Was sagt die Norm? – Elektromechanische Bauteile nach Teil 2 der Norm

Tabelle D.8 aus DIN EN ISO 13849-2 gilt für Schalter, z. B. elektromechanische Positionsschalter und Handschalter, und ist daher für alle oben genannten elektromechanischen Bauteile anwendbar. Für einen Ausschluss des Feh-

lers „Nichtöffnen von Kontakten“ werden dort folgende Bedingungen genannt:

- Die Schalter müssen DIN EN 60947-5-1:2018, Anhang K erfüllen, also zwangsöffnende Kontaktelemente besitzen.
- Der Fehlerausschluss gilt nur bis maximal PL d. Für PL e sind redundante Bauteile erforderlich, also ein zweiter (Positions-)Schalter (Ausnahme: Not-Halt-Geräte).

Damit ergibt sich für Positionsschalter (mit und ohne separatem Betätiger), Zuhaltungen, Zustimmungsschalter und Drucktaster unabhängig von der Zahl der elektrischen Kontaktelemente folgende Bewertung:

- bis PL d: Fehlerausschluss ist zulässig, der auch für die Mechanik erfolgen kann, was auch eine Bestätigung des Herstellers voraussetzt. Modellierung als gekapseltes Teilsystem der Kategorie 3 (einfehlersicher) und direkte Angabe von PL d und *PFH* Null. In SISTEMA (unter Teilsystem, Registerkarte „PL“) muss dazu die Kopplung zwischen PL und *PFH* aufgehoben werden.
- PL e: kein Fehlerausschluss (für mechanische und elektrische Aspekte) zulässig.

Für Not-Halt-Geräte nach DIN EN 60947-5-5 ist ein Fehlerausschluss hinsichtlich des „Nichtöffnens von Kontakten“ für mechanische Aspekte bis PL e zulässig, wenn eine Höchstzahl von Betätigungen berücksichtigt wird. In der Vergangenheit wurde hier die Lebensdauerschaltspielzahl von 6 050 Betätigungen nach DIN EN 60947-5-5 herangezogen.

Wie im vorherigen Abschnitt erwähnt, ist die prinzipielle Zulässigkeit von Fehlerausschlüssen nur von begrenzter praktischer Relevanz.

Im Folgenden werden die in der Norm genannten Anforderungen auf häufig verwendete elektromechanische Bauteile angewendet. Die $B_{10\,D}$-Angaben in den folgenden Tabellen beziehen sich auf Tabelle D.2 dieses Reports.

Der Hersteller sollte im Datenblatt oder in den Applikationsbeispielen die Kategorie-Eignung angeben, damit das Risiko eines Ausfalls infolge gemeinsamer Ursache berücksichtigt ist.

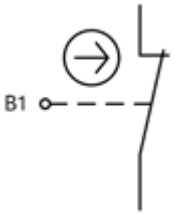
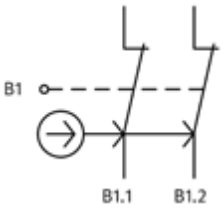
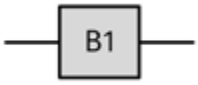
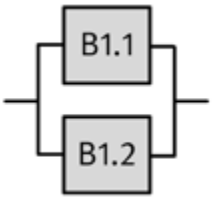
D.2.5.2 Positionsschalter

Nach DIN EN 60947-5-1 hergestellte elektromechanische Positionsschalter mit einem oder zwei zwangsöffnenden elektrischen Kontaktelementen nach DIN EN 60947-5-1, Anhang K können wie in **Tabelle D.3** beschrieben betrachtet werden. Der (ein- oder zweikanalig) ansetzbare $B_{10\,D}$-Wert nach dem Verfahren guter ingenieurmäßiger Praxis beträgt für Positionsschalter mit separatem Betätiger 2 000 000 Zyklen und für alle anderen Positionsschalter 20 000 000 Zyklen.

Neben dem Schalter selbst ist auch seine formschlüssige Betätigung (z. B. die Anfahrmechanik oder die Betätigerbefestigung) relevant. Für die dazu erforderliche Fehlerbetrachtung inkl. möglicher Fehlerausschlüsse sind zusätzlich die relevanten Anforderungen aus DIN EN ISO 13849-2, Anhang A zu erfüllen. Nach DIN EN ISO 13849-2, Tabelle D.8 ist mit einem einzelnen Positionsschalter (auch bei zwei Kontaktelementen) maximal PL d erreichbar. In den relevanten C-Normen für Maschinen können gegebenenfalls abweichende Vorgaben aufgeführt sein, z. B. die Verwendung von zwei Positionsschaltern für Kategorie 3.

Hinweise über die Auswahl und Anbringung von Positionsschaltern sind in der DGUV Information 203-079 [D7] aufgeführt.

Tabelle D.3 Modellierung von Positionsschaltern im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Prinzipschaltbild		
Sicherheitsbezogenes Blockdiagramm		
Modellierung	Block B1 B_{10D} = 2 000 000 bzw. 20 000 000 Zyklen oder Herstellerangabe	Blöcke B1.1 und B1.2 jeweils B_{10D} = 2 000 000 bzw. 20 000 000 Zyklen oder Herstellerangabe
Kategorie und PL	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

D.2.5.3 Zuhaltungen

Mit Zuhaltungen sind an dieser Stelle Einrichtungen zum mechanischen Blockieren geschlossener Schutzeinrichtungen mit integrierten Positionsschaltern als Baueinheit gemeint, mit denen die Sicherheitsfunktionen „Zuhaltung“ und „Verriegelung“ (Stellungsüberwachung der Schutzeinrichtung) realisiert werden können. Von der Sicherheitsfunktion „Zuhaltung“ wird im Folgenden nur die Stellungsüberwachung des Sperrmittels betrachtet (zur vollständigen Betrachtung der Sicherheitsfunktion Zuhaltung siehe Abschnitt 11.2.14, Beispiel 14). Neben den Mitteln zur Überwachung der Stellung einer Schutzeinrichtung besitzt eine Verriegelungseinrichtung mit Zuhaltung zusätzlich eine Vorrichtung zum Blockieren der beweglichen

Schutzeinrichtung in der geschlossenen Position. Solange diese Vorrichtung aktiv ist, kann die Schutzeinrichtung nicht geöffnet werden.

Für Zuhaltungen gibt es keine Produktnorm. Grundlegende sicherheitstechnische Anforderungen sind jedoch in DIN EN ISO 14119 aufgeführt. Zusätzlich gibt es für Zuhaltungen als „Baueinheit“ den Prüfgrundsatz GS-ET-19 [D8]. Demnach enthalten elektromechanische Zuhaltungen einen Positionsschalter für die Stellungsüberwachung der Schutzeinrichtung („Schutztür“) und einen Positionsschalter für die Stellungsüberwachung des Sperrmittels (siehe **Abbildung D.4**).

Ist die Zuhaltung konstruktiv mit einer „Fehlschließsicherung“ ausgeführt, kann auf den Positionsschalter für die Stellungsüberwachung der Schutzeinrichtung verzichtet werden: Wenn sich das Sperrmittel in zuhaltender Stellung befindet, kann von einer geschlossenen Schutzeinrichtung ausgegangen werden. Befindet sich das Sperrmittel in nicht zuhaltender Stellung, kann keine Aussage über die Stellung der Schutzeinrichtung gemacht werden.

Zuhaltungen können, unter Berücksichtigung der Anforderungen aus DIN EN ISO 14119 und dem Prüfgrundsatz GS-ET-19, wie in den **Tabellen D.4** und **D.5** beschrieben betrachtet werden.

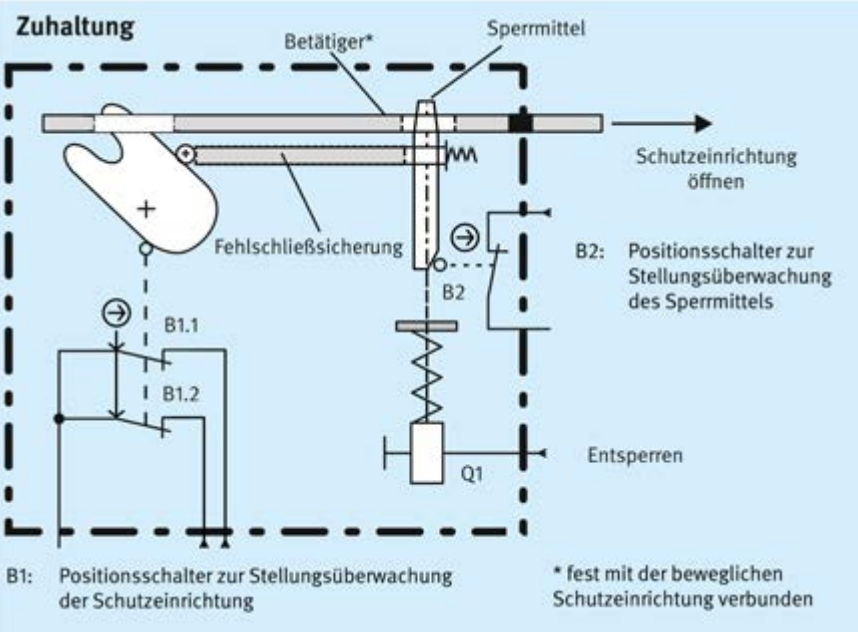


Abb. D.4
Prinzipielle Darstellung einer Zuhaltung mit Fehlschließsicherung und zusätzlicher Stellungsüberwachung der Schutzeinrichtung („Verriegelung“)

Tabelle D.4 Modellierung von Zuhaltungen **ohne** Fehlschließsicherung im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

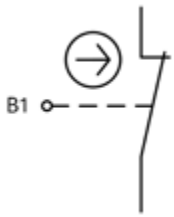
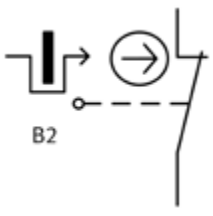
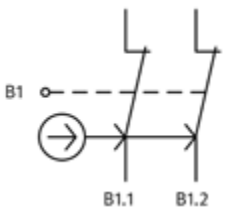
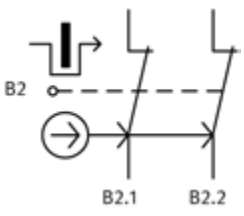
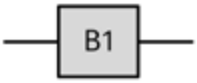
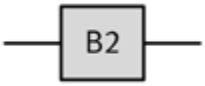
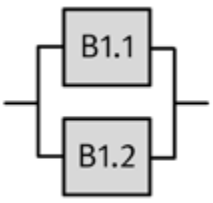
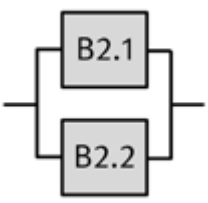
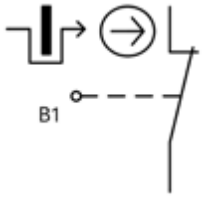
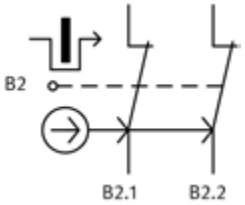
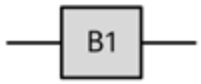
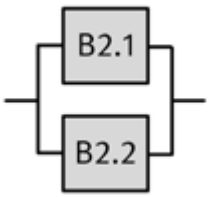
Zuhaltung ohne Fehlschließsicherung				
Prinzipschaltbild	Stellungsüberwachung Schutzeinrichtung	Stellungsüberwachung Sperrmittel	Stellungsüberwachung Schutzeinrichtung	Stellungsüberwachung Sperrmittel
				
Sicherheitsbezogenes Blockdiagramm				
Modellierung	Blöcke B1 und B2 jeweils B_{10D} = 2 000 000 Zyklen oder Herstellerangabe		Blöcke B1.1, B1.2, B2.1 und B2.2 jeweils B_{10D} = 2 000 000 Zyklen oder Herstellerangabe	
Kategorie und PL	Kategorie 1 maximal PL c		Kategorie 3 maximal PL d	

Tabelle D.5 Modellierung von Zuhaltungen **mit** Fehlschließsicherung im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Zuhaltung mit Fehlschließsicherung		
Prinzip-schaltbild	Stellungsüberwachung Sperrmittel	Stellungsüberwachung Sperrmittel
		
Sicherheits-bezogenes Blockdia-gramm		
Modellierung	Block B1 B_{10D} = 2 000 000 Zyklen oder Herstellerangabe	Blöcke B2.1 und B2.2 jeweils B_{10D} = 2 000 000 Zyklen oder Herstellerangabe
Kategorie und PL	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

Zusammengefasst gilt für Zuhaltungen:

- Der (ein- oder zweikanalig) ansetzbare B_{10D}-Wert nach dem Verfahren guter ingenieurmäßiger Praxis beträgt für Zuhaltungen 2 000 000 Zyklen.
- Das Vorhandensein der „Fehlschließsicherung“ sowie den zugehörigen Fehlerausschluss für die Mechanik muss der Hersteller bestätigen.
- Mit einer einzelnen Zuhaltung als „Baueinheit“ ist für die „Verriegelungsfunktion“ (auch bei zwei Kontaktelementen je Positionsschalter) nach DIN EN ISO 13849-2, Tabelle D.8 maximal PL d erreichbar. Möchte man einen PL e erreichen, ist dies nur mit einem externen zusätzlichen Positionsschalter zur Stellungsüberwachung der Schutzeinrichtung möglich.
- Bei Zuhaltungen als „Baueinheit“ ist die „Zuhaltefunktion“ auf PL d beschränkt, da der Positionsschalter für die Sperrmittelüberwachung und die zugehörige Anfahrmechanik nur einmal vorhanden ist.
- In den relevanten C-Normen für Maschinen gegebene Einschränkungen sind zu beachten.

Hinweise über die Auswahl und Anbringung von Zuhaltungen sind in der DGUV Information 203-079 aufgeführt.

D.2.5.4 Not-Halt-Gerät

Nach der Produktnorm DIN EN 60947-5-5 gebaute Not-Halt-Geräte können wie in **Tabelle D.6** beschrieben betrachtet werden.

D.2.5.5 Zustimmungsschalter

Nach der Produktnorm DIN EN 60947-5-8 oder dem Prüfgrundsatz GS-ET-22 [D9] gebaute Drei-Stellungs-Zustimmungsschalter können wie in Tabelle D.7 beschrieben betrachtet werden. In der Praxis existieren Zustimmungsschalter mit unterschiedlichen Kontaktsätzen (unterschiedliche Anzahl Öffner/Schließer).

Die sicherheitsrelevante Aufhebung der Zustimmungsfunktion wird bei Drei-Stellungs-Zustimmungsschaltern durch das Loslassen oder Durchdrücken erreicht. Beide Funktionen können in gleicher Weise bewertet werden, zusätzlich muss beim Loslassen aber besonders auf die Überdimensionierung der elektrischen Kontakte (hier: Schließerkontakte) bezogen auf die Last geachtet werden. Nachfolgend werden die Funktionen „Loslassen“ und „Durchdrücken“ in einer Sicherheitsfunktion zusammengefasst, da die Betätigungsrichtung nicht vorhersehbar ist.

Die Produktnorm DIN EN 60947-5-8 stellt keine konstruktiven Anforderungen an die Öffnungsfunktion. Dies gilt sowohl für die Schließer- als auch für die Öffnerkontakte (Loslassen oder Durchdrücken). Im Besonderen werden keine zwangsöffnenden elektrischen Kontaktelemente nach DIN EN 60947-5-1, Anhang K gefordert. In diesem Fall handelt es sich daher nicht um bewährte Bauteile und dadurch ist Kategorie 1 nicht möglich.

Der Prüfgrundsatz GS-ET-22 stellt besondere konstruktive Anforderungen, z. B.

- für die Funktion „Loslassen“ die Verwendung bewährter Federn oder einen zweikanaligen Aufbau mit Kontaktüberwachung,
- für die Funktion „Durchdrücken“ zwangsöffnende elektrische Kontaktelemente nach DIN EN 60947-5-1, Anhang K oder zweikanalige Signalgabe mit entsprechender steuerungstechnischer Überwachung.

Durch die konstruktive Ausführung nach GS-ET-22 ist eine vergleichbare Sicherheit zu einem bewährten Bauteil gegeben.

Zwei-Stellungs-Zustimmungsschalter realisieren nur die Sicherheitsfunktion „Loslassen“ und sind in der Produktnorm DIN EN 60947-5-8 nicht enthalten. Wenn sie dem Prüfgrundsatz GS-ET-22 entsprechen, gilt die gleiche Bewertung wie in **Tabelle D.7** für Schließerkontakte der Drei-Stellungs-Zustimmungsschalter angegeben: einkanalig in Kategorie 1 mit max. PL c oder zweikanalig in Kategorie 3 mit max. PL d.

Tabelle D.6 Modellierung von Not-Halt-Geräten im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie- und PL-Zuordnung

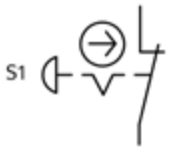
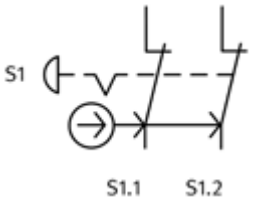
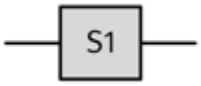
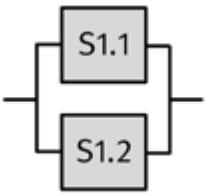
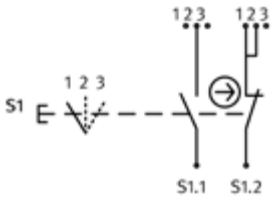
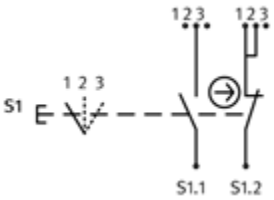
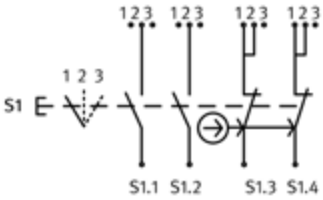
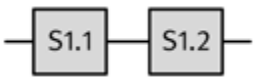
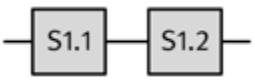
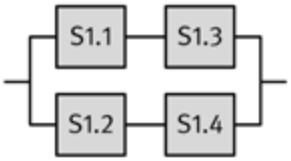
Prinzip-schaltbild		
Sicherheits-bezogenes Blockdia-gramm		
Modellie-rung	Block S1 B_{10D} = 100 000 Zyklen oder Herstellerangabe	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen oder Herstellerangabe
Kategorie und PL	Kategorie 1 maximal PL c	Kategorie 3 oder 4 maximal PL e

Tabelle D.7 Modellierung von Drei-Stellungs-Zustimmungsschaltern im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Prinzip-schaltbild			
Bedingung	Öffnerkontakt entsprechend DIN EN 60947-5-1 Anh. K	Zustimmungsschalter nach GS-ET-22	Zustimmungsschalter nach GS-ET-22
Sicherheits-bezogenes Blockdia-gramm	Loslassen Durchdrücken 	Loslassen Durchdrücken 	Loslassen Durchdrücken  b)
Modellie-rung	Block S1.1 B_{10D} = 100 000 Zyklen oder Herstellerangabe Block S1.2 Fehlerausschluss, *PFH* = 0	Block S1.1 B_{10D} = 100 000 Zyklen oder Herstellerangabe Block S1.2 Fehlerausschluss, *PFH* = 0	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen oder Herstellerangabe Blöcke S1.1 und S1.2 jeweils Fehlerausschluss, *PFH* = 0
Kategorie und PL	Kategorie B maximal PL b[a)]	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

a) Schließer S1.1 limitiert den erreichbaren PL auf b

b) Im nachfolgenden SRP/CS ist eine ausreichende Fehlererkennung für die elektrischen Kontakte vorhanden.

D.2.5.6 Drucktaster für den Tippbetrieb

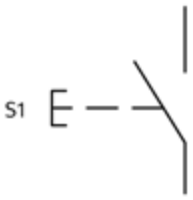
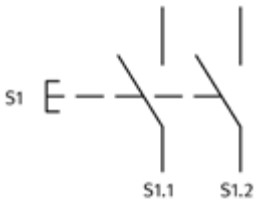
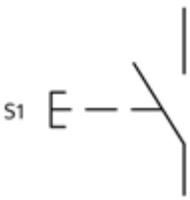
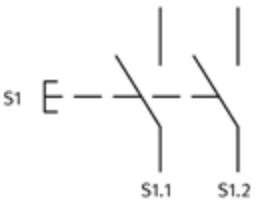
Drucktaster nach DIN EN ISO 13849-2, Tabelle D.8 kommen beispielsweise zum Auslösen einer zeitlich und/oder örtlich begrenzten Bewegung im Rahmen des Tippbetriebes zur Anwendung und können wie in **Tabelle D.8** beschrieben betrachtet werden. Sie sind in diesem Anwendungsfall immer als „Schließer“ ausgeführt, wobei für die Sicherheitsfunktion das zuverlässige Öffnen des Schließers nach vorhergehender Betätigung entscheidend ist (vergleichbar mit dem grundlegenden Sicherheitsprinzip der Energietrennung – „Ruhestromprinzip“ – nach DIN EN ISO 13849-2, Tabelle D.1). Hierbei gilt dieselbe Betrachtung wie für die Funktion „Loslassen“ des Zwei-Stellungs-Zustimmungsschalters. Auch hier muss besonders auf Überdimensionierung der elektrischen Kontakte bezogen auf die Last geachtet werden.

C-Normen für Maschinen fordern oft für den Tippbetrieb ein Not-Halt-Gerät in der Nähe des Drucktasters. Kommt es nach Loslassen des Druck- bzw. Tipptasters zu einem Nichtöffnen des Schließers, lässt sich die gefahrbringende Bewegung durch Betätigen des Not-Halt-Gerätes stoppen. Weiterhin ist der Tippbetrieb oft auch nur weg- oder zeitbegrenzt und/oder bei aktivierter Sicherheitsfunktion SLS (Sicher begrenzte Geschwindigkeit) erlaubt. Diese Maßnahmen lassen sich bei der Bestimmung des PL (z. B. mit SISTEMA) nicht quantifizieren, da sie dem willensabhängigen Handeln unterliegen. Es ist daher ratsam, die spezifischen ergänzenden Anforderungen in einer C-Norm für den Tippbetrieb bei der Festlegung des PL_r zu berücksichtigen.

Weiterhin muss die Verhinderung eines unerwarteten Anlaufs beachtet werden, was dazu führt, dass schon für die beiden PL b-Varianten in Tabelle D.8 Befehlsgeräte nach DIN EN 60947-5-1 verwendet werden müssen, um beispielsweise nach DIN EN ISO 13849-2, Tabelle D.8 den Kurzschluss von benachbarten Kontakten, die voneinander isoliert sind, ausschließen zu können.

Für höhere Risiken (PL c oder d) sind Befehlsgeräte nur nach DIN EN 60947-5-1 nicht ausreichend, da diese wegen des möglichen Öffnungsversagens nur Kategorie B entsprechen. Hier können alternativ „sichere“ Drucktaster, beispielsweise zweistufige Zustimmungstaster nach GS-ET-22, verwendet werden. Diese eignen sich bei Ausführungen mit einem Schließer bis maximal PL c oder als zweikanalige Ausführung bis maximal PL d.

Tabelle D.8 Modellierung von Drucktastern für den Tippbetrieb im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

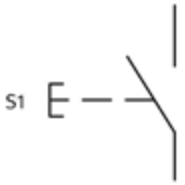
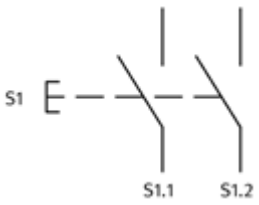
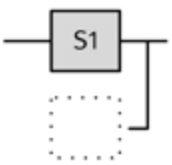
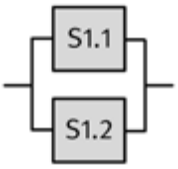
Prinzipschaltbild				
Bedingung	Drucktaster nach DIN EN 60947-5-1	Drucktaster nach DIN EN 60947-5-1	2-stufiger Zustimmungstaster nach GS-ET-22	2-stufiger Zustimmungstaster nach GS-ET-22
Sicherheitsbezogenes Blockdiagramm				
Modellierung	Block S1 B_{10D} = 100 000 Zyklen oder Herstellerangabe	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen oder Herstellerangabe	Block S1 B_{10D} = 100 000 Zyklen oder Herstellerangabe	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen oder Herstellerangabe
Kategorie und PL	Kategorie B maximal PL b	Kategorie B maximal PL b	Kategorie 1 maximal PL c	Kategorie 3 maximal PL d

D.2.5.7 Drucktaster für die manuelle Rückstellung

Drucktaster nach DIN EN ISO 13849-2, Tabelle D.8 können auch für die manuelle Rückstellung eingesetzt werden. Diese spezielle Sicherheitsfunktion wird in der DIN EN ISO 13849-1 im Abschnitt 5.2.2.3 mit besonderen Anforderungen belegt und dient zur manuellen Quittierung, um den Wiederanlauf einer Maschine nach dem Auslösen einer Sicherheitsfunktion zu ermöglichen. Dazu muss zunächst das auslösende Ereignis und damit die Anforderung der Sicherheitsfunktion aufgehoben sein. Je nach Risiko kann es dann erforderlich sein, dass eine manuelle, separate und beabsichtigte Handlung erforderlich ist, bevor der Steuerung ermöglicht wird, einen erneuten Startbefehl entgegenzunehmen. Dies ist zum Beispiel bei hintertretbaren Schutzbereichen der Fall, bei denen zunächst lokal bestätigt werden muss, dass der komplette Gefahrenbereich, auch zwischen Zutrittssicherung und Gefahrenquelle, frei von Personen ist. Um einen unerwarteten Anlauf in Folge eines gefahrbringenden Ausfalls der manuellen Rückstellung oder durch vorhersehbare Fehlanwendung zu verhindern, fordert die Norm unter anderem einen überwachten Signalwechsel der Rückstelleinrichtung. Der PL_r der manuellen Rückstellfunktion kann sich je nach Anwendung und Risiko vom PL_r der zugehörigen Sicherheitsfunktion, die zurückgesetzt wird, unterscheiden. In der Norm werden weitere Anforderungen an die Positionierung des Aktuators zum Rücksetzen und zur sequentiellen Quittierung bei eingeschränkter Einsehbarkeit genannt.

Wird ein Drucktaster als Aktuator zum Rücksetzen eingesetzt, ergeben sich aus den vorgenannten Anforderungen in ähnlicher Weise wie beim Einsatz für den Tippbetrieb (siehe D.2.5.6) eine Reihe von konstruktiven Vorgaben. Grundsätzlich können nur nach DIN EN 60947-5-1 gebaute Befehlsgeräte verwendet werden und auch hier muss besonders auf Überdimensionierung der elektrischen Kontakte bezogen auf die Last geachtet werden. Um die Forderung nach einem überwachten Signalwechsel zu erfüllen, kann die nachfolgende Logik in der Steuerungskette das Ausgangssignal des Drucktasters auf eine steigenden, gefolgt von einer fallenden Flanke überwachen. Dabei müssen beide Flanken mindestens 200 ms auseinanderliegen, um ein Prellen des Tasters nicht fehlerhaft als fallende Flanke zu interpretieren. Zusätzlich sollten beide Flanken höchstens z. B. 3 s auseinanderliegen, um andere systematische Fehler wie Spannungsschwankungen, die zu einem ungewollten Rückstellen führen könnten, zu beherrschen. Mit einer so ausgeführten Einbindung kann je nach Anzahl der Schließerkontakte eine Umsetzung in Kategorie 2 oder 3 bis maximal PL d erfolgen, siehe **Tabelle D.9**. Mit der beschriebenen Flankenüberwachung, einschließlich des überwachten Zeitfensters zwischen den Flanken, kann ein mittlerer Diagnosedeckungsgrad (*DC* = 90 %) erreicht werden. Schaltungsbeispiel 30 in Kapitel 11 zeigt eine mögliche Umsetzung.

Tabelle D.9 Modellierung von Drucktastern für die manuelle Rückstellung im Prinzipschaltbild und im sicherheitsbezogenen Blockdiagramm mit Kategorie und PL-Zuordnung

Prinzipschaltbild		
Bedingung	Drucktaster nach DIN EN 60947-5-1, Auswertung steigende und fallende Flanke mit Zeitüberwachung	
Sicherheitsbezogenes Blockdiagramm		
Modellierung	Block S1 B_{10D} = 100 000 Zyklen oder Herstellerangabe	Blöcke S1.1 und S1.2 jeweils B_{10D} = 100 000 Zyklen oder Herstellerangabe
Kategorie und PL	Kategorie 2 maximal PL d	Kategorie 3 maximal PL d

D.2.5.8 Drucktaster für Zweihandschaltungen

Eine besondere Anwendung finden Drucktaster auch in Zweihandschaltungen zur Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches. Anwendungsbeispiele dafür sind im mitlaufenden Beispiel einer Planschneidemaschine (siehe Abschnitte 6.8, 8.4, 9.12 und 10.10) und im Schaltungsbeispiel 27 für mechanische Pressen (Abschnitt 11.2.27) gezeigt. Für Zweihandschaltungen gelten besondere normative Anforderungen, die in DIN EN ISO 13851 festgelegt sind.
Die als Stellteile eingesetzten Drucktaster müssen demnach DIN EN 60947-5-1 entsprechen und werden in den genannten Anwendungen durch eine Logikeinheit mit Selbstüberwachung und Erkennung interner Fehler ausgewertet, die Typ III C gemäß DIN EN ISO 13851 entspricht. Diese Logikeinheit überwacht unter anderen die Synchronität der Betätigung beider Stellteile. Für diese besondere Anwendung ist nach der Recommendation for Use (RfU) CNB/M/11.033/R/E Rev 09 [D10] ein Fehlerausschluss für mechanische Fehler in den Stellteilen möglich. Auf diese Weise kann insgesamt für die Sicherheitsfunktion „Ortsbindung der Hände der Bedienperson außerhalb des Gefährdungsbereiches“ ein PL e erreicht werden.

In den beiden genannten Beispielen dieses Reports enthalten die Stellteile jeweils einen Öffner- und einen Schließerkontakt, die mit ihren B_{10D}-Werten in redundanten Kanälen einer Kategorie-4-Struktur eingebunden

sind. Schon beim mechanischen Öffnungsversagen eines Stellteils wäre die Sicherheitsfunktion gefährlich ausgefallen, da jede Hand der Bedienperson einzeln durch Ortsbindung geschützt werden muss. Im Fehlerfall steht der Bedienperson durch das Loslassen des zweiten Stellteils aber auch noch eine schnelle und intuitive zweite Abschaltmöglichkeit zur Verfügung.

D.2.6 $MTTF_D$ elektronischer Steuerungskomponenten

Wie bereits erwähnt, ist die Angabe der Ausfallraten λ bzw. λ_D, z. B. als FIT-Werte (Failures In Time, d. h. Ausfälle in 10^9 Bauteilstunden), für elektronische Bauteile schon seit Längerem üblich. Daher ist die Chance recht hoch, über den Hersteller an Zuverlässigkeitsinformationen zu kommen. Unter Umständen müssen diese Angaben in $MTTF_D$-Werte umgerechnet werden, z. B. mithilfe der vereinfachenden Annahme, dass nur 50 % aller Ausfälle gefahrbringend sind. Sind keine Herstellerangaben erhältlich, so kann eine Reihe von bekannten Datensammlungen herangezogen werden, von denen folgende in DIN EN ISO 13849-1 beispielhaft zitiert werden:

- Siemens Standard SN 29500, Ausfallraten Bauelemente, Erwartungswerte, Hrsg.: Siemens AG, CT TIM Regulation & Standardization, München und Erlangen 2004-2016 (wird unregelmäßig aktualisiert, Bestellanfragen an michaela.pabst@siemens.com oder thomas.haizmann@siemens.com)
- IEC 61709, Electric components – Reliability – Reference conditions for failure rates and stress models for conversion, Hrsg.: International Electrotechnical Commission (IEC), Genf 2017
- HDBK-217Plus: 2015, Notice 1, Reliability Prediction Models, Quanterion Solutions Incorporated, Utica, New York, 2017 (Fortführung des MIL-HDBK-217F), www.quanterion.com
- Telcordia SR-332, Reliability Prediction Procedure for Electronic Equipment, Issue 4, March 2016, Ericsson Information Superstore, https://telecom-info.njdepot.ericsson.net/
- EPRD-2014, Electronic Parts Reliability Data (RAC-STD-6100), Quanterion Solutions Incorporated, Utica, New York, 2015, www.quanterion.com
- NPRD-2016, Nonelectronic Parts Reliability Data (RAC-STD-6200), Quanterion Solutions Incorporated, Utica, New York, 2015, www.quanterion.com
- British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)
- Chinese Military Standard, GJB/z 299B & 299C.

Neben diesen Datensammlungen gibt es auf dem Markt eine Reihe von Hilfsprogrammen, die diese oder andere Datenbanken per Software zugänglich 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 der Norm sind in den Tabellen C.2 bis C.7 sogar für einige typische elektronische Komponenten Werte aufgelistet, die der Datensammlung SN 29500 entnommen sind. In der dritten Ausgabe der Norm wurden allerdings die vorher vorhandenen Spalten mit eingerechnetem Sicherheitsfaktor von 10 („ungünstigster Fall“) gelöscht. Bei korrekter Verwendung der Datenquellen ist ein zusätzlicher Sicherheitsfaktor in der Regel nicht erforderlich. Die Anpassung an Beanspruchungen erheblich außerhalb der Referenzbedingungen wird in der Norm zwar grundsätzlich empfohlen. Sie sollte im Sinne der Einfachheit aber mit Augenmaß angewendet werden.

