BGIA-Report 2/2008

Funktionale Sicherheit von Maschinensteuerungen

– Anwendung der DIN EN ISO 13849 –

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

Redaktion: Zentralbereich des BGIA, Referat Informationsmanagement

Broschürenversand: info@dguv.de

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

Satz und Layout: Deutsche Gesetzliche Unfallversicherung (DGUV)

Druck: Plump OHG, Rheinbreitbach

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

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

Die Norm DIN EN ISO 13849 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ macht Vorgaben für die Gestaltung von sicherheitsbezogenen Teilen von Steuerungen. Dieser Report stellt die wesentlichen Inhalte der Norm in ihrer stark überarbeiteten Fassung von 2007 vor und erläutert deren Anwendung an zahlreichen Beispielen aus den Bereichen Elektromechanik, Fluidtechnik, Elektronik und programmierbarer Elektronik, darunter auch Steuerungen gemischter Technologie. Der Zusammenhang der Norm mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie wird aufgezeigt und mögliche Verfahren zur Risikoabschätzung werden vorgestellt. Auf der Basis dieser Informationen erlaubt der Report die Auswahl des erforderlichen Performance Level PL_r für steuerungstechnische Sicherheitsfunktionen. Die Bestimmung des tatsächlich erreichten Performance Level PL wird detailliert erläutert. Auf die Anforderungen zum Erreichen des jeweiligen Performance Level und seine zugehörigen Kategorien, auf die Bauteilzuverlässigkeit, Diagnosedeckungsgrade, Softwaresicherheit und Maßnahmen gegen systematische Ausfälle sowie Fehler gemeinsamer Ursache wird im Detail eingegangen. Hintergrundinformationen zur Umsetzung der Anforderungen in die steuerungstechnische Praxis ergänzen das Angebot. Zahlreiche Schaltungsbeispiele zeigen bis auf die Ebene der Bauteile hinunter, wie die Performance Level a bis e mit den Kategorien B bis 4 in den jeweiligen Technologien technisch umgesetzt werden können. Sie geben dabei Hinweise auf die verwendeten Sicherheitsprinzipien und sicherheitstechnisch bewährte Bauteile. Zahlreiche Literaturhinweise dienen einem tieferen Verständnis der jeweiligen Beispiele. Der Report zeigt, dass die Anforderungen der DIN EN ISO 13849 in die technische Praxis umgesetzt werden können, und leistet damit einen Beitrag zur einheitlichen Anwendung und Interpretation der Norm auf nationaler und internationaler Ebene.

Abstract
Functional safety of machine controls
- Application of DIN EN ISO 13849 -

The DIN EN ISO 13849 standard, “Safety of machinery – Safety-related parts of control systems”, contains provisions governing the design of such parts. This report describes the essential subject-matter of the standard in its heavily revised 2007 edition, and explains its application with reference to numerous examples from the fields of electromechanics, fluidics, electronics and programmable electronics, including control systems employing mixed technologies. The standard is placed in its context of the essential safety requirements of the Machinery Directive, and possible methods for risk assessment are presented. Based upon this information, the report can be used to select the required Performance Level PL_r for safety functions in control systems. The Performance Level PL which is actually attained is explained in detail. The requirements for attainment of the relevant Performance Level and its associated categories, component reliability, diagnostic coverage, software safety and measures for the prevention of systematic and common-cause failures are all discussed comprehensively. Background information is also provided on implementation of the requirements in real-case control systems. Numerous example circuits show, down to component level, how Performance Levels a to e can be engineered in the selected technologies with categories B to 4. The examples also provide information on the safety principles employed and on components with well-tried safety functionality. Numerous literature references permit closer study of the examples provided. The report shows that the requirements of DIN EN ISO 13849 can be implemented in engineering practice, and thus makes a contribution to consistent application and interpretation of the standard at national and international level.

Résumé
Sécurité fonctionnelle des commandes de machines – Application de la norme DIN EN ISO 13849 –

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

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

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

Inhaltsverzeichnis

Seite

Seite

Seite

Anhang

Vorwort

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

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

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

Dr. Karlheinz Meffert
Direktor des BGIA

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

2 Einleitung

Seit dem 1. Januar 1995 müssen alle Maschinen, die innerhalb des europäischen Wirtschaftsraumes in Verkehr gebracht werden, den grundlegenden Anforderungen der Maschinenrichtlinie [1] genügen. Als Maschine gilt nach Artikel 1 dieser Richtlinie die Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist, sowie gegebenenfalls von Betätigungsgeräten, Steuer- und Energiekreisen, die für eine bestimmte Anwendung, z.B. Verarbeitung, Behandlung, Fortbewegung und Aufbereitung eines Werkstoffes, zusammengefügt sind. Mit der kodifizierten Fassung 98/37/EG [1] der Maschinenrichtlinie fallen neben Maschinen auch Sicherheitsbauteile, die vom Hersteller mit dem Verwendungszweck der Gewährleistung einer Sicherheitsfunktion in Verkehr gebracht werden und deren Ausfall oder Fehlfunktion die Sicherheit oder die Gesundheit von Personen im Wirkbereich der Maschine gefährden können, unter den Anwendungsbereich dieser Richtlinie.

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

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

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

Die Norm erhält als harmonisierte Norm nach Inkrafttreten der neuen Maschinenrichtlinie [8] am 29. Dezember 2009 ein stärkeres Gewicht. Wesentliche Neuerung ist beispielsweise die Aufnahme von sicherheitsrelevanten Logiken – auch sicherheitsbezogene Teile von Steuerungen genannt – in den Anhang IV der neuen Richtlinie. Solche Anhang-IV-Produkte erfahren nach der Richtlinie eine besondere Behandlung, sofern sie nicht nach harmonisierten und im Amtsblatt veröffentlichten Normen hergestellt werden. Anhang-IV-Produkte sind dann zwar nicht mehr EG-baumusterprüfpflichtig[1] – sie können u.a. auch durch

---

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

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

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

Der vorliegende BGIA-Report hat zum Ziel, die Anwendung der DIN EN ISO 13849 zu erläutern und insbesondere anhand zahlreicher Lösungen die praktische Realisierung beispielhaft aufzuzeigen. Weder die Erläuterungen noch die Beispiele sind als offizieller nationaler oder europäischer Kommentar zu DIN EN ISO 13849-1 aufzufassen. Vielmehr sind in diesem Report die Erfahrungen des BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung aus fast dreißigjähriger Praxis bei der Beurteilung von Schutz- und Steuereinrichtungen der unterschiedlichen Technologien und aus der langjährigen Mitwirkung in einschlägigen nationalen und internationalen Normungsgremien zusammengetragen.

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

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

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

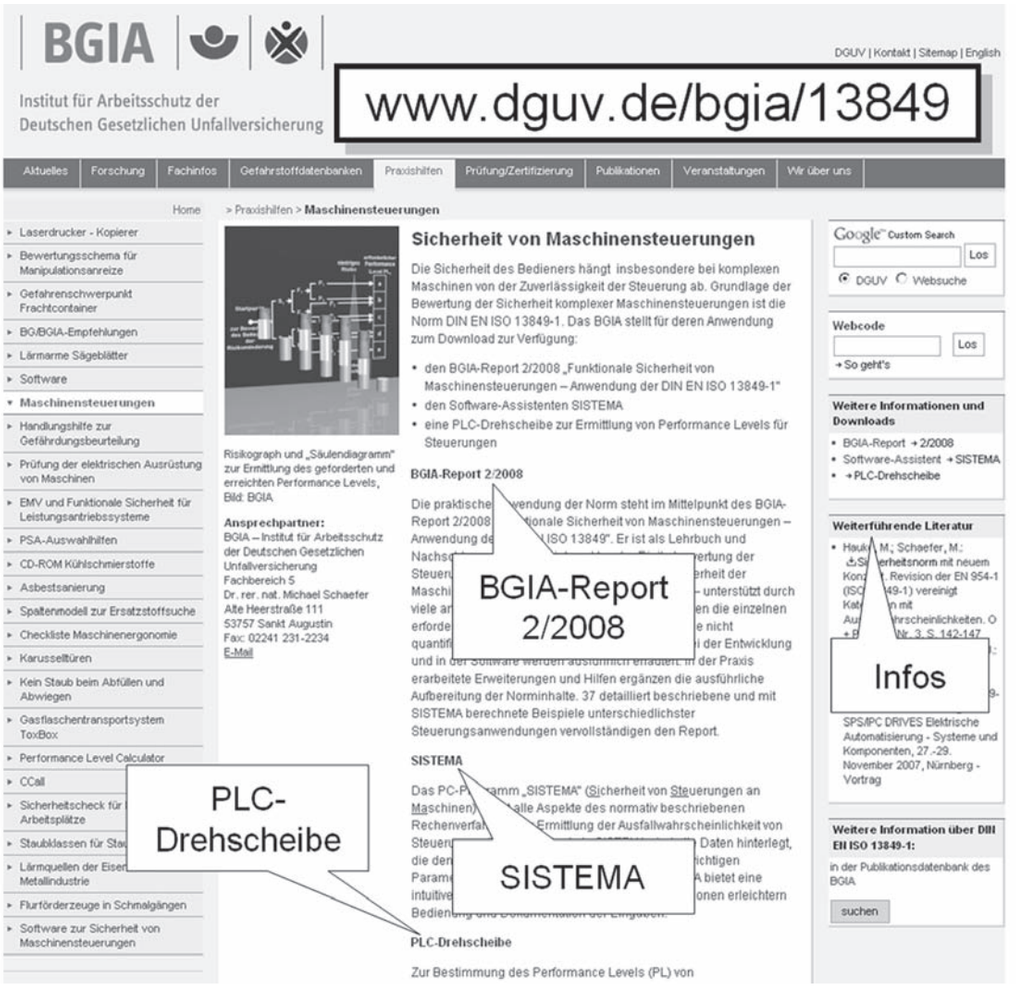


Abbildung 2.1: Die Internetseite „www.dguv.de/bgia/13849“ bietet Links zu allen Praxishilfen zur Sicherheit von Maschinensteuerungen

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

3 Basisnormen zur funktionalen Sicherheit von Maschinensteuerungen

Neben der in diesem Report behandelten Norm DIN EN ISO 13849 gibt es alternative, aber relevante Normen im Bereich der funktionalen Sicherheit[1]. Dies sind, wie in Abbildung 3.1 dargestellt, die Normen der Reihe DIN EN 61508 [12] und ihre Sektornorm DIN EN 62061 [13] für die Maschinenindustrie. Beide sind im Anwendungsbereich auf elektrische, elektronische und programmierbar elektronische Systeme beschränkt.

Als Klassifizierungsschema sind in DIN EN 61508 und DIN EN 62061 sogenannte Sicherheits-Integritätslevel (SIL) festgelegt. Diese sind ein Gradmesser für die sicherheitsgerichtete Zuverlässigkeit. Es handelt sich um Ausfallgrenzwerte, die jeweils eine Dekade umfassen[2]. In der Betriebsart mit niedriger Anforderungsrate ist die Maßzahl die mittlere Ausfallwahrscheinlichkeit der entworfenen Funktion bei Anforderung *PFD* (Average **P**robability of **F**ailure to Perform its Design Function on **D**emand), während die Definition für die Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung als Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde *PFH* (**P**robability of a Dangerous **F**ailure per **H**our) erfolgt (weitere Informationen siehe auch [14]). Im Maschinenbereich und damit in DIN EN 62061 ist nur die zweite Definition relevant. Auch sind SIL-4-Systeme mit höheren Risiken im Maschinenbereich nicht bekannt und werden daher in DIN EN 62061 nicht betrachtet (Abbildung 3.2, siehe Seite 16). Der grundlegende Ansatz dieser Normen, Ausfallwahrscheinlichkeiten und nicht speziell auch Strukturen als charakteristische Kenngröße zu definieren, erscheint zunächst universeller. Der Ansatz der DIN EN ISO 13849-1 bietet Anwendern jedoch die Möglichkeit, Sicherheitsfunktionen von einem Sensor bis hin zu einem Aktor (z.B. Ventil), auch wenn sie verschiedene Technologien umfassen, unter dem Dach einer Norm zu entwickeln und zu bewerten. Neben Teil 1 der DIN EN ISO 13849 existiert seit 2003 auch ein Teil 2 mit dem Titel „Validierung“, der mit dem Erscheinen des revidierten Teils 1 jedoch überarbeitet und angepasst werden muss. Trotzdem passen die dort genannten Anforderungen bereits erstaunlich gut zum überarbeiteten Teil 1. Die Anhänge A bis D des Teils 2 enthalten umfangreiches Material zu den Themen „grundlegende Sicherheitsprinzipien“, „bewährte Sicherheitsprinzipien“, „bewährte Bauteile“ und „Fehlerlisten“, das auch unter dem neuen Teil 1 gültig ist; Details hierzu sind im Anhang C dieses Reports dargestellt.