D.3 Integration bereits zertifizierter Komponenten und Geräte

In zunehmendem Maß versehen Hersteller ihre Komponenten bereits mit der Angabe einer $MTTF_D$ im Datenblatt. Bei Komponenten, die als Teilsysteme in einem SRP/CS eingesetzt werden sollen, nennt der Hersteller einen PL nach DIN EN ISO 13849-1 oder einen SIL nach DIN EN 61508, DIN EN 62061 oder DIN EN 61800-5-2, verbunden mit der Angabe einer „mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde“ *PFH*. Falls solche Komponenten nur in einem Kanal des SRP/CS verwendet werden, kann die angegebene Ausfallhäufigkeit je Stunde (*PFH*) als Ersatzwert für die Ausfallrate in die gefährliche Richtung betrachtet werden (siehe Gleichung (D.6)), wobei komponenteninterne Merkmale wie Redundanz und Eigendiagnose bereits berücksichtigt sind. Ausführlichere Hinweise dazu gibt das SISTEMA-Kochbuch 4 [D11] in Kapitel 2.

$$MTTF_D = \frac{1}{\lambda_D} \approx \frac{1}{PFH} \quad \text{(D.6)}$$

(„Black-Box“-Komponente mit *PFH* innerhalb eines Kanals)

D.4 „Parts Count“-Verfahren

Sind die $MTTF_D$-Werte aller sicherheitsrelevanten Komponenten bekannt, so muss hieraus zunächst die $MTTF_D$ jedes Blocks berechnet werden. Dieser Schritt lässt sich zwar per FMEA (Ausfalleffektanalyse) sehr detailliert durchführen (siehe Anhang B). Allerdings müssen dazu im Idealfall die unterschiedlichen Ausfallarten jeder sicherheitsrelevanten Komponente und ihre Wirkung für den Block analysiert werden. Dieser Ansatz lohnt sich – gemessen am Aufwand – daher meist nur für Komponenten mit einer hohen Ausfallrate, d. h. einem kleinen $MTTF_D$-Wert. Als schnelle Alternative, die im Mittel auch nicht zu viel schlechteren Werten führt, bietet DIN EN ISO 13849-1

das sogenannte „Parts Count“-Verfahren an. Im Wesentlichen handelt es sich dabei um eine Summation mit zwei Hauptannahmen:

- Für alle Ausfallarten einer Komponente und deren Auswirkungen auf den Block wird pauschal eine Aufteilung je zur Hälfte in ungefährliche und gefahrbringende Ausfälle angesetzt. Dies bedeutet, dass die Hälfte der Ausfallrate λ einer Komponente zur gefahrbringenden Ausfallrate λ_D des zugehörigen Blocks beiträgt. Wurde für die Komponente bereits der gefahrbringende Anteil der Ausfallrate λ_D bestimmt, so wird der gleiche Wert λ_D auch dem Block angerechnet.
- Die gefahrbringende Ausfallrate λ_D des Blocks wird dann durch Summation der λ_D-Beiträge aller N im jeweiligen Block vorhandenen sicherheitsrelevanten Komponenten gebildet (wobei sich die Beiträge identischer Komponenten einfach zusammenfassen lassen):

$$\lambda_D = \frac{1}{2}\sum_{i=1}^{N}\lambda_i \quad \text{bzw.} \quad \lambda_D = \sum_{i=1}^{N}\lambda_{Di} \qquad \text{(D.7)}$$

Da die Norm wie oben erläutert von konstanten Ausfallraten ausgeht, lassen sich Ausfallraten λ_D einfach durch Kehrwertbildung in $MTTF_D$-Werte umrechnen. Wird dieser Zusammenhang zugrunde gelegt, so ergibt sich der $MTTF_D$-Wert eines Blocks leicht aus den $MTTF_D$-Werten der zugehörigen Komponenten. Ein Beispiel für die Anwendung des „Parts Count“-Verfahrens findet sich in Kapitel 8, Abschnitt 8.4.5.

D.5 Logische 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 Gleichung (D.7) die $MTTF_D$ für jeden Kanal berechnen. Dabei wird unterstellt, dass der gefahrbringende Ausfall eines beliebigen Blocks in der Kette der Blöcke, die einen Kanal darstellt, auch als gefahrbringender Ausfall des Kanals zu werten ist. In dieser Phase der $MTTF_D$-Bestimmung greift die Kappungsregel der Norm: Mit Ausnahme von Kategorie 4 wird jeder $MTTF_D$-Wert eines Kanals, der rechnerisch > 100 Jahre ist, regelgemäß auf den Höchstwert von 100 Jahren reduziert. Bei Kategorie 4 beträgt die Kappungsgrenze 2500 Jahre. Durch diese Regel wird die Überbewertung der Bauteilzuverlässigkeiten gegenüber den anderen für den PL relevanten Größen wie Architektur, Tests und Ausfälle infolge gemeinsamer Ursache vermieden.

D.6 Symmetrisierung bei zwei logisch parallelgeschalteten Kanälen

Sobald zwei Funktionskanäle in einer Steuerung vorhanden sind (dies ist in der Regel bei Kategorie 3 und 4 der Fall), die unterschiedliche $MTTF_D$-Werte aufweisen, stellt sich die Frage, welcher für jeden der beiden Kanäle repräsentative $MTTF_D$-Wert bei der Bestimmung des PL mithilfe des Säulendiagramms verwendet werden soll. Auch für diese Frage hält DIN EN ISO 13849-1 eine einfache Formel als Antwort bereit:

$$MTTF_D = \frac{2}{3}\left(MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right) \qquad \text{(D.8)}$$

Die mittlere $MTTF_D$ pro Kanal ergibt sich also durch eine Mittelungsformel aus den $MTTF_D$-Werten beider redundanter Funktionskanäle 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 [D12]. 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 Ausfälle infolge gemeinsamer Ursache (CCF, vgl. Anhang F). Während $MTTF_D$ bereits für jeden beteiligten Funktionskanal auf 100 Jahre (Kategorie 4: 2500 Jahre) begrenzt wird, ist die Einteilung der $MTTF_D$-Werte in eine der drei Klassen „niedrig“, „mittel“ oder „hoch“ erst nach der Symmetrisierung sinnvoll. Der symmetrisierte Wert geht als ein Parameter neben der Kategorie, dem durchschnittlichen Diagnosedeckungsgrad und den Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in die numerische Bestimmung des PL ein. Daneben wird je nach zu erreichender Kategorie ein minimaler $MTTF_D$-Wert von drei Jahren (für Kategorie B, 2 und 3) oder 30 Jahren (für Kategorie 1 und 4) benötigt.

Literatur

[D1] *Birolini, A.*: Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management. 3. Aufl. Springer, Berlin 1991

[D2] *Bork, T.; Schaefer, M.*: Aus Aktivität wird Vorsicht – Sinn und Unsinn der Quantifizierung. O + P Ölhydraulik und Pneumatik 51 (2007) Nr. 3, S. 78–85. www.dguv.de/medien/ifa/de/pub/grl/pdf/2007_016.pdf

[D3] *Hablawetz, D.; Knödler, M.; Matalla, N.; Schmitt-Pauksztat, G.*: Systematisch richtig, statt zufällig falsch. atp magazin 1-2/2021, S. 70–75

[D4] *Schuster, U.*: Untersuchung des Alterungsprozesses von hydraulischen Ventilen. BGIA-Report 6/2004. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2004. https://www.dguv.de/medien/ifa/de/pub/rep/pdf/rep04/biar0604/rep6_04.pdf

[D5] *Weibull, W.*: A statistical distribution function of wide applicability. J. Appl. Mech. 18 (1951), S. 292–297

[D6] DIN EN 60947-4-1: Niederspannungsschaltgeräte – Teil 4-1: Schütze und Motorstarter – Elektromechanische Schütze und Motorstarter (5/2020). DIN Media, Berlin 2020

[D7] DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2014. https://publikationen.dguv.de/regelwerk/dguv-informationen/2849/auswahl-und-anbringung-von-verriegelungseinrichtungen

[D8] Grundsätze für die Prüfung und Zertifizierung von Verriegelungseinrichtungen mit Zuhaltung, Prüfgrundsatz GS-ET-19. Hrsg.: DGUV Test, Prüf- und Zertifizierungsstelle Elektrotechnik, Juni 2019. https://www.bgetem.de/arbeitssicherheit-gesundheitsschutz/pruefen-zertifizieren/pruef-und-zertifizierungsstelle-elektrotechnik/pruefgrundsaetze

[D9] Grundsätze für die Prüfung und Zertifizierung von elektromechanischen Zustimmungsschaltern und Zustimmungseinrichtungen mit und ohne Anlaufsteuerung, Prüfgrundsatz GS-ET-22. Hrsg.: DGUV Test, Prüf- und Zertifizierungsstelle Elektrotechnik, Januar 2022. https://www.bgetem.de/arbeitssicherheit-gesundheitsschutz/pruefen-zertifizieren/pruef-und-zertifizierungsstelle-elektrotechnik/pruefgrundsaetze

[D10] Vertical Recommendation for Use Sheets (RfUs) – Status on November 2023, Number CNB/M/11.033/R/E Rev 09, S. 144. Hrsg.: European Co-Ordination of Notified Bodies Machinery Directive 2006/42/EC + Amendment, 2023. https://ec.europa.eu/docsroom/documents/57275

[D11] *Hauke, M.; Apfeld, R.; Huelke, M.; Bömer, T.; Werner, C.:* Das SISTEMA-Kochbuch 4: Wenn die vorgesehenen Architekturen nicht passen – Version 2.0 (DE). Hrsg. Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2020.https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-sistema/sistema-kochbuecher

[D12] *Goble, W. M.*: Control Systems Safety Evaluation & Reliability. 3rd ed. Hrsg.: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010. https://www.isa.org

Anhang E

Bestimmung des Diagnosedeckungsgrades (DC)

Änderung gegenüber dem IFA Report 2/2017

- Tabelle E.2 vereinfacht, die Maßnahmen-Beschreibung wurden in den Text verschoben und erweitert
- Für Maßnahmen mit einer Spanne möglicher *DC*-Werte wurde der Hinweis auf eine FMEA ergänzt („Selbsttests bei Anlauf“ wurde auf 60 bis 90 % geändert)
- Für die *DC*-Maßnahmen „Kreuzvergleich ohne Dynamisierung“ und „Fehlererkennung im Prozess“ wurde die Begrenzung des erreichbaren *DC* abhängig von der Testrate aufgenommen

Der Diagnosedeckungsgrad *DC* (Diagnostic Coverage) ist ein Maß für die Wirksamkeit der Selbsttest- und Überwachungsmaßnahmen in einer Steuerung. Er kann sich auf Bauelemente, Blöcke oder ganze Teilsysteme (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 auch ohne das Vorhandensein spezieller Fehlererkennungs- und Fehlerreaktionsmechanismen dazu, dass ein sicherer Zustand eingenommen wird, aus dem heraus keine Gefährdungen entstehen (Beispiele: Offenbleiben der Arbeitskontakte eines Schützes oder Geschlossenbleiben eines Ventils, beides jeweils mit der Folge der Energieunterbrechung und damit eines Stillstands potenziell gefahrbringender Bewegungen).
- Erkennbare gefahrbringende Ausfälle DD (dangerous detectable): Diese potenziell gefahrbringenden Ausfälle werden durch Test- oder Überwachungsmaßnahmen erkannt und daraufhin das System in einen sicheren Zustand überführt (Beispiel: Geschlossenbleiben von Schützkontakten oder Offenbleiben eines Ventils, was durch einen Rücklesekontakt bzw. eine Stellungsüberwachung erkannt und sicher abgefangen wird).
- Unerkennbar gefahrbringende Ausfälle DU (dangerous undetectable): Diese potenziell gefahrbringenden Ausfälle werden nicht erkannt (Beispiel: unbemerktes Geschlossenbleiben der Kontakte eines Schützes oder Offenbleiben eines Ventils, wodurch dieses Element seinen Beitrag zum Stillsetzen einer gefahrbringenden Bewegung nicht erbringen kann, wenn eine Sicherheitsfunktion dies anfordert).

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 *DC* ergibt sich aus dem 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. Obwohl die Güte der Diagnose vom Fehleraufdeckungsvermögen der Testeinrichtung bestimmt wird, wird die Kenngröße *DC* nicht der Testeinrichtung, sondern der getesteten Einheit (z. B. einem Block) zugeordnet. Um die *DC*-Bestimmung zu vereinfachen, bietet DIN EN ISO 13849-1 neben der FMEA einen anderen Weg an: Sie schlägt für typische Diagnosemaßnahmen *DC*-Schätzwerte vor, von deren Erreichung ausgegangen werden kann, wenn die entsprechende Maßnahme korrekt umgesetzt wird. Auf diese Weise reicht eine tabellarische Bewertung der pro Einheit umgesetzten Diagnosemaßnahmen aus. Dies ist in ähnlicher Weise oft gängige und ökonomisch sinnvolle Praxis von Prüfstellen.

Da der Anteil der unerkennbar gefahrbringenden Ausfälle (also 1 – *DC*) die für die Ausfallhäufigkeit relevante Größe zur Bewertung der realisierten Test- und Überwachungsmaßnahmen ist, erklärt sich die Wahl der Schätzwerte (60, 90 und 99 %), mit deren Hilfe vier *DC*-Klassen (Qualitätsstufen) gebildet werden (**Tabelle E.1**).

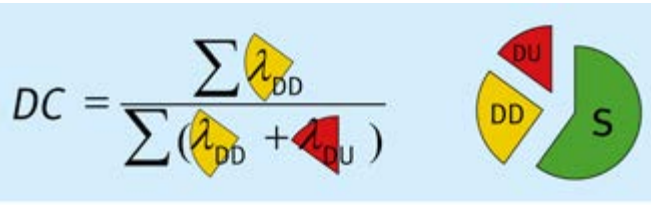


Abb. E.1 Illustration des Diagnosedeckungsgrades

Tabelle E.1 Die vier Stufen des Diagnosedeckungsgrades (*DC*) im vereinfachten Ansatz der DIN EN ISO 13849-1

Bezeichnung des *DC*	Bereich des *DC*
kein	$DC < 60\ \%$
niedrig	$60\ \% \leq DC < 90\ \%$
mittel	$90\ \% \leq DC < 99\ \%$
hoch	$99\ \% \leq DC$

Grundsätzlich muss unterschieden werden zwischen dem *DC*, den ein einzelner Test für eine bestimmte Komponente bzw. einen Block bewirkt, und dem durchschnittlichen Diagnosedeckungsgrad DC_{avg} (average) für das gesamte betrachtete Teilsystem einer sicherheitsbezogenen Steuerung (SRP/CS). Die Gruppenbildung mithilfe der Schätzwerte wird dabei sowohl zur Einstufung der einzelnen Tests herangezogen als auch zur Klassifzierung von DC_{avg}. Da DC_{avg} eine der Eingangsgrößen für die vereinfachte Quantifizierung der Ausfallhäufigkeit mithilfe des Säulendiagramms ist, wird der berechnete DC_{avg}-Wert auf den nächstniedrigeren der vier Eckwerte (0, 60, 90 und 99 %) aus Tabelle E.1 abgerundet und dadurch in eine der vier *DC*-Klassen (kein, niedrig, mittel, hoch) eingeordnet. Beispielsweise wird ein DC_{avg}-Wert von 80 % im vereinfachten Ansatz auf einen Wert von 60 % herabgestuft. (Der IFA Software-Assistent SISTEMA vermeidet in seiner Grundeinstellung diese De-facto-Abwertung der tatsächlichen Diagnosegüte, indem er mit DC_{avg}-Zwischenwerten rechnet, siehe Anhang H.) Im Folgenden wird zunächst auf den *DC* einzelner Tests und danach auf die Berechnung von DC_{avg} eingegangen.

In **Tabelle E.2** auf Seite 268 sind typische Test- und Überwachungsmaßnahmen bezogen auf Komponenten (in der Regel Elemente oder Blöcke) und ihre *DC*-Bewertung nach DIN EN ISO 13849-1 dargestellt. Für jede Funktion (I, L, O bzw. Eingabe, Logik, Ausgabe), Kategorie und Technologie sind spezifische Maßnahmen üblich. Ihre Bewertung kann abhängig von der Ausführung oder äußeren Umständen schwanken, z. B. je nach Anwendung, in der die Steuerung betrieben wird. Zu den in Tabelle E.2 genannten Maßnahmen sind im folgenden weitere Hinweise und Einschränkungen sowie typische Realisierungen in verschiedenen Technologien aufgeführt.

Zyklische Testung/Dynamisierung von Eingängen (I):

- Für die Eingabe-Signale wird ein Signalwechsel generiert (Dynamisierung), der mit einer Überwachung der erwarteten Ergebnisse einhergeht. Ein Beispiel für diese Maßnahme sind automatisch erzeugte kurzzeitige Testimpulse auf den Signalleitungen, die zur Fehlererkennung dienen, ohne die Sicherheitsfunktion auszulösen.

Kreuzvergleich ohne Dynamisierung (I, O):

- Redundante Eingänge oder Ausgänge werden in beiden Kanälen auf Gleichheit geprüft. Bei redundanten Ausgängen erwähnt die Norm auch den Vergleich nur in einem Kanal.
- Da Stuck-At-Fehler (statische Fehler oder Einfrieren von Zuständen, z. B. durch Kurzschlüsse oder Unterbrechungen) nur bei einem Signalwechsel erkannt werden können, ist die Effektivität dieser Maßnahme davon abhängig, wie häufig (dynamisch) sich dieser Signalwechsel in der jeweiligen Applikation ergibt. Nur wenn ein solcher mit einem Signalwechsel verbundener Test mindestens einmal pro Monat erfolgt, kann ein *DC* von 99 % beansprucht werden. Für seltenere Tests, die aber mindestens einmal pro Jahr stattfinden, kann maximal ein *DC* von 90 % angesetzt werden. Erfolgen die Tests noch seltener als einmal pro Jahr, wird ein *DC* von 0 % unterstellt. Der Einfluss der Testhäufigkeit wird auch in Abschnitt 6.2.14 dieses Reports thematisiert.

Kreuzvergleich mit Dynamisierung, aber ohne hochwertige Fehlererkennung (I, O):

- Diese Variante des Kreuzvergleichs unterscheidet sich von der vorgenannten Maßnahme dadurch, dass ein ausreichend häufiger Signalwechsel aus der Anwendung heraus oder automatisiert durch die Steuerung vorliegt. Allerdings erfolgt keine hochwertige Fehlererkennung, d. h., dass Querschlüsse zwischen mehreren Ein- oder Ausgängen nicht erkannt werden. Hier sind Querschlüsse zwischen redundanten Signalleitungen besonders kritisch, da damit die Fehlererkennung durch den Vergleich zunichte gemacht wird.

Kreuzvergleich mit Dynamisierung und hochwertiger Fehlererkennung (I, O):

- Diese dritte Variante des Kreuzvergleichs ist sowohl an einen ausreichend häufigen Signalwechsel als auch eine hochwertige Fehlererkennung gebunden. Dabei werden statische Zustände und Querschlüsse zwischen mehreren Ein- oder Ausgängen, insbesondere zwischen redundanten Signalleitungen, erkannt. Indem nicht nur die Eingangs- und Ausgangssignale, sondern auch Zwischenergebnisse in der Logik verglichen werden sowie eine zeitliche und logische Überwachung des Programmablaufs erfolgt, werden nahezu alle möglichen Fehler detektiert. Diese Art der Fehlererkennung wird typischerweise in elektrischen Sicherheitsbausteinen zur Überwachung der angeschlossenen Ein- und Ausgänge umgesetzt. Bei unabhängig durch verschiedene Sensoren gewonnenen Stellungs- oder Geschwindigkeitsinformationen, die in beiden Kanälen einer programmierbaren elektronischen Logik verglichen werden, wird diese hochwertige Fehlererkennung ebenfalls angewendet.

Direkte Überwachung (I, L, O):
- Eine direkte, unmittelbare Überwachung erfolgt typischerweise am Steuerungselement. Dabei werden das Ansteuersignal und die Rückleseinformation bei jedem Signalwechsel auf Plausibilität geprüft. Bei pneumatischen oder hydraulischen Ventilen kann dies beispielsweise durch eine Stellungsüberwachung direkt am Ventilschieber über den gesamten Hub erfolgen. Elektromechanische Bauteile können mittels zwangsgeführter Rücklesekontakte (antivalente Öffnerkontakte) direkt überwacht werden. Digitale elektronische Signale können rückwirkungsfrei z. B. mittels Optokopplern zurückgelesen werden.

Indirekte Überwachung (I, L, O):
- Hier findet die Überwachung mittelbar statt, indem beispielsweise Wegaufnehmer oder Endschalter an den Aktoren (Zylinder, Motor) statt an den Steuerungselementen genutzt werden. In pneumatischen oder hydraulischen Steuerungen können auch hinter den Ventilen angebrachte Druckschalter eingesetzt werden.
- Je nach Anwendung kann hier ein mittlerer bis hoher *DC* erreicht werden. Die indirekte Überwachung kann also in bestimmten Situationen genauso effektiv sein wie die direkte Überwachung. Um die Wirksamkeit in der konkreten Anwendung verlässlich abzuschätzen, sind die Betrachtung aller relevanten gefährlichen Fehler (siehe Fehlerlisten in Anhang C) und eine Einschätzung ihrer Erkennbarkeit erforderlich. Im Zweifel sollte eine Ausfalleffektanalyse (FMEA) die Basis für die Ermittlung des *DC* sein. Die indirekte Überwachung durch Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen lässt in manchen Anwendungen z. B. keinen Rückschluss zu, ob jeder von zwei redundanten Funktionskanälen die Sicherheitsfunktion noch unabhängig ausführen kann.

Fehlererkennung durch den Prozess (I, L, O):
- Zur *DC*-Maßnahme „Fehlererkennung durch den Prozess“ gibt die Norm Erläuterungen in Form von Beispielen: „*Die DC-Maßnahme „Fehlererkennung durch den Prozess“ kann nur angewendet werden, wenn das sicherheitsbezogene Bauteil am Fertigungsprozess beteiligt ist, z. B. wenn eine normale SPS oder normale Sensoren für die Fertigung eines Werkstücks benutzt werden, und als Teil von einem von zwei Kanälen, die die Sicherheitsfunktion ausführen, fungieren. Das geeignete DC-Level hängt von der Überschneidung der gewöhnlich verwendeten Ressourcen (Logik, Eingänge/Ausgänge) ab. Wenn beispielsweise alle Fehler eines Drehreglers in einer Druckmaschine zu stark sichtbaren Fehlern im Druckvorgang führen, kann der DC für diesen Sensor, der zur Überwachung einer sicher begrenzten Geschwindigkeit genutzt wird, zwischen 90 % und 99 % abgeschätzt werden.*“
- Da die Effektivität dieser Maßnahme zur Fehlererkennung sehr stark von der jeweiligen Anwendung abhängt und ihr *DC* zwischen 0 und *99* % liegen kann, ist die Einschätzung der Erkennbarkeit aller möglichen gefährlichen Fehler in Form einer FMEA hier angeraten.
- Die Wirksamkeit der Fehlererkennung im Prozess ist unter anderem davon abhängig, wie oft im Vergleich zur Anforderungsrate der Sicherheitsfunktion im Prozess getestet wird (Prozessdiagnoserate bzw. Testrate). Wird mehr als 100-mal häufiger getestet als angefordert, ist der *DC* nicht begrenzt und kann mit bis zu *99* % abgeschätzt werden. Wird nur mehr als zehnmal häufiger getestet als angefordert, so ist der *DC* auf 90 % limitiert. Wird gerade einmal das Verhältnis 1:1 überschritten, dann ist 60 % die Obergrenze für den *DC*. Erfolgt die Testung seltener als die Anforderung, ist in der Regel keine nennenswerte Fehlererkennung mehr gegeben.
- Für PL_r = e ist die Maßnahme „Fehlererkennung durch den Prozess“ allein nicht ausreichend und führt bei der Verwendung von SISTEMA zu einer roten Warnmeldung. Bei ausreichender Rechtfertigung, z. B. durch weitere *DC*-Maßnahmen, die auf denselben Block wirken, oder wenn der komplementäre Block des redundanten Kanals eine andere *DC*-Maßnahme umsetzt, deren *DC* mindestens so groß ist wie der angenommene *DC* durch den Prozess, kann diese Maßnahme trotzdem in Rechnung gestellt werden. In SISTEMA kann dies durch eine direkte *DC*-Eingabe mit manueller Wahl der Prozentstufe erfolgen, bei gleichzeitiger Dokumentation der Rechtfertigung.

Überwachung von Eigenschaften (I):
- Diese Maßnahme bezieht sich auf die Überwachung einiger Merkmale von Sensoren, wie die Antwortzeit oder den Bereich analoger Kenngrößen, z. B. Widerstand oder Kapazität. Verlassen die Merkmale den gültigen oder erwarteten Bereich, so kann dies je nach Anwendung zur Fehlererkennung auf niedrigem Niveau genutzt werden.
- Beispiele sind analoge Wegaufnehmer sowie andere Sensoren mit analogen elektrischen Schnittstellen, bei denen nur bestimmte Wertebereiche von Strom oder Spannung einem in der Applikation gültigen Zustand entsprechen.

Einfache zeitliche Programmlaufüberwachung (L):
- Diese Maßnahme eignet sich zur Überwachung des Logikteils auf fehlerhafte Inaktivität.
- Ein typisches Beispiel für die Umsetzung ist die Überwachung eines programmierbaren Bauteils durch einen separaten Watchdog, wenn der Watchdog lediglich aus dem Programm heraus Signale zum Zurücksetzen seines Zeitglieds erhält, ohne dass die Rücksetzsignale eine logische Information enthalten, die beispielsweise auf eine korrekte Abfolge oder Plausibilität bei der Programmabarbeitung überprüft werden.

Zeitliche und logische Programmlaufüberwachung (L):
- Hier enthalten die zwischen programmierbarem Bauteil und Watchdog ausgetauschten Signale zusätzliche logische Informationen, die neben der Überwachung auf Aktivität auch Plausibilitätstest des Verhaltens der Logik ermöglichen und damit Rückschlüsse über einen korrekten Programmablauf zulassen.

Selbsttests bei Anlauf (L, O):
- Diese Selbsttests werden beim Anlauf einer Maschine, z. B. zu Schichtbeginn oder beim Einschalten, ausgeführt und erlauben die Erkennung bestimmter Fehler in Teilen der Logik.
- Typische Beispiele sind RAM- und ROM-Tests zur Erkennung von verborgenen Fehlern in Programm- und Datenspeichern, sowie Tests der Eingangs- und Ausgangsanschlüsse oder von Schnittstellen. Auch das Verschweißen elektromechanischer Kontakte kann durch testweise kurzzeitige Absteuerung des Elements und Rücklesung von zwangsgeführten Meldekontakten erkannt werden.
- Der erreichte *DC* ist abhängig von der Testausführung. Darum ist mit der vierten Normausgabe die Spanne für den geschätzten *DC* nach unten erweitert worden und nun mit 60 bis 90 % angegeben. Auch hier ist eine Fehlerbewertung, im Zweifel durch eine FMEA, für die *DC*-Schätzung angeraten.

Testung der Überwachungseinrichtung (L):
- Die Beschreibung dieser Maßnahme ist interpretationsbedürftig, da sie sich nicht auf die Fehlererkennung eines Bauteils in einem Funktionskanal bezieht, sondern darauf, die Funktionsfähigkeit einer Überwachungseinrichtung zu überprüfen. Der angegebene *DC*-Schätzwert von 90 % gilt daher für die Erkennung eines Ausfalls der Überwachungseinrichtung. Wie in Abschnitt 8.2.14 zur Zuverlässigkeit einer Testeinrichtung bereits erläutert, hat eine solche Testung meist nur geringen Einfluss auf die Ausfallhäufigkeit eines Teilsystems. In Teilsystemen der Kategorie 2 ist zunächst die Zuverlässigkeit des Funktionskanals gefragt und in zweiter Linie die durch den Testkanal bewirkte Fehlererkennung für den Funktionskanal, deren Güte in Form des *DC* angegeben wird. Im vereinfachten Verfahren zur PL-Abschätzung (siehe Abschnitt 8.2.16) wird bei Kategorie 2 eine Erkennung von Fehlern im Testkanal überhaupt nicht berücksichtigt – der *DC*-Schätzwert von 90 % für die Maßnahme „Testung der Überwachungseinrichtung“ geht dort also gar nicht in die *PFH*-Berechnung ein. Für eine rechnerische Berücksichtigung wäre daher ein komplexeres Verfahren zur *PFH*-Bestimmung erforderlich. Bei Teilsystemen der Kategorie 3 gibt es allerdings einen Spezialfall, der ebenfalls einen Funktionskanal und einen Testkanal verwendet. Um mit dieser Struktur die bei Kategorie 3 geltende Anforderung der Einfehlersicherheit einzuhalten, müssen zwei Bedingungen erfüllt sein: Der Testkanal muss gefahrbringende Ausfälle des Funktionskanals praktisch lückenlos aufdecken und er muss in der Lage sein, auf einen erkannten Fehler schnell genug (innerhalb der spezifizierten Reaktionszeit der Sicherheitsfunktion) zu reagieren und einen sicheren Zustand herzustellen. Durch die Einhaltung dieser Bedingungen wird der Testkanal ertüchtigt, unabhängig vom eigentlichen Funktionskanal ebenso wie dieser einen sicheren Zustand herbeizuführen. Somit übernimmt der Testkanal bei diesem Spezialfall praktisch die Rolle eines zweiten Funktionskanals. Die für Kategorie 3 ebenfalls geltende Anforderung, einen Fehler „wann immer vernünftigerweise durchführbar“ zu erkennen, kann in einer solchen besonderen Struktur dazu führen, dass eine Erkennung von Fehlern im Testkanal erfolgen muss. Zudem muss bei Kategorie 3 der *DC* des gesamten Teilsystems (hier also Funktions- und Testkanal einschließend) mindestens niedrig (60 %) sein. Die Testmaßnahme „Testung der Überwachungseinrichtung“ bietet hier eine Möglichkeit, einen *DC* von 90 % für den Testkanal in seiner Rolle als zweiter Funktionskanal bereitzustellen. Dazu wird das Ansprechvermögen der Überwachungseinrichtung durch den Funktionskanal überprüft. Dieser Test kann z. B. beim Anlauf der Maschine erfolgen oder bei einer Anforderung der Sicherheitsfunktion. Auch eine Initiierung durch ein externes Signal ist hier denkbar. Die *PFH*-Ermittlung kann in diesem Spezialfall mit dem vereinfachten Verfahren der Norm erfolgen, wobei der Funktions- und der Testkanal wie die beiden Kanäle einer Kategorie 3 behandelt werden. In die Berechnung von DC_{avg} fließt der nach Norm mit 90 % abgeschätzte *DC* für den Testkanal ein. Ebenso fließt auch der *DC* für den perfekten Test des Funktionskanals ein, der üblicherweise konservativ mit 99 % abgeschätzt wird.

Dynamisierung der Logik (L):
- Hier wird die Steuerung so ausgelegt, dass alle Bauteile der Logik eine Zustandsänderung EIN-AUS-EIN erfordern, wenn die Sicherheitsfunktion angefordert wird.
- Beispiele sind Verriegelungsschaltungen in der Pneumatik oder Relaistechnik, die einen sicheren Zustand einnehmen, wenn kein ordnungsgemäßes Ein- und Ausschalten der Steuerungselemente möglich ist.

Speicher- und CPU-Tests (L):
- In Tabelle E.2 sind verschiedene Tests für Speicher und CPU (Verarbeitungseinheit) mit entsprechenden Schätzwerten für *DC* genannt. Bei den beiden CPU-Tests ist eine Bandbreite für *DC* angegeben, sodass für jede konkrete Anwendung eine Fehlerbewertung, im Zweifel durch eine FMEA, angeraten ist.
- 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.

Redundanter Abschaltpfad mit Überwachung der Ausgänge durch die Logik und Testeinrichtung (O):

- Diese Maßnahme bezieht sich auf die Überwachung der Ausgänge eines Teilsystems, speziell die Leistungssteuerungselemente (Ausgänge der SRP/CS-Steuerungskette), die sowohl in der Logik als auch in der Testeinrichtung erfolgt.

Generell wird bei der Bewertung mittels eines *DC*-Zahlenwertes nicht unterschieden zwischen automatischen (z. B. regelmäßig ablaufenden Programmroutinen) oder willensabhängigen Tests (z. B. manuell durch den Bediener in regelmäßigen Abständen eingeleitete Tests), siehe dazu auch Abschnitt 8.2.14. Prinzipiell ist für den *DC*-Zahlenwert unerheblich, welche Einheit einen Test durchführt, ob es sich z. B. um einen Selbsttest handelt oder die Fehlererkennung durch einen nachgeordneten Block im selben oder einem anderen Funktionskanal handelt. Allerdings ist ein Test nur bei sichergestellter Unabhängigkeit von testender und getesteter Einheit überhaupt wirksam. Beispielsweise wird die für Kategorie 3 erforderliche Einfehlersicherheit nicht erreicht, wenn ein Fehler, der zum Ausfall der Sicherheitsfunktion führt, zugleich auch die Erkennung dieses Fehlers ausfallen lässt, sei es wegen einer Überlappung zwischen funktionsausführender und testender Hardware oder wegen einer unzureichenden Widerstandsfähigkeit gegen Ausfälle infolge gemeinsamer Ursache. Wichtig ist weiterhin, dass nach Erkennung eines gefahrbringenden Ausfalls auch der sichere Zustand eingenommen wird. Wird z. B. das Verschweißen eines Hauptschützes erkannt, aber ohne eine Möglichkeit zur rechtzeitigen Stillsetzung einer gefahrbringenden Bewegung, so ist die Erkennung nutzlos und mit einem *DC* von 0 % zu bewerten.

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* [%]	Maßnahmenbeschreibung
	I	L	O		
Zyklische Testung/Dynamisierung von Eingängen	X			90	Periodische Generierung eines Signalwechsels mit Überwachung des Ergebnisses
Kreuzvergleich					Gleichheitsprüfung redundanter Ein-/Ausgänge
• ohne Dynamisierung	X		X	0-99	*DC*-Wert abhängig von der Häufigkeit eines Signalwechsels in der Anwendung
• mit Dynamisierung, ohne hochwertige Fehlererkennung	X		X	90	Erkennung statischer Fehler, ohne Querschlusserkennung
• mit Dynamisierung, mit hochwertiger Fehlererkennung	X		X	99	Erkennung statischer und logischer Fehler, mit Querschlusserkennung, sowie zeitlicher und logischer Programmlaufüberwachung
Direkte Überwachung	X	X	X	99	unmittelbar am Steuerungselement
Indirekte Überwachung	X	X	X	90-99	mittelbar, z. B. an den Aktoren, *DC*-Wert abhängig von der Anwendung
Fehlererkennung durch den Prozess	X	X	X	0-99	*DC*-Wert abhängig von der Anwendung, Diese Maßnahme alleine ist nicht ausreichend für PL e
Überwachung von Eigenschaften	X			60	gültige Wertebereiche von Signalen
Programmlaufüberwachung					z. B. Watchdog oder gegenseitige Überwachung
• einfache zeitliche		X		60	reine Aktivitätsüberwachung
• zeitlich und logisch		X		90	Überwachung der Aktivität und korrekten Funktion
Selbsttests bei Anlauf		X	(X)	60-90	zur Erkennung verborgener Fehler, *DC* abhängig von der Testausführung
Testung der Überwachungseinrichtung		X		90	bei einfehlersicheren Steuerungen, bestehend aus einem Funktions- und einem Testkanal
Dynamisierung der Logik		X		99	Verriegelungsschaltungen in Pneumatik oder Relaistechnik

Maßnahme	hauptsächlich relevant für			*DC* [%]	Maßnahmenbeschreibung
	I	L	O		
Speicher- und CPU-Tests					
• Invariabler Speicher: Signatur einfacher Busbreite (8 Bit)		X		90	
• Invariabler Speicher: Signatur doppelter Busbreite (16 Bit)		X		99	
• Variabler Speicher: RAM-Test durch Kreuzvergleich redundanter Daten		X		60	z. B. Flags, Merker, Konstanten, Timer
• Variabler Speicher: Test der Lesbarkeit und Beschreibbarkeit		X		60	nur für benutzte Speicherzellen erforderlich
• Variabler Speicher: RAM Selbsttest oder doppeltes RAM mit Hardware- oder Software-Vergleich und Schreib-/Lese-Tests		X		99	z. B. Selbsttests "Galpat" oder "Abraham"
• Verarbeitungseinheit: Selbsttest durch Software		X		60-90	siehe IEC 61508-7:2010, A.3
• Verarbeitungseinheit: Kodierte Verarbeitung		X		90-99	siehe IEC 61508-7:2010, A.3
Redundanter Abschaltpfad mit Überwachung der Ausgänge durch die Logik und Testeinrichtung			X	99	siehe Beispiel in ISO 13849-2:2012, Anhang E

Weitere Informationen zur *DC*-Bestimmung für typische Testmaßnahmen finden sich z. B. in den Tabellen A.2 bis A.14 der DIN EN 61508-2 [E1]. Dort sind die Eckwerte von „niedrig“ (60 %), „mittel“ (90 %) und „hoch“ (99 %) als maximaler durch die jeweilige Maßnahme zu erreichender *DC* notiert. Bei geeigneter uneingeschränkter Umsetzung der genannten Maßnahmen kann dieser Höchstwert aber in der Regel zur Abschätzung herangezogen werden. Anhang E der DIN EN ISO 13849-2 [E2] zeigt ein ausführliches Beispiel für die Validierung des Ausfallverhaltens und der Diagnosemaßnahmen an einer automatischen Montagemaschine.

Nach der Bestimmung des *DC* für einzelne Testmaßnahmen und vor der Berechnung des DC_{avg} muss der *DC*-Wert pro Block ermittelt werden. Meist wirkt eine einzelne Testmaßnahme auf einen gesamten Block (z. B. Kreuzvergleich). Dann kann der Einzelwert einfach für den Block übernommen werden. Es sind aber weitere Konstellationen möglich:

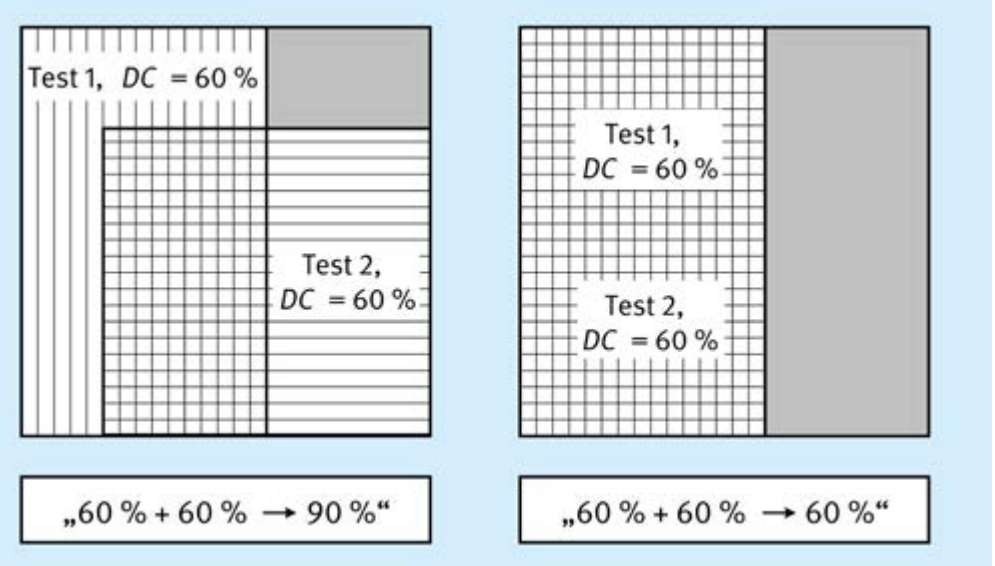


Abb. E.2
Wirken auf einen Block mehrere Tests, so kann deren Überlappung zu einem höheren Gesamt-*DC* führen (links) oder auch nicht (rechts); die schraffierten Flächen repräsentieren den Anteil der erkannten gefahrbringenden Ausfälle; die quadratische Gesamtfläche repräsentiert alle gefahrbringenden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

- 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 eine Analyse der durch jeden Test abgedeckten Ausfälle, üblicherweise in Form einer FMEA (siehe Anhang B).
- Ein Block besteht aus mehreren Einheiten, von denen jede durch andere Maßnahmen getestet wird, z. B. programmierbare Elektronik mit separaten Tests für Speicher und Verarbeitungseinheit (siehe **Abbildung E.3**). Dann ist der Block-*DC* mindestens so gut wie der schlechteste Einzel-*DC*. Ob es zulässig ist, dass hier Einheiten ohne Testung vorkommen, muss mit der entsprechenden Kategorie-Definition, siehe Abschnitte 8.2.5 bis 8.2.7, geprüft werden. Für den *DC* der Logik gelten weitere Anforderungen, siehe Seite 267 unten. Ein besserer und genauerer Wert für den Block-*DC* lässt sich durch Gewichtung des Einzel-*DC*-Wertes mit der zugehörigen Ausfallrate λ_D (= 1/$MTTF_D$) erreichen. Auch auf Block-Ebene kann hierzu Gleichung (E.1) aus Abbildung E.1 als Mittelungsformel verwendet werden. Je nach Genauigkeit gipfelt eine solche Analyse allerdings ebenfalls in einer FMEA.
- Bei einer Kaskadierung, z. B. von elektromechanischen Positionsschaltern, die über gemeinsame Anschlussleitungen mit einem Sicherheitsbaustein verbunden sind, kann es zu einer Reduzierung des *DC* kommen. Durch eine elektrisch zweikanalige Ausführung können bestimmte Fehler eines Positionsschalters durch logisch nicht plausible Signale beider elektrischen Kontakte vom Sicherheitsbaustein aufgedeckt werden. So wird nach Schließen der Tür mit dem defekten Schalter der Start der Maschine verhindert. Wird außer der Tür mit dem gefährlich ausgefallenen Positionsschalter noch eine weitere geöffnet, kann – je nach Reihenfolge – die Fehlererkennung nicht erfolgen. Die Kaskadierung führt damit zu einer Reduzierung des *DC*, die u. a. abhängig ist von der Anzahl der Schutztüren und der Häufigkeit ihres Öffnens. Details dazu und zur Abschätzung des *DC* für solche Konstellationen sind in ISO/TR 24119 [E3] dargestellt. Dort wird in Abschnitt 6.1 bei Kaskadierung PL e ausgeschlossen. Wird für jeden Positionsschalter ein zusätzlicher Kontakt zur Fehlererkennung eingesetzt, dann ist die Fehlererkennung auch bei Kaskadierung nicht eingeschränkt und PL e erreichbar.

Der durchschnittliche *DC* für ein Teilsystem wird mit DC_{avg} bezeichnet und errechnet sich aus den *DC*-Werten aller Blöcke in Funktionskanälen. Im Gegensatz zur $MTTF_D$ pro Kanal wird nicht zwischen den Steuerungskanälen unterschieden, sondern direkt ein Gesamtwert ermittelt. Die Mittelungsformel gewichtet die Einzel-*DC*-Werte mit der zugehörigen Ausfallrate λ_D (= 1/$MTTF_D$) jedes Blocks. Dies gewährleistet, dass Blöcke mit einer hohen Ausfallrate, d. h. geringen $MTTF_D$, stärker berücksichtigt werden als Blöcke, deren gefahrbringender Ausfall vergleichsweise unwahrscheinlich ist. Die Mittelungsformel, bei der N Funktionsblöcke vorausgesetzt sind, lautet:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}} \qquad \text{(E.1)}$$

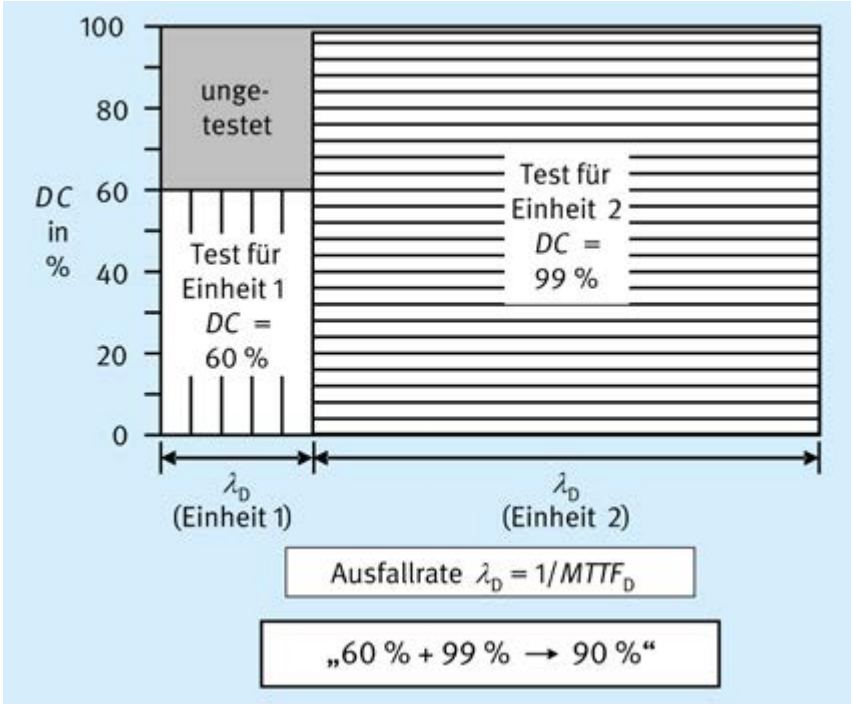


Abb. E.3
Bei der *DC*-Mittelung für mehrere Einheiten eines Blocks ergibt die Gewichtung der Einzel-DC für 60 % und 99 % mit λ_D einen anderen Wert (90 %) als z. B. das ungewichtete arithmetische Mittel (79,5 %)

Die Summation läuft über alle in Funktionskanälen enthaltenen Blöcke im Teilsystem mit folgender Festlegung:

- Für Blöcke ohne Diagnose wird ein *DC* von 0 % eingesetzt. Diese Blöcke tragen damit nur zum Nenner des Bruchs bei. Ob fehlende Diagnose für Blöcke im Einklang mit den Anforderungen der jeweiligen Kategorie steht, muss im Einzelfall entschieden werden. Kategorie 2 fordert die „Testung des Funktionskanals (I, L, O)“, Kategorie 3 die Fehlererkennung „wann immer vernünftigerweise durchführbar“. Kategorie 4 fordert ebenfalls die Erkennung des einzelnen Fehlers und nur, „wenn diese Erkennung nicht möglich ist“, die Ausführung der Sicherheitsfunktion auch bei Anhäufung unerkannter Fehler.
- Für Blöcke mit Fehlerausschluss bezüglich der gefahrbringenden Ausfallrichtung (verschwindende Ausfallrate λ_D bzw. unendlich hohe $MTTF_D$) wird der entsprechende Summand im Zähler und im Nenner weggelassen.
- Alle Blöcke ohne Fehlerausschluss, die Sicherheitsfunktionen in den verschiedenen Funktionskanälen ausführen, werden berücksichtigt. Blöcke, die allein der Testung dienen, werden nicht berücksichtigt. Für Kategorie-2-Strukturen bedeutet dies, dass Blöcke des Testkanals („TE“ und „OTE“) nicht in die DC_{avg}-Berechnung einbezogen werden. In Kategorie 3 und 4 wird der *DC*-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 Ausfallhäufigkeit des Gesamtsystems sind neben dem *DC* weitere Größen zu berücksichtigen. Dazu zählt neben der Testrate z. B. die Ausfallrate der Testeinrichtung selbst. In mehrkanaligen Systemen hat allerdings die Häufigkeit eines Tests geringere Auswirkungen, weil die Testintervalle 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 kürzer bleiben als die $MTTF_D$ eines Kanals. Abschnitt 8.2.14 gibt ausführlichere Erläuterungen zur notwendigen Testhäufigkeit. In Kategorie 2-Strukturen macht jedoch der Ausfall der Testeinrichtung aus einem einkanalig getesteten System ein einkanalig ungetestetes System, das beim nächsten Ausfall die Sicherheitsfunktion nicht mehr ausführen kann. Daher gelten für die vereinfachte Beurteilung der Ausfallhäufigkeit von Kategorie 2-Teilsystemen neben Anforderungen zum *DC* weitere Voraussetzungen:

- Alle Testraten sollten mindestens 100-mal und müssen mindestens 25-mal größer sein als die Anforderungsrate der Sicherheitsfunktion, wobei die Norm den Faktor 100 als den Normalfall betrachtet und den Faktor 25 als die Ausnahme. Alternativ kann die Testung bei Anforderung der Sicherheitsfunktion so schnell ausgeführt werden, dass der sichere Zustand erreicht wird, bevor es zu einer Gefährdung kommt. Damit soll gewährleistet werden, dass ein Ausfall von einem Test erkannt werden kann, bevor eine Anforderung der Sicherheitsfunktion nicht bedient werden kann (siehe auch Anhang G).
- Die $MTTF_D$ des Testkanals (TE und OTE) muss mindestens halb so groß sein wie die $MTTF_D$ des Funktionskanals (I, L und O). Durch diese Annahme wird sichergestellt, dass die Ausfallhäufigkeit des Testkanals nicht unangemessen hoch ist. Ist diese Bedingung verletzt (auch nach Begrenzung der $MTTF_D$ des Funktionskanals auf 100 Jahre), so ist es natürlich zulässig, die Ausfallhäufigkeit des Teilsystems mit einer $MTTF_D$ des Funktionskanals zu berechnen, die rechnerisch auf die doppelte $MTTF_D$ des realisierten Testkanals reduziert wird.

Literatur

[E1] DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (2/2011). DIN Media, Berlin 2011

[E2] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (2/2013). DIN Media, Berlin 2013

[E3] ISO/TR 24119: Safety of machinery – Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts (11/2015). DIN Media, Berlin 2015

Anhang F

Ausfälle infolge gemeinsamer Ursache (CCF)

Änderung gegenüber dem IFA Report 2/2017

- Vorgaben für die Bewertung der Maßnahmen und Maßnahmenbeschreibungen gemäß der vierten Ausgabe der Norm erweitert

Der Begriff „Ausfall infolge gemeinsamer Ursache“ (Common Cause Failure, CCF) beschreibt die Tatsache, dass in einem redundanten System oder einem einkanaligen System mit separatem Testkanal durch eine Ursache mehrere Kanäle außer Funktion gesetzt werden können. Dadurch wird beispielsweise die gewünschte Einfehlersicherheit einer zweikanaligen Struktur 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 eines zweikanaligen Teilsystems.

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 gefahrbringenden Ausfälle in einem Kanal infolge derselben Ursache auch gefahrbringende Ausfälle im zweiten Kanal einhergehen. Dieser Sachverhalt ist in **Abbildung F.1** dargestellt: Die gefahrbringenden Ausfallraten beider Kanäle (symbolisch dargestellt als Ellipsenflächen) besitzen eine schraffiert dargestellte CCF-Überlappung. Der Proportionalitätsfaktor zwischen der CCF-Rate und der gefahrbringenden 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. Anhang D der DIN EN 61508-6 [F1] bedient sich dazu eines Punkteschemas, um β-Werte zwischen 0,5 und 10 % zu ermitteln. Gemäß einer langen Liste aus nach verschiedenen CCF-Ursachen sortierten Gegenmaßnahmen 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 unter Berücksichtigung von technischen Maßnahmen vorgenommen, die von Fachleuten als besonders hilfreich zur CCF-Vermeidung angesehen wurden. Es handelt sich hierbei um einen methodischen Ansatz, der nicht wissenschaftlich begründet ist, sondern auf Erfahrung beruht und auf die Technologien im Maschinenschutz Rücksicht nimmt.

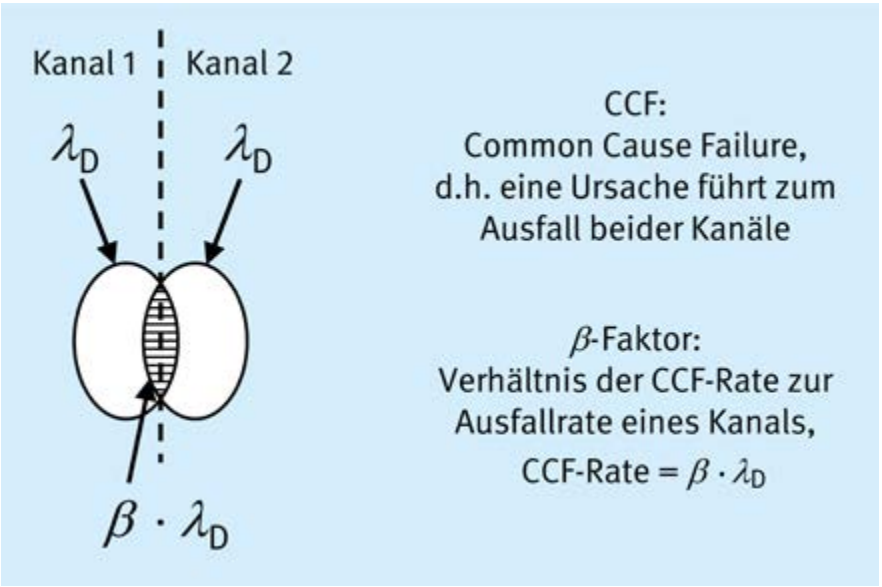


Abb. F.1
Illustration des Ausfalls infolge gemeinsamer Ursache (CCF) anhand des Beta-Faktor-Modells

Der CCF-Ansatz der Norm berücksichtigt Folgendes:

- 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. Grundlage dieser Festlegung ist die Annahme, dass ein Beta-Faktor von 2 % von einem guten Design ohne überzogene Maßnahmen erreichbar ist, weshalb auch die vereinfachte Methode zur Ermittlung des PL nach DIN EN ISO 13849-1 auf diesen Wert abgestimmt wurde.
- Die Regel für die Punktevergabe lässt nur zwei Fälle zu: Jede Maßnahme kann entweder vollständig umgesetzt (volle Punktzahl) oder nicht umgesetzt sein (Punktzahl Null). Anteilige Punktzahlen für unvollständig durchgeführte Maßnahmen werden nicht angerechnet.
- Die Bewertung der Maßnahmen (z. B. Diversität, Verwendung bewährter Bauteile) erfolgt für jedes Teilsystem separat, da sich sowohl die Struktur der Teilsysteme, ihre Anfälligkeit gegenüber CCF als auch die dagegen ergriffenen Maßnahmen zwischen den Teilsystemen unterscheiden können. Die Mindestpunktzahl von 65 Punkten muss für die Kategorien 2, 3 und 4 erfüllt und dokumentiert werden, um die vereinfachte Methode zur Bestimmung des PL 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 mit ingenieurmäßigem Sachverstand zu beurteilen, ob diese Einwirkungen als Ursachen für gemeinsame Fehler wirksam minimiert wurden. Dabei sind die bestimmungsgemäße Verwendung des SRP/CS, vorhersehbare Fehler und vernünftigerweise vorhersehbare Fehlanwendung zu berücksichtigen.
- 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 betreffen CCF den gemeinsamen Ausfall des Funktions- und Testkanals. Ein gemeinsamer Ausfall führt dazu, dass der durch die Testung angestrebte Strukturvorteil durch CCF zunichte gemacht wird. Die Bewertung der Maßnahmen ist dazu in diesem Sinne auf die Besonderheiten der Kategorie 2-Struktur anzupassen.
- Es kann sein, dass in einem Teilsystem Bauteile verwendet werden, die von sich aus noch nicht ausreichend gegen mögliche CCF-Ursachen, beispielsweise Überspannung oder klimatische Umgebungseinflüsse, geschützt sind. Hier können ausreichende CCF-Maßnahmen auch darin bestehen, durch zusätzliche externe Schutzkomponenten wie Filter oder Abschirmung die erforderliche Sicherheit gegen CCF zu erreichen.
- Für eine Maßnahme gegen Ausfälle infolge gemeinsamer Ursache, die aufgrund der inhärenten Eigenschaften der Steuerung nicht auftreten können, darf die volle Punktzahl angerechnet werden.

Eine ausführliche Beschreibung der Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache findet sich in allgemeiner Form in Anhang F der Norm und exemplarisch für ein Steuerungsbeispiel in Tabelle I.1 der Norm. Die einzelnen Maßnahmen und assoziierten Punktzahlen aus DIN EN ISO 13849-1 werden im Folgenden kurz aufgelistet:

- Trennung (15 Punkte): Physikalische Trennung zwischen den Signalpfaden, z. B.:
  - getrennte Verdrahtung/Verrohrung,
  - Erkennung von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Testung,
  - separate Schirmung der Signalpfade beider Kanäle,
  - für beide Kanäle getrennte Leiterplatten oder Bauteile in separaten Gehäusen oder Schaltschränken,
  - ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen.
- Diversität (20 Punkte): Verwendung unterschiedlicher Technologien/Gestaltung oder physikalischer Prinzipien in beiden Steuerungskanälen, z. B.:
  - ein Kanal aus programmierbarer Elektronik aufgebaut, der andere elektromechanisch fest verdrahtet,
  - Initiierung der Sicherheitsfunktion auf unterschiedliche Art, z. B. mittels Position, Druck oder Temperatur,
  - digitale und analoge Messung von physikalischen Größen (z. B. Abstand, Druck oder Temperatur),
  - Bauteile unterschiedlicher Bauart (z. B. Ventile mit Gummidichtung und Metalldichtung) oder von unterschiedlichen Herstellern produziert (keine baugleichen oder weitgehend baugleichen und nur mit verschiedenen Markennamen versehene Bauteile),
  - Positionsschalter in einem Kanal als Öffner (bei geöffneter Schutzeinrichtung betätigt) und im anderen als Schließer (bei geschlossener Schutzeinrichtung betätigt),
  - redundante Ventile oder elektromechanische Bauteile in einem Kanal unter Last schaltend und in dem anderen ohne Last.

- Entwicklung/Anwendung/Erfahrung: Schutz der Ein- und Ausgänge eines Teilsystems sowie seiner Energieversorgung, gegen Überspannung, Überdruck, Überstrom, Übertemperatur usw. (15 Punkte):
  - Beachtung der maximalen Überspannung unter Einfehlerbedingungen, besonders bei Verwendung von Schaltnetzteilen als Energieversorgung,
  - Schutz vor unbeabsichtigtem Druck, z. B. durch ein Druckentlastungsventil, wie auch nach ISO 4414 gefordert (ein einkanaliges System zum Schutz gegen Überdruck kann ausreichend sein, wenn im Fehlerfall höchstens der anderthalbfache Betriebsdruck auftritt).
- Ausschließliche Verwendung bewährter Bauteile (5 Punkte): siehe 8.2.4
- Beurteilung/Analyse (5 Punkte): Durchführung einer Ausfalleffektanalyse für jedes Teil des Teilsystems und Berücksichtigung ihrer Ergebnisse im Entwicklungsprozess, um CCF zu vermeiden
- Ausbildung (5 Punkte): Schulung des Entwicklungspersonals darin, die Ursachen und Auswirkungen von CCF zu verstehen
- Umgebungsbedingungen hinsichtlich Schutz vor schädlichen Einflüssen auf elektrische/elektronische und fluidtechnische Systeme (25 Punkte):
  - Elektrische/elektronische Systeme: Störfestigkeit und Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMI) im Einklang mit den zutreffenden Normen, siehe auch Anhang L zu Anforderungen an die elektromagnetische Störfestigkeit für funktionale Sicherheit,
  - Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums.

  Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.
- Umgebungsbedingungen hinsichtlich anderer Einflüsse (10 Punkte): Berücksichtigung der Anforderungen hinsichtlich der Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den relevanten Normen für funktionale Sicherheit festgelegt)

Auch systematische Ursachen, beispielsweise das begrenzte Detektionsvermögen eines Sensors, können zu CCF beitragen. Hier sind zusätzlich zu den in diesem Anhang beschriebenen allgemeinen Maßnahmen gegen CCF die Vorgaben und Verwendungsgrenzen des jeweiligen Herstellers und aus zutreffenden Produktnormen einzuhalten. Beispiele dafür finden sich in der Normenreihe IEC 62024 für die Anwendung von Schutzeinrichtungen zum Erkennen von anwesenden Personen oder ISO 14119:2013 für die Auswahl und Anwendung von Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen.

Literatur

[F1] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (2/2011). DIN Media, Berlin 2011

Anhang G

Was steckt hinter dem Säulendiagramm in Bild 12 der DIN EN ISO 13849-1?

Änderung gegenüber dem IFA Report 2/2017

- Schreibung von *PFH* (früher: PFH_D) und Definition dieser Größe an die neue Normversion angepasst (Ersetzung von Wahrscheinlichkeit durch Häufigkeit), Fußnote 1 hinzugefügt zur Erläuterung der Herkunft der Abkürzung *PFH*
- Textanpassungen aufgrund der in Normabschnitt 6.1.3.2.4 erhöhten Anforderungen für Kategorie 2 hinsichtlich des $MTTF_D$-Verhältnisses von Test- und Funktionskanal sowie des Verhältnisses von Test- und Anforderungsrate
- Aktualisierung der Angaben im Abschnitt „Literatur“

Die DIN EN ISO 13849-1 sieht für SRP/CS und selbst entwickelte Teilsysteme neben der Kategorieprüfung den Nachweis des Performance Levels (PL) vor. Der numerische Aspekt des PL leitet sich gemäß Tabelle 7.1 dieses Reports aus der mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde ab, die auch als *PFH*[1] bezeichnet wird. Auf der Ebene des SRP/CS, das die gesamte Sicherheitsfunktion ausführt, ergibt sich die *PFH* auf einfache Weise als Summe der *PFH*-Beiträge aller Teilsysteme (siehe Abschnitt 7.4). Für selbst entwickelte Teilsysteme muss diese Größe aus der Teilsystemstruktur, den Bauelementausfallraten, dem Diagnosedeckungsgrad der automatischen Tests, der Gebrauchsdauer des Teilsystems und, bei entsprechender Teilsystemstruktur, der Empfänglichkeit des Teilsystems gegenüber Ausfällen infolge gemeinsamer Ursache (CCF, Common Cause Failures) ermittelt werden. Die folgenden Erläuterungen beziehen sich daher nur auf die *PFH*-Bestimmung für Teilsysteme, die eine Teilfunktion ausführen. Dies schließt den Sonderfall ein, dass ein SRP/CS nur aus einem einzigen Teilsystem besteht, das die komplette Sicherheitsfunktion alleine ausführt.

Zu diesem Zweck dienen Rechenmodelle, die das Zusammenwirken der genannten Faktoren berücksichtigen und als Ergebnis die *PFH* liefern (als Mittelwert bezogen auf die Gebrauchsdauer). Für eine möglichst genaue *PFH*-Abschätzung müsste bei der Anwendung der Norm für jedes zu untersuchende Teilsystem ein maßgeschneidertes Modell erstellt werden. Zur Vereinfachung wurden für die gebräuchlichsten Strukturvarianten, die „vorgesehenen Architekturen“ aus DIN EN ISO 13849-1, Abschnitt 6.1.3.2 (vgl. Abschnitte 8.2.1 bis 8.2.7 dieses Reports), im IFA *Markov*-Modelle entwickelt, deren numerische Ergebnisse als „Säulendiagramm“ in der Norm in Abschnitt 6.1.8, Bild 12 (Abbildung 8.7 bzw. **Abbildung G.1** dieses Reports), dargestellt sind. Dadurch kann auf die Entwicklung eines eigenen Rechenmodells und eine komplexe Berechnung verzichtet werden, falls das Teilsystem im Wesentlichen die Gestalt einer der vorgesehenen Architekturen hat oder es sich in mehrere Teilsysteme von solcher Gestalt zerlegen lässt (vgl. hierzu Abschnitt 6.2 und Anhang H der DIN EN ISO 13849-1 oder die Abschnitte 7.2 bis 7.4 dieses Reports). Eine grundlegende Einführung in die Anwendung der *Markov*-Modellierung zur Berechnung der Ausfallwahrscheinlichkeit findet man z. B. in [G1] und [G2].

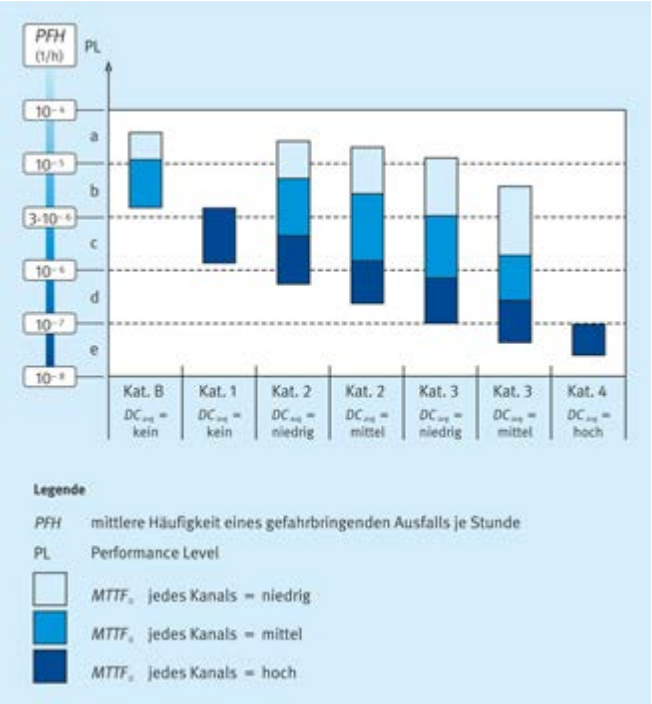


Abb. G.1 *PFH* und PL in Abhängigkeit von Kategorie, DC_{avg} und $MTTF_D$

[1] Die Bezeichnung *PFH* entstammt der ehemaligen Beschreibung als „Probability of a dangerous failure per hour“, die früher in IEC 61508 und IEC 62061 verwendet wurde. Auch nach dem Wechsel zu „Average frequency of a dangerous failure per hour“, der den Häufigkeitscharakter dieser Kenngröße ausdrückt, wurde die ursprüngliche Abkürzung beibehalten.

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 (Abschnitt 8.2.13 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. Für verschleißbehaftete Bauteile kann ersatzweise eine konstante Ausfallsrate zur sicheren Seite abgeschätzt werden (siehe Abschnitt D.2.4). Bei Zweikanaligkeit mit unterschiedlicher Kanal-$MTTF_D$ wird mit einer gemittelten Ersatz-$MTTF_D$ gearbeitet. In vergleichbarer Weise gibt der Wert DC_{avg} einen Mittelwert des Diagnosedeckungsgrades für das gesamte System an, der für die Zuordnung zu einer der vier DC_{avg}-Stufen (vgl. Tabelle 8.3) benutzt wird.

Die Sinnhaftigkeit und Zulässigkeit dieser Zusammenfassungen innerhalb der geforderten Quantifizierungsgenauigkeit wurden durch umfangreiche Testrechnungen nachgewiesen. Das gilt auch für die in Abschnitt 6.1.3.2.4 der Norm jetzt verbindlich gemachte Anforderung hinsichtlich des Verhältnisses 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 beider Funktionskanäle dürfen eine gemeinsame Ursache haben. Dies ist bei der Anwendung der Norm mit einem einfachen Schätzverfahren (Anhang F) jeweils zu belegen.

Die Markov-Modelle, die dem Säulendiagramm aus DIN EN ISO 13849-1 (bzw. Abbildung G.1 dieses Reports) zugrunde liegen, berücksichtigen den Betrieb der Teilsysteme unter Randbedingungen, die für den Maschinenbereich realistisch sind. Sie gehen davon aus, dass die Teilsysteme

- mindestens einer Anforderung der Sicherheitsfunktion pro Jahr ausgesetzt sind (genaugenommen ist hier die Anforderung der Teilfunktion gemeint, die aber in der Regel mit der Anforderung der Sicherheitsfunktion einhergeht),
- sich bei selbsttätiger Erkennung eines internen Fehlers in den sicheren Zustand „Betriebshemmung“ versetzen und dann in der Regel kurz darauf (spätestens nach einigen Stunden) manuell abgeschaltet werden,
- 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 je Stunde dar. Bei kontinuierlich vorliegender Anforderung (Continuous Mode of Operation) gibt sie die Anzahl der gefährlichen Teilsystemausfälle je Stunde an. Bei Kategorie 2 wird vorausgesetzt, dass die Testung im Hinblick auf die Zeitverhältnisse optimal wirksam ist. Dies kann durch ein adäquates Verhältnis von Test- und Anforderungsrate oder durch ausreichend schnelle Fehlerreaktion erreicht werden (vgl. Abschnitt 8.2.14). 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.1).

Trotz der prinzipiellen Berücksichtigung von Anforderungen der Sicherheitsfunktion und der Reparatur wirken sich die absoluten Größen von Anforderungsrate und Reparaturrate (Kehrwert der mittleren Reparaturzeit) nur in vernachlässigbar kleinem Maß auf die so verstandene *PFH* aus. Lediglich bei der für Kategorie 2 vorgesehenen Architektur muss gefordert werden, dass die Testung sehr viel häufiger erfolgt als die Anforderung der Sicherheitsfunktion. Dazu gibt es eine gleichwertige Alternative: Die Testung erfolgt unmittelbar bei der Anforderung und die Zeiten für die Fehlererkennung und die sicherheitsgerichtete Reaktion sind zusammen kürzer als die spezifizierte Systemreaktionszeit, vgl. DIN EN ISO 13849-1, Abschnitt 6.1.3.2.4. Die Norm fordert eine mindestens 100-mal größere Testrate im Vergleich zur Anforderungsrate. Aber selbst bis hinunter zu einem Verhältnis von 25 : 1 erhöht sich die *PFH* lediglich um ca. 10 %, was durch einen Korrekturfaktor von 1,1 berücksichtigt werden kann (vgl. Anhang K der Norm, Anmerkung 1 am Ende von Tabelle K.1). Durch diese Anforderungen an die Testhäufigkeit wird eine inakzeptabel große Wirkungseinbuße der Diagnose durch zu seltene Testausführung vermieden. Bei den Kategorien B, 1, 3 und 4 ist der Einfluss der Anforderungsrate auf die *PFH* vernachlässigbar gering. Die per Diagramm ermittelten *PFH*-Werte für diese Kategorien gelten daher für beliebige Anforderungsraten und beliebige (mittlere) Reparaturzeiten. Bei weniger als einer Anforderung pro Jahr liefert das Säulendiagramm eine Abschätzung zur sicheren Seite. Bei den Kategorien 3 und 4 gelten die *PFH*-Werte für ausreichend große Testhäufigkeiten (siehe Erläuterungen in Abschnitt 8.2.14).

Soll die Gebrauchsdauer eines Teilsystems 20 Jahre überschreiten, so verlieren die nach dem vereinfachten Verfahren (Anhang K der Norm) ermittelten *PFH*-Werte in den meisten Fällen ihre mathematische Grundlage. [G3] beschreibt dieses Problem ausführlich und nennt einige Handlungshilfen. Einige Situationen können mit wenigen

Nachbesserungen trotzdem im Rahmen des vereinfachten Verfahrens behandelt werden. Dabei sind sind aus Sicht der mathematischen Modellierung der Ausfallhäufigkeit zwei Fälle zu unterscheiden:

- Im ersten Fall ist das Teilsystem von vornherein für eine Gebrauchsdauer größer als 20 Jahre spezifiziert. Dann kann der Einfluss der höheren Gebrauchsdauer aus den *Markov*-Modellen, die Anhang K der Norm zugrunde liegen, zur sicheren Seite hin folgendermaßen abgeschätzt werden: Pro fünf Jahre längere Gebrauchsdauer als 20 Jahre wird bei den Kategorien 2, 3 und 4 ein prozentualer *PFH*-Zuschlag von 15 % eingerechnet (Kategorie B oder 1 erfordern keine *PFH*-Anpassung). Es ist nicht sinnvoll, die Gebrauchsdauer über 30 Jahre hinaus zu vergrößern. Das vereinfachte Verfahren und der danach rechnende IFA Softwareassistent „SISTEMA“ sind also trotzdem nutzbar. Voraussetzung sind konstante Ausfallraten unabhängig von der Gebrauchsdauer. Für Verschleißbauteile bedeutet dies, dass sie für die spezifizierte höhere Gebrauchsdauer T_M ausgelegt werden müssen ($T_{10D} \geq T_M$) oder nach Ablauf von T_{10D} jeweils vorsorglich ausgetauscht werden müssen.
- Im zweiten Fall war das Teilsystem für 20 Jahre Gebrauchsdauer ausgelegt, soll aber nun darüber hinaus weiterverwendet werden. Dann kann die aus der Markov-Modellierung zu erwartende *PFH*-Verschlechterung mit einem wie im ersten Fall beschriebenen Zuschlag abgeschätzt werden. Kritisch wird es bei enthaltenen Verschleißbauteilen oder sich durch Alterung verschlechternden Bauteilen, zu denen typischerweise „chemische“ Bauteile (z. B. „nasse“ Elektrolytkondensatoren, Batterien, elektrochemische Sensoren), mechanische Bauteile (z. B. Bremse, Kupplung), elektromechanische Bauteile (z. B. Schalter, Relais, Schütze), fluidtechnische Bauteile (z. B. Ventile) und manche optische Bauteile (z. B. Optokoppler) gehören. Hier kann der Betreiber der Maschine in der Regel nicht selbst beurteilen, ob alle enthaltenen Bauteile auch für eine verlängerte Gebrauchsdauer geeignet sind oder welche Maßnahmen, z. B. vorsorglicher Austausch einzelner Bauteile, Proof-Test usw., in diesem Fall durchzuführen sind. Eine Verlängerung der Gebrauchsdauer – bei oben genannten *PFH*-Zuschlag – kann dann nur erfolgen, wenn Herstellerangaben darüber vorliegen, was bei einer Verlängerung der Gebrauchsdauer zu tun ist, und wenn diese Maßnahmen vom Betreiber umgesetzt werden.