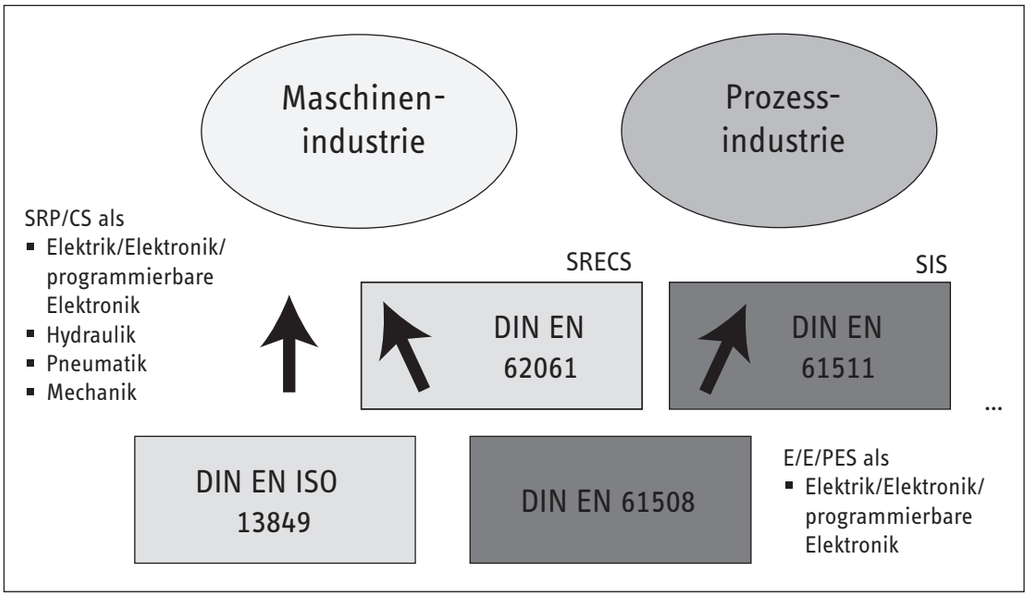


Abbildung 3.1: Anwendungsbereiche verschiedener Basisnormen zur funktionalen Sicherheit; SRP/CS: sicherheitsbezogene Teile einer Steuerung; SRECS: sicherheitsbezogenes elektrisches Steuerungssystem; SIS: sicherheitstechnisches System; E/E/PES: elektrisch/elektronisch/programmierbar elektronisches System

---

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

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

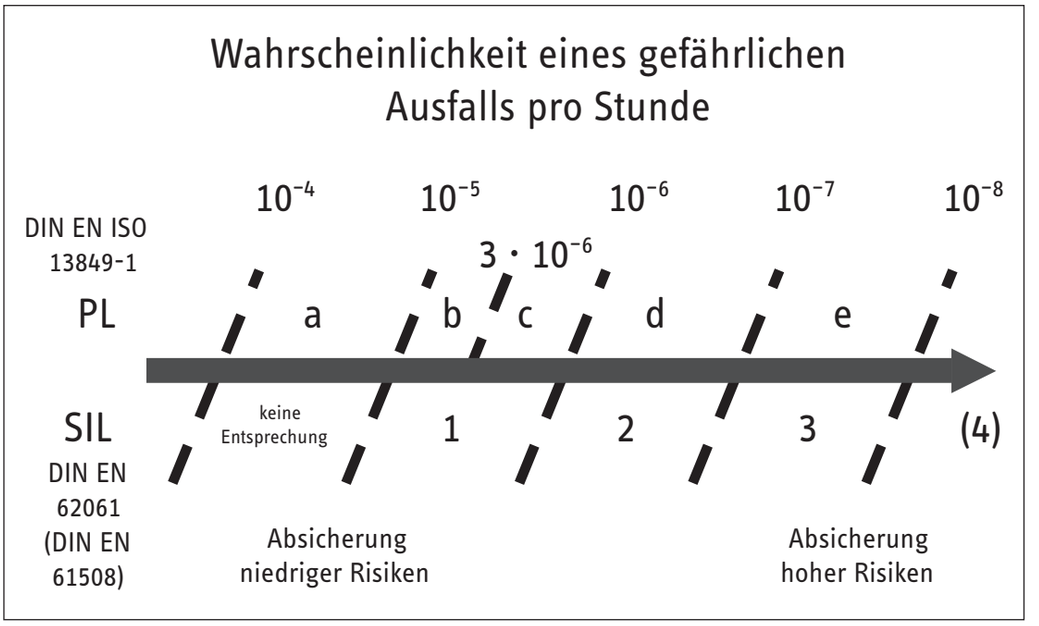


Abbildung 3.2: Performance Level (PL) und Sicherheits-Integritätslevel (SIL) als Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde

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

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

Um eine maximale Kompatibilität zur IEC-Welt zu erreichen sowie möglicherweise auf langfristige Sicht eine Zusammenlegung beider Normenwelten zu ermöglichen und außerdem die Vorteile des Wahrscheinlichkeitsansatzes zu nutzen, ohne die bewährten Kategorien über Bord zu werfen, hat die Revision der DIN EN ISO 13849-1 den Balanceakt gewagt, sowohl den deterministischen Ansatz der Kategorien als auch den Aspekt der sicherheitstechnischen Zuverlässigkeit mit der Definition des Performance Level (PL) zu vereinen (siehe auch [15]). Zahlenmäßig gibt es dabei korrespondierende Klassen (siehe Abbildung 3.2), die im praktischen Alltag schnell erste Abschätzungen erlauben. Schon im Entwurfsstadium der beiden Normen DIN EN ISO 13849-1 und DIN EN 62061 wurde von Mitgliedern der Normenkomitees eine Information zur empfohlenen Anwendung erarbeitet und nahezu wortgleich in den Einleitungen der Normen veröffentlicht. Zentrales Element ist dabei eine Tabelle, die dem Leser eine Hilfestellung zur Auswahl der passenden Norm für seinen Anwendungsfall geben soll. Diese Übersicht muss jedoch als veraltet gelten, da sie in Bezug auf DIN EN ISO 13849-1 den Stand des Entwurfs wiedergibt. Die genannten Einschränkungen sind für die aktuelle Fassung der Norm nicht mehr gültig. Faktisch gibt es keine Beschränkungen mehr, lediglich muss sicherheitsbezogene Embedded-Software (SRESW) bei Nichtvorliegen vollständiger Diversität dem Abschnitt 7 der DIN EN 61508-3:2002 entsprechen (siehe auch Abschnitt 6.3 dieses Reports). Auch sind die vorgesehenen Architekturen im Sinne der Norm eher ein Angebot (vereinfachter Ansatz) als eine Verpflichtung. Sie sind jedoch als zentrales Element der Vereinfachung des nun in DIN EN ISO 13849 implementierten probabilistischen Ansatzes zu verstehen und ihre Anwendung ist einer der Hauptaspekte dieses Reports. In Bezug auf DIN EN 62061 legt die Tabelle nahe, dass auch komplexe, z.B. programmierbare Elektronik in den Anwendungsbereich der Norm fällt. Dies ist zwar korrekt, jedoch muss die Entwicklung von sogenannten SRECS (siehe Abbildung 3.1) dieser Technologie gemäß den Anforderungen der Norm nach DIN EN 61508 erfolgen. Abbildung 3.3 zeigt eine „angepasste Empfehlung“, die sich an den aktuellen Ständen der Norm und deren Anwendungsbereichen orientiert.