Die Säulen für Kategorie B und 1 in Abbildung G.1 wurden mithilfe eines Modells berechnet, das die Anforderung der Sicherheitsfunktion und die Reparatur berücksichtigt. Die *PFH*-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 ($DC_{avg} = 0$) praktisch dessen Ausfallrate in die gefährliche Richtung entspricht.

Für die anderen Kategorien ist jedoch eine aufwendigere Rechenmethode erforderlich. Die prinzipielle Modellierungsweise wird im Folgenden beispielhaft an der „vorgesehenen Architektur“ für Kategorie 2 erläutert. Diese Struktur ist in **Abbildung G.2** nochmals dargestellt. Es gibt fünf Funktionsblöcke, von denen die Blöcke I (Input), L (Logic) und O (Output) die eigentliche Sicherheitsfunktion in logischer Reihenschaltung ausführen. Der Block L testet die Blöcke I, O und sich selbst im Zusammenspiel mit dem Block TE (Test Equipment). Der Block OTE (Output of TE) kann bei Ausfall des Funktionskanals I-L-O einen sicheren Zustand herbeiführen. Die nicht direkt funktionsnotwendigen zusätzlichen Blöcke TE und OTE stellen somit einen Testkanal für den Fehlerfall zur Verfügung, der jedoch – anders als ein „echter“ zweiter Funktionsanal – nur bei erkannten Ausfällen im Funktionskanal wirkt.

Aus dem sicherheitsbezogenen Blockdiagramm in Abbildung G.2 kann der Zustandsgraph in **Abbildung G.3** abgeleitet werden. Dazu werden zunächst alle $2^5 = 32$ Ausfallkombinationen der fünf Funktionsblöcke gebildet. Der Zustand ohne Ausfall ist der oben abgebildete OK-Zustand. Darunter folgt eine Reihe von Zuständen mit nur einem ausgefallenen Funktionsblock, dann eine Reihe mit zwei ausgefallenen Blöcken usw. Die Zustandsbezeichnung benennt jeweils die ausgefallenen Funktionsblöcke mit einem nachgestellten „D“ für „dangerous“, das den Ausfall des Blocks in dessen „gefahrbringende“ (= sicherheitstechnisch ungünstige) Ausfallrichtung symbolisiert. Durch Ausfälle von Funktionsblöcken, abgebildet durch Pfeile, werden Folgezustände erreicht. Zustände, in denen das Teilsystem die Sicherheitsfunktion nicht mehr ausführen kann, sind rot 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 Teilsystem in gefährlicher Richtung und (für sich selbst) unerkennbar ausgefallen ist. Dieser Sammelzustand mit der Bezeichnung „System DU“ (dangerous undetectable) ist rechts dargestellt. Er kann aus verschiedenen Zuständen durch den Ausfall von Funktionsblöcken erreicht werden. In Abbildung G.3 ist unten der Zustand „Gefährliche Situation/Schaden“ zu sehen. In ihn gelangt das Teilsystem nur aus gefahrbringenden (rot dargestellten) Vorzuständen – und zwar immer dann, wenn die Sicherheitsfunktion angefordert wird. Wie der Zustand „Betriebshemmung“ 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 einer gemeinsamen Ursache (CCF). Es wird angenommen, dass bei 2 % der Ausfälle eines der Blöcke L und TE in gefährliche Richtung aufgrund derselben Ursache auch der jeweils andere Block gefährlich ausfällt. Dasselbe wird auch von den Blöcken 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 CCF an verschiedenen Stellen eine Änderung der ursprünglichen Übergangsrate. Bei der Berechnung des Säulendiagramms wird der ungünstige Fall angenommen, dass die im Teilsystem eingesetzte Testeinrichtung selbst nicht getestet wird. Darum wird einigen Übergängen in Abbildung G.3 die Rate Null zugewiesen. Systeme, die ihre Testeinrichtung testen, sind dadurch zur sicheren Seite abgeschätzt. Zur vereinfachten Berechnung nach der Markov-Methode wird angenommen, dass alle Übergangsprozesse durch konstante Übergangsraten beschrieben werden können, obwohl dies streng genommen nur für die Ausfälle von Blöcken gilt. Separate Betrachtungen rechtfertigen diese Vereinfachung.

Man geht davon aus, dass sich das Teilsystem zu Beginn der Gebrauchsdauer mit der Wahrscheinlichkeit Eins im OK-Zustand befindet und die Wahrscheinlichkeit aller anderen möglichen Systemzustände Null beträgt. Während der angenommenen Gebrauchsdauer von 20 Jahren ändern sich alle Zustandswahrscheinlichkeiten allmählich: Ausgehend vom OK-Zustand verteilen sie sich entlang der Übergangspfeile um. Die Summe aller 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 „Gefährdungsrate“ (hazard rate) darstellt. Sie kann bei hoher bis kontinuierlicher Anforderung der Sicherheitsfunktion (mindestens eine Anforderung pro Jahr), also im Anwendungsbereich der DIN EN ISO 13849-1, mit der *PFH* gleichgesetzt werden, d. h. mit der mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde.

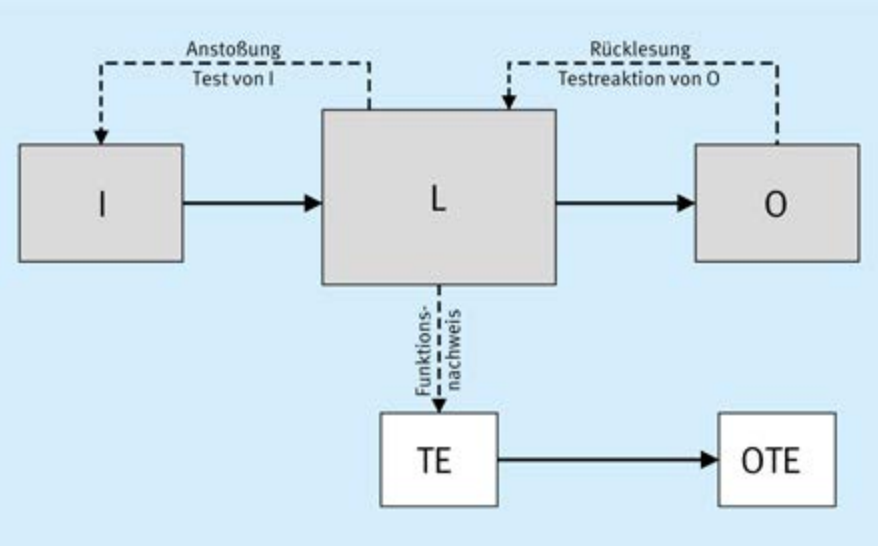


Abb. G.2
Vorgesehene Architektur für Kategorie 2 nach DIN EN ISO 13849-1, Abschnitt 6.1.3.2.4

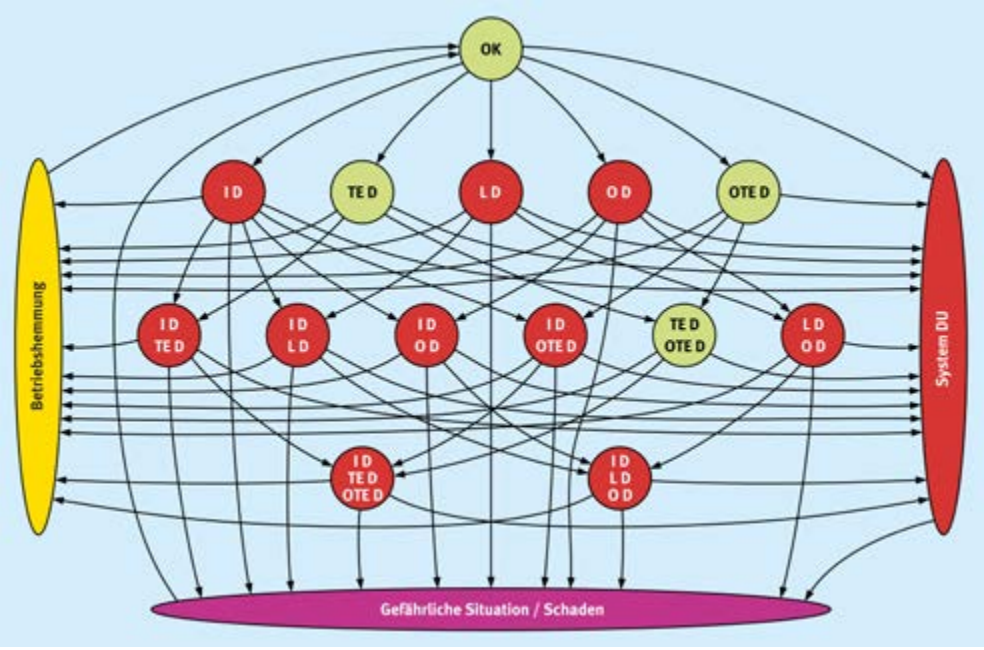


Abb. G.3
Zustandsgraph des *Markov*-Modells zur vorgesehenen Architektur für Kategorie 2 für die Ermittlung der PFH

Diese *PFH* ist auf der vertikalen Achse des Säulendiagramms von Abbildung G.1 für die verschiedenen „vorgesehenen Architekturen“ nach Abschnitt 6.1.3.2 der Norm (vgl. Abschnitte 8.2.3 bis 8.2.7 dieses Reports) aufgetragen, wobei die Kategorien 2 und 3 noch nach dem DC_{avg} differenziert wurden. Die Säulen entstehen, indem für eine Kombination aus Architektur (bzw. dem zugeordneten *Markov*-Modell) und DC_{avg} die $MTTF_D$, d. h. die mittlere Zeit bis zum Ausfall des (bzw. eines) Funktionskanals in dessen gefährliche Richtung, variiert wird. So können beispielsweise mit dem Markov-Modell in Abbildung G.2 die beiden Säulen für die vorgesehene Kategorie-2-Architektur berechnet werden. (Tatsächlich wurde aus rechentechnischen Gründen ein einfacheres äquivalentes Ersatzmodell benutzt, das den Funktionskanal und den Testkanal jeweils auf einen Block reduziert. Das vereinfachte Ersatzmodell wird hier nicht dargestellt, weil sein Zusammenhang mit dem Blockbild von Abbildung G.2 weniger leicht einsichtig ist. Das Ersatzmodell liefert praktisch identische Ergebnisse.) Die übrigen Säulen basieren auf weiteren Markov-Modellen, die für die entsprechenden vorgesehenen Architekturen ebenfalls nach den oben beschriebenen Prinzipien entwickelt wurden.

Gemäß Tabelle 7.1 wurden den *PFH*-Intervallen auf der logarithmisch geteilten *PFH*-Skala die PL a bis e zugewiesen. Dies ist in Abbildung G.1 gezeigt, die Bild 12 der Norm DIN EN ISO 13849-1 entspricht.

Eine Besonderheit gibt es beim *PFH*-Intervall von 10^{-6}/h bis 10^{-5}/h. Es ist den beiden benachbarten Performance Leveln b und c zugeordnet, die gemeinsam dieses Intervall ausfüllen. Durch die mittige Teilung der logarithmischen Skala liegt die Grenze zwischen PL b und PL c beim geometrischen Mittelwert von 10^{-6}/h und 10^{-5}/h, d. h. bei $\sqrt{10} \cdot 10^{-6}$/h $\approx 3 \cdot 10^{-6}$/h. Die Zuordnung von *PFH*-Intervallen und PL steht im Einklang mit DIN EN 61508-1, Tabelle 3 und DIN EN 61508-5, Bild E.2 [G3, G4].

In Anhang K der Norm ist der Inhalt von Abbildung G.1 in Form von Tabelle K.1 numerisch wiedergegeben. Mithilfe von Tabelle K.1 kann der PL präziser ermittelt werden als mit der Abbildung, was insbesondere dann nützlich ist, wenn *PFH*-Beiträge von mehreren Teilsystemen aufsummiert werden müssen, um den *PFH*-Wert für ein SRP/CS zu ermitteln. Hingegen bietet das Säulendiagramm vor allem eine schnelle Übersicht über die PL-Tauglichkeit verschiedener technischer Lösungswege und kann somit bei deren Vorauswahl helfen. Die Informationen aus Tabelle K.1 der Norm sind auch in dem „Performance Level Calculator“ (PLC) enthalten, einer handlichen Drehscheibe aus Karton zur PL-Bestimmung, die beim IFA erhältlich ist [G6].

Mitunter kommt es vor, dass der für ein System ermittelte DC_{avg}-Wert nur geringfügig unterhalb einer der Schwellen „niedrig“ (60 %), „mittel“ (90 %) oder „hoch“ (99 %) liegt. Wird dann das vereinfachte Quantifizierungsverfahren aus DIN EN ISO 13849-1 angewendet, muss rein formal jeweils mit der nächstkleineren DC_{avg}-Stufe, also mit „kein“, „niedrig“ bzw. „mittel“, weitergearbeitet werden. Diese Vorgehensweise schätzt das Teilsystem zur sicheren Seite ab. Wegen der wenigen Stufen der DC_{avg}-Skala kann jedoch manchmal eine nur kleine Änderung, die den Wert DC_{avg} eine der Schwellen gerade unterschreiten lässt, zu einer deutlich schlechteren Bewertung des Teilsystems 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 8.2.14). Die kleine Verbesserung der Kanal-$MTTF_D$ wird dann durch die formal vollzogene Herabstufung von DC_{avg} auf die nächstkleinere Stufe überkompensiert, wodurch die ermittelte *PFH* schlechter (größer) wird. Dieser paradox erscheinende Effekt ist eine Folge der Grobstufigkeit der DC_{avg}-Skala, also letztlich eine Konsequenz der beabsichtigten Einfachheit von Bild 12 (bzw. Tabelle K.1) der Norm.

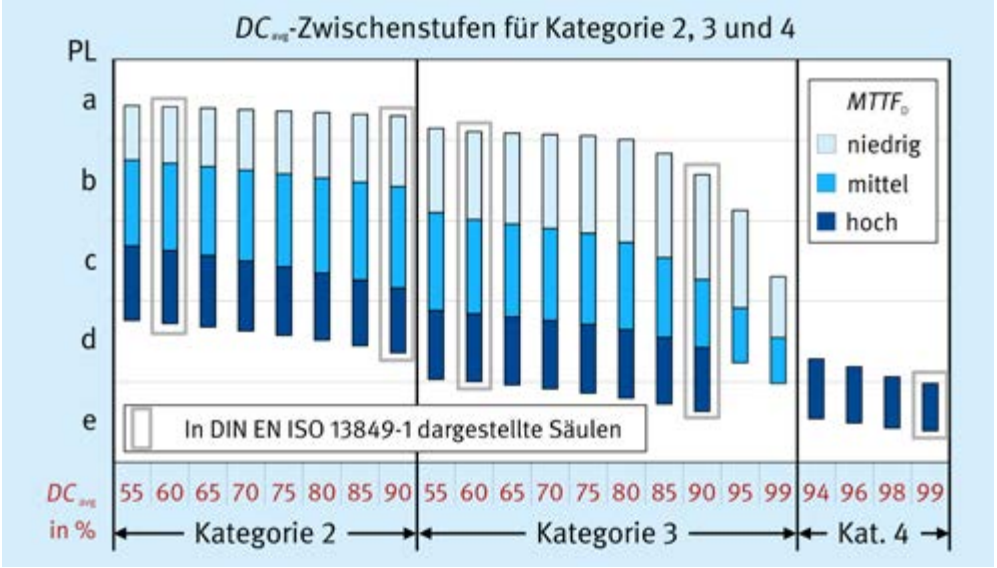


Abb. G.4
PL bei feinstufigerer Auflösung der DC_{avg}-Skala (Erweiterung von Bild 12 aus DIN EN ISO 13849-1 um DC-Zwischenstufen)

Der beschriebene Effekt kann verhindert oder gemildert werden, indem anstelle von Abbildung G.1 eine Grafik mit feinerer Abstufung der DC_{avg}-Werte benutzt wird (**Abbildung G.4**). Mit Rücksicht auf die begrenzte Genauigkeit von DC_{avg}-Werten (vgl. DIN EN ISO 13849-1, Tabelle 7, Anmerkung 2) wurden für alle Kategorien die minimal möglichen DC_{avg}-Werte berücksichtigt. Zur praktischen *PFH*-Bestimmung bietet sich der IFA Softwareassistent „SISTEMA“ an (siehe Anhang H). Er interpoliert sogar zwischen den in Abbildung G.4 gezeigten Säulen. Generell kann dadurch eine starke Herabstufung von DC_{avg} vermieden und oft ein genauerer und zugleich besserer *PFH*-Wert ermittelt werden.

Literatur

[G1] *Goble, W. M.*: Control Systems Safety Evaluation & Reliability. 3rd ed. Hrsg.: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010. https://www.isa.org

[G2] *Signoret, J.-P., Leroy,* A.: Reliability Assessment of Safety and Production Systems. Springer Nature Switzerland, Cham 2021

[G3] VDI-Handlungsempfehlung für Betreiber von Maschinen: Gebrauchsdauer in der funktionalen Sicherheit, Ende der Gebrauchsdauer erreicht - was nun? Hrsg. VDI Verein Deutscher Ingenieure e.V., Düsseldorf 2024.
https://www.vdi.de/ueber-uns/vdi-mediathek

[G4] DIN EN 61508-1: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (2/2011). DIN Media, Berlin 2011

[G5] DIN EN 61508-5: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (2/2011). DIN Media, Berlin 2011

[G6] *Schaefer, M.; Hauke, M.*: Performance Level Calculator – PLC. 5. Aufl. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, (IFA); Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) – Fachverband Automation und Verband Deutscher Maschinen- und Anlagenbau (VDMA), 2015.
https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/performance-level-calculator

Anhang H

SISTEMA – Der Softwareassistent zur Bewertung von SRP/CS

H.1 Was kann SISTEMA?

Mit dem Softwareassistenten Sicherheit von Steuerungen an Maschinen (SISTEMA) steht zur Entwicklung und Prüfung von sicherheitsbezogenen Maschinensteuerungen eine umfassende Hilfestellung bei der Bewertung der Sicherheit im Rahmen der DIN EN ISO 13849-1 zur Verfügung [H1, H2]. Das Windows-Tool bildet die Struktur der sicherheitsbezogenen Steuerungsteile, die als sicherheitsbezogenes Blockdiagramm vorliegen, auf der Basis der sogenannten vorgesehenen Architekturen nach und ermöglicht daraus eine automatisierte Berechnung der Zuverlässigkeitswerte auf verschiedenen Detailebenen einschließlich des erreichten Performance Levels (PL) und der Ausfallhäufigkeit *PFH* (average frequency of a dangerous failure per hour).

Über Eingabemasken werden relevante Parameter wie Risikoparameter zur Bestimmung des erforderlichen Performance Levels (PL_r), die Kategorie von Teilsystemen, die Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) bei mehrkanaligen Systemen, die mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$) und der Diagnosedeckungsgrad (*DC*) von Bauelementen bzw. Blöcken Schritt für Schritt erfasst. Nachdem die geforderten Daten in SISTEMA eingetragen wurden, sind die berechneten Ergebnisse praktischerweise sogleich sichtbar: Jede Parameteränderung wird in ihrer Auswirkung auf das Gesamtsystem über die Programmoberfläche direkt angezeigt. Das umständliche Nachschlagen in Tabellen und Berechnen nach Formeln (Bestimmung der $MTTF_D$ nach dem „Parts Count"-Verfahren, Symmetrisierung der $MTTF_D$ für jeden Kanal, Abschätzung des DC_{avg}, Ermittlung von *PFH* und PL etc.) wird durch die Software übernommen und entfällt daher weitestgehend. Dies ermöglicht es auch, Parameterwerte wie *DC* zu variieren, um so die Auswirkungen bzw. den Effekt auf die Ausfallhäufigkeit zu beurteilen. Die Resultate und alle Daten können in einem druckbaren Report zusammengefasst werden.

H.2 Wie wird SISTEMA verwendet?

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

Man eröffnet zunächst ein Projekt und kann darin die Maschine bzw. die Gefahrenstelle, die weiter betrachtet werden soll, definieren. Dem Projekt werden danach Sicherheitsfunktionen zugewiesen. Diese können festgelegt und dokumentiert sowie mit einem PL_r belegt werden. Der tatsächlich erreichte PL des parametrierten SRP/CS wird automatisch aus den Teilsystemen ermittelt, die – in Serie geschaltet – die Sicherheitsfunktion ausführen. Den Teilsystemen liegt jeweils – in Abhängigkeit von der gewählten Kategorie – eine sogenannte vorgesehene Architektur aus der Norm zugrunde. Aus der Architektur bestimmt sich unter anderem, ob die Steuerung einkanalig, einkanalig getestet oder redundant ausgelegt ist und ob bei der Auswertung ein spezieller Testkanal zu berücksichtigen ist. Jeder Kanal kann sich wiederum in beliebig viele Blöcke unterteilen, für die entweder direkt ein $MTTF_D$-Wert und ein *DC*-Wert

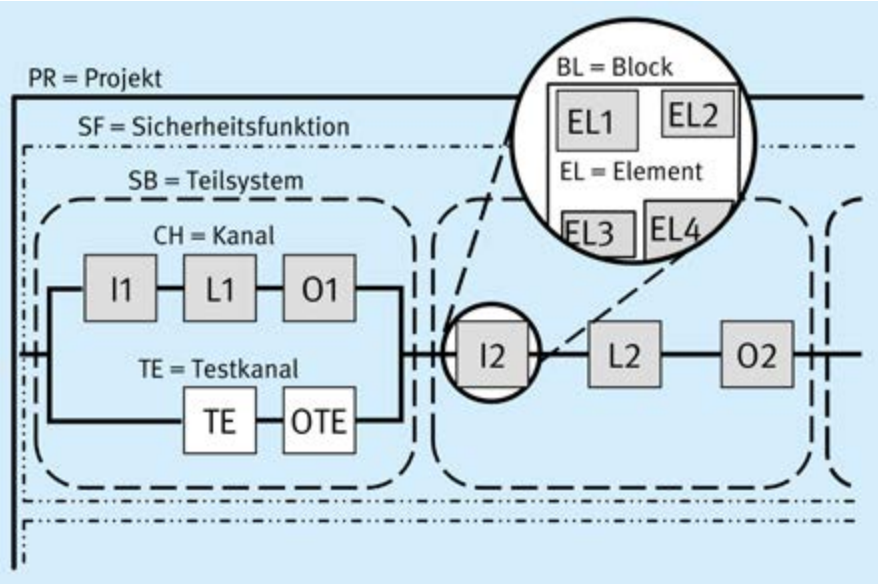


Abb. H.1
In SISTEMA betrachtete Hierarchieebenen

Gerätetypen nach VDMA-Einheitsblatt 66413

- Gerätetyp 1 entspricht dem SISTEMA-Teilsystem. Es sind gekapselte Teilsysteme, die als Sicherheitsgeräte vom Hersteller entweder nach DIN EN ISO 13849-1 mit *PFH*, PL und Kategorie oder nach IEC 62061 [H4] mit *PFH* und SIL (Sicherheits-Integritätslevel) bereitgestellt werden.
- Gerätetyp 2 ist für nicht verschleißbehaftete Bauteile als SISTEMA-Block bzw. Element verwendbar. Diese Geräte sind nicht zwangsläufig nach Sicherheitsnormen entwickelt, was einen Einsatz nach EN ISO 13849-1 oder IEC 62061 aber nicht ausschließt. Die Geräte verfügen über *MTTF*, $MTTF_D$, *MTBF* oder λ_D. Beispiele für Geräte des Typs 2 sind Näherungsschalter, Hydraulikventil, Sensor oder SPS.
- Gerätetyp 3 ist für verschleißbehaftete Bauteile als SISTEMA-Block bzw. -Element verwendbar. Es sind Geräte mit einem Ausfallverhalten, das von der Schalthäufigkeit abhängig ist. Diese Geräte werden in der Regel mit einem B_{10}- oder B_{10D}-Wert gelistet (z. B. Not-Halt-Befehlsgerät, Positionsschalter, Pneumatikventil, Schütze).
- Gerätetyp 4 sind Sonderfälle eines gekapselte Teilsystems. Geräte des Typs 4 haben keine gefahrbringenden Ausfälle und werden daher mit einer *PFH* = 0 vom Hersteller in Verkehr gebracht. Dies kann ein Bauteil sein, für das der Bauteilhersteller einen durchgängigen Fehlerausschluss machen kann, was in der Praxis aber äußerst selten vorkommt.

eingetragen wird, oder aber auf der niedrigsten Hierarchieebene die Werte für die einzelnen Elemente eingetragen werden, aus denen sich der Block zusammensetzt.

Weiterhin runden komfortable Bibliotheksfunktionen den Leistungsumfang von SISTEMA ab. Viele Hersteller von Komponenten und Bauteilen bieten Bibliotheken mit Daten ihrer Produkte an. Auf den Internetseiten des IFA sind Links zu diesen Bibliotheken gelistet (www.dguv.de/ifa/13849). Man kann aber auch eigene Bibliotheken erstellen, in denen selbst entwickelte Teilsysteme oder häufig verwendete Bauteile abgespeichert werden können. Bibliotheken können lokal, aber auch zentral auf Servern abgelegt sein.

Neben den SISTEMA-Bibliotheken gibt es auch das VDMA-Einheitsblatt 66413 [H3], dass ein XML-Datenformat definiert. Gerätehersteller können mithilfe dieser universellen Datenbasis ihre Bauteilkennwerte standardisiert an Maschinenhersteller bzw. an Berechnungstools (wie SISTEMA), im Bereich der Funktionalen Sicherheit, weitergeben. In einer Bauteilbibliothek kann ein Hersteller ein oder beliebig viele Geräte listen. Jedes einzelne Gerät besitzt immer einen oder mehrere Anwendungsfälle. Ein Anwendungsfall definiert für die beschriebene Anwendung des Geräts den passenden Satz von erforderlichen Zuverlässigkeitskennwerten. Jeder Anwendungsfall entspricht weitestgehend einem der vier im VDMA-Einheitsblatt 66413 (und EN ISO 13849-1:2023) definierten Gerätetypen (Device Types).

Seit der vierten Normausgabe sind die Gerätetypen auch in einem neuen Anhang O der Norm erwähnt. Abweichend zum VDMA-Einheitsblatt 66413 wird dort für Gerätetyp 2 und 3 die Angabe einer Kategorie nahegelegt. Dies kann so verstanden werden, dass ein Bauteilhersteller für diese Gerätetypen dem Integrator alle Informationen zur Einhaltung der grundlegenden und bewährten Sicherheitsprinzipien zur Verfügung stellen sollte, damit dieser bei der Teilsystem-Integration eine Kategoriebewertung vornehmen kann. Dafür dient z. B. ein ausführliches technisches Datenblatt mit Anwendungshinweisen, das auch in SISTEMA zur Dokumentation verlinkt werden kann. Je nach Anwendung kann dann z. B. ein Ventil als Block in einem Teilsystems der Kategorie 1, 2 oder – bei redundanter Ausführung – als Block in einem Kanal eines Teilsystems der Kategorie 3 oder 4 verwendet werden.

H.3 Die Benutzerschnittstelle von SISTEMA

Die Programmoberfläche von SISTEMA gliedert sich in vier Bereiche (Abbildung H.2). Den größten Anteil der Ansicht nimmt der Arbeitsbereich in der Mitte ein. Im Arbeitsbereich werden die editierbaren Eingabemasken, des ausgewählten Projektes, angezeigt. Ist das oberste Elemente der Baumansicht ausgewählt (Projekte) wird die SISTEMA-Readme Datei, die allen wichtigen Informationen zur SISTEMA-Version enthält, angezeigt. Der Inhalt Eingabemasken werden durch das ausgewählte Grundelement bestimmt, dass über die Selektion in der Baumansicht auf der linken Seite festgelegt wird. Jede Verzweigung in der Baumansicht steht für ein Grundelement. Über den Baum lassen sich auch Grundelemente auf den verschiedenen Ebenen neu erzeugen, entfernen, verschieben oder kopieren. Die Details des angewählten Grundelements werden in der Editieransicht über die Eingabemaske eingetragen. Jede Eingabemaske ist selbst über Register in verschiedene Bereiche untergliedert. Die jeweils letzte Registerkarte enthält eine Tabelle, die alle untergeordneten Verzweigungen zusammenfasst und die wichtigsten Informationen auflistet. Wird beispielsweise ein Block in der Baumansicht markiert, so zeigt diese Tabelle alle darin enthaltenen Elemente mit ihren $MTTF_D$- und *DC*-Werten an.

Ferner enthält die Baumansicht zu jedem Grundelement eine Statusinformation durch eine farbliche Markierung neben der Verzweigung. Ein rotes Kreuz zeigt an, dass eine Bedingung der Norm nicht erfüllt ist, ein Grenzwert

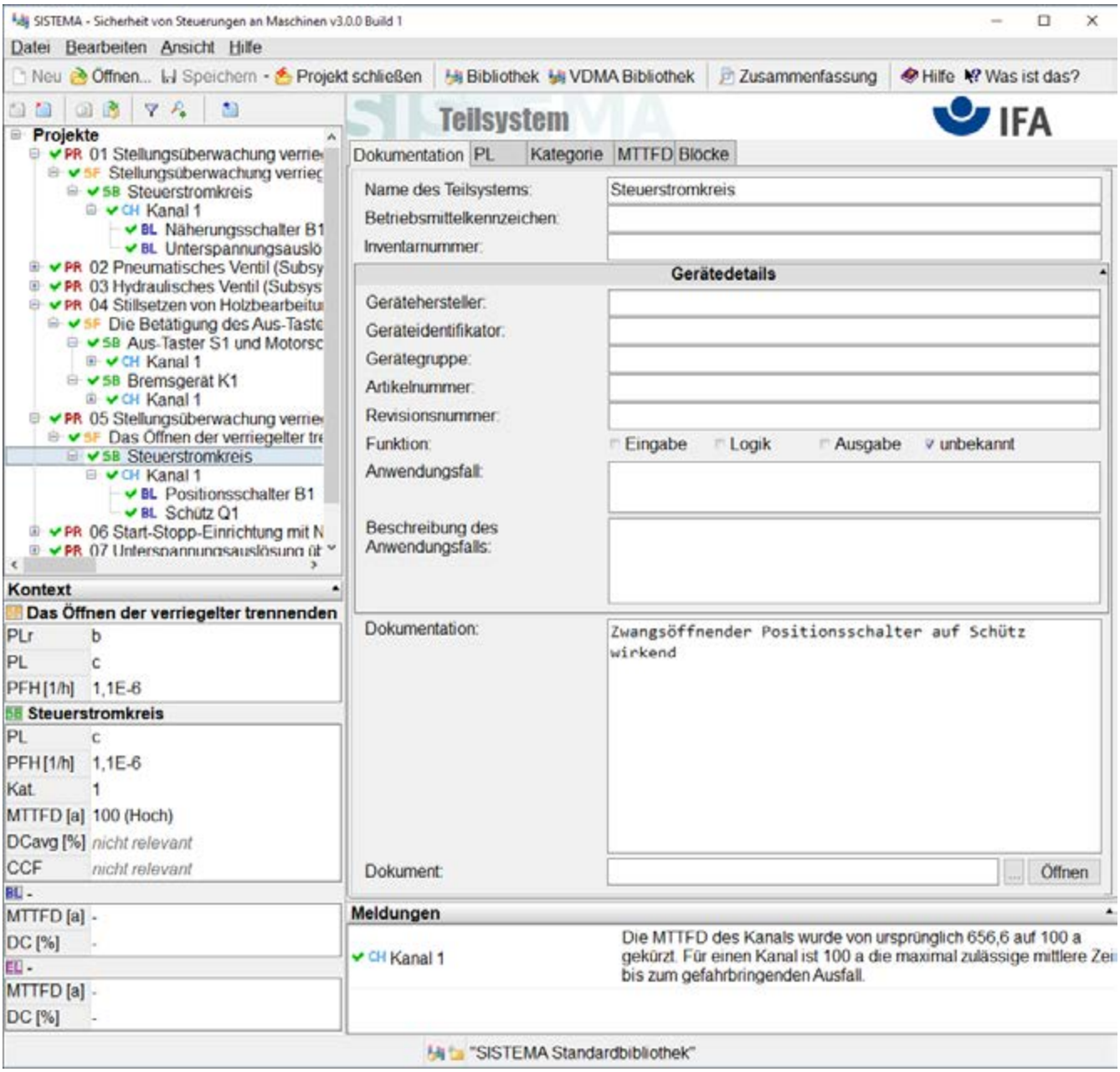


Abb. H.2 Programmoberfläche von SISTEMA

überschritten ist oder eine allgemeine Inkonsistenz vorliegt, durch die ein erforderlicher Wert nicht berechnet werden kann. In diesem Fall wird eine Warnung ausgegeben. Ein gelber Punkt bedeutet, dass ein Hinweis vorliegt, der meist für den Betreiber der Maschine wichtig ist. Alle anderen Grundelemente werden mit grünem Häkchen gekennzeichnet. Eine Farbkennzeichnung vererbt sich immer auch auf die übergeordneten Verzweigungen, wobei rot (nicht ausreichend) die höchste und grün (alles OK) 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-Punktezahl des übergeordneten Teilsystems sowie PL_r, PL und *PFH* der übergeordneten Sicherheitsfunktion (das gilt natürlich nur für Grundelemente, die in tieferen Hierarchieebenen liegen). So ist jederzeit sichtbar, wie sich Änderungen in den grundlegenden 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 beim ersten Kontakt Schritt für Schritt bei der virtuellen Nachbildung der Steuerung begleitet und einen schnellen Zugang gewährleistet.

H.4 Wo ist SISTEMA zu erhalten?

Das Programm SISTEMA kann nach Registrierung kostenlos unter https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-sistema heruntergeladen werden. Die Weitergabe an Dritte ist erlaubt. Eine Veränderung von SISTEMA ist aber nicht gestattet. SISTEMA enthält folgende Sprachversionen: Deutsch, Englisch, Französisch, Italienisch, Spanisch, Finnisch und Japanisch. Weitere Sprachversionen werden folgen. Anleitungen zur Benutzung von SISTEMA bieten die SISTEMA-Kochbücher (https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-sistema/sistema-kochbuecher), die installierte Hilfedatei und vor allem das Dokument „Erste Schritte“, zu finden auf der SISTEMA-Webseite. Informationen und Hilfen zur DIN EN ISO 13849-1 finden Sie unter www.dguv.de/ifa/13849.

Literatur

[H1] ISO 13849-1:2023: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. International Organization for Standardization 2023

[H2] *Huelke, M.; Lungfiel, A.*: Reliability Databases used by the ISO 13849 tool SISTEMA. SIAS 2012

[H3] VDMA 66413:2012-10: Funktionale Sicherheit – Universelle Datenbasis für sicherheitsbezogene Kennwerte von Komponenten oder Teilen von Steuerungen. DIN Media, Berlin 2012

[H4] DIN EN IEC 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (IEC 62061:2021);. DIN Media, Berlin 2023

Anhang I

SOFTEMA – Softwareassistent zur Projektierung und Dokumentation sicherheitsbezogener Anwendersoftware (SRASW) an Maschinen

I.1 Was kann SOFTEMA?

Mit dem Softwareassistenten SOFTEMA (Software von Steuerungen an Maschinen) können Maschinenhersteller ihre sicherheitsbezogene Anwendungssoftware projektieren und dokumentieren. SOFTEMA bietet bei der Entwicklung z. B. nach der DIN EN ISO 13849 eine umfassende Hilfestellung. Dazu implementiert SOFTEMA die Matrixmethode des IFA (https://www.dguv.de/ifa/publikationen/reports-download/reports-2016/ifa-report-2-2016) und hilft so, sicherheitsbezogene Anwendungssoftware zu entwickeln.

Anwender können die Eingabefelder in SOFTEMA nutzen, um wesentliche Parameter (z. B. Eingänge und Ausgänge) ihrer Maschine zu beschreiben. Der wesentliche Fokus liegt auf den Sicherheitsfunktionen der sicherheitsbezogenen Anwendungssoftware der Maschine.

Bei der Risikoanalyse nach DIN EN ISO 12100 „Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung“ werden vor dem Bau der Maschine mögliche Risiken für den Anwender/Bediener identifiziert. Diese müssen im Rahmen der Risikominderung systematisch behoben werden. Dabei spielt die sicherheitsbezogene Anwendungssoftware eine wesentliche Rolle, welche die Bauteile der Sicherheitsfunktion (z. B. Not-Halt-Gerät) überwacht und im Falle eines Auslösens die Maschine in einen sicheren Zustand überführt.

Die Verknüpfung zwischen sicherheitsbezogenen Bauteilen und der Maschine wird in den Sicherheitsfunktionen beschrieben. Maschinenhersteller realisieren immer häufiger die Sicherheitsfunktionen ihrer Maschinen selbst. Die funktionale Sicherheit der Steuerungen hängt daher zunehmend von hochwertig entwickelten und geprüften Anwendungsprogrammen ab.

Die Sicherheitsfunktionen können mithilfe der Matrixmethode des IFA spezifiziert, verifiziert und validiert werden. Software kann nicht wie Hardware durch Verschleiß, sondern nur durch systematische Fehler ausfallen. Die Resultate werden schließlich in einem druckbaren Report zusammengefasst.

I.2 Wie wird SOFTEMA verwendet?

SOFTEMA nutzt kein eigenes Dateiformat, sondern das gängige Microsoft-Excel-Format (.xlsx) und ist wie Excel selbst tabellarisch aufgebaut (**Abbildung I.1**). Eine SOFTEMA-Projektdatei ist eine Exceldatei mit Tabellen, die für die IFA-Matrixmethode benötigt werden. Für die Anwendung der IFA-Matrixmethode muss aus diesem Grund nicht zwingend SOFTEMA verwendet werden. Es wird empfohlen, für die Bearbeitung des Projektes SOFTEMA zu verwenden, da die Software einige spezifische Funktionalitäten, Automatismen und Kontrollen mit sich bringt. SOFTEMA nutzt das Dateiformat von Excel, es ist jedoch keine Voraussetzung Microsoft Excel installiert zu haben.

Beim Installieren von SOFTEMA werden zwei Dateien als Einführung mitgegeben (SOFTEMA-Beispiel und Template). Das Template kann verwendet werden, um ein neues Projekt anzulegen. Es empfiehlt sich, das Template erstmalig zu kopieren und es auf die „Bedürfnisse“ der Firma anzupassen. Beim Ausfüllen der Tabellen, wird zuerst das Projekt beschrieben. Hierbei sind einige Felder vordefiniert. In allen SOFTEMA-Tabellen können jedoch eigene Felder bzw. Kommentarzeilen hinzugefügt werden. Pflicht-Spalten in SOFTEMA, die ausgefüllt werden müssen, werden unterstrichen dargestellt.

Der Projekttabelle folgend, werden die Sicherheitsfunktionen, Input/Output, Maßnahmen, Anforderungen und Modularchitektur beschrieben. Eine genaue Anwendungsdokumentation und einen Projektierungsleitfaden finden Sie in den SOFTEMA-Kochbüchern (https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-softema/softema-kochbuecher).

Das Herzstück von SOFTEMA stellt die Matrix C+E-Tabelle dar. Hier werden wie oben beschrieben die Verknüpfungen zwischen sicherheitsbezogenen Bauteilen und der Maschine implementiert (Abbildung I.2). Die Verknüpfungen werden in den Sicherheitsfunktionen als „Wenn-Dann“-Anweisung (Cause + Effect, C+E) beschrieben. In den Zeilen stehen die automatisch übernommen Sicherheitsfunktionen (aus der Tabelle Sicherheitsfunktionen) und in den Spalten die Ausgänge der einzelnen Komponenten der Maschine. Am Schnittpunkt von Zeile und Spalte wird in dem jeweiligen Feld mithilfe von boolescher Algebra das Verhalten beschrieben.

Die Matrix C+E-Tabelle wird zusätzlich in komprimierter Form in der Matrix Kompakt-Tabelle dargestellt. Nach erfolgter Validierung ist dies gerade für die Inbetriebnahme an der Maschine nützlich. In den Tabellen Codereview und Validierung werden die jeweiligen Felder aus den vorherigen Tabellen zusammengefasst dargestellt. Dies dient zur Übersicht über das gesamte Projekt. Nach Abschluss des Projektes kann ein druckbarer Report erstellt werden.

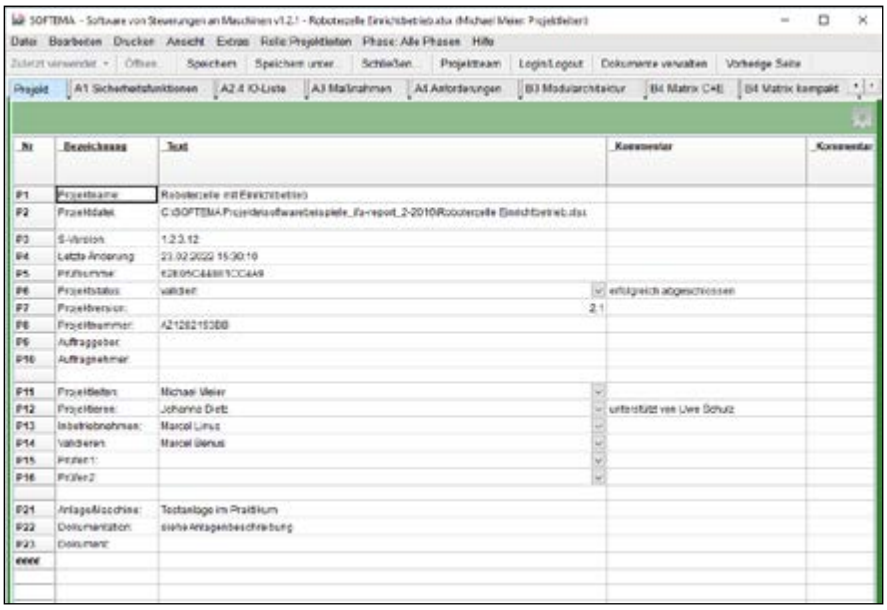


Abb. I.1 SOFTEMA nach dem Öffnen einer Projektdatei

Abb. I.2 SOFTEMA Tabelle: Matrix C+E

I.3 Wo ist SOFTEMA zu erhalten?

Das Programm SOFTEMA kann kostenlos unter https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-softema heruntergeladen werden. Die Weitergabe an Dritte ist erlaubt. Eine Veränderung von SOFTEMA ist aber nicht gestattet. SOFTEMA enthält die Sprachversionen Deutsch und Englisch; weitere werden folgen. Anleitungen zur Benutzung von SOFTEMA bieten die SOFTEMA-Kochbücher (https://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-softema/softema-kochbuecher) sowie die installierte Hilfedatei. Informationen und Hilfen zur DIN EN ISO 13849-1 finden Sie unter www.dguv.de/ifa/13849.

I.4 Der SOFTEMA-Codegenerator

Zu SOFTEMA gibt es eine eigenständige Erweiterung: den SOFTEMA-Codegenerator. Dieser generiert aus der C+E Matrix-Tabelle einen ausführbaren Programmcode. Hierzu hat der Anwender die Möglichkeit auszuwählen, ob aus der C+E Matrix Strukturierter Text (Structured Text, ST) oder ein Funktionsblockdiagramm (Function Block Diagram, FBD) erstellt wird. Als Dateiaustauschformat gibt es für den ST-Code die Möglichkeiten, zwischen einer reinen Textdatei oder dem PLCopen XML Format (https://plcopen.org/technical-activities/xml-exchange) zu wählen. Für das FBD steht dem Nutzer nur das PLCopen XML Format zur Verfügung. Je nach Anwendungsfall kann der Anwender den ST-Code einfach in seine Programmierumgebung kopieren oder wahlweise, falls verfügbar, die interne PLCopen XML Importfunktion verwenden.

Darüber hinaus hat der Anwender die Möglichkeit, sich die generierter FBD im SOFTEMA-FBD-Viewer, als Funktionsblockdiagramm darstellen zu lassen.

Anhang J

Sicherheitsfunktion Betriebsartenwahl

J.1 Einleitung

In der Regel erfordert die Arbeit an einer Maschine neben dem automatisch ablaufenden Betrieb auch manuelle Eingriffe in den Gefahrenbereich. Da solche Eingriffe – wie sie etwa für das Einrichten, die Störungsbeseitigung oder die Reinigung notwendig werden können – meist mit einem erhöhten Risiko einhergehen, kommen je nach durchzuführender Tätigkeit andere Betriebsarten zum Einsatz.

Mit der Anwahl einer Betriebsart werden an der Maschine Sicherheitsfunktionen aktiviert, die das vorherrschende Risiko für die jeweils an der Maschine durchzuführenden Tätigkeiten auf ein akzeptables Maß mindern. Versagt die Betriebsartenwahl, so kann dies dazu führen, dass erforderliche Sicherheitsfunktionen nicht ausgelöst werden können, was zu einer unmittelbaren Erhöhung des Risikos führt.

Folgerichtig definiert die Norm die Betriebsartenwahl in Abschnitt 5.2.2.9 als eigenständige Sicherheitsfunktion. Durch die Sicherheitsfunktion Betriebsartenwahl werden andere Sicherheitsfunktionen aktiviert oder deaktiviert. Die hierzu notwendigen Eigenschaften werden in den Unterpunkten a bis d wie folgt konkretisiert:

- Die Anwahl einer Betriebsart muss eindeutig sein, d. h. es darf immer nur eine Betriebsart gleichzeitig aktiv sein. Die angewählte Betriebsart muss für den Anwender deutlich erkennbar sein bzw. angezeigt werden (a).
- Durch die Betriebsartenwahl selbst darf keine Maschinenbewegung ausgelöst werden. Hierzu muss eine separate Betätigung der Starteinrichtung erforderlich sein (b).
- Beim Wechsel der Betriebsart darf in keinem Moment die vorgesehene Risikominderung verloren gehen (c). Bis zur Aktivierung der für die anzuwählende Betriebsart geforderten Sicherheitsfunktionen müssen die Sicherheitsfunktionen der zuvor angewählten Betriebsart aktiv bleiben.
- Die Vorrichtungen für die Wahl der Betriebsart dürfen den PL der Sicherheitsfunktionen, die in dieser Betriebsart aktiv sind, nicht herabsetzen (d). Dies bedeutet, dass dort, wo für die Betriebsartenwahl ein PL_r durch keine Produktnorm vorgegeben ist, der höchste PL_r aller an der Maschine aktivierbaren Sicherheitsfunktionen anzusetzen ist. Diese Regel ergibt sich daraus, dass ein Versagen der Betriebsartenwahl dazu führen kann, dass erforderliche Sicherheitsfunktionen nicht ausgelöst werden können. Dies könnte z. B. an Werkzeugmaschinen beim Wechsel von der Betriebsart Prozessbeobachtung in den Einrichtbetrieb zu einer starken Erhöhung des Risikos führen. Eine Risikobeurteilung kann alternative Festlegungen ergeben.

Zusätzlich zu den in der Norm genannten Anforderungen fordert die derzeit noch gültige Maschinenrichtlinie [J1] und die neue Maschinenverordnung [J2], dass für den Wechsel der Betriebsart ein in jeder Position abschließbarer Wahlschalter verwendet wird. Die Formulierung weist darauf hin, dass die Verfasser hier vor allem elektromechanische Wahlschalter vor Augen hatten, wobei ausdrücklich auch andere Mittel der Betriebsartenwahl zugelassen werden, solange die Nutzung bestimmter Funktionen der Maschine auf bestimmte Kreise von Bedienern beschränkt werden. Die weiteren Vorgaben decken sich im Wesentlichen mit den Schutzzielen der Norm.

Zusätzlich zu den Vorgaben zur Betriebsartenwahl listet der entsprechende Abschnitt in der Maschinenverordnung Anforderungen für Betriebsarten, die bei „geöffneter oder abgenommener trennender Schutzeinrichtung und/oder ausgeschalteter nichttrennender Schutzeinrichtung“ erforderlich sind. Diese beziehen sich aber im Wesentlichen auf die Auslegung der zu der jeweiligen Betriebsart zugeordneten Sicherheitsfunktionen.

Es wird ergänzt, dass der Betätigungsplatz des Betriebsartenwahlschalters als Standort für den Betrieb der gefahrbringenden Bewegungen der Maschine dienen soll.

Mit Einstufung der Betriebsartenwahl als Sicherheitsfunktion im Sinne der DIN EN ISO 13849-1 wird die Norm für die Bewertung der verwendeten Steuerungstechnik relevant. Hier können je nach den verwendeten Bauteilen unter Umständen Fehlerausschlüsse geltend gemacht werden. Dieses Vorgehen soll im Folgenden für übliche Bedienelemente zur Betriebsartenwahl gezeigt werden. Weitere Hinweise zur Betriebsartenwahl als Sicherheitsfunktion finden sich in Abschnitt 4.1 von [J3].

J.2 Nockenbetätigte Wahlschalter

Für Schalter mit zwangsöffnenden Kontaktelementen nach DIN EN 60947-5-1 [J4], Anhang K kann für das Nichtöffnen von Kontakten ein Fehlerausschluss gemäß Tabelle D.8 der DIN EN ISO 13849-2 [J5] vorgenommen werden. Diese Schalter gelten auch als bewährte Bauteile, weswegen mit ihrem Einsatz eine Einstufung der Sicherheitsfunktion in Kategorie 1 nach der Norm möglich ist.

Sind bei Schaltern mit zwangsöffnenden Kontaktelementen zusätzlich die Fehlerausschlüsse für den Kurzschluss von benachbarten isolierten Kontakten und den gleichzei-

tigen Kurzschluss zwischen den drei Klemmen von Wechselkontakten gemäß Tabelle D.8 der DIN EN ISO 13849-2 möglich, müssen diese Bauteilfehler nicht angenommen werden. So ist bei einer elektrisch zweikanaligen Schaltung durch Fehlerausschluss in der einkanaligen Mechanik eine Modellierung als Kategorie 3 Teilsystem und eine Realisierung bis PL d möglich (siehe auch IFA Report 4/2018, Beispiel 8).

Für PL e können Fehlerausschlüsse nicht geltend gemacht werden. Hier sind zusätzliche Maßnahmen erforderlich. Es ist z. B. möglich, die angewählte Betriebsart nach Anzeige über eine Benutzerschnittstelle durch die Bedienperson der Maschine bestätigen zu lassen. Gleichzeitig ist durch ein Aktivierungssystem (siehe J3) in der sicherheitsgerichteten Steuerung in PL e sicherzustellen, dass auf der Maschine niemals mehr, aber auch nicht weniger als eine Betriebsart angewählt ist.

J.3 Elektronische Betriebsmittel

Bei elektronischen Betriebsmitteln ist ein Fehlerausschluss nicht möglich. Für die Fehlerbetrachtung der Betriebsartenwahl über elektronische Betriebsmittel ist daher eine weitere Analyse notwendig. Hierfür ist zunächst herauszustellen, welche Funktionen der Betriebsartenwahl durch die Wahleinrichtung abgebildet werden müssen. Es ergeben sich folgende Teilfunktionen [J6]:

1. Zugang zur Betriebsartenwahl
2. Auswahl der Betriebsart
3. Aktivierung der Betriebsart

Bei einer mit elektronischen Betriebsmitteln realisierten Wahleinrichtung können die genannten Teilfunktionen in drei Teilsystemen realisiert werden (Abbildung J.1).

Zugangssystem

Das Zugangssystem ist der Teil der Wahleinrichtung, der die Möglichkeit zur Betriebsartenwahl auf bestimmte Personengruppen einschränkt und eine versehentliche oder missbräuchliche Betätigung des Auswahlsystems verhindert. Da die Anwahl jeder Betriebsart mit der Aktivierung anderer Sicherheitsfunktionen einhergeht, wird das Zugangssystem als sicherheitsrelevant betrachtet.

Bei elektromechanischen Wahleinrichtungen wird der Zugang durch den Schlüssel realisiert. Hier kann durch eine mechanische Codierung des Schlüssels die Anwahl nur bestimmter Betriebsarten freigegeben werden. Hinzu kommen organisatorische Maßnahmen, die den Zugriff auf den oder die Schlüssel auf bestimmte Personenkreise einschränken sollen.

Bei elektronischen Wahleinrichtungen kann der Zugang beispielsweise über RFID-Schlüssel oder Passwörter und entsprechende organisatorische Maßnahmen realisiert werden. Für die sicherheitstechnische Betrachtung ist zu bewerten, ob im Hinblick auf die Zugangsbeschränkung eine vergleichbare Sicherheit wie bei elektromechanischen Wahleinrichtungen durch einen Schlüssel besteht (Integrität der Zugangsdaten, Codierung, Kopierschutz, organisatorische Maßnahmen etc.).

Auswahlsystem

Das Auswahlsystem legt die Betriebsart fest, die durch das Aktivierungssystem in der Steuerung aktiviert werden soll. Bei elektromechanischen Wahleinrichtungen entspricht das Auswahlsystem dem handbetätigten Schaltknopf, dessen Stellung z. B. über eine Achse und Nockenscheiben mechanisch auf die elektrischen Kontaktelemente übertragen wird. Hier ist, wie oben beschrieben, durch Fehlerausschluss eine sicherheitstechnische Realisierung bis PL d sowie unter Einbeziehung zusätzlicher Maßnahmen bis PL e möglich.

Bei elektronischen Wahleinrichtungen wird das Auswahlsystem in der Regel über eine Benutzerschnittstelle (Human Machine Interface, HMI) realisiert, beispielsweise über Touchpad oder Folientastatur. Über die Benutzerschnittstelle und eventuell weitere elektronische Komponenten wird durch die Bedienperson die in der Maschinensteuerung zu aktivierende Betriebsart festgelegt. Da hier in der Regel Standardkomponenten zum Einsatz kommen, ist eine Einstufung eines in dieser Art realisierten Auswahlsystems in PL c oder höher nur mit zusätzlichen Maßnahmen möglich. Eine Möglichkeit bietet Abschnitt 6.3 der Norm, in dem Vorgaben zur softwarebasierten manuellen Parametrierung (siehe Abschnitt 8.3) genannt werden. Da die Betriebsartenwahl über Benutzerschnittstelle und elektronisches Auswahlsystem einer softwarebasierten manuellen Parametrierung gleichkommt, kann der genannte Abschnitt der Norm für die sicherheitstechnische Bewertung dieses Auswahlsystems herangezogen werden. Das dort beschriebene Verfahren umfasst die Auswahl der Betriebsart durch die Bedienperson, die Prüfung der aus-

Abb. J.1 Struktur der Betriebsartenwahl

gewählten Betriebsart in der sicheren Steuerung sowie die Bestätigung der ausgewählten Betriebsart durch die Bedienperson. Dadurch wird sichergestellt, dass die Integrität der für die Parametrierung verwendeten Daten entlang der gesamten Kommunikationskette aufrechterhalten bleibt und Verfälschungen erkannt werden. Insbesondere wird vermieden, dass ein Fehler in einer der Komponenten der Wahleinrichtung zur Anwahl oder Bestätigung einer falschen Betriebsart führen kann.

Aktivierungssystem

Auf dem Aktivierungssystem wird die eigentliche Sicherheitsfunktion Betriebsartenwahl, d. h. die Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen, ausgeführt. Bei der Verwendung elektronischer Wahleinrichtungen geht nur das Aktivierungssystem in die Quantifizierung der Betriebsartenwahl ein, wenn das Auswahlsystem – wie oben beschrieben – nach den Anforderungen der softwarebasierten Parametrierung bewertet wird.

Für das Aktivierungssystem wird in Abhängigkeit der hierfür verwendeten steuerungstechnischen Komponenten eine *PFH* ermittelt, die mindestens zu dem erforderlichen Performance Level (PL_r) der Sicherheitsfunktion Betriebsartenwahl führen muss.

Anforderungen an die Software

Die für die Auswahl der Betriebsart verwendete Software und das darin umgesetzte Verfahren muss als sicherheitsbezogener Aspekt des SRP/CS in einer SRS beschrieben werden. Softwaremodule, die für die Codierung/Decodierung innerhalb des Übertragungs- bzw. Rückübertragungsprozesses oder für die Anzeige von sicherheitsbezogenen Parametern für den Anwender verwendet werden, müssen mindestens Diversität in ihren Funktionen nutzen, um systematische Ausfälle zu verhindern.

Laut Abschnitt 6.3.5 der Norm ist zudem jede Änderung der Parametrierung umfassend zu dokumentieren. Für die Parametrierung der Sicherheitsfunktion Betriebsartenwahl, also für die Wahl einer Betriebsart, kann diese Anforderung jedoch entfallen. Um einen Missbrauch bei der Betriebsartenwahl vorzubeugen, empfiehlt es sich jedoch, jede Parametrierung im Zugangssystem per Software durch die Speicherung der folgenden Daten zu registrieren:

- Datum und Uhrzeit der Parametrierung,
- Die eindeutige Identifizierung des für die Parametrierung verwendeten elektronischen Schlüssels,
- Die Identifizierung der sicherheitsbezogenen Parameter, hier: die gewählte Betriebsart.

Im Folgenden soll die Betriebsartenwahl über elektronische Wahleinrichtungen anhand eines Beispiels weiter erläutert werden.

J.4 Betriebsartenwahl mit einem elektronischen Schlüsselsystem als Zugangssystem – PL e

Sicherheitsfunktion

Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen

Struktur

In dem Beispiel wird das Zugangssystem durch ein elektronisches Schlüsselsystem gebildet. Auf dem elektronischen Schlüssel ist die Berechtigungsstufe des Schlüsselinhabers gespeichert.

Das Auswahlsystem besteht aus drei Komponenten: einem HMI mit Touchscreen zur Anzeige und Auswahl der je nach Berechtigungsstufe wählbaren Betriebsarten, einer Sicherheits-SPS zur Prüfung der Berechtigungsstufe und der angewählten Betriebsart sowie einer Standard-SPS zur Kommunikation zwischen den Komponenten.

Das Aktivierungssystem wird durch die Sicherheits-SPS gebildet. Die Sicherheits-SPS setzt die Umschaltung der Betriebsart und so die Aktivierung der für die Betriebsart erforderlichen Sicherheitsfunktionen um. Zusätzlich wird durch die Sicherheits-SPS sichergestellt, dass immer eine Betriebsart und die dazugehörigen Sicherheitsfunktionen angewählt sind.

Funktionsbeschreibung

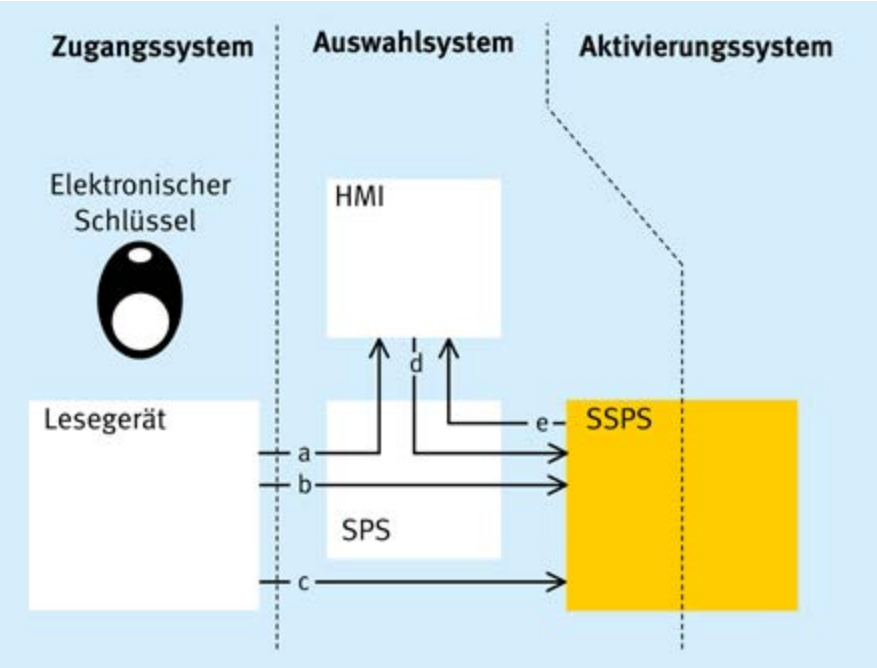
Schlüsselsystem/Standard-SPS

Bei Stecken eines Schlüssels in das Lesegerät wird die Berechtigungsstufe des Schlüsselinhabers ausgelesen. Die Berechtigungsstufe legt in Abhängigkeit der fachlichen Qualifizierung des Schlüsselinhabers fest, zur Anwahl welcher Betriebsarten dieser berechtigt sein soll. Das Lesegerät ist über eine Datenschnittstelle mit der Standard-SPS verbunden. Über die Datenschnittstelle wird nach dem Auslesen der Schlüsseldaten die Berechtigungsstufe an das HMI (a) und die Sicherheits-SPS (b) gesendet.

Zusätzlich zur Datenschnittstelle verfügt das Lesegerät über einen Relaisausgang, der abgeschaltet ist, solange sich kein Schlüssel in der Schlüsselaufnahme befindet oder die Schlüsseldaten nicht ausgelesen werden können. Der Relaisausgang ist mit einem sicheren Eingang der Sicherheits-SPS verbunden (c).

HMI

Auf dem HMI werden in Abhängigkeit der Berechtigungsstufe die Betriebsarten angezeigt, zu deren Auswahl der



HMI	Human Machine Interface
SPS	Speicherprogrammierbare Steuerung (Standard)
SSPS	Sicherheits-SPS
a bis e	Informationsfluss (siehe Funktionsbeschreibung)

Abb. J.2
Beispiel Betriebsartenwahl mit einem elektronischen Schlüsselsystem als Zugangssystem

Schlüsselinhaber berechtigt ist. Nach Auswahl einer Betriebsart durch den Schlüsselinhaber wird diese über die Standard-SPS an die Sicherheits-SPS übermittelt (d). Die Sicherheits-SPS sendet auf gleichem Wege eine Rückmeldung über die gespeicherte Betriebsart an das HMI zurück, wo sie vom Bediener quittiert werden muss.

Sicherheits-SPS

Sobald nach Stecken des Schlüssels auf dem sicheren Eingang der Sicherheits-SPS ein Signalwechsel erfolgt, wird in der Sicherheits-SPS ein Verfahren gestartet, an dessen Ende die durch den Schlüsselinhaber angewählte Betriebsart in der Maschinensteuerung freigegeben wird. Das Verfahren umfasst folgende Einzelschritte:

1. Die auf dem Schlüssel gespeicherte Berechtigungsstufe wird auf Gültigkeit geprüft.
2. Die auf dem HMI durch den Schlüsselinhaber angewählte Betriebsart wird daraufhin überprüft, ob sie einer gültigen Betriebsart entspricht und der Bediener auf Basis der Berechtigungsstufe zu deren Anwahl berechtigt ist.
3. Die Betriebsart wird an das HMI zur Quittierung zurückgegeben (e).
4. Nach Quittierung der Betriebsart durch den Schlüsselinhaber wird überprüft, ob die quittierte Betriebsart mit der zuvor angewählten übereinstimmt.
5. Die für die Betriebsart erforderlichen Sicherheitsfunktionen werden in der Maschinensteuerung aktiviert.

Sicherheitstechnische Bewertung

Das Lesegerät erfüllt in diesem Beispiel die strukturellen Anforderungen der Kategorie 3. Das bedeutet, dass es durch einen einzelnen Fehler nicht zu einer gleichzeitigen fehlerhaften Ausgabe auf der Datenschnittstelle und dem Relaisausgang kommen kann. Einzelne Fehler werden durch Kreuzvergleich im Lesegerät und die Erwartungshaltung in der Sicherheits-SPS erkannt. Damit erreicht das Lesegerät in Kombination mit dem elektronischen Schlüssel in seiner Funktion als Zugangssystem eine vergleichbare Sicherheit zum Schlüssel elektromechanischer Wahleinrichtungen.

Zur Reduzierung der Restfehlerrate für eine unerkannte Verfälschung bei der Verarbeitung oder Übertragung wird für die Berechtigungsstufen und die Betriebsarten ein gesichertes Datenübertragungsverfahren verwendet.

Das beschriebene Verfahren zur Auswahl, Prüfung und Bestätigung der Betriebsart sowie die Programmierung dieses Verfahrens erfüllt die Anforderungen an eine softwarebasierte manuelle Parametrierung nach Abschnitt 6.3 der Norm.

Die Programmierung der SRASW der Sicherheits-SPS erfolgt entsprechend den Anforderungen des PL e und den Hinweisen in Abschnitt 7.4 der Norm.

Bei der Sicherheits-SPS handelt es sich um ein Sicherheitsbauteil für den Einsatz in Sicherheitsfunktionen bis PL e.

Die mittlere Häufigkeit eines gefahrbringenden Ausfalls wird aus der *PFH* des Aktivierungssystems gebildet, im Beispiel durch die Sicherheits-SPS. Die *PFH* der Sicherheitsfunktion Betriebsartenwahl entspricht somit der *PFH* der eingesetzten Sicherheits-SPS.

Literatur

[J1] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). ABl. EU (2006) Nr. L 157, S. 24–86

[J2] Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates (kurz: MVO), L 165/1. Amtsblatt der Europäischen Union vom 29.6.2023.

[J3] *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld,* R.: Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 4/2018. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2018. https://publikationen.dguv.de/forschung/ifa/ifa-report/3500/sichere-antriebssteuerungen-mit-frequenzumrichtern-ifa-report-4/2018

[J4] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (3/2018). DIN Media, Berlin 2018

[J5] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (2/2013). DIN Media, Berlin 2013

[J6] DGUV Information: Sicherheitsbezogene Betriebsarten an spanenden Werkzeugmaschinen der Metallbearbeitung (FB HM-073). Ausg. 05/2021. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2021. https://www.dguv.de/fb-holzundmetall/publikationen/dguv_infos

Anhang K

Überlagerte Gefährdungen

Der folgende Inhalt ist aus dem Informationsblatt Nr. 47 des Fachausschusses Maschinenbau, Fertigungssysteme und Stahlbau der DGUV übernommen (siehe [26] in Kapitel 12 „Literatur“). Dieses Informationsblatt wurde nach Veröffentlichung der dritten Normausgabe zurückgezogen, da seine regulatorischen Inhalte in Abschnitt A.4 der Norm übernommen wurden. Zur Illustration der Handhabung von überlagerten Gefährdungen wird es hier abgedruckt.

Fachausschuss-Informationsblatt Nr. 047

Ausgabe 05/2010

Deutsche Gesetzliche Unfallversicherung
Fachausschuss
Maschinenbau, Fertigungssysteme, Stahlbau

Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen

In Arbeitsbereichen an komplexen Fertigungssystemen und Werkzeugmaschinen kann es zu Überlagerungen von Gefährdungen durch gefahrbringende Bewegungen kommen, hervorgerufen z. B. durch eine Vielzahl geregelter Achsantriebe. Dieses Fachausschuss-Informationsblatt beschreibt eine mit Arbeitsschutzexperten und dem Institut für Arbeitsschutz der DGUV abgestimmte Vorgehensweise, die es unter Anwendung der DIN EN ISO 13849-1 [1] oder DIN EN 62061 [2] erlaubt, Sicherheitsfunktionen bei überlagerten Gefährdungen abzubilden und zu berechnen.

Quelle: WFL Millturn Technologies GmbH & Co. KG

Bild 1: Achsschema einer Werkzeugmaschine

Überlagerte Gefährdungen sind charakterisiert durch das gleichzeitige Einwirken mehrerer Einzelgefährdungen auf eine oder mehrere zu schützende Personen, Körperteile oder Gliedmaßen, welche sich an einem Ort aufhalten oder gefahrbringende Bereiche erreichen können (siehe Bild 1).

Unter einer Einzelgefährdung wird sowohl die Bewegung einer einzelnen Achse, als z. B. auch eine Gefährdung durch die Bewegung eines gesamten Maschinenteils verstanden. Resultiert also die Bewegung eines Maschinenteils aus dem kinematischen Zusammenwirken einer oder mehrerer Achs- und Spindelantriebe (z. B. ein Fräswerkzeug am Support eines Bearbeitungszentrums), so kann dies als Einzelgefährdung betrachtet werden.

Inhaltsverzeichnis

1 Ausgangslage

Die Betrachtung von Einzelgefährdungen ist in der Sicherheitstechnik gängige Praxis und hat sich bewährt. Aus der probabilistischen Betrachtung nach DIN EN ISO 13849-1 oder DIN EN 61508 [3, 4] und DIN EN 62061 und der Risikobeurteilung für eine Gefährdungssituation ergibt sich jedoch, dass auch die Überlagerung von Gefährdungen betrachtet werden muss. Eine Diskussionsvorlage zu den Auswirkungen des probabilistischen Ansatzes auf die Betrachtung überlagerter Gefährdungen findet sich in [5], welcher durch dieses Fachausschuss-Informationsblatt präzisiert und erweitert wird.

Auf Grund der weitgefächerten Bandbreite von Gefährdungssituationen an den oben genannten Mensch-Maschine-Schnittstellen kann dieses Fachausschuss-Informationsblatt hinsichtlich deren Betrachtungsweise keine universelle bzw. allgemeingültige Festlegung geben. Es ist sowohl die Freiheit als auch die Aufgabe der Normung diesbezüglich maschinenspezifische Festlegungen in den jeweiligen Produkt- oder C-Normen zu beschreiben.

Problematisch ist, dass für Mensch-Maschine-Schnittstellen, auf die eine hohe Anzahl überlagerter Gefährdungen wirken, eine ausreichend kleine Ausfallwahrscheinlichkeit aller beteiligten sicherheitsbezogenen Steuerungsteile (Sensoren, Logik, mehrere Aktoren) kaum oder nur mit sehr hohem rechnerischen Aufwand (z.B. Markov-Modellierung) nachweisbar ist.