[1] *IEC = International Electrotechnical Commission*

Auch wenn von vielen Experten die annähernde Gleichwertigkeit der Ergebnisse bei Anwendung der einen oder anderen Norm diskutiert wird, sind die Anforderungen im Detail durchaus unterschiedlich; so beschreibt DIN EN 62061 als Sektornorm der DIN EN 61508 natürlich den Aspekt des „Managements der funktionalen Sicherheit“ sehr explizit. Entwicklung und Verifikation von Embedded-Software nach DIN EN ISO 13849-1 basieren auf heute gängigen und auch in DIN EN 61508 beschriebenen wesentlichen Anforderungen für sicherheitsrelevante Software. Die Darstellung orientiert sich (wohl bewusst) mit Verzicht auf Komplexität am „Normalfall“. Weitgehende Einigkeit besteht aber darin, dass keine Mischung der Anforderungen aus beiden Normen vorgenommen werden soll.

Entscheidende Argumente für die Wahl von DIN EN ISO 13849 als Basis zur Realisierung funktionaler Sicherheit im Maschinenbereich können also aus Sicht des Anwenders der technologieübergreifende Ansatz und der vereinfachte Quantifizierungsansatz unter Verwendung der vorgesehenen Architekturen sein. Dies schließt die detaillierte Betrachtung von nichtelektrischen und elektromechanischen Bauteilen ein. Natürlich werden insbesondere Hersteller von in großer Anzahl hergestellten Sicherheitskomponenten, z.B. einer speicherprogrammierbaren Steuerung (SPS) für Sicherheitsanwendungen, weltweit auch andere Märkte als den Maschinenbereich bedienen wollen und daher neben DIN EN ISO 13849 auch DIN EN 61508 als Basis einer Entwicklung heranziehen.

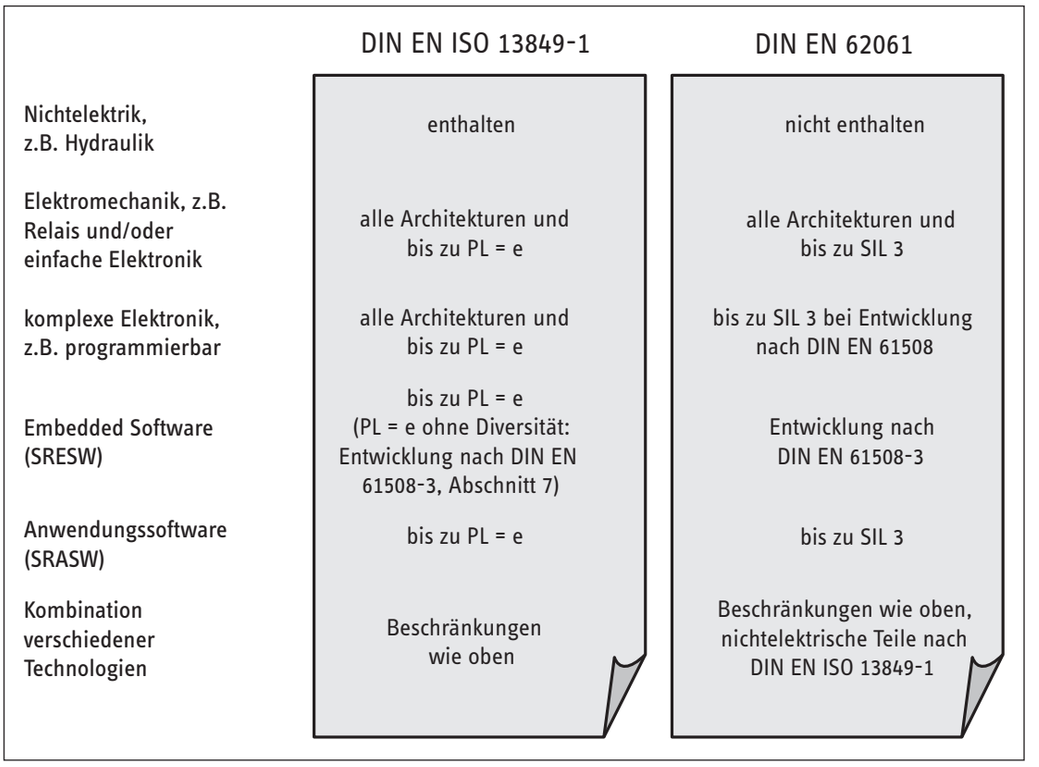


Abbildung 3.3: „Angepasste Empfehlung“ zur Anwendung von DIN EN ISO 13849-1 und DIN EN 62061

4 Report und Norm im Überblick

Dieses Kapitel stellt für den Leser die Querbezüge zwischen der Norm und den weiteren Kapiteln und Anhängen dieses Reports her. Gleichzeitig gibt es einen Überblick über den iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen und orientiert sich dabei an Abbildung 4.1, die Bild 3 der Norm entspricht.