Ferner erhöhen überlagerte Gefährdungen mit unterschiedlichem Risiko (mit unterschiedlichem PL_r oder SIL) die Komplexität der Bestimmung der Ausfallwahrscheinlichkeit von Sicherheitsfunktionen, welches wiederum den Aufwand der Berechnung drastisch erhöht.

2 Praktische Behandlung überlagerter Gefährdungen

Eine genaue Überprüfung, welche Gefährdungen sich in einem konkreten Gefährdungsbereich tatsächlich überlagern, ist unerlässlich. Dabei sind die Maße der gefährdeten Körperteile und die bestimmungsgemäßen Handlungen des Maschinenpersonals genauso zu berücksichtigen

Hinweis: Zu den Zielen der Fachausschuss- Informationsblätter siehe Fachausschuss- Informationsblatt Nr. 001

Anhang L

Bewertung der elektromagnetischen Störfestigkeit von Maschinen

Die DIN EN ISO 13849-1 bietet Maschinenherstellern unterschiedliche Möglichkeiten Sicherheitsfunktionen umzusetzen. Die eingesetzten Komponenten müssen dabei unter anderem für den bestimmungsgemäßen Einsatz und Umgebungsbedingungen ausgelegt sein. Dementsprechend können auch Standardbauteile zur Realisierung verwendet werden, wenn diese für den industriellen Einsatz ausgelegt sind. Solche Standardkomponenten erfüllen aber in der Regel nicht die Anforderungen hinsichtlich elektromagnetischer Störfestigkeit nach „Funktionaler Sicherheit“ mit den erhöhten Prüfpegeln, wie sie z. B. in der Fachgrundnorm DIN EN IEC 61000-6-7 [L1] gefordert werden.

Da durch elektromagnetische Störfelder und Hochspannungstransienten Standardkomponenten wie Steuerungen, Aktoren und Sensoren gefahrbringend ausfallen können, sind für diese Industrieanlagen zusätzliche Bewertungen und notfalls zusätzliche Maßnahmen zur Verbesserung hinsichtlich elektromagnetischer Störfestigkeit notwendig. Elektromagnetische Störungen können z. B. beide Kanäle einer Sicherheitsfunktion gleichzeitig zum Ausfall bringen und zählen somit zu den Risiken der Fehler gemeinsamer Ursache (Common Cause Failure, CCF).

Die im Anhang L der Norm aufgeführte neue Bewertungsmethode legt nun Prüfanforderungen hinsichtlich der elektromagnetischen Störfestigkeit abhängig vom Performance Level (PL) der Sicherheitsfunktion fest. Gleichzeitig zeigt sie Möglichkeiten auf, wie ein Nachweis erbracht werden kann, das ausreichende Maßnahmen hinsichtlich elektromagnetischer Störungen (electromagnetic interference, EMI) getroffen worden sind.

In Abbildung L.1 sind vier mögliche Pfade dargestellt, die als Nachweis der elektromagnetischen Störfestigkeit in Abhängigkeit des PL gewählt werden können. Der Pfad A beschreibt die Möglichkeit, dass eine Produktnorm mit entsprechenden EMI-Anforderungen vorhanden ist. Ist dies der Fall, ist ein Einsatz der Komponente in Sicherheitsfunktionen bis PL e möglich. Gleiches gilt, wenn ein Nachweis nachDIN EN IEC 61000-6-7 oder einer anderen Fachgrundnorm für EMI für die funktionale Sicherheit vorhanden ist. Dieses entspräche dem Pfad D.

Für Komponenten, die in Sicherheitsfunktionen bis PL b eingesetzt werden, reicht die Einhaltung der Fachgrundnorm DIN EN IEC 61000-6-2 [L2] (für den Einsatz in industriellen Umgebungen) aus, wie in Pfad B dargestellt.

Aus Kostengründen werden oft Komponenten in Sicherheitsfunktionen eingesetzt, die nicht auf ihre elektromagnetische Störfestigkeit geprüft wurden. Da diese Komponenten in der Regel nicht die erhöhten Anforderungen an die elektromagnetische Störfestigkeit erfüllen, werden Maßnahmen auf der Systemebene notwendig, um die Anforderungen an die elektromagnetische Störfestigkeit zu erfüllen. Um den Maschinenbauern und Integratoren eine Hilfestellung zu geben, wurde der Pfad C entwickelt. Er ist also für Maschinen mit integrierten Sicherheitsfunktio-

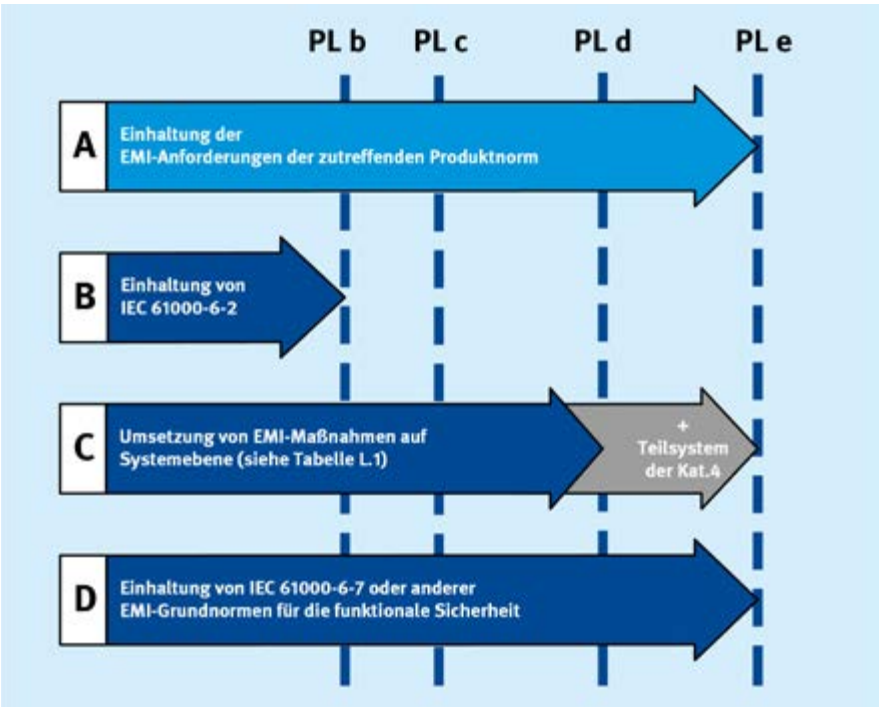


Abb. L.1
Vier Pfade zur Auswahl der EMI-Maßnahmen und zum Erreichen der geforderten elektromagnetischen Störfestigkeit

nen gedacht, die Komponenten enthalten, welche keinen Nachweis zur elektromagnetischen Störfestigkeit aufweisen. Dieser neue Ansatz ergibt sich unter anderem aus der Anmerkung 1 im Kapitel 4.1 der IEC 61000-6-7, wonach alternative Ansätze möglich sind, um eine ausreichende Störfestigkeit nachzuweisen.

Der Ansatz für den Pfad C sieht die Implementierung von meist technischen Maßnahmen auf Maschinenebene vor. Anhand Tabelle L.1 der DIN EN ISO 13849-1 werden Punkte für die realisierte Maßnahme, ähnlich wie bei der CCF-Betrachtung, vergeben. Maximal können 390 Punkte (320 Punkte für einkanalige Systeme) erreicht werden. Bei Erreichen von 280 Punkten (230 Punkte für einkanalige Systeme gelten) werden die Anforderungen für die elektromagnetische Störfestigkeit als erfüllt angesehen. Sollte die Mindestpunktzahl nicht erreicht werden, sind Nachbesserungen an der Maschine so lange zwingend erforderlich, bis die Mindestpunktzahl erreicht wird.

Die angegebenen Maßnahmen stützen sich auf bekannte Maßnahmen und Verbesserungen bei den elektromagnetischen Eigenschaften von Maschinen, die sich in den letzten 30 Jahre etabliert haben.

Bei der Erarbeitung der Tabelle wurde insbesondere auf die praktische Umsetzbarkeit geachtet. Hierzu wurden die Erfahrungen aus der Prüfpraxis an funktional sicheren Anlagen und der Zertifizierung von Komponenten in die Methode implementiert. Im Folgenden ist eine beispielhafte Aufzählung von Maßnahmen aus der Tabelle L.1 der DIN EN ISO 13849-1 angegeben:

- Schirmungsmaßnahmen eines Gehäuses,
- Schirmungsmaßnahmen eines Kabels,
- Verwendung von verdrillten Signalkabel,
- Filterung der kritischen Signaleingänge,
- Einsatz von Netzfilter,
- Trennung der Komponenten im Schaltschrank nach starken Störern und empfindlichen Komponenten,
- Getrennte Verlegung von Strom- und Signalleitungen,
- Einhaltung von Abständen der Komponenten im Schaltschrank nach Störer und empfindlicher Komponenten,
- Trennung bei der Verlegung der Kabel oder Eingänge der Kabel in den Schaltschrank,
- Einhaltung von Abständen bei der Verlegung der Kabel oder Eingänge der Kabel in den Schaltschrank.

Literatur

[L1] DIN EN 61000-6-7: Elektromagnetische Verträglichkeit (EMV) – Teil 6-7: Fachgrundnormen – Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind (12/2015). DIN Media, Berlin 2015

[L2] DIN EN 61000-6-2: Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen – Störfestigkeit für Industriebereiche (11/2019). DIN Media, Berlin 2019

Anhang M

Vertrauenswürdige Künstliche Intelligenz

M.1 Einleitung

Verfahren der Künstlichen Intelligenz (KI) kommen zur Lösung komplexer Aufgaben zum Einsatz, beispielsweise zum Verarbeiten natürlicher Sprache oder zur Klassifikation von Objekten in Bildern. Durch sie lassen sich nicht nur wesentlich höhere Automatisierungsgrade erreichen, sondern auch gänzlich neue Anwendungsfelder erschließen.

Der Begriff KI wird heute hauptsächlich im Kontext des maschinellen Lernens verwendet, z. B. in neuronalen Netzen, Entscheidungsbäumen oder Support Vector Machines, schließt aber auch eine Vielzahl anderer Anwendungen wie Expertensysteme oder Wissensgraphen ein.

Derartige Methoden ermöglichen vollkommen neue intelligente Systeme und Anwendungen. Daher sieht man KI oft als die Schlüsseltechnologie der Zukunft an.

M.2 Vertrauenswürdige KI

Der Einsatz von KI bietet viele Möglichkeiten und kann in vielerlei Hinsicht neue Innovationen befördern. Der Einsatz von Systemen – insbesondere von Maschinen, die Verfahren der KI nutzen – kann jedoch auch die physische und psychische Belastung von Beschäftigten verändern. Um auszuschließen, dass vom Einsatz dieser Technologie neue Gefährdungen ausgehen oder um diese zu vermindern, ist eine vertrauenswürdige KI (Trustworthy Artificial Intelligence) erforderlich.

Der Begriff der Vertrauenswürdigkeit geht dabei in der Breite weit über den der Sicherheit hinaus und schließt die in **Abbildung M.1** dargestellten Aspekte ein.

Diese lassen sich grob in zwei verschiedene Blöcke unterteilen. Der erste Block befasst sich mit ethischen Aspekten. Dazu gehören Fairness, Privatsphäre und der Grad der Automatisierung und Kontrolle.

Der zweite Block befasst sich mit verschiedenen Aspekten, die die Zuverlässigkeit und Robustheit des KI-Systems beeinflussen können und somit einen direkten Einfluss auf die Sicherheit des Systems haben. Im Allgemeinen bezieht sich die Robustheit auf die Fähigkeit eines Systems, sein Leistungsniveau unter allen Umständen seiner Nutzung aufrechtzuerhalten. Robustheit unterscheidet sich von Zuverlässigkeit insofern, als ein zuverlässiges System sein Leistungsniveau nur unter den vorgegebenen Bedingungen aufrechterhalten muss. Die Robustheit hingegen umfasst auch die Stabilität gegenüber Fehlern oder unter Bedingungen, die sich stark von denen unterscheiden, für die das System trainiert wurde und stellt somit eine Erweiterung des Konzepts der Zuverlässigkeit dar. Ziel ist es, mit bisher nicht bekannten Daten das gleiche Leistungsniveau beizubehalten, das mit Trainingsdaten oder Daten für typische Operationen erreicht wurde.

Robustheit ist eine neue Herausforderung im Zusammenhang mit KI-Systemen, da diese Systeme für sehr komplexe Aufgaben in komplexen Nutzungsumgebungen eingesetzt werden, die ein gewisses Maß an Unsicherheit beinhalten. Neuronale Netzarchitekturen stellen eine besonders schwierige Herausforderung dar, da sie sowohl schwer zu erklären sind als auch aufgrund ihrer nichtlinearen Natur manchmal ein unerwartetes Verhalten zeigen. Darüber hinaus bieten einige Methoden des maschinellen Lernens neue Angriffsvektoren, die die Sicherheit des Systems gegen externe Angriffe verringern können. Es ist auch wichtig, die vielfältigen Einflüsse von Hardwarefehlern und die damit verbundenen spezifischen Aspekte zu berücksichtigen, die sich ebenfalls negativ auswirken können. Schließlich ist die technologische Reife der eingesetzten KI-Methode ein weiterer wichtiger Aspekt, der zu berücksichtigen ist. Eine nähere Beschreibung der einzelnen Aspekte ist in *A. Steimers* et al. [M1] zu finden.

Abb. M.1 Taxonomie der Vertrauenswürdigkeit von KI-Systemen

M.3 Maßnahmen

Das Gebiet der Risikobeherrschung wird stark von sicherheitsgerichteten Systemen sowie von Schutz- und Assistenzsystemen geprägt. Die Entwicklung solcher Systeme findet dabei üblicherweise in einem regulierten Kontext auf Basis harmonisierter Normen statt, die Anforderungen an die Qualität solcher Systeme, aber auch an die Gestaltung ihrer Entwicklung definieren. Technische Maßnahmen basieren dabei auf inhärent sicherem Design, Sicherheitsreserven, sicherem Ausfall und entwicklungstechnischen Maßnahmen zur Fehlervermeidung. Für KI-Systeme lassen sich daraus aufgrund der aktuellen technischen, regulativen und normativen Besonderheiten vier Grundprinzipien zur Risikominderung ableiten, die jeweils mit entsprechenden Maßnahmen in Verbindung stehen.

Gute ingenieurswissenschaftliche und datenwissenschaftliche Praxis

Um ein Mindestmaß an Qualität für ein KI-System sicherzustellen, muss sich die Entwicklung an etablierten grundlegenden Praktiken orientieren. Dazu gehört die Einhaltung eines konsistenten Prozesses, der alle Phasen der Entwicklung eines KI-Systems umfasst. Die aus der klassischen funktionalen Sicherheit bekannten Prozesse (siehe Kapitel 5 „Management der funktionalen Sicherheit und Entwicklungsablauf) können hier eine Basis bilden, lassen sich aber insgesamt nur bedingt auf KI-Systeme übertragen. Hierfür gibt es eigene Prozesse, wie etwa CRISP-DM, der ursprünglich aus dem Data Mining stammt. Neben der Sicherstellung eines guten Entwicklungsprozesses gehört zu den grundlegenden Praktiken auch die Anwendung von Normen zur Datenqualität (z. B. ISO/IEC 25012) und der Einsatz von Programmierrichtlinien (z. B. MISRA C).

Anwendung/Re-Interpretation bestehender Normen der funktionalen Sicherheit

Je nach Komplexität des gewählten Modells können einzelne Methoden zur Vermeidung und Reduzierung systematischer Fehler während der Softwareentwicklung aus den bestehenden Normen reinterpretiert werden (siehe ISO/IEC TR5469 [M2], Anhang A.2). Es kann daher vorteilhaft sein, Modelle niedriger Komplexität zu wählen, die der Mensch interpretieren und somit auch prüfen und warten kann. Auf diese Weise lassen sich Merkmale, die nicht kausal zum Ergebnis beitragen und zu fehlerhaften Ergebnissen führen würden, wieder manuell entfernen. Ein Nachteil interpretierbarer Modelle besteht allerdings darin, dass ihre Einfachheit oft auch mit einer geringeren Güte der Ergebnisse einhergeht. Bei wenig komplexen Aufgaben kann ein einfaches Modell aber auch ähnlich gute oder sogar bessere Ergebnisse liefern wie ein komplexes. Bei sehr komplexen Problemen wie der Bilderkennung gibt es derzeit häufig noch keine interpretierbaren Modelle, welche die Aufgabe adäquat lösen können.

Minderung KI-spezifischer Risiken durch weiterführende Maßnahmen

Spezifische Risikokategorien, die sich aus den technischen Besonderheiten von KI ergeben, lassen sich etwa anhand der oben skizzierten Taxonomie aus den Dimensionen der Vertrauenswürdigkeit ableiten. Ergeben sich aus bestimmten Kategorien innerhalb der geplanten Anwendung des KI-Systems Gefährdungen, sollten verschiedene spezialisierte Methoden während der Entwicklung eingesetzt werden, um diese KI-spezifischen Risiken zu minimieren. Beispiele wären hier etwa robustes Training oder Methoden der Erklärbarkeit. Oft lässt sich die erreichte Risikominimierung noch nicht ausreichend quantifizieren, daher genügt die Anwendung dieser Methoden allein aktuell nicht den Anforderungen für einen rigorosen Sicherheitsnachweis. Eine Bewertung und Einteilung dieser Methoden anhand ihrer Effektivität ist ein Ziel aktueller und zukünftiger Normungsprojekte im Bereich funktionaler Sicherheit von KI-Systemen.

Gesamtsystemische Absicherung/Run-time Monitoring

Betrachtet man ein mechanisches System, so existiert ein Punkt, an dem eine Belastung zum Versagen des Systems führt. Da dieser Punkt meist nur innerhalb eines gewissen Toleranzbereiches bestimmt werden kann, werden diese Systeme weit unter diesen Grenzbereichen betrieben, indem ein gewisser Sicherheitsabstand bzw. Sicherheitsfaktor eingeführt wird.

Auch beim maschinellen Lernen lassen sich solche Unsicherheiten identifizieren. Wird die Unsicherheit während der Laufzeit erfasst und in der Implementierung berücksichtigt, lässt sich so auch für ein KI-System ein Maß für die Zuverlässigkeit bestimmen. Neben den modellbedingten Unsicherheiten können Umweltbedingungen dazu beitragen, dass die Vorhersagen eines Modells nicht zuverlässig sind. So wird beispielsweise ein kamerabasiertes System zur Personenerkennung bei fehlender Beleuchtung mit hoher Konfidenz vorhersagen, dass sich keine Person in seinem Sichtfeld befindet. Die Absicherung eines solchen KI-Systems sollte daher auf einer gesamtsystemischen Ebene betrachtet werden. Im genannten Beispiel könnte etwa ein klassischer Helligkeitssensor verwendet werden, um die Glaubhaftigkeit des Modells hinsichtlich dieses speziellen möglichen Fehlers zu überprüfen. Ist die Gesamtunsicherheit des KI-Systems relativ hoch, sollte das Prinzip des sicheren Ausfalls angewendet werden. Dazu könnte das System etwa auf einen klassischen Entscheider zurückgreifen oder zunächst in den sicheren Zustand übergehen und eine weitere Überprüfung durch einen Menschen anfordern.

Tabelle M.1 Klassifizierungsschema zum Einsatz KI-basierter Systeme nach ISO/IEC TR 5469

KI-Technologie Klasse ⇢ KI-Anwendung und Anwendungsebene	Beschreibung der Anwendungsebene	KI-Technologie Klasse I	KI-Technologie Klasse II	KI-Technologie Klasse III
Anwendungsebene A1*	KI in sicherheitsrelevantem System eingesetzt, automatisierte Entscheidungsfindung	Anwendung der Risikominderungskonzepte bestehender internationaler Normen zur funktionalen Sicherheit möglich	geeigneter Anforderungskatalog Anmerkung: Der geeignete Anforderungskatalog für jede Anwendungsebene wird durch Nutzung der Risikominderungskonzepte bestehender internationaler Normen zur funktionalen Sicherheit und die zusätzlichen Überlegungen auf Grundlage der in den Abschnitten 8, 9, 10 und 11 des ISO/IEC TR 5469 durchgeführten Literaturrecherche festgelegt.	zum Zeitpunkt der Veröffentlichung des ISO/IEC TR 5469 ist kein angemessener Satz von Eigenschaften mit zugehörigen Methoden und Techniken bekannt, um eine ausreichende Risikominderung zu erreichen
Anwendungsebene A2*	KI in sicherheitsrelevantem System eingesetzt, keine automatisierte Entscheidungsfindung (z. B. Diagnosefunktionen)			
Anwendungsebene B1*	KI während der Entwicklung des sicherheitsrelevanten Systems eingesetzt, automatisierte Entscheidungsfindung			
Anwendungsebene B2*	KI während der Entwicklung des sicherheitsrelevanten Systems eingesetzt, keine automatisierte Entscheidungsfindung			
Anwendungsebene C*	KI nicht Teil einer Sicherheitsfunktion, aber indirekte Auswirkung auf diese Funktion möglich z. B. durch Einfluss auf die Anforderungsrate			
Anwendungsebene D**	KI nicht Teil einer Sicherheitsfunktion, keine Auswirkungen auf Sicherheit durch ausreichende Trennung und Verhaltenskontrolle	Anwendung der Risikominderungskonzepte bestehender internationaler Normen zur funktionalen Sicherheit		

* nur statisches (offline) Anlernen oder Lernen (während der Entwicklung)

** dynamisches (online) Anlernen oder Lernen möglich

M.4 Normungsaktivitäten

Es existieren bisher keine etablierten internationalen oder europäischen Regelwerke, die das Verhältnis von Funktionaler Sicherheit zur KI klären bzw. besondere Maßnahmen für KI-Systeme im sicherheitsgerichteten Umfeld beschreiben. Auf internationaler Ebene gab es beginnend 2020 erste Aktivitäten, Anforderungen für den Einsatz von KI im Rahmen funktional sicherer Systeme zu beschreiben. Diese sind in dem Technischen Report ISO/IEC TR 5469 [M2] gemündet. Bereits vor seinem Erscheinen wurde von den Normungsgremien der Beschluss gefasst, eine technische Spezifikation als Überarbeitung dieses Reports zu erstellen. Der Arbeitstitel lautet ISO/IEC TS 22440-1 „Artificial intelligence – Functional Safety and AI systems – Requirements“. Zwei weitere Teile der Reihe beschreiben die Themen „Guidance“ und „Examples of application“. Mit einem Erscheinen ist frühestens Ende 2026 zu rechnen. Mehr als ein Jahr schneller will die Europäische Kommission sein, die Mitte 2023 einen Auftrag zur KI-Normung an die europäischen Normungsorganisationen CEN und CENELEC gegeben hat. Zehn strategisch wichtige Normen zum Thema KI sollen erarbeitet werden. Besonders die Themen „Robustheit von KI-Systemen“ und „Cybersicherheit von KI-Systemen“ werden auch im Kontext der funktionalen Sicherheit von Maschinensteuerungen wichtig sein.

ISO/IEC TR 5469 definiert für den Einsatz von KI-basierten Systemen ein Klassifizierungsschema (Tabelle M1). Das Schema ist entlang zweier Achsen organisiert. Die erste Achse betrachtet die KI-Anwendung und die Anwendungsebene. Die Klassifizierung erfolgt von A bis D, wobei es auch Zwischenstufen für A und B gibt. Die Anwendungsebene A wird zugewiesen, wenn die KI-Technologie einen direkten Einfluss auf das sicherheitsrelevante System hat. Die Verwendungsebene B hingegen wird zugeordnet, wenn die KI-Technologie während der Entwicklung eines sicherheitsrelevanten Systems eingesetzt wird. Die Verwendungsebenen A und B werden jeweils weiter unterteilt – abhängig davon, ob eine automatisierte Entscheidungsfindung stattfindet (A1/A2, B1/B2). Die Verwendungsebene C bezieht sich auf KI-Techniken, die indirekt Einfluss auf die Funktion haben können, aber kein Teil der funktionalen Sicherheitsfunktion im System sind. Die Verwendungsebene D wird schließlich zugewiesen, wenn die KI-Technologie keine Auswirkungen auf die Sicherheitsfunktion hat.

Die zweite Achse des Schemas betrachtet verschiedene Klassen der KI-Technologie. Klasse I liegt vor, wenn die KI-Technologie nach vorhandenen internationalen Normen der funktionalen Sicherheit entwickelt und überprüft werden kann. Klasse II bedeutet, dass dies nur teilweise möglich ist, aber zusätzliche Methoden und Techniken ermittelt werden können, mit denen die notwendige Risikoreduzierung erreicht werden kann. Klasse III wird angewendet, wenn weder Klasse I noch II zutreffen.

M.5 Zusammenfassung

KI hat bereits heute viele Anwendungsfelder und ist ein rasant wachsender Markt. Es ist zu erwarten, dass KI-Verfahren in Zukunft zunehmend zur Realisierung neuer innovativer Applikationen beitragen und somit dauerhaft Einzug in verschiedene Domänen halten werden. Insbesondere zur Wahrung der Sicherheit und Gesundheit bei der Arbeit darf diese Entwicklung jedoch nur unter Beachtung von grundsätzlichen Prinzipen der Entwicklung sicherer Systeme geschehen. Hierzu bedarf es eines genauen Verständnisses der spezifischen Aspekte der KI-Verfahren sowie ihrer Auswirkungen auf die Qualität und Sicherheit des Systems.

Literatur

[M1] *Steimers A, Schneider M.:* Sources of Risk of AI Systems. Int. J. Environ. Res. Public Health 2022, 19, 3641

[M2] ISO/IEC TR 5469:2024 Artificial intelligence – Functional safety and AI systems. ISO, Genf 2024.

Anhang N

ISO/TR 13849-3 – Formeln für die PFH-Berechnung von Teilsystemen mit vorgesehener Architektur

Zum Nachweis, dass ein Design zur Realisierung einer Sicherheitsfunktion oder einer Teilfunktion einen bestimmten Performance Level (PL) erreicht, gehört unter anderem die Ermittlung der Kenngröße *PFH* (Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde). Für jedes Teilsystem müssen die folgenden quantifizierbaren Aspekte analysiert und bewertet werden, die in DIN EN ISO 13849-1, Abschnitt 6.1.1 genannt sind. Sie bilden die Grundlage für die *PFH*-Ermittlung:

- Systemarchitektur,
- $MTTF_D$-Wert der Bauteile,
- Diagnosedeckungsgrad (*DC*),
- Empfänglichkeit für Ausfälle gemeinsamer Ursache (Common Cause Failures, CCF).

Für die *PFH*-Ermittlung sind weitere Parameter relevant, die von der Norm in Abschnitt 6.1.1 nur am Rande erwähnt werden, weil sie hierzu bestimmte Annahmen trifft:

- Testraten,
- Anforderungsrate der Sicherheitsfunktion (bei manchen Fällen der Kategorie 2),
- Gebrauchsdauer T_M.

All diese Einflussfaktoren müssen in ihrem Zusammenspiel bewertet werden, um daraus die Kenngröße *PFH* zu ermitteln. Hierfür werden Methoden verwendet, die von verschiedener Art sein können. Die bekannteste Methode ist das in der Norm vorgestellte vereinfachte Verfahren für die Abschätzung des PL mit seiner grafischen Darstellung, dem Säulendiagramm (siehe Abschnitt 8.2.16 dieses Reports).

Der Technische Report ISO/TR 13849-3 [N1] bietet als Alternative zum vereinfachten Verfahren Gleichungen zur *PFH*-Berechnung für Teilsysteme an, die eine der vorgesehenen Architekturen aus DIN EN ISO 13849-1 aufweisen. Die vorgesehenen Architekturen aus dem Normabschnitt 6.1.3.2 werden in den Abschnitten 8.2.3 bis 8.2.7 dieses Reports vorgestellt. Die im Technischen Report präsentierten *PFH*-Gleichungen wurden auf Basis von *Markov*-Modellen hergeleitet. Mit diesen Gleichungen können alle Fälle behandelt werden, die auch mit dem vereinfachten Verfahren behandelbar sind und darüber hinaus viele weitere Fälle, in denen das vereinfachte Verfahren nicht anwendbar ist. Der Anhang N dieses IFA Reports erläutert den Anwendungsbereich des ISO/TR 138493 und stellt dessen nutzbare Inhalte in Kurzfassung zusammen.

N.1 Grenzen des vereinfachten Quantifizierungsverfahrens der Norm

Wenn die Teilsysteme zur Realisierung der Teilfunktionen jeweils einer der vorgesehenen Architekturen der Norm entsprechen, kommt zur *PFH*-Ermittlung grundsätzlich das vereinfachte Verfahren in Betracht. Allerdings müssen eine Reihe von Randbedingungen erfüllt sein, die sicherstellen, dass die dabei verwendete Tabelle K.1 aus Anhang K der Norm zutreffende *PFH*-Werte liefert. Ein Teil dieser Randbedingungen ist im Abschnitt 8.2.16 dieses Reports aufgeführt. Für Kategorie 2 finden sich im Abschnitt 8.2.5 weitere Einschränkungen, die mit der vierten Ausgabe der Norm erstmals verbindlich für diese Kategorie gemacht wurden. Insgesamt ist die Anwendung des vereinfachten Verfahrens zur *PFH*-Ermittlung an folgende Voraussetzungen geknüpft:

a) Alle Kategorien: Übereinstimmung der Architektur jedes Teilsystems oder des Gesamtsystems mit einer der vorgesehenen Architekturen nach den Abbildungen 8.2 bis 8.5
b) Alle Kategorien: zeitkonstante Ausfallraten; bei Verschleißteilen Nutzung einer als zeitkonstant angesetzten Ersatz-Ausfallrate (bzw. der entsprechenden $MTTF_D$) mit zeitbegrenzter Gültigkeit (vgl. Anhang D, Abschnitt D.2.4)
c) Alle Kategorien: Gebrauchsdauer T_M festgelegt auf 20 Jahre
d) Kategorien B, 1, 2, 3: $MTTF_D \leq 100$ Jahre (Begrenzung durch Norm-Tabelle K.1, im Einklang mit den Anforderungen dieser Kategorien, siehe auch Abschnitt 8.2.13)
e) Kategorie 4: $MTTF_D \leq 2500$ Jahre (Begrenzung durch Norm-Tabelle K.1, im Einklang mit den Anforderungen dieser Kategorie, siehe auch Abschnitt 8.2.13)
f) Kategorie 2: $MTTF_D$ des Testkanals $> 0{,}5 \cdot MTTF_D$ des Funktionskanals
g) Kategorie 2: zeitoptimale Testung, d.h. idealerweise Ausfallerkennung und -beherrschung stets vor Gefahreneintritt, bei Konkurrenz von Testung und Anforderung der Sicherheitsfunktion Testrate $\geq 100 \cdot$ Anforderungsrate der Sicherheitsfunktion, bei $25 \leq$ Testrate/Anforderungsrate < 100: Werte der Norm-Tabelle K.1 nutzbar mit 10 % *PFH*-Aufschlag
h) Kategorien 2, 3, 4: Common-Cause-Faktor β festgelegt auf 2 %
i) Kategorien 3, 4: Testintervalle << Kanal-$MTTF_D$ (von der Norm vorausgesetzt, aber dort nur indirekt in Tabelle E.1 berücksichtigt; Einfluss der Testintervalllänge nicht abgebildet)

Keine Voraussetzung für die Nutzung, aber eine Nebenwirkung der Anwendung des vereinfachten Verfahrens sind die folgenden Punkte:

j) Kategorie B: $MTTF_D \leq 27$ Jahre (Begrenzung durch Norm-Tabelle K.1)
k) Kategorien 2, 3: Berücksichtigung eines maximalen DC_{avg}-Wertes von 90 % (begrenzt durch Norm-Tabelle K.1)
l) Kategorien 2, 3, 4: Verwendung stets des unteren Grenzwertes der DC_{avg}-Intervalle: niedrig ⇢ 60 %, mittel ⇢ 90 %, hoch ⇢ 99 %

Wegen Punkt l) kann es im Einzelfall zu einer starken *DC*-Herunterstufung und infolgedessen einer deutlichen *PFH*-Verschlechterung kommen. Dies kann durch Interpolation zwischen den *PFH*-Werten aus der Norm-Tabelle K.1 vermieden werden, was die Ermittlung realitätsnäher macht und zugleich bessere *PFH*-Werte ermöglicht. Diese Interpolation führt der Softwareassistent SISTEMA (siehe Anhang H) automatisch durch, sofern sie nicht in den Experteneinstellungen deaktiviert wurde. Bei den Kategorien 2 und 3 können auf Basis der Norm-Tabelle K.1 keine DC_{avg}-Werte über 90 % berücksichtigt werden, weil diese Tabelle hierfür keine *PFH*-Werte enthält. Jedoch ermöglicht SISTEMA bei Kategorie 3 mit aktivierter Interpolation die Berücksichtigung von DC_{avg}-Werten bis zu 99 %.

Wenn ein Teilsystem nicht die hier genannten Voraussetzungen erfüllt, kann das vereinfachte Verfahren aus DIN EN ISO 13849-1 nicht angewendet werden. Mitunter ist damit noch eine Abschätzung der *PFH* zur sicheren Seite möglich, indem Eingangsparameter künstlich verschlechtert werden, um die Voraussetzungen des vereinfachten Verfahrens einzuhalten. Dies führt jedoch verfahrensbedingt zu einem verschlechterten (erhöhten) *PFH*-Wert.

N.2 *PFH*-Ermittlung ohne das vereinfachte Verfahren der Norm

Das vereinfachte Verfahren der Norm ermöglicht in vielen Fällen die Ermittlung der *PFH* von Teilfunktionen, ohne dass eine aufwändige Modellierung des Systems durchgeführt werden muss. Allerdings besteht kein Zwang, dieses Verfahren anzuwenden, denn es ist lediglich ein Angebot. Die Norm überlässt Anwendenden grundsätzlich die Wahl des Berechnungsverfahrens und zählt in Abschnitt 6.1.1 Zuverlässigkeitsblockdiagramme, *Markov*-Modelle sowie verallgemeinerte stochastische Petri-Netze (GSPN) als Beispiele für mögliche Methoden auf. Derselbe Normabschnitt nennt als Mindestanforderung an das gewählte Berechnungsverfahren, dass die eingangs zitierten quantitativen Größen $MTTF_D$-Wert der Bauteile, *DC*, Empfänglichkeit für CCF sowie die Systemarchitektur angemessen berücksichtigt werden müssen.

N.2.1 Modellierung von Teilsystemen oder des Gesamtsystems in Eigenregie

Um die in N.1 genannten Grenzen des vereinfachten Verfahrens der Norm zu überschreiten, können für betroffene Teilsysteme Rechenmodelle in Eigenregie entwickelt werden. Der ggf. erforderliche Erwerb der entsprechenden Kenntnisse ist jedoch mit Aufwand verbunden. Als Einführung in geeignete Modellierungstechniken eignen sich *Goble* [N2] und*Signoret* et al. [N3]. Für Leserinnen und Leser mit Grundkenntnissen in der Zuverlässigkeitsmodellierung und *Markov*-Technik beschreibt Anhang B des ISO/TR 13849-3, wie *PFH*-Gleichungen auf Basis von Zustands-Übergangs-Modellen gewonnen werden können. Die Vorgehensweise wird anhand der *PFH*-Gleichungen aus dem Hauptteil des TR demonstriert.

Die in DIN EN 61508-6 [N4] präsentierten Modelle und Gleichungen sind stark an der Prozessindustrie mit ihren Randbedingungen orientiert und daher für den typischen Maschinenbereich meist weniger geeignet.