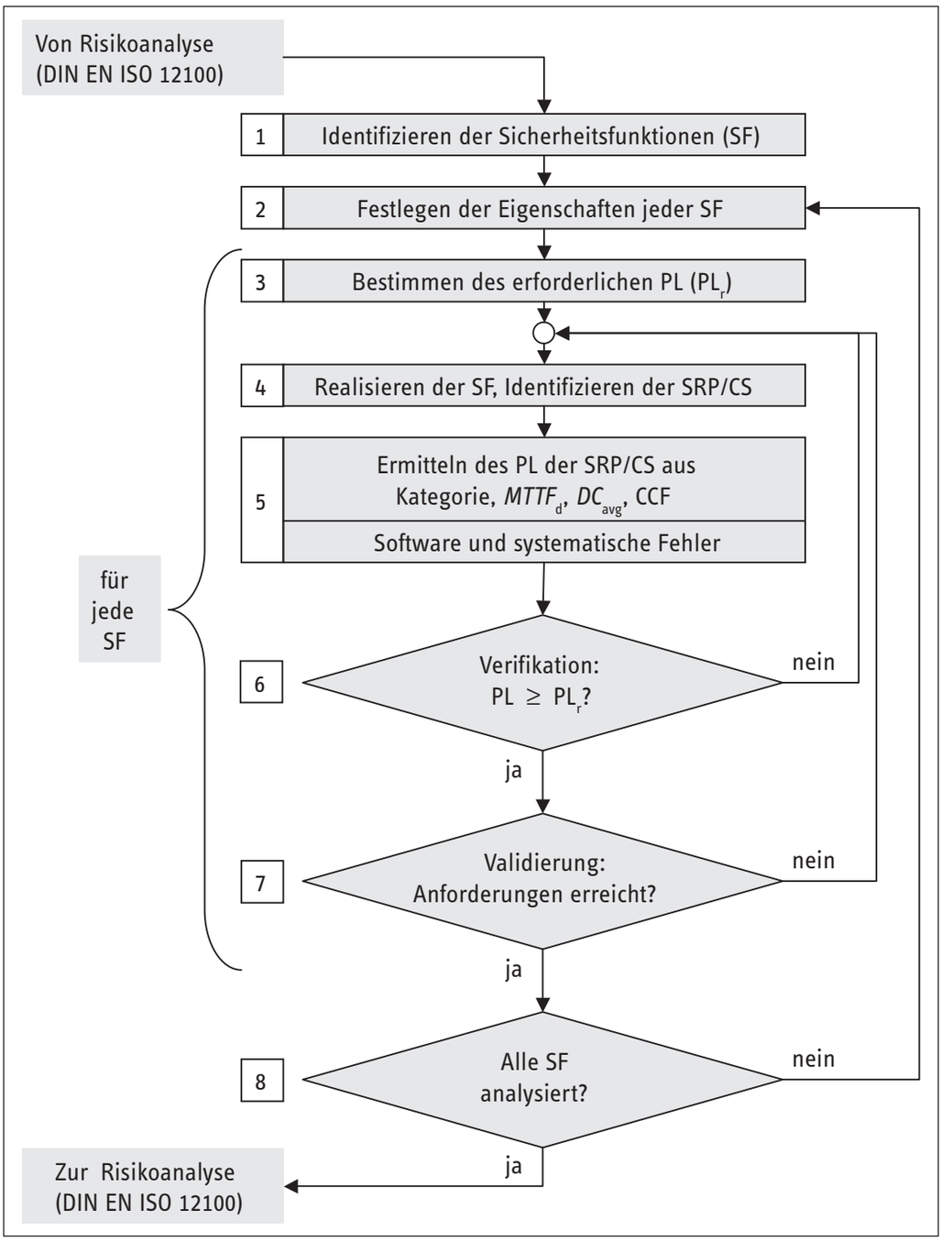


Abbildung 4.1: Iterativer Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen: SF = Sicherheitsfunktion; PL = Performance Level; PL_r = erforderlicher Performance Level; SRP/CS = Safety-Related Parts of Control Systems (sicherheitsbezogene Teile der Steuerung); $MTTF_d$ = Mean Time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

4.1 Identifikation von Sicherheitsfunktionen und ihren Eigenschaften

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

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

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

Das Risiko einer Gefährdung an einer Maschine kann außer durch die Steuerung z.B. auch durch trennende Schutzeinrichtungen, z.B. eine Schutztür, oder Persönliche Schutzausrüstung, z.B. eine Schutzbrille, verringert werden. Hat man einmal festgelegt, was die Steuerung anteilig leisten muss, dann hilft ein einfaches Diagramm, der „Risikograph“, bei der schnellen und direkten Bestimmung des geforderten Performance Levels PL_r (Beispiele im Anhang A). Ist die Verletzung irreversibel (z.B. Tod, Verlust von Körperteilen) oder reversibel (z.B. Quetschungen, die verheilen können)? Hält sich der Bediener häufig und lange im Gefahrenbereich auf (z.B. öfter als einmal pro Stunde) oder selten und kurz? Hat er eine Möglichkeit, den Unfall noch zu vermeiden (z.B. wegen langsamer Maschinenbewegung)? Diese drei Fragen entscheiden über den PL_r. Details findet der Leser in Abschnitt 5.4.

4.2 Gestaltung und technische Realisierung der Sicherheitsfunktionen

Stehen die Anforderungen an die sicherheitsbezogenen Teile von Steuerungen fest, folgen zunächst der Entwurf und danach dessen Realisierung. Abschließend wird überprüft, ob durch die geplante Realisierung (Blöcke 4 und 5 in Abbildung 4.1) mit dem Istwert PL die erforderliche Risikominderung, der Sollwert PL_r, erreicht werden kann (Block 6 in Abbildung 4.1). Die Schritte der Blöcke 4 und 5 sind im Kapitel 6 ausführlich beschrieben. In der Tradition des BIA-Reports 6/97 enthält auch dieser Report im Kapitel 8 viele gerechnete Schaltungsbeispiele für alle Steuerungstechnologien und jede Kategorie. Ein ausführlich beschriebenes Schaltungsbeispiel begleitet zusätzlich die allgemeinen Ausführungen in den Kapiteln 5, 6 und 7. Dadurch werden dem Entwickler die nachfolgend beschriebenen Methoden und Parameter anschaulich vermittelt.

Sicherheitsbezogene Teile von Steuerungen sind voraussichtlich nur so gut wie zunächst die Sinnfälligkeit ihrer Sicherheitsfunktion. Danach folgen als Qualitätskriterien die Güte der verwendeten Bauteile (Lebensdauer), ihr Zusammenspiel (Dimensionierung), die Wirksamkeit der Diagnose (z.B. Selbsttests) und die Fehlertoleranz (Fehlersicherheit) der Struktur. Aus diesen Parametern bestimmt sich die Wahrscheinlichkeit eines gefährlichen Ausfalls und somit der erreichte PL. Die Revision der DIN EN ISO 13849-1 lässt die zu verwendenden Berechnungsmethoden offen. So darf man durchaus die hoch komplexe Markov-Modellierung unter Berücksichtigung der oben genannten Parameter nutzen. Die Norm beschreibt jedoch ein sehr vereinfachtes Vorgehen, nämlich die Benutzung eines Säulendiagramms (siehe Abbildung 6.10), in dem diese Modellierung des PL schon vorweggenommen ist. Für Experten: Die Herleitung des Säulendiagramms findet sich in Anhang G.

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

Einen Überblick über die Kategorien liefert Tabelle 6.2, in der die drei rechten Spalten die Neuerungen in der Norm aufzeigen. Ein wesentlicher Aspekt bei der Verwendung der vorgeschlagenen einfachen Rechenmethoden ist die Darstellung der Kategorien als logische Blockschaltbilder, den sogenannten vorgesehenen Architekturen (Designated Architectures).

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

Tabelle 4.1:
Deterministische und probabilistische Merkmale der Kategorien; Ergänzungen nach der Revision der Norm sind grau hinterlegt

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

Eine der meistgestellten Fragen zur Ausfallwahrscheinlichkeit betrifft die Beschaffung zuverlässiger Ausfalldaten, der $MTTF_d$-Werte (Mean Time to Dangerous Failure), für die sicherheitsbezogenen Komponenten. Hier ist der Bauteile- oder Komponentenhersteller mit seinem technischen Datenblatt allen anderen Quellen vorzuziehen. Viele Komponentenhersteller, auch im Bereich der Pneumatik, haben bereits signalisiert, dass solche Daten künftig erhältlich sein werden. Aber auch wenn es (noch) wenig Herstellerangaben gibt, lassen sich typische Beispielwerte aus etablierten Datensammlungen (z.B. SN 29500 oder IEC/TR 62380) ermitteln. Die Norm und Anhang D dieses Reports listen ebenfalls einige realistische Werte aus der Praxis auf.

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

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

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

4.3 Verifikation und Validierung der Steuerung für jede Sicherheitsfunktion

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

4.4 Künftige Entwicklung von DIN EN ISO 13849-1

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

5 Sicherheitsfunktionen und ihr Beitrag zur Risikominderung

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

5.1 Anforderungen der EG-Maschinenrichtlinie

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

Sofern für die zu konstruierende Maschine eine harmonisierte produktspezifische Norm (Typ-C-Norm) vorliegt, die im Amtsblatt der EU veröffentlicht wurde [17], kann von einer Berücksichtigung der grundlegenden Sicherheits- und Gesundheitsanforderungen bereits ausgegangen werden. Man spricht in diesen Fällen von einer Norm mit Vermutungswirkung, denn bei Anwendung der Norm darf man die Übereinstimmung mit den Anforderungen der EG-Maschinenrichtlinie vermuten. Die Strategie zur Risikominderung ist aber immer dann anzuwenden, wenn eine Norm mit Vermutungswirkung nicht existiert, wenn davon abgewichen wurde oder wenn zusätzliche Aspekte vorliegen, die von der Produktnorm nicht abgedeckt sind. Zur Feststellung der von einer Produktnorm nicht berücksichtigten Sachverhalte sind die ersten beiden Schritte der im Folgenden beschriebenen Strategie zur Risikominderung immer durchzuführen, also die Grenzen der Maschine festzulegen und die Gefährdungen zu identifizieren.

5.2 Strategie zur Risikominderung

Das in DIN EN ISO 12100-1 vorgestellte Verfahren zur Risikominderung wurde in Bild 1 der DIN EN ISO 13849-1 übernommen und um die in dieser Norm konkretisierten Aspekte ergänzt (siehe Abbildung 5.1 auf Seite 24). Als Erstes erfolgt eine Risikobeurteilung. Dabei ist es wichtig zu wissen, dass man bei den folgenden Schritten zunächst einmal von einer Maschine ausgeht, an der noch keine Schutzmaßnahmen getroffen wurden. Letztendlich dient der gesamte Prozess der Risikominderung dazu, die Art und auch die „Qualität“ der zu treffenden Schutzmaßnahme bzw. Schutzeinrichtung zu bestimmen.

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

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

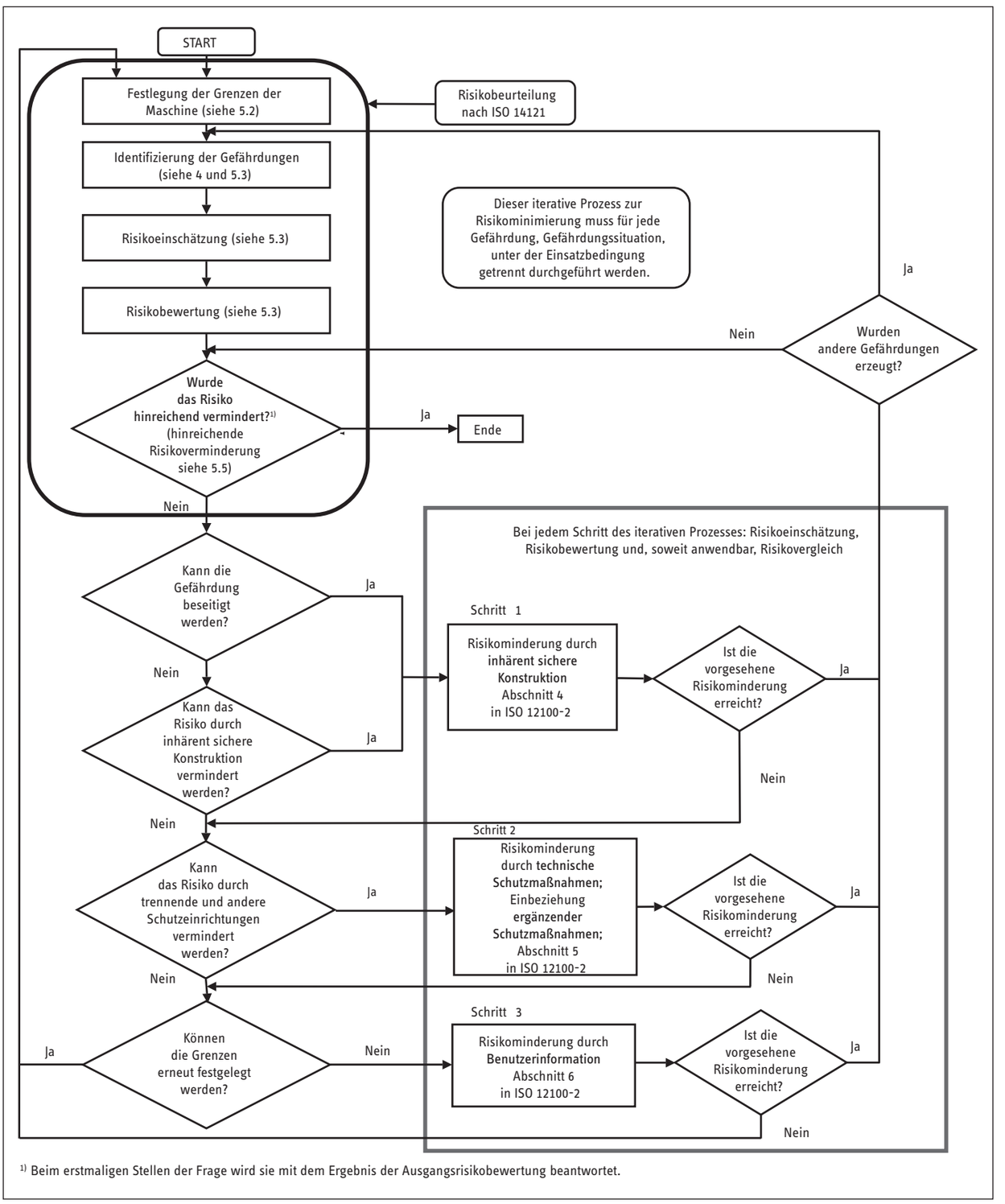
- das Einrichten,
- das Prüfen,
- das „Teachen“/Programmieren,
- die Inbetriebnahme,
- die Maschinenbeschickung,
- die Produktentnahme,
- die Fehlersuche und Fehlerbeseitigung,
- die Reinigung,
- die Instandhaltung.