N.2.2 Anwendungsgebiet des ISO/TR 13849-3

Sofern die Struktur von Teilsystemen einer der vorgesehenen Architekturen aus Abschnitt 8.2 entspricht, aber durch mindestens eine der in Abschnitt N.1 in den Punkten c) bis i) genannten Parameterbeschränkungen die Anwendung des vereinfachten Verfahrens ausgeschlossen ist oder die Nebenwirkungen dieses Verfahrens entsprechend den Punkten j) bis l) nicht akzeptabel sind, kommt die Berechnung der Teilsystem-*PFH* mit den in ISO/TR 13849-3 angebotenen Gleichungen in Betracht. Dadurch entfällt für Anwendende der Aufwand zur Entwicklung eines eigenen Rechenmodells.

Natürlich gelten die *PFH*-Gleichungen des ISO/TR 13849-3 auch in den vom vereinfachten Verfahren abgedeckten Parameterbereichen. So kann etwa das Säulendiagramm (vgl. Abbildung 8.7) in nahezu unveränderter Gestalt mit den *PFH*-Gleichungen für die allgemeinen Fälle aus ISO/TR 13849-3 erzeugt werden, die in diesem Report-Anhang in den Abschnitten N.2.5.2 bis N.2.5.4 angegeben sind. Der Technische Report bietet zusätzlich einige einfachere Gleichungen an, welche die *PFH* zur sicheren Seite, d. h. mit höheren Werten, abschätzen.

Die *PFH*-Ermittlung für ein SRP/CS aus Teilsystemen mit den vorgesehenen Architekturen nach DIN EN ISO 13849-1 mit dem ISO/TR 13849-3 kommt beispielsweise in folgenden Fällen infrage:

- Spezifikation des Systems für eine andere Gebrauchsdauer als 20 Jahre
- Bei einem Teilsystems mit der vorgesehenen Architektur für Kategorie 2: Berücksichtigung der *PFH*-Verbesserung, wenn die $MTTF_D$ des Testkanals deutlich größer ist als die Hälfte der $MTTF_D$ des Funktionskanals

- Bei einem Teilsystem mit der vorgesehenen Architektur für Kategorie 2, das hinsichtlich $MTTF_D$ oder Testrate nicht den Anforderungen der Kategorie 2 entspricht: *PFH*-Berechnung für die Bewertung im Rahmen von DIN EN IEC 62061 [N5] oder DIN EN 61508
- Bei Teilsystemen mit der vorgesehenen Architektur für die Kategorien 2 oder 3: Berücksichtigung der *PFH*-Verbesserung durch Diagnosedeckungsgrade über 90 % (SISTEMA ermöglicht dies nur bei Kategorie 3)
- Bei Teilsystemen mit der vorgesehenen Architektur für die Kategorie 4 Berücksichtigung der *PFH*-Verbesserung durch Diagnosedeckungsgrade über 99 %. Generell sollten DC-Werte über 99 % nur bei stichhaltiger Begründung durch eine FMEA oder einen rechnerischen Nachweis verwendet werden
- Bei Teilsystemen mit der vorgesehenen Architektur für die Kategorien 2, 3 oder 4: *PFH*-Berechnung bei Vorliegen eines von 2 % abweichenden Common-Cause-Faktors β (abgeschätzt z. B. mittels DIN EN 61508-6, Anhang D oder DIN EN IEC 62061, Anhang E)
- Bei Teilsystemen mit der vorgesehenen Architektur für die Kategorien 3 oder 4: Berücksichtigung der realisierten Testintervalllängen von bis zu einem Jahr bei der *PFH*-Ermittlung
- Bei stark unsymmetrischen Funktionskanälen in Kategorie 3 oder 4 genauere *PFH*-Berechnung
- Berücksichtigung von Soft Errors bei der *PFH*-Ermittlung (Soft Errors sind die Verfälschung von Daten in flüchtigen Digitalspeichern durch kleinste radioaktive Materialverunreinigungen in den Bauelementen oder durch kosmische Strahlung. Das vereinfachte Verfahren der Norm führt oft zu unnötig schlechten *PFH*-Werten, wenn typische Soft Error-Raten mitverwendet werden. Grund hierfür ist, dass dieses Verfahren die CCF-Ausfallrate nicht separat berücksichtigt. Soft Errors tragen jedoch wegen ihrer lokalen Wirkung nicht zu Ausfällen gemeinsamer Ursache bei. Die Berücksichtigung von Soft Errors ist in DIN EN ISO 13849-1:2023-12 und DIN EN IEC 62061:2023-02 nicht gefordert, aber bereits in DIN EN 61508:2011-02. In der aktuellen Überarbeitung von Teil 2 der DIN EN ISO 13849 wird dieses Thema allerdings aufgegriffen.)

Grundsätzlich eignen sich die im ISO/TR 13849-3 angebotenen Gleichungen zur *PFH*-Berechnung nicht nur in den genannten Spezialfällen. Sie kommen immer dann infrage, wenn das zu bewertende System aus Teilsystemen mit den vorgesehenen Architekturen nach DIN EN ISO 13849-1 besteht. Selbstverständlich gelten auch für die Rechenmodelle, aus denen die Gleichungen im ISO/TR 13849-3 abgeleitet wurden, bestimmte Randbedingungen, die für die Gültigkeit der Gleichungen einzuhalten sind. Zu den Randbedingungen gehören etwa die Zeitkonstanz der Ausfallraten, die hohe Anforderungsrate der Sicherheitsfunktion oder die Reparatur nach Fehlererkennung. Diese Randbedingungen passen zu den typischen Gegebenheiten im Maschinenbereich und sind in Abschnitt N.2.4 aufgeführt.

N.2.3 Mathematischer Hintergrund des ISO/TR 13849-3

Die *PFH*-Gleichungen des ISO/TR 13849-3 beziehen sich auf die vorgesehenen Architekturen aus Abschnitt 8.2. Im Technischen Report werden diese Architekturen in einer vereinfachten Gestalt verwendet, bei der die Kanäle jeweils zu einem Block zusammengefasst werden, statt als Reihenschaltungen von Blöcken (I, L, O) dargestellt zu werden. Diese Zusammenfassung dient dazu, die Anzahl der Variablen in den *PFH*-Gleichungen klein zu halten.

Die Gewinnung der *PFH*-Gleichungen erfolgte in mehreren Schritten, die im Detail im Anhang B des TR beschrieben werden. Dabei handelt es sich lediglich um Informationen für Interessierte, weil für die Anwendung der *PFH*-Gleichungen die Kenntnis ihrer Herleitung nicht erforderlich ist. Aus den Blockdiagrammen wurden Zustands-Übergangs-Diagramme abgeleitet, deren Zustandsanzahl durch Ausnutzung der typischen Größenverhältnisse der Übergangsraten zueinander verkleinert wurden. Diese Vereinfachung führt dazu, dass nur noch Übergangsprozesse in den Zustands-Übergangs-Modellen auftreten, die Ausfallsprozesse repräsentieren und die *PFH* dominant bestimmen. Wegen der Beschränkung auf zeitkonstante Ausfallraten enthalten die reduzierten Zustands-Übergangs-Modelle nur noch exponentialverteilte Übergangsprozesse, was ihre analytische Auswertung als *Markov*-Modelle durch Lösen von Differentialgleichungssystemen ermöglicht. Auf diese Weise gelingt es, die zeitlichen Verläufe der Zustandswahrscheinlichkeiten in Gleichungsform anzugeben. Die zeitlichen Wahrscheinlichkeitsverläufe der Zustände ermöglichen wiederum die Berechnung der Häufigkeit von Übergängen in den Gefahrenzustand, der Hazard Rate. Deren Mittelwert über die Gebrauchsdauer kann bei den vorliegenden Systemen für hohe bis kontinuierliche Anforderung der Sicherheitsfunktion (mindestens eine Anforderung pro Jahr) mit der *PFH* gleichgesetzt werden, der mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde.

Auf die Zustands-Übergangsmodelle der zweikanaligen Architektur wendet der Technische Report ergänzend eine einfachere Auswertungsmethode an. Damit werden als Alternative zu den Markov-basierten Gleichungen einfachere *PFH*-Gleichungen gewonnen, die weniger genau sind und eine konservative Abschätzung der *PFH* bieten (höhere *PFH*-Werte).

N.2.4 Voraussetzungen für die Anwendung des ISO/TR 13849-3

In die Entwicklung der *PFH*-Gleichungen sind bestimmte Annahmen eingeflossen, die üblicherweise im Maschinenbereich zutreffen, etwa über die Durchführung und Dauer von Reparaturen. Dazu kommen weitere Annahmen, die auch bei anderen Quantifizierungsverfahren oft gemacht werden, um die Komplexität der Berechnung zu begrenzen, z. B. konstante Ausfallraten und perfekte Reparatur. Für den ISO/TR 13849-3 gelten folgende Randbedingungen, die erfüllt sein müssen bzw. deren Einhaltung unterstellt werden muss, damit seine *PFH*-Gleichungen gültig sind:

- Realisierung der Sicherheitsfunktion durch ein System, das eine der vorgesehenen Architekturen nach DIN EN ISO 13849-1 aufweist oder eine logische Reihenschaltung von solchen Teilsystemen darstellt
- Nichtberücksichtigung der Ausfallraten in die sichere Richtung (Dies stellt in Bezug auf die *PFH* eine Abschätzung zur sicheren Seite dar.)
- Zeitkonstante Ausfallraten während der System-Gebrauchsdauer (Hieraus folgt, dass die $MTTF_D$ dem Kehrwert der gefährlichen Ausfallrate entspricht.)
- Nichtberücksichtigung von systematischen Ausfällen (Es werden nur Zufallsausfälle berücksichtigt, weil es für systematische Ausfälle keine allgemeinen Modelle gibt und diese per Design vermieden werden müssen. Ausfälle gemeinsamer Ursache, denen hinsichtlich der Gemeinsamkeit ihres Auftretens eine systematische Komponente eigen ist, werden jedoch berücksichtigt.)
- Im Falle von Diagnose: Testintervalle, die kürzer als die Gebrauchsdauer sind (Üblicherweise gelten nach Teil 1 der Norm nur Testintervalle von maximal einem Jahr als akzeptabel; Testintervalle ab der Länge der Gebrauchsdauer sind gleichbedeutend mit Nichttestung.)
- Perfekte Reparatur nach einem durch Diagnose erkannten Ausfall
- Perfekte Reparatur nach einem gefährlichen Vorfall (Hazardous Event), d. h. wenn die Sicherheitsfunktion ausgefallen ist und dies durch ihre Nichtausführung bei Anforderung aufgedeckt wird
- Die mittlere Reparaturdauer (Mean Repair Time, *MRT*) und die mittlere Dauer bis zur Wiederherstellung (Mean Time to Restoration, *MTTR*) sind bedeutend kleiner als die $MTTF_D$-Werte der Kanäle, also die Kehrwerte der gefährlichen Ausfallraten der Kanäle.
- Bei Umsetzung einer Wiederholungsprüfung (Proof Test): Setzen der Gebrauchsdauer auf die Länge des Intervalls der Wiederholungsprüfung (Wiederholungsprüfungen werden offline ausgeführt und streben die Wiederherstellung eines perfekten Wie-neu-Zustands an. Sie sind im Maschinenbereich unüblich, aber in DIN EN IEC 62061 und DIN EN IEC 61508 genannt.)
- Interpretation der *PFH* als mittlere Häufigkeit nichtbedienter Anforderungen der Sicherheitsfunktion (Dies entspricht der Häufigkeit gefährlicher Vorfälle, der Hazard Rate.)

N.2.5 Die wichtigsten Gleichungen aus dem ISO/TR 13849-3

Im Kapitel 9 des ISO/TR 13849-3 werden *PFH*-Gleichungen präsentiert, die zu den vorgesehenen Architekturen für die Kategorien B, 1 und 2 passen. Dem allgemeinen Fall des getesteten einkanaligen Systems folgen einfachere Sonderfälle mit entsprechend einfacheren *PFH*-Gleichungen. Dazu gehören die Sonderfälle für die Kategorien B und 1, die mathematisch als Spezialfall der Kategorie 2 mit Wegfall der Diagnose ($DC = 0$) betrachtet werden können. Im Kapitel 10 des Technischen Reports folgen *PFH*-Gleichungen für die vorgesehenen Architekturen der Kategorien 3 und 4. Auch hier werden nach dem allgemeinsten Fall *PFH*-Gleichungen für einfachere Spezialfälle vorgestellt. Für zweikanalige Systeme werden auch alternative Gleichungen geboten, die ohne das Markov-Verfahren gewonnen wurden und die *PFH* zur sicheren Seite abschätzen. Verglichen mit den Markov-basierten Gleichungen liefern sie einen höheren *PFH*-Wert, sind dafür aber besonders einfach.

In den folgenden Abschnitten N.2.5.1 bis N.2.5.5 werden die wichtigsten Gleichungen aus dem ISO/TR 138493 wiedergegeben. Von den *PFH*-Gleichungen (Abschnitte N.2.5.2 bis N.2.5.4) werden nur jene mit der größten Anwendungsbreite und der besten Genauigkeit aufgeführt, da mit ihnen durch entsprechende Wahl der Eingangsvariablen auch die einfacheren Sonderfälle behandelt werden können.

N.2.5.1 Reihenschaltungen von Elementen oder Funktionsblöcken

Die *PFH*-Gleichungen enthalten Eingangsvariablen (etwa Ausfallraten, *DC*-Werte oder Testraten), welche die Daten für komplette Funktions- oder Testkanäle repräsentieren. Häufig findet man in solchen Kanälen jedoch eine logische Reihenschaltung aus mehreren Elementen oder Funktionsblöcken. Dies ist in Abbildung N.1 für einen Kanal (Channel, CH) aus den n Elementen E_1 bis E_n dargestellt. Logische Reihenschaltung besagt, dass der ganze Kanal gefahrbringend ausfällt, wenn mindestens eines seiner Elemente gefahrbringend ausfällt. Jedes dieser Elemente könnte auch für einen seinerseits aus Einzelbauteilen zusammengesetzten Funktionsblock stehen. Abbildung N.1 zeigt auch das Bezeichnungsschema für die gefährlichen Ausfallraten der Elemente ($\lambda_{E/D}$), die für die Elemente jeweils realisierten Diagnosedeckungsgrade (DC_i) und die dabei verwendeten Testraten (r_{ti}). Falls eines der Elemente ein zusammengesetzter Funktionsblock ist, beziehen sich diese Daten natürlich auf den Block als Ganzen. Anhang B dieses Reports erläutert, wie die benötigten Blockdaten, die gefährliche Ausfallrate des Blocks

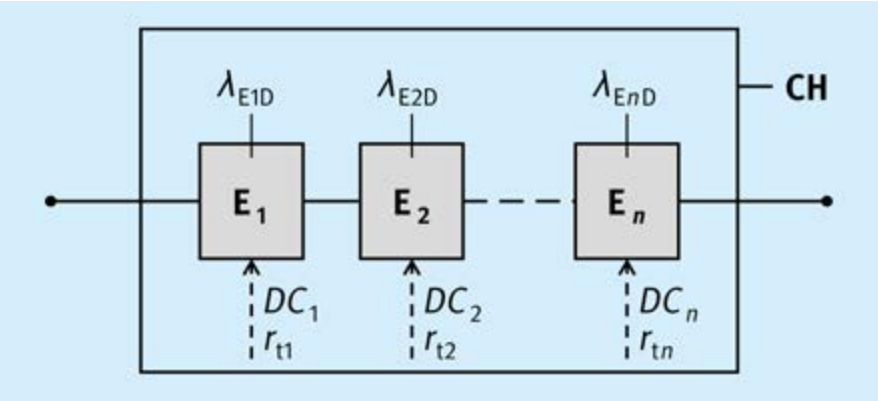


Abb. N.1
Kanal CH aus einer logischen Reihenschaltung von Elementen

und der ggf. für den Block realisierte Diagnosedeckungsgrad mithilfe einer FMEA aus den Daten seiner Elemente und der inneren Blockstruktur (Schaltung) ermittelt werden können.

Die Ausfallraten λ_{EiD} mit $i = 1 \ldots n$ beziehen sich auf die gefährliche Ausfallrichtung. Bei einem Funktionskanal ist diese mit dem Verlust der Fähigkeit des Kanals verbunden, die Teilfunktion auszuführen. Im Falle von Redundanz bedeutet ein solcher Ausfall noch nicht zwingend den gefahrbringenden Ausfall des Teilsystems. Trotzdem signalisiert auch hier der Index D, dass die Ausfallrate in die sicherheitstechnisch ungünstige Richtung gemeint ist. Bei einem Testkanal ist mit gefährlicher Ausfallrichtung diejenige Richtung gemeint, die den Test unwirksam werden lässt.

Die gefährliche Ausfallrate des Kanals CH ergibt sich als Summe der gefährlichen Ausfallraten seiner Elemente entsprechend Gleichung (N.1) aus dem **Kasten N.1**. Auch die in diesem Abschnitt genannten Gleichungen (N.2) bis (N.4) sind in diesem Kasten enthalten. Diese Gleichung entspricht der Gleichung (D.1) aus DIN EN ISO 13849-1. Der Diagnosedeckungsgrad des Kanals CH kann mit Gleichung (N.2) berechnet werden. Sie entspricht formal der Gleichung (E.1) aus DIN EN ISO 13849-1. Im Unterschied zu dieser wird die Gleichung (N.2) jedoch für die *PFH*-Berechnung mit dem ISO/TR 13849-3 nur auf einen einzelnen Kanal angewendet und nicht kanalübergreifend. Unabhängig von der Nutzung von Gleichung (N.2) muss bei Teilsystemen der Kategorien 2, 3 und 4 die Einhaltung der jeweils geltenden Anforderung an den Mindest-*DC* entsprechend DIN EN ISO 13849-1 überprüft werden. Diese Anforderungen sind auch in den Abschnitten 8.2.5 bis 8.2.7 dieses Reports wiedergegeben.

Sind die Testraten der Kanal-Elemente unterschiedlich, muss als Testrate des Kanals die niedrigste Element-Testrate angesetzt werden.

Statt der gefährlichen Ausfallraten können die $MTTF_D$-Werte der Elemente gegeben sein. Da von zeitkonstanten Ausfallraten ausgegangen wird, kann dann die gefährliche Ausfallrate eines Elements E bzw. eines Kanals CH mithilfe des Kehrwerts nach Gleichung (N.3) berechnet werden.

Umgekehrt können die $MTTF_D$-Werte mit Gleichung (N.4) aus den gefährlichen Ausfallraten berechnet werden. Mit-

Kasten N.1 Reihenschaltungen von Elementen oder Funktionsblöcken

$$\lambda_{CHD} = \lambda_{E1D} + \lambda_{E2D} + \ldots + \lambda_{EnD} \tag{N.1}$$

$$DC_{CH} = \frac{\lambda_{E1D}}{\lambda_{CHD}} DC_1 + \frac{\lambda_{E2D}}{\lambda_{CHD}} DC_2 + \ldots + \frac{\lambda_{EnD}}{\lambda_{CHD}} DC_n \tag{N.2}$$

$$\lambda_{EiD} = \frac{1}{MTTF_{D,\,Ei}} \quad , \quad \lambda_{CHD} = \frac{1}{MTTF_{D,\,CH}} \tag{N.3}$$

$$MTTF_{D,\,Ei} = \frac{1}{\lambda_{EiD}} \quad , \quad MTTF_{D,\,CH} = \frac{1}{\lambda_{CHD}} \tag{N.4}$$

hilfe von Gleichung (N.4) kann geprüft werden, ob ein Kanal die Anforderung der DIN EN ISO 13849-1 an die Mindest-$MTTF_D$ der Kategorie seines Teilsystems erfüllt. Diese Anforderungen können auch den Abschnitten 8.2.3 bis 8.2.7 dieses Reports entnommen werden.

Verschleißteile weisen keine zeitkonstanten Ausfallraten auf. Darum muss für sie auch bei der *PFH*-Berechnung nach dem ISO/TR 13849-3 mit einer als konstant angenommenen Ersatz-Ausfallrate bzw. Ersatz-$MTTF_D$ gearbeitet und die Einsatzdauer begrenzt werden. In Anhang D, Abschnitt D.2.4 dieses Reports wird die Vorgehensweise für pneumatische und elektromechanische Elemente beschrieben. Aus DIN EN ISO 13849-1 sind diesbezüglich die Gleichungen (C.3) und (C.5) des Anhangs C relevant.

N.2.5.2 Vorgesehene Architektur für Teilsysteme der Kategorie B oder 1

Bei dieser Architektur gibt es nur einen einzigen, ungetesteten Funktionskanal, der die Teilfunktion ausführt. Dieser ist in Abbildung N.2 als Block F dargestellt.

Abb. N.2 Vereinfachte vorgesehene Architektur für Kategorie B oder 1

Der Funktionskanal, Block F, entspricht der Reihenschaltung aus den Blöcken I, L und O in DIN EN ISO 13849-1. Abbildung N.2 zeigt auch die einzige *PFH*-relevante Eingangsvariable für diesen Fall: λ_{FD}, die Ausfallrate des Blocks F in die gefährliche Richtung. Ausfall in die gefährliche Richtung bedeutet den Ausfall der Sicherheitsfunktion.

Die *PFH* kann mit der besonders einfachen Gleichung (N.5) aus **Kasten N.2** berechnet werden.

Bei jedem Teilsystem muss geprüft werden, welcher maximale PL *in quantitativer Hinsicht* mit ihm erreichbar ist. Bei Teilsystemen der Kategorien B und 1 muss dazu die $MTTF_D$ des Funktionskanals F auf 100 Jahre gekappt werden, falls ihr Originalwert über 100 Jahre liegt. Dies bedeutet nach Gleichung (N.3), dass für λ_{FD} kein kleinerer Wert als $1{,}14 \cdot 10^{-6}\ h^{-1}$ verwendet werden darf. Mit Gleichung (N.5) und Tabelle 7.1 (Hauptteil dieses Reports, Abschnitt 7.1) ergibt diese Prüfung, dass ein Teilsystem mit der Architektur nach Abbildung N.2 aus quantitativer Sicht keinen höheren PL als c erreichen kann. Dies entspricht auch dem normativ festgelegten maximalen PL bei Kategorie 1, siehe Abschnitt 8.2.4 dieses Reports. Für ein Teilsystem der Kategorie B begrenzt die Norm den PL unabhängig von der *PFH* sogar auf b, siehe Abschnitt 8.2.3 dieses Reports.

Kasten N.2
PFH bei Teilsystemen der Kategorie B oder 1

$$PFH = \lambda_{FD} \qquad \text{(N.5)}$$

Die einfache Architektur nach Abbildung N.2 findet in DIN EN IEC 62061 ihre Entsprechung in der Basis-Teilsystemarchitektur A. Die Gleichungen (N.1) und (N.5) entsprechen der *PFH*-Berechnung für diese Architektur in DIN EN IEC 62061. Zur Ermittlung des aus quantitativer Sicht maximal erreichbaren Safety Integrity Levels (SIL) müssen nach DIN EN IEC 62061:2023-02 neben der *PFH* zusätzlich die Architektur-Einschränkungen für die Hardware-Fehlertoleranz 0 aus der dortigen Tabelle 6 beachtet werden.

N.2.5.3 Vorgesehene Architektur für Teilsysteme der Kategorie 2

Auch bei dieser Architektur gibt es einen Funktionskanal, der die Teilfunktion ausführt. Zusätzlich gibt es einen Testkanal, der gefahrbringende Ausfälle des Funktionskanals aufdeckt und im Falle einer solchen Aufdeckung einen sicheren Zustand herstellt. In Abbildung N.3 ist der Funktionskanal als Block F und der Testkanal als Block M (Monitor) dargestellt.

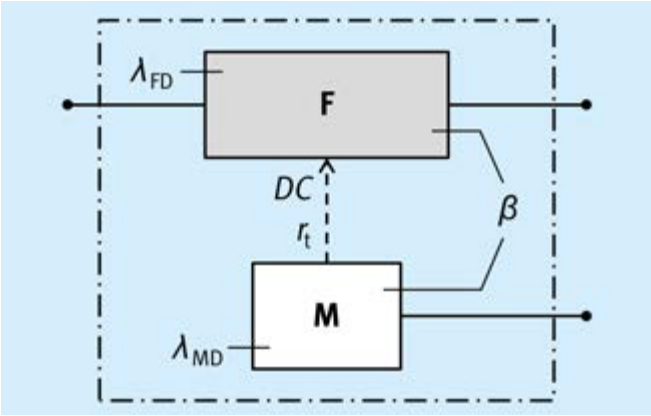


Abb. N.3 Vereinfachte vorgesehene Architektur für Kategorie 2

Diese Architektur schließt sowohl den Fall ein, bei dem der Testkanal M den Funktionskanal F „von außen“ testet, als auch den Fall, bei dem Selbsttest-Routinen innerhalb des Funktionskanals F ablaufen, die bei Fehlererkennung mithilfe des Testkanals M einen sicheren Zustand herstellen. Im letztgenannten Fall wird der Testkanal auch als „Watchdog“ bezeichnet.

Dem Funktionskanal, Block F, entspricht in DIN EN ISO 13849-1 eine Reihenschaltung aus den Blöcken I, L und O, während

dem Testkanal, Block M, in der Norm eine Reihenschaltung aus den Blöcken TE und OTE entspricht.

In Abbildung N.3 sind die meisten der für die *PFH* relevanten Eingangsvariablen angegeben: λ_{FD} ist die Ausfallrate des Funktionskanals in die gefährliche Richtung, also jene Richtung, bei der F die Teilfunktion nicht mehr ausführen kann. λ_{MD} ist die Ausfallrate des Testkanals in jene Richtung, bei der M die Fähigkeit verliert, Ausfälle von F zu erkennen oder nach einer solchen Erkennung einen sicheren Zustand herbeizuführen. Die Variable *DC* bezeichnet den Diagnosedeckungsgrad, den der Testkanal M für den Funktionskanal F realisiert. Mit r_t ist die Testrate bezeichnet, mit der F von M getestet wird.

Der Zweck dieser Anordnung wird unterlaufen, wenn aufgrund *einer* Ursache sowohl der Funktionskanal F als auch der Testkanal M in die ungünstige Richtung ausfallen. Darum müssen Maßnahmen gegen CCF umgesetzt werden, deren Wirksamkeit mithilfe des Common-Cause-Faktors β abgeschätzt wird, siehe hierzu Anhang F. Um die CCF bei der *PFH*-Ermittlung zu berücksichtigen, wird vorab als Hilfsgröße die Common-Cause-Ausfallrate λ_{CC}, mit Gleichung (N.6) aus dem **Kasten N.3** berechnet. Die darin enthaltene Minimum-Funktion wählt als ihr Ergebnis stets das kleinere ihrer beiden Argumente aus. Die Argumente $\lambda_{FD\ SER\text{-}free}$ und $\lambda_{MD\ SER\text{-}free}$ sind die Ausfallraten der Blöcke F und M in die ungünstige Richtung, d. h. in Richtung Verlust der Teilfunktion bzw. Verlust der Diagnose für F durch M. Der Index-Zusatz „SER-free“ bedeutet, dass bei diesen Ausfallraten der ggf. enthaltene Beitrag von Soft Error-Raten (SER) weggelassen werden soll. Zum Thema „Soft Errors“ gibt es im letzten Aufzählungspunkt von Abschnitt N.2.2 eine kurze Erläuterung.

Das hier benutzte Modell kann das Zusammenspiel von Test- und Anforderungsrate berücksichtigen. Dabei wird im günstigsten Fall eine „zeitoptimale Testung“ realisiert. Das bedeutet, dass Ausfälle im Funktionskanal, die vom Diagnosedeckungsgrad abgedeckt sind, immer rechtzeitig erkannt werden, d. h. vor dem Eintritt einer Gefahrensituation wird ein sicherer Zustand herbeigeführt. Dies kann durch eine kontinuierliche Testung mit ausreichend schneller sicherheitsgerichteter Reaktion bei Ausfallerkennung gegeben sein (Beispiel: Überspannungserkennung mit einem Komparator). Auch eine periodische Testung kann zeitoptimal sein, wenn – bedingt durch die Art der Applikation – nach dem Funktionskanal-Ausfall der sichere Zustand schnell genug erreicht wird, bevor es zu einer tatsächlichen Gefährdung kommt. In diesem Fall muss die Summe aus dem Testintervall und der Zeit zum Herbeiführen des sicheren Zustands kleiner als die Prozesssicherheitszeit sein. Bei universell einzusetzenden Steuerungen oder Komponenten für Steuerungen tritt deren spezifizierte Systemreaktionszeit an die Stelle der nicht bekannten Prozesssicherheitszeit.

Wenn keine „zeitoptimale Testung“ vorliegt, finden die Tests häufig bei einem durch die Applikation ausgelösten Signalwechsel oder Software-getriggert periodisch statt. Dabei können auch längere Testroutinen ablaufen, z. B. für Digitalspeicher. Eine solche Testung ist nicht zeitoptimal, denn es besteht eine zeitliche Konkurrenz zwischen der Testung und der Anforderung der Sicherheitsfunktion. Damit die Konkurrenz möglichst oft zugunsten des Tests ausgeht, muss die Testrate viel höher sein als die Anforderungsrate der Sicherheitsfunktion.

Unabhängig davon, ob eine zeitoptimale Testung vorliegt oder nicht, kann die *PFH* des Teilsystems mithilfe der Gleichung (N.7) aus Kasten N.3 berechnet werden. Neben der mit Gleichung (N.6) zu berechnenden Common-Cause-Ausfallrate λ_{CC} und den weiteren bereits genannten Größen muss in Gleichung (N.7) auch die Gebrauchsdauer T_M (Mission Time) sowie die Anforderungsrate der Sicherheitsfunktion r_t eingesetzt werden. Gleichung (N.7) setzt voraus, dass die Testung und die Anforderung zeitlich unkorreliert sind, also keine systematische zeitliche Kopplung vorliegt. Bei einer periodischen Testung und zufällig auftretenden Anforderungen der Sicherheitsfunktion ist diese Bedingung erfüllt.

Um eine zeitoptimale Testung abzubilden, wird in Gleichung (N.7) der dort enthaltene Faktor $r_t/(r_t + r_d)$ durch den Faktor 1 ersetzt. Gibt es eine Konkurrenz von Testung und Anforderung der Sicherheitsfunktion, so stellt dieser Faktor, der auch *TRTE* (Time-related Test Efficiency) genannt wird, ein Maß für die Testeffektivität in zeitlicher Hinsicht dar. Beträgt die Testrate das 100-fache der Anforderungsrate, dann hat der Faktor *TRTE* ungefähr den Wert 0,99, was der zeitoptimalen Testung in solchen Fällen sehr nahekommt, bei denen der *DC* deutlich unter 99 % liegt. Wird *TRTE* ausgehend von 0,9 verkleinert, so wird das Prinzip „getestete Einkanaligkeit“ zunehmend unterlaufen, weil die Testung immer weniger zur *PFH*-Reduktion beiträgt und sich die *PFH* der des ungetesteten Kanals annähert. Um dies zu unterbinden, fordert DIN EN ISO 13849-1 für Kategorie 2, dass bei nicht zeitoptimaler Testung die Testrate mindestens das 100-fache (in Ausnahmefälle mindestens das 25-fache) der Anforderungsrate beträgt. Dies entspricht der Forderung, dass der Wert von *TRTE* sogar mindestens 0,9615 betragen muss.

Soll mit der Architektur aus Abbildung N.3 ein Teilsystem der Kategorie 2 nach DIN EN ISO 13849-1 realisiert werden, dann genügt es zur quantitativen Bewertung nicht, mit Gleichung (N.7) den *PFH*-Beitrag des Teilsystems zu ermitteln. Zusätzlich müssen die speziellen quantitativen Anforderungen der Kategorie 2 erfüllt werden. Sie betreffen die $MTTF_D$ des Funktionskanals F und das Verhältnis der $MTTF_D$-Werte von Test- und Funktionskanal. Weitere Anforderungen beziehen sich auf den *DC* für den Funktionskanal und, wie oben beschrieben, das Verhält-

Kasten N.3 *PFH* bei Teilsystemen der Kategorie 2

$$\lambda_{CC} = \beta \cdot \min(\lambda_{FD\,SER\text{-}free}, \lambda_{MD\,SER\text{-}free}) \quad \text{(N.6)}$$

$$PFH = \lambda_{FD} - DC\frac{r_t}{r_t + r_d} \cdot \frac{(\lambda_{FD} - \lambda_{CC})\left[\lambda_{FD}\,(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})\,T_M + (\lambda_{MD} - \lambda_{CC})\left(1 - e^{-(\lambda_{FD}+\lambda_{MD}-\lambda_{CC})T_M}\right)\right]}{(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})^2\,T_M} \quad \text{(N.7)}$$

nis von Test- und Anforderungsrate bei nicht zeitoptimaler Testung. All diese Anforderungen können dem Abschnitt 8.2.5 dieses Reports entnommen werden.

Zur Prüfung des mit dem Teilsystem erreichbaren PL müssen die $MTTF_D$-Werte sowohl des Funktionskanals F als auch des Testkanals M vor Anwendung der Gleichungen (N.6) und (N.7) auf 100 Jahre gekappt werden, falls ihr jeweiliger Originalwert über 100 Jahre liegt. Dies bedeutet nach Gleichung (N.3), dass für λ_{FD} und für λ_{MD} keine kleineren Werte als $1{,}14 \cdot 10^{-6}$ h^{-1} für die *PFH*-Berechnung verwendet werden dürfen, wenn mit diesem *PFH*-Wert und Tabelle 7.1 (Abschnitt 7.1 dieses Reports) geprüft werden soll, welcher maximale PL aus quantitativer Sicht mit dem Teilsystem erreichbar ist. Unabhängig hiervon ist der PL bei Kategorie 2 auf d begrenzt, siehe Abschnitt 8.2.5 dieses Reports.

Ein Sonderfall ist die Nutzung der Architektur nach Abbildung N.3 zur Realisierung eines Teilsystems der Kategorie 3. Voraussetzung hierfür ist, dass der Testkanal gefahrbringende Ausfälle des Funktionskanals praktisch lückenlos aufdecken kann und nach einem erkannten Fehler innerhalb der spezifizierten Reaktionszeit der Teilfunktion einen sicheren Zustand herstellt. Hierdurch wird die für Kategorie 3 obligatorische Einfehlersicherheit erreicht und der Testkanal nimmt die Rolle eines zweiten Funktionskanals ein. Bei Anwendung der *PFH*-Gleichung (N.7) schätzt man in diesem Spezialfall den *DC* des Funktionskanals F üblicherweise konservativ mit 99 % ab. Zusätzlich müssen natürlich auch die weiteren quantitativen Anforderungen der Kategorie 3 erfüllt werden, darunter die Forderung, dass DC_{avg} unter Berücksichtigung des Funktions- und Testkanals mindestens 60 % betragen muss. Die Berechnung von DC_{avg} mit Gleichung (8.4) aus dem Hauptteil bzw. Gleichung (E.1) aus dem Anhang E dieses Reports kann eine eventuell vorhandene Diagnose für den Testkanal berücksichtigen. Eine solche Diagnose wird jedoch bei Nutzung von Gleichung (N.7) vernachlässigt, sodass mit ihr ein konservativer *PFH*-Wert berechnet wird. In Abschnitt N.2.5.4 wird gezeigt, dass diese technische Lösung alternativ auch als zweikanaliges System interpretierbar ist, wodurch auch eine Diagnose des Testkanals bei der *PFH*-Berechnung Berücksichtigung finden kann.