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

---

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

Abbildung 5.1:
Iterativer Prozess zur Risikominderung



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

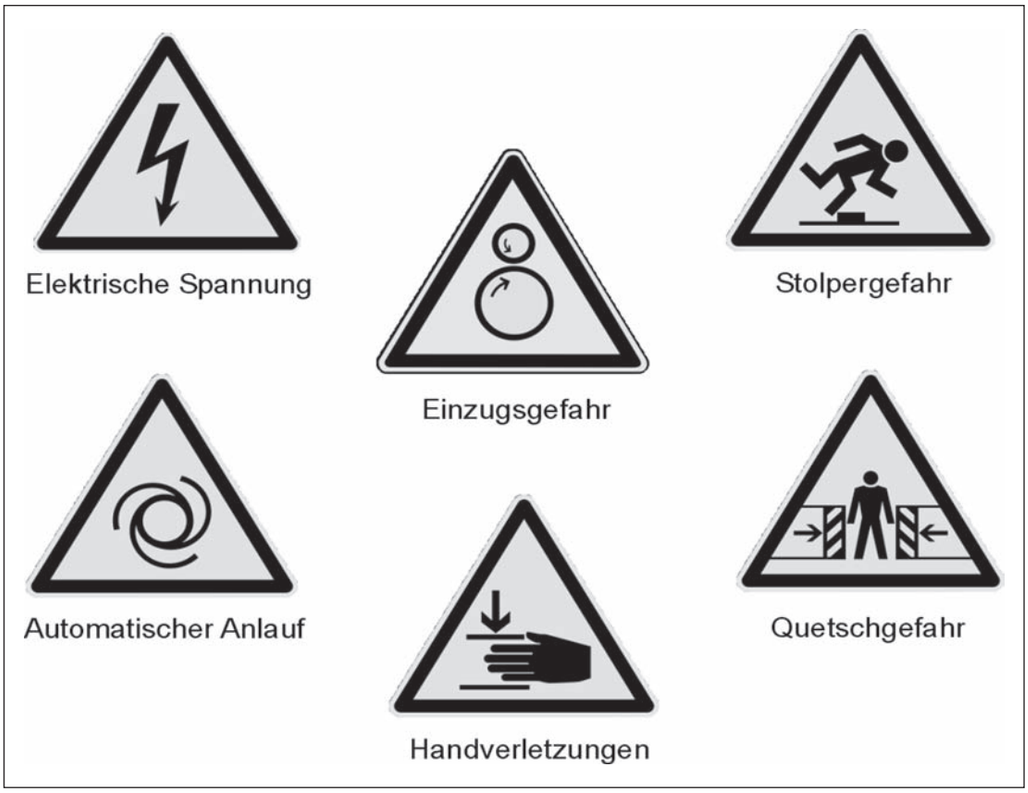


Abbildung 5.2: Beispiele für Gefährdungen (Quelle: Wikipedia)

5.2.1 Risikoeinschätzung

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

a) Schadensausmaß

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

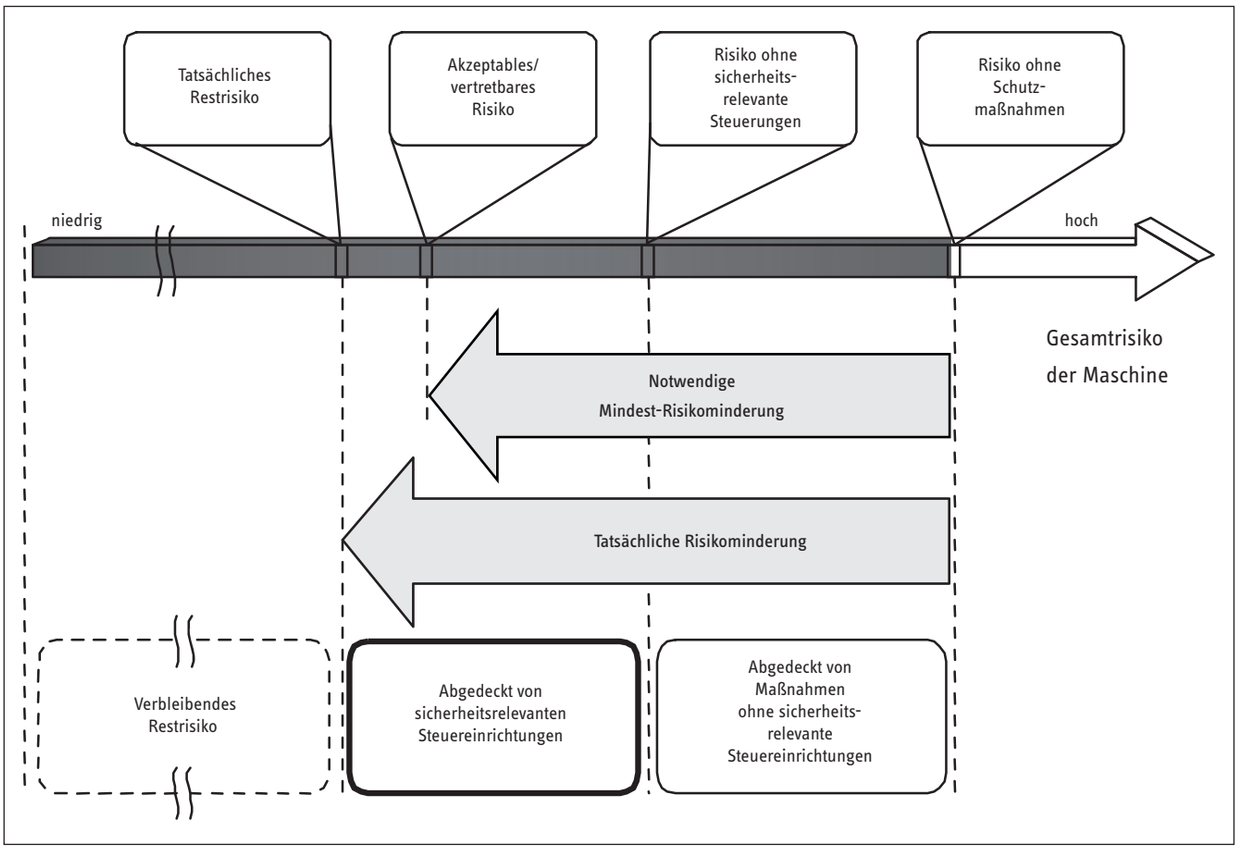
Ziel des weiteren Vorgehens ist es, das Risiko auf ein akzeptables Maß zu reduzieren. Abbildung 5.3 (siehe Seite 26) zeigt hierzu die Anteile der Risikoreduzierung mit und ohne sicherheitsrelevante Teile einer Steuerung. Weitere Informationen zum Thema Risiko enthält das BGIA-Handbuch [18].