Die Architektur nach Abbildung N.3 entspricht der Basis-Teilsystemarchitektur C aus DIN EN IEC 62061. Darum eignen sich die Gleichungen (N.6) und (N.7) bei Vorliegen dieser Architektur auch zur *PFH*-Berechnung im Rahmen der Anwendung dieser IEC-Norm. Um den aus quantitativer Sicht maximal erreichbaren SIL zu ermitteln, müssen nach DIN EN IEC 62061:2023-02 neben der *PFH* zusätzlich die Architektur-Einschränkungen für die Hardware-Fehlertoleranz 0 aus der dortigen Tabelle 6 beachtet werden.

Bei den Gleichungen (H.4) und (H.5) mit (H.7) der DIN EN IEC 62061:2023.02 handelt es sich um durch Linearisierung vereinfachte Varianten der Gleichungen (N.6) und (N.7) dieses Report-Anhangs. Die Gleichungen (H.4) und (H.5) mit (H.7) gelten nur für zeitoptimale Testung und liefern wegen der Linearisierung höhere *PFH*-Werte.

N.2.5.4 Vorgesehene Architektur für Teilsysteme der Kategorie 3 oder 4

Diese Architektur verfügt über zwei Kanäle, die beide unabhängig voneinander die Teilfunktion ausführen. Zugleich kann jeder Kanal dann einen sicheren Zustand herstellen, wenn im jeweils anderen Kanal ein erkennbarer Ausfall aufgetreten ist. In **Abbildung N.4** sind die beiden Kanäle als Block A und Block B dargestellt.

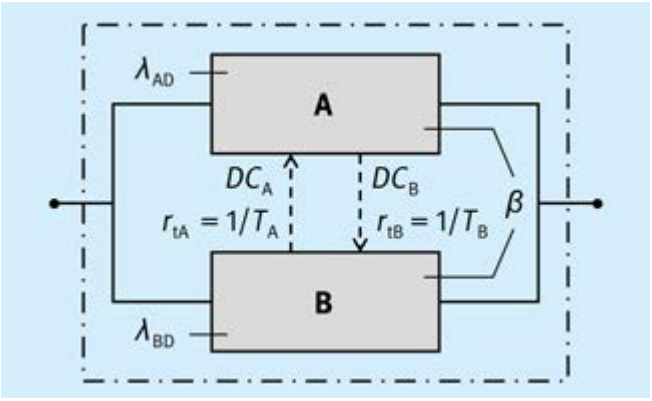


Abb. N.4 Vereinfachte vorgesehene Architektur für Kategorie 3 oder 4

Jedem der beiden Kanäle, Block A und Block B, entspricht in DIN EN ISO 13849-1 wieder eine Reihenschaltung aus den Blöcken I, L und O.

Die meisten der für die *PFH* relevanten Eingangsvariablen sind in Abbildung N.4 angegeben: λ_{AD} und λ_{BD} sind die Ausfallraten des Funktionskanals A bzw. B in die gefährliche Richtung – also jene Richtung, bei der der Kanal die Teilfunktion oder die Diagnose für den jeweiligen Parallelkanal bzw. seinen Beitrag hierzu nicht mehr ausführen kann. Die Variable DC_A bezeichnet den Diagnosedeckungsgrad, der für den Kanal allein durch Kanal B oder unter Mitwirkung von Kanal B realisiert ist. Das schließt sowohl Fälle ein, bei denen Kanal B den Kanal A „von außen" testet, als auch Fälle, bei denen Selbsttestroutinen innerhalb von Kanal A ablaufen, die bei Fehlererkennung mittels Kanal B einen sicheren Zustand herstellen. Durch umgekehrte Rollenverteilung der Kanäle A und B ist für Kanal B der Diagnosedeckungsgrad DC_B durch oder unter Mitwirkung von Kanal A realisiert. Mit T_A und T_B sind die Testintervalle bezeichnet, in denen die Kanäle A bzw. B getestet werden. Ihre Kehrwerte r_{tA} und r_{tB} bezeichnen die dazugehörigen Testraten.

Der Zweck der Redundanz aus parallelen Kanälen wird unterlaufen, wenn aufgrund *einer* Ursache sowohl der Kanal A als auch der Kanal B in die gefährliche Richtung ausfallen. Folglich müssen Maßnahmen gegen CCF ergriffen werden, deren Wirksamkeit mithilfe des Common-Cause-Faktors β abgeschätzt wird, siehe hierzu Anhang F. Für die Berücksichtigung der CCF bei der *PFH*-Ermittlung, wird vorab als Hilfsgröße die Common-Cause-Ausfallrate λ_{CC}, mit Gleichung (N.8) aus dem Kasten N.4 berechnet. Auch die Gleichungen (N.9) bis (N.17), die für diese Art von Teilsystem benötigt werden, sind in diesem Kasten enthalten. Die darin enthaltene Minimum-Funktion wählt als ihr Ergebnis stets das kleinere ihrer beiden Argumente aus. Die Argumente $\lambda_{AD\ SER\text{-}free}$ und $\lambda_{BD\ SER\text{-}free}$ sind die Ausfallraten der Blöcke A und B in die ungünstige Richtung, d. h. in Richtung Verlust der Sicherheitsfunktion oder Verlust der Diagnose für den jeweiligen Parallel-Block. Der Index-Zusatz „SER-free" bedeutet, dass bei diesen Ausfallraten der ggf. enthaltene Beitrag von Soft Error-Raten (SER) weggelassen werden soll. Zum Thema „Soft Errors" gibt es im letzten Aufzählungspunkt von Abschnitt N.2.2 eine kurze Erläuterung.

Das hinter Abbildung N.4 stehende Modell unterstellt, dass das Teilsystem nur dann gefahrbringend ausfällt, wenn beide Kanäle, A und B, gefahrbringend ausfallen. Mit dem gefahrbringenden Ausfall nur eines der Blöcke A oder B zeigt das Teilsystem weiterhin ein sicheres Verhalten („Einfehlersicherheit"). Das Modell setzt weiterhin voraus, dass das System nach einem einzelnen erkennbarer Blockausfall nicht weiterbetrieben, sondern zeitnah repariert wird. Der Reparaturbedarf wird hierzu typischerweise durch das Herbeiführen einer Betriebshemmung nach außen signalisiert.

Das Modell hinter Abbildung N.4 nimmt außerdem an, dass die Aufdeckung erkennbarer Ausfälle in einem der Kanäle und die im Aufdeckungsfall notwendige Herstellung eines sicheren Zustands nur stattfinden, wenn der Parallelkanal noch funktioniert. Dies schließt ein, dass für Common-Cause-Ausfälle keine Diagnose besteht.

Wegen dieser Annahmen eignet sich das Modell auch für Anwendungsfälle, in denen die Diagnose und Einleitung eines sicheren Zustands nach einem erkannten gefährlichen Fehler außerhalb des betrachteten Teilsystems stattfindet. Beispiele dafür sind Teilsysteme aus zwei Sensoren, die in einem nachgelagerten Teilsystem z. B. durch Vergleich der Sensorsignale getestet werden, oder Teilsysteme aus zwei Aktoren, die in einem vorgelagerten Teilsystem auf ihre korrekte Funktion überwacht werden, sodass bei einem einzelnen Aktor-Ausfall über den noch intakten Aktor ein sicherer Zustand hergestellt wird. Die vor- oder nachgelagerten Teilsysteme liefern dabei einen separat zu berücksichtigenden Beitrag zur Gesamt-*PFH* der Sicherheitsfunktion.

In den genannten Fällen können die Gleichungen (N.8) bis (N.17), die aus dem hinter Abbildung N.4 stehenden Modell abgeleitet wurden, zur *PFH*-Ermittlung benutzt werden.

Zur Erleichterung ihrer Handhabung verwendet die eigentliche *PFH*-Gleichung (N.17) eine Reihe von Hilfsgrößen, die aufeinander aufbauen. Die *PFH*-Ermittlung startet mit der Berechnung der Common-Cause-Ausfallrate λ_{CC} mittels der Gleichung (N.8).

Im nächsten Schritt werden mit den Gleichungen (N.9) und (N.10) die Hilfsgrößen L_A und L_B berechnet. In diese Gleichungen fließt auch die Gebrauchsdauer T_M ein, die später nochmals in Gleichung (N.17) verwendet wird. Bei den Gleichungen (N.9) und (N.10) dürfen die Testintervalle T_A und T_B – rechnerisch betrachtet – maximal den Wert der Gebrauchsdauer T_M annehmen, wobei die Gleichsetzung des Testintervalls mit der Gebrauchsdauer eine Testung erst am Ende der Systemnutzung bedeutet, also der Nichttestung des Systems gleichkommt. Üblicherweise werden nach Teil 1 der Norm nur Testintervalle von maximal einem Jahr als akzeptabel betrachtet. Die kontinuierliche Testung eines Kanals wird durch Nullsetzung seines Testintervalls berücksichtigt.

Sind statt der Testintervalle T_A und T_B die Testraten r_{tA} und r_{tB} gegeben, können zur Berechnung von L_A und L_B anstelle der Gleichungen (N.9) und (N.10) die Gleichungen (N.11) und (N.12) benutzt werden. Wird ein Kanal nicht getestet, so kann in den Gleichungen (N.9) bis (N.12) der dazugehörige Diagnosedeckungsgrad, DC_A bzw. DC_B zu Null gesetzt werden. Ein völliger Verzicht auf Diagnose in beiden Kanä-

Kasten N.4 *PFH* bei Teilsystemen der Kategorie 3 oder 4

$$\lambda_{CC} = \beta \cdot \min(\lambda_{AD\,SER\text{-}free}, \lambda_{BD\,SER\text{-}free}) \quad \text{(N.8)}$$

$$L_A = \left[1 - \left(1 - \frac{T_A}{T_M}\right) DC_A\right](\lambda_{AD} - \lambda_{CC}) \quad \text{(N.9)}$$

$$L_B = \left[1 - \left(1 - \frac{T_B}{T_M}\right) DC_B\right](\lambda_{BD} - \lambda_{CC}) \quad \text{(N.10)}$$

$$L_A = \left[1 - \left(1 - \frac{1}{r_{tA}\, T_M}\right) DC_A\right](\lambda_{AD} - \lambda_{CC}) \quad \text{(N.11)}$$

$$L_B = \left[1 - \left(1 - \frac{1}{r_{tB}\, T_M}\right) DC_B\right](\lambda_{BD} - \lambda_{CC}) \quad \text{(N.12)}$$

$$L_1 = \sqrt{(L_A + L_B)^2 + 2(L_A - L_B)(\lambda_{BD} - \lambda_{AD}) + (\lambda_{BD} - \lambda_{AD})^2} \quad \text{(N.13)}$$

$$L_2 = L_A + L_B + \lambda_{AD} + \lambda_{BD} \quad \text{(N.14)}$$

$$C_P = 2\frac{\lambda_{AD} L_B + \lambda_{BD} L_A + (\lambda_{AD} + \lambda_{BD})\lambda_{CC}}{L_1 (L_1 + L_2)} - 4\frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_1 (L_1 + L_2)^2} - \frac{\lambda_{CC}}{L_1} \quad \text{(N.15}$$

$$C_N = 2\frac{\lambda_{AD} L_B + \lambda_{BD} L_A + (\lambda_{AD} + \lambda_{BD})\lambda_{CC}}{L_1 (L_1 - L_2)} + 4\frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_1 (L_1 - L_2)^2} + \frac{\lambda_{CC}}{L_1} \quad \text{(N.16)}$$

$$PFH = \frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_A \lambda_{AD} + L_B \lambda_{BD} + \lambda_{AD}\lambda_{BD}} - \frac{C_P}{T_M}\left[1 - e^{-\frac{1}{2}(L_1 + L_2)T_M}\right] - \frac{C_N}{T_M}\left[1 - e^{-\frac{1}{2}(L_2 - L_1)T_M}\right] \quad \text{(N.17)}$$

len schließt allerdings das Erreichen der Kategorie 3 und der Kategorie 4 nach DIN EN ISO 13849-1 aus. In Kategorie 3 darf nur im Ausnahmefall, d. h. nur bei fehlender technischer Diagnosemöglichkeit, ein Kanal ungetestet bleiben. Dies ist zudem nur zulässig, wenn trotzdem der Wert von DC_{avg}, berechnet über beide Kanäle, mindestens 60 % beträgt, siehe hierzu die Abschnitte 8.2.6 und 8.2.14 sowie Gleichung (8.4) im Hauptteil bzw. Gleichung (E.1) in Anhang E dieses Reports.

Der nächste Schritt besteht in der Berechnung der Hilfsgrößen L_1 und L_2 unter Verwendung von L_A und L_B mit den Gleichungen (N.13) und (N.14). Mit L_1 und L_2 können als weitere Hilfsgrößen C_P und C_N mit den Gleichungen (N.15) und (N.16) berechnet werden.

Durch die Gleichungen (N.8) bis (N.16) können alle benötigten Hilfsgrößen ermittelt werden, die für die Gleichung (N.17) zur abschließenden Berechnung der *PFH* des Teilsystems nach Abbildung N.4 benötigt werden.

Auch für diese Architektur gilt, dass es zur quantitativen Bewertung nicht genügt, mit Gleichung (N.17) den *PFH*-Beitrag des Teilsystems zu ermitteln, wenn das Teilsystem der Kategorie 3 oder 4 nach DIN EN ISO 13849-1 entsprechen soll. Vielmehr müssen zusätzlich kategoriespezifische quantitative Anforderungen erfüllt werden, welche die $MTTF_D$ der Funktionskanäle und ihre Diagnosedeckungsgrade betreffen. Diese Anforderungen können Abschnitt 8.2.6 (Kategorie 3) bzw. Abschnitt 8.2.7 (Kategorie 4) dieses Reports entnommen werden.

Wird ein Teilsystem der Kategorie 3 realisiert, so müssen zur Prüfung des erreichbaren PL die $MTTF_D$-Werte beider Funktionskanäle A und B vor Anwendung der Gleichungen (N.8) bis (N.17) auf 100 Jahre gekappt werden, falls ihr jeweiliger Originalwert über 100 Jahre liegt. Dies bedeutet nach Gleichung (N.3) aus Kasten N.1, dass für λ_{AD} und für λ_{BD} keine kleineren Werte als $1{,}14 \cdot 10^{-6}\ h^{-1}$ für die *PFH*-Berechnung verwendet werden dürfen, wenn mit diesem *PFH*-Wert und Tabelle 7.1 (in Abschnitt 7.1) geprüft werden soll, welcher maximale PL aus quantitativer Sicht mit dem Teilsystem erreichbar ist.

Handelt es sich um ein Teilsystem der Kategorie 4, müssen für diese Prüfung die $MTTF_D$-Werte beider Funktionskanäle A und B vor Anwendung der Gleichungen (N.8) bis (N.17) auf 2500 Jahre gekappt werden, falls ihr jeweiliger Originalwert über 2500 Jahre liegt. Entsprechend Gleichung (N.3) bedeutet dies, dass für λ_{FD} und für λ_{MD} keine kleineren Werte als $4{,}57 \cdot 10^{-8}\ h^{-1}$ für die *PFH*-Berechnung verwendet werden dürfen, wenn mit diesem *PFH*-Wert und Tabelle 7.1 (in Abschnitt 7.1) der aus quantitativer Sicht mit dem Teilsystem maximal erreichbare PL ermittelt werden soll.

In Abschnitt N.2.3 wurde darauf hingewiesen, dass mit der Architektur für Kategorie 2 nach Abbildung N.3 unter besonderen Voraussetzungen ein Teilsystem der Kategorie 3 realisiert werden kann. Konkret muss der Testkanal gefahrbringende Ausfälle des Funktionskanals praktisch lückenlos aufdecken und nach einem erkannten Fehler innerhalb der spezifizierten Reaktionszeit der Teilfunktion einen sicheren Zustand herstellen. Den Diagnosedeckungsgrad des Funktionskanals F, schätzt man bei diesem Spezialfall üblicherweise konservativ mit 99 % ab. Während man den Diagnosedeckungsgrad des Funktionskanals F als *DC* in Gleichung (N.7) in Kasten N.3 einsetzen kann, bietet diese Gleichung keine Möglichkeit, einen für den Testkanal M realisierten, zweiten Diagnosedeckungsgrad *PFH*-mindernd zu berücksichtigen. Hier kommt alternativ die im Folgenden beschriebene Modellierung als zweikanaliges Teilsystem in Betracht.

Weil der Testkanal alle Ausfälle des Funktionskanals rechtzeitig erkennt, verhält er sich hinsichtlich der Fähigkeit, einen sicheren Zustand herbeizuführen, vergleichbar zu einem zweiten Funktionskanal. Somit ist es in diesem Sonderfall zulässig, den Funktionskanal F und den Testkanal M als zwei parallele Kanäle A und B entsprechend der Architektur nach Abbildung N.4 zu interpretieren. Die gefährliche Ausfallrate und der Diagnosedeckungsgrad von 99 % für den Funktionskanal werden beispielsweise dem Kanal A aus Abbildung N.4 zugewiesen, während die gefährliche Ausfallrate und der Diagnosedeckungsgrad für den Testkanal dem Kanal B zugeordnet werden. Auf diese Weise kann, anders als bei Gleichung (N.7), auch die für den Testkanal realisierte Diagnose berücksichtigt werden, nämlich als „DC_B“. Auch Anhang E dieses Reports beschreibt diesen Spezialfall in seinem Abschnitt über die Testung der Überwachungseinrichtung.

Die Architektur nach Abbildung N.4 weist trotz ihrer einfachen Darstellung mit nur zwei Funktionsblöcken A und B funktional die Merkmale der Basis-Teilsystemarchitektur D aus DIN EN IEC 62061 auf. Darum eignen sich die Gleichungen (N.8) bis (N.17) bei Vorliegen dieser Architektur auch zur *PFH*-Berechnung im Rahmen der Anwendung dieser IEC-Norm. Durch Setzen von $DC_A = DC_B = 0$ in den Gleichungen (N.9) und (N.10) bzw. (N.11) und (N.12) kann mit den Gleichungen (N.8) bis (N.17) ebenfalls die *PFH* für die Basis-Teilsystemarchitektur B aus DIN EN IEC 62061 berechnet werden. Um den aus quantitativer Sicht maximal erreichbaren SIL zu ermitteln, müssen neben der *PFH* zusätzlich die Architektur-Einschränkungen für die Hardware-Fehlertoleranz 1 nach der Tabelle 6 in DIN EN IEC 62061:2023-02 beachtet werden.

N.2.5.5 Reihenschaltung von Teilsystemen

In vielen Fällen wird eine Sicherheitsfunktion mittels einer logischen Reihenschaltung aus Teilsystemen realisiert, die jeweils eine Teilfunktion ausführen. Logische Reihenschaltung bedeutet, dass die Sicherheitsfunktion ausfällt, wenn mindestens eines der Teilsysteme gefahrbringend ausfällt. Abbildung N.5 zeigt eine solche Reihenschaltung aus *n* Teilsystemen.

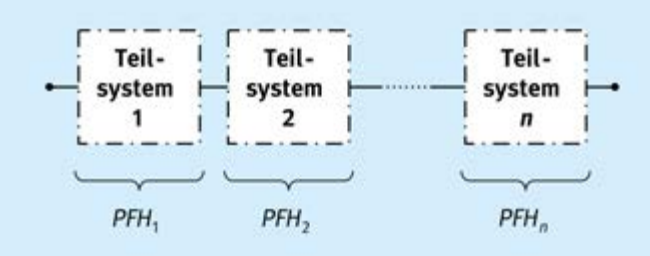


Abb. N.5 Logische Reihenschaltung von Teilsystemen

Die *PFH* der Reihenschaltung ergibt sich nach Gleichung (N.18) durch Addition der *PFH*-Beiträge ihrer Teilsysteme.

Kasten N.5
***PFH* bei Reihenschaltung von Teilsystemen**

$$PFH = PFH_1 + PFH_2 + \ldots + PFH_n \qquad \text{(N.18)}$$

Führt die logische Reihenschaltung aus den Teilsystemen die komplette Sicherheitsfunktion aus (Informationsgewinnung, Informationsverarbeitung, sicherheitsgerichtete Reaktion im Bedarfsfall), liefert Gleichung (N.18) die *PFH* für die Sicherheitsfunktion. Für die Anwendung der Gleichung (N.18) ist es unerheblich, ob die *PFH*-Beiträge der

einzelnen Teilsysteme mit Gleichungen aus den Abschnitten N.2.5.2, N.2.5.3 oder N.2.5.4 oder mithilfe eines anderen seriösen Modellierungsverfahrens ermittelt wurden. Ebenso gut können auch sogenannte „gekapselte Teilsysteme“ eingereiht werden, deren Dokumentation den *PFH*-Wert ausweist.

N.2.6 Ergebnisvergleich zwischen ISO/TR 13849-3 und dem vereinfachten Normverfahren

Ebenso wie das vereinfachte Verfahren aus Teil 1 der Norm mit Verwendung ihrer Tabelle K.1 basieren die *PFH*-Gleichungen aus ISO/TR 13849-3 auf Markov-Modellen. Im Vergleich zu jenen Modellen, mit denen die Norm-Tabelle K.1 berechnet wurde, sind für den ISO/TR Modelle mit weniger Blöcken verwendet worden. Dies war erforderlich, um daraus praktikable *PFH*-Gleichungen gewinnen zu können. Die Vereinfachung besteht im Wesentlichen darin, dass bei den vorgesehenen Architekturen der DIN EN ISO 138491 logisch in Reihe geschaltete Funktionsblöcke zu einem einzigen Block zusammengefasst wurden. Dieses höhere Abstraktionsniveau schränkt die Vielfalt der Anwendungen, die damit abgebildet werden können, aber nicht ein. Auch nach dem vereinfachten Verfahren der Norm ist die Aufteilung eines Funktionskanals in die Blöcke I, L und O nicht zwingend, sondern eher als Beispiel zu sehen.

Durch die unterschiedlich komplexen Modelle liefern das vereinfachte Verfahren aus DIN EN ISO 13849-1, Abschnitt 6.1.8, und die *PFH*-Berechnung mit den Formeln aus ISO/TR 13849-3 nicht exakt dieselben Ergebnisse. Die Abweichungen fallen jedoch kaum ins Gewicht und sind akzeptabel angesichts der oft nur geschätzten Eingangsparameter wie beispielsweise des *DC* und des Common-Cause-Faktors β. Bei stark asymmetrischen zweikanaligen Systemen ergeben sich Abweichungen durch das Symmetrisierungsverfahren der DIN EN ISO 13849-1 unter Verwendung der Norm-Gleichungen D.2 und E.1. Dieses Verfahren wird mit wachsender Asymmetrie zunehmend ungenau.

N.2.7 Anhänge des ISO/TR 13849-3

Der ISO/TR 13849-3 enthält neben seinem Hauptteil mit den *PFH*-Formeln zwei Anhänge.

In Anhang A wird anhand der Schaltungsbeispiele A und B aus DIN EN ISO 13849-1, Anhang I demonstriert, wie sich die *PFH* mithilfe des ISO/TR 13849-3 berechnen lässt. Dabei werden auch die Ursachen für die moderate Abweichung des *PFH*-Ergebnisses bei Beispiel B vom Ergebnis aus der Norm erörtert. Eine wesentliche Ursache dafür ist die beim vereinfachten Verfahren der Norm notwendige Symmetrisierung. Sie führt in Verbindung mit der starken Asymmetrie dieses Kategorie-3-Beispiels zu einer gewissen Ungenauigkeit beim vereinfachten Verfahren.

Der Anhang B enthält die Herleitung der im Hauptteil des ISO/TR 13849-3 vorgestellten *PFH*-Gleichungen. Er folgt damit dem Open-Source-Gedanken und will Vertrauen in die *PFH*-Gleichungen und die ihnen zugrunde liegende Modellierungstechnik schaffen. Zugleich kann der Anhang Interessierten als Einführung in die Vorgehensweise zur Gewinnung von *PFH*-Gleichungen aus Zustands-Übergangs-Diagrammen dienen. Er stellt damit die Grundlagen für eigene Erweiterungen oder Varianten zur Verfügung. Anhand der zweikanaligen Architektur wird gezeigt, wie bereits ohne die Markov-Methode Näherungsgleichungen für die *PFH* gewonnen werden können. Diese Gleichungen sind vergleichsweise kompakt, liefern jedoch durch Abschätzungen zur sicheren Seite in der Regel erhöhte *PFH*-Werte. Der Anhang B demonstriert darüber hinaus, wie unter Einbeziehung der Markov-Modellierung Gleichungen hergeleitet werden können, die genauere und zugleich bessere (kleinere) *PFH*-Werte liefern. Es wird ebenfalls gezeigt, wie die *PFH*-Gleichungen für einfache Spezialfälle aus den allgemeinen Gleichungen gewonnen werden können. Außerdem erläutert der Anhang, warum die Gleichungen (N.6) und (N.8) für die Common-Cause-Ausfallrate eine Minimum-Funktion enthalten.

Literatur

[N1] ISO/DTR 13849-3: PFH calculation of safety functions for machines using Markov model-based formulas (2024). ISO, Genf 2024

[N2] *Goble, W. M.*: Control Systems Safety Evaluation & Reliability. 3rd ed. Hrsg.: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010. https://www.isa.org

[N3] *Signoret, J.-P., Leroy, A.*: Reliability Assessment of Safety and Production Systems. Springer Nature Switzerland, Cham 2021

[N4] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (2/2011). DIN Media, Berlin 2011

[N5] DIN EN IEC 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (2/2023). DIN Media, Berlin 2023

Anhang O

Hinweise zu Security

Für Hersteller und Betreiber ist es wichtig zu wissen, dass Anforderungen an die Security derzeit noch nicht im Anwendungsbereich der DIN EN ISO 13849 sind.

Zum Zeitpunkt der Drucklegung dieses Reports sind neue europäische Verordnungen dazu teils verabschiedet und teilweise noch in Arbeit. Voraussichtlich werden die neuen Anforderungen aus den europäischen Verordnungen in die harmonisierten Normen über einen Verweis eingepflegt. Ein wesentlicher Schwerpunkt darin ist die Verbesserung der Zusammenarbeit zwischen folgenden Rollen:

- Personen und Institutionen, die Sicherheitslücken entdecken und melden,
- Behörden,
- Betreiber,
- Hersteller.

Die Europäische Gesetzgebung benennt dazu die jeweiligen Verantwortlichen und ihre Pflichten. Für die meisten Hersteller, die ein Produkt nach DIN EN ISO 13849 für den europäischen Markt herstellen, ist es wichtig, die rechtlichen Anforderungen aus O.1 zu kennen.

O.1 Rechtliche Anforderungen

Ab dem 20. Januar 2027 ist die neue Maschinenverordnung (MV) anzuwenden [O1]. Während die Maschinenrichtline [O2] zum Schutz vor Korrumpierung oft noch Diskussionsspielraum gelassen hat, stellt die Maschinenverordnung sehr deutliche Anforderungen an den Schutz vor Korrumpierung. Eine wesentliche Anforderung wird dazu in Artikel 20 (9) beschrieben:

„*Bei Maschinen und dazugehörigen Produkten, die im Rahmen eines gemäß der Verordnung (EU) 2019/881 angenommenen Schemas für die Cybersicherheitszertifizierung, dessen Fundstellen im Amtsblatt der Europäischen Union veröffentlicht worden sind, zertifiziert wurden oder für die eine Konformitätserklärung erteilt wurde, wird davon ausgegangen, dass sie den in Anhang III Abschnitte 1.1.9 und 1.2.1 aufgeführten grundlegenden Sicherheits- und Gesundheitsschutzanforderungen in Bezug auf den Schutz vor Korrumpierung und die Sicherheit und Zuverlässigkeit von Steuerungssystemen entsprechen, soweit diese Anforderungen durch das Cybersicherheitszertifikat oder die Konformitätsbescheinigung oder -erklärung oder Teile davon abgedeckt sind*.“

Die Abschnitte 1.1.9 „Schutz gegen Korrumpierung“ und 1.2.1 „Sicherheit und Zuverlässigkeit von Steuerungen“ stellen die Zielvorgaben wie etwa den Schutz vor vorsätzlicher Korrumpierung auf. Bestimmte Eingriffe müssen in einem Rückverfolgungsprotokoll als Beweise archiviert werden. Ein Normungsentwurf dazu wird in PrEN50742 erarbeitet [O2].

Zur Drucklegung ist das Verfahren einer „Cybersicherheits-Zertifizierung“ noch im Aufbau. Der Cyber Securiy Act beauftragt die European Network and Information Security Agency (ENISA) damit, den Aufbau einer entsprechenden Zertifizierung zu fördern [O3].

Während sich die Maschinenverordnung bei der Korrumpierung im Wesentlichen auf die Anwendungen bezieht, die zu einer gefährlichen Situation führen können, umfasst der Cyberresilience Act (CRA) auch rein wirtschaftliche Schäden [O4].

Der CRA enthält einige Anforderungen, die Hersteller von Produkten mit digitalen Elementen in Ihre Prozesse nach DIN EN ISO 13849 einbinden können. So wird etwa die Erstellung einer Software-Stückliste (Software Bill of Materials, SBOM) gefordert. Darin steht in einem standardisierten Format, welche Software einschließlich aller Softwarebibliotheken in welcher Version eingebunden wurden. Der CRA beschreibt in Artikel 13 besondere Pflichten der Hersteller und fordert auch, dass Hersteller einen Notfallkontakt hinterlegen:

„*Für die Zwecke dieser Verordnung benennen die Hersteller eine zentrale Anlaufstelle, die es den Nutzern ermöglicht, direkt und schnell mit ihnen zu kommunizieren, auch um die Meldung von Schwachstellen des Produkts mit digitalen Elementen zu erleichtern*.“

Eine Erstellung des Notfallkontaktes ist in O.3 beschrieben und kann in wenigen Minuten bereits heute umgesetzt werden.

Die Richtlinie NIS 2 wird die NIS-Richtlinie ablösen und stellt die Anforderungen an die Betreiber und zeigt auch auf, wie Betreiber mit Herstellern und Behörden zusammenarbeiten müssen [O5, O6].

Die jeweils aktuellen Links zu den Originaltexten der europäischen Verordnungen, Zusatzinformationen werden auf der Onlineplattform für Industrial Security https://cert.dguv.de gepflegt.

O.2 Normenwerke zu Security

PrEN50742

Zum Zeitpunkt der Drucklegung wird in PrEN50742 ein Normungsentwurf erarbeitet, der die Security Anforderungen aus 1.1.9 und 1.2.1 a und f der Maschinenverordnung abbildet und zur Harmonisierung geeignet sein soll. Davon unabhängig sollen weitere Normen für die Anforderungen aus dem CRA erstellt werden.

IEC 62443

Die 19-bändige Normenserie der IEC 62443 [O7] hat ihren Ursprung in der Automatisierungstechnik der Prozessindustrie. Die IEC 62443 kann aber nicht nur Kritische Infrastrukturen (KRITIS), sondern alle Steuerungen in der Industrie abbilden. In der Normenreihe DIN EN IEC 62443 werden insgesamt fünf Security Level genannt (SL 0 bis SL 4). Eine allgemeingültige Abbildung, bei welchem PL oder SIL ein bestimmter Security Level notwendig ist, ist nicht möglich. Welcher Security Level für eine Komponente oder ein System angesetzt werden sollte, muss durch eine individuelle Risikoanalyse ermittelt werden.

Die Security Level werden wie folgt beschrieben:

Security Level	Beschreibung
SL 0	Keine besonderen Anforderungen oder Schutzmaßnahmen notwendig
SL 1	Schutz gegen gelegentlichen oder zufälligen Verstoß
SL 2	Schutz gegen einen absichtlichen Verstoß mit einfachen Mitteln und geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation
SL 3	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und mittlerem Aufwand, automatisierungstechnischen Fertigkeiten und mittlerer Motivation
SL 4	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und erheblichem Aufwand, automatisierungstechnischen Fertigkeiten und hoher Motivation

IEC TS 63074

Die technische Spezifikation IEC TS 63074 „Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen“ [O8] fasst Anforderungen and die Security für Komponenten der funktionalen Sicherheit nach der IEC 62443 Serie zusammen.

ISO/IEC 15408 Common Criteria

Die Normenserie ISO/IEC 15408 „Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit“ [O9] ist besser bekannt unter dem Namen Common Criteria. Sie definiert sieben Qualitätsstufen von rein „funktional getestet“ bis „formal verifizierter Entwurf und getestet“.

Evaluation assurance levels (EAL)	Bedeutung
EAL1	funktionell getestet
EAL2	strukturell getestet
EAL3	methodisch getestet und überprüft
EAL4	methodisch entwickelt, getestet und durchgesehen
EAL5	semiformal entworfen und getestet
EAL6	semiformal verifizierter Entwurf und getestet
EAL7	formal verifizierter Entwurf und getestet

O.3 Erste Umsetzungsmöglichkeiten

Eine Möglichkeit der Spezifikation für einen Notfallkontakt wird in RFC 9116 beschrieben. Die Spezifikation ist weltweit anwendbar und kostenlos verfügbar. Zur Umsetzung werden in einer einfachen Textdatei mit dem festgelegten Namen „security.txt“ und in einem vorgegebenen Format Kontaktinformationen und Angaben zur Verschlüsselung etc. hinterlegt. Diese Datei wird dann auf dem Webserver im Verzeichnis .well-known/ unterhalb des Wurzelverzeichnisses abgelegt. Sie ist dann über HTTPS unter https://www.example.com/.well-known/security.txt verfügbar.

Diesen Ablageort kennen alle Sicherheitsforscher und Behörden weltweit. Viele Unternehmen wenden diese Spezifikation bereits an. Die DGUV legt nach RFC9116 dazu etwa ihren Notfallkontakt unter https://www.dguv.de/.well-known/security.txt ab.

```
Contact: mailto:isb@dguv.de
Expires: 2024-08-15T10:00:00.000Z
Preferred-Languages: de, en
```

Minimalistisches Beispiel einer security.txt

Hersteller können die security.txt um weitere Felder ergänzen. Besonders großes Potential wird hier künftig das Feld CSAF haben, mit dem jeder Hersteller seine Handlungsempfehlungen zu Schwachstellen in spezifischen Produkten veröffentlichen kann. Ein Generator für die security.txt

und die Spezifikationen und ein FAQ sind auf der Onlineplattform für Industrial Security https://cert.dguv.de/ [O10] verfügbar.

Weiterführende Literatur

[O1] Internationale Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates, L 165/1. Amtsblatt der Europäischen Union vom 29.6.2023. http://data.europa.eu/eli/reg/2023/1230/oj

[O2] 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). http://data.europa.eu/eli/dir/2006/42/oj

[O3] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit). http://data.europa.eu/eli/reg/2019/881/oj

[O4] Cyber Resilience Act (CRA): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (finale Veröffentlichung im Oktober 2024 erwartet)

[O5] NIS-Richtlinie: Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

[O6] NIS-2-Richtlinie: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148

[O7] DIN EN IEC 62443: IT-Sicherheit für industrielle Automatisierungssysteme, diverse Teile. IEC-Verlag, Genf 2024.

[O8] IEC TS 63074: Maschinensicherheit – Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen (5/2021). DIN Media, Berlin 2021.

[O9] DIN EN ISO/IEC 15408: Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 1 bis 5 (12/2020). DIN Media, Berlin 2020.

[O10] Onlineplattform für Industrial Security: Gesetzliche Regelungen und Notfallkontakt security.txt, Videos und Downloads. https://cert.dguv.de/

Stichwortverzeichnis

Symbole

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Deutsche Gesetzliche
Unfallversicherung e.V. (DGUV)

Glinkastraße 40
10117 Berlin
Telefon: 030 13001-0 (Zentrale)
E-Mail: info@dguv.de
Internet: www.dguv.de