5.2.2 Risikobewertung

Im Anschluss an die Risikoeinschätzung wird eine Risikobewertung durchgeführt, um zu entscheiden, ob eine Risikominderung notwendig ist. Die Kriterien für eine hinreichende Risikominderung gibt DIN EN 12100-1 vor:

- Wurden alle Betriebsbedingungen und alle Eingriffsmöglichkeiten berücksichtigt?
- Wurden die Gefährdungen durch angemessene Schutzmaßnahmen beseitigt oder die Risiken soweit vermindert, wie dies praktisch umsetzbar ist?
- Ist sichergestellt, dass die durchgeführten Maßnahmen nicht neue Gefährdungen schaffen?
- Sind die Benutzer hinsichtlich der Restrisiken ausreichend informiert und gewarnt?
- Ist sichergestellt, dass die Arbeitsbedingungen der Bedienpersonen und die Benutzerfreundlichkeit der Maschine durch die ergriffenen Schutzmaßnahmen nicht konterkariert werden?
- Sind die durchgeführten Schutzmaßnahmen miteinander vereinbar?
- Wurden die Folgen ausreichend berücksichtigt, die sich durch den Gebrauch einer für den gewerblichen/industriellen Einsatz konstruierten Maschine im nicht gewerblichen/nicht industriellen Bereich ergeben können?
- Ist sichergestellt, dass die durchgeführten Schutzmaßnahmen die Arbeitsbedingungen der Bedienpersonen oder die Benutzerfreundlichkeit der Maschine nicht negativ beeinflussen?

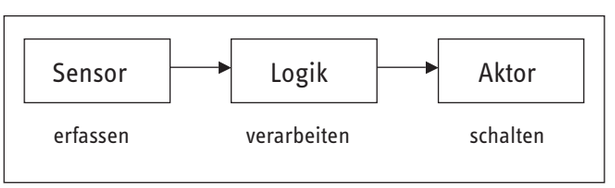
Abbildung 5.3:
Risikoeinschätzung und Risikominderung



5.3 Identifizierung der notwendigen Sicherheitsfunktionen und ihrer Eigenschaften

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

Abbildung 5.4:
Sicherheitsfunktionen werden von SRP/CS ausgeführt



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

5.3.1 Festlegung von Sicherheitsfunktionen

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

a) gesteuertes Stillsetzen der Bewegung und Einfallen der Haltebremse im Stillstand

b) Verhindern einer Quetschstelle infolge der Absenkung von Maschinenteilen

c) Leistung des Schneidlasers bei direkter Exposition am Auge absenken

d) Verhinderung des Absturzes der Achse im Einrichtbetrieb

e) Ausweichen des Roboters bei Betreten seines Gefahrenbereiches

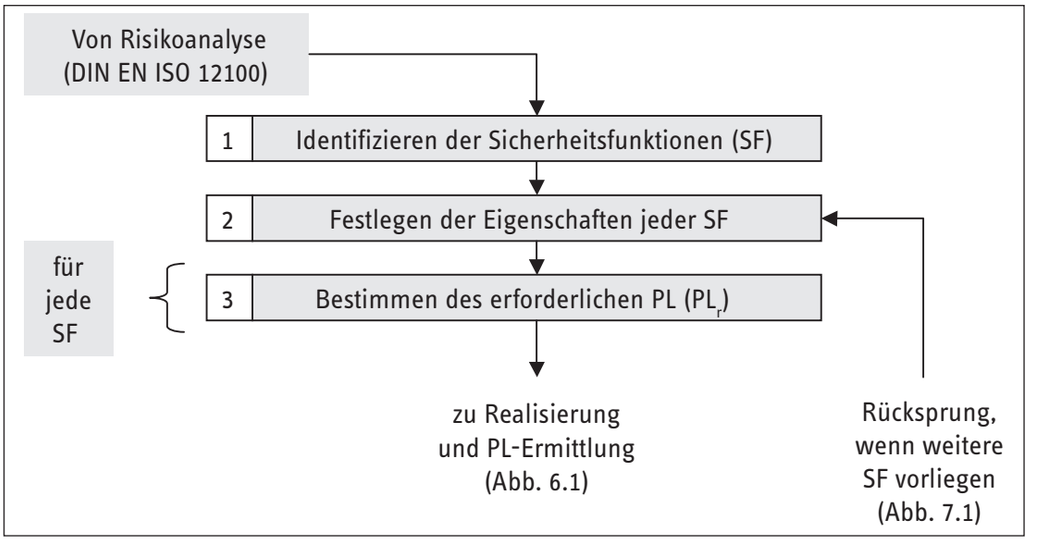


Abbildung 5.5: Ausschnitt aus dem iterativen Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP/CS)

f) Verhinderung des Einzugs von Personen

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

Häufig verwendet man zusammengesetzte Sicherheitsfunktionen wie im Beispiel in Abschnitt 5.7 (siehe Seite 32). Durch die elektronische Ansteuerung wird die Bewegung zunächst bis zum Stillstand abgebremst und anschließend fällt eine mechanische Haltebremse ein. Hinweise zu möglichen Sicherheitsfunktionen geben die folgenden Tabellen. In Tabelle 5.1 sind die Sicherheitsfunktionen nach Abschnitt 5.1 der DIN EN ISO 13849-1 zusammengefasst und um Beispiele für mögliche Anwendungen ergänzt. Hier ist auch die „Funktion zum Stillsetzen im Notfall" enthalten, die zwar kein Bestandteil einer Schutzeinrichtung ist, aber zur Realisierung einer ergänzenden Schutzmaßnahme verwendet wird (siehe Abschnitt 5.5). Tabelle 5.2 (siehe Seite 28) zeigt weitere Sicherheitsfunktionen für sichere Antriebssteuergeräte nach DIN EN 61800-5-2 (PDS/SR, Power Drive Systems/ Safety Related) [19]. Diese Norm enthält u.a. die häufig angewendeten Sicherheitsfunktionen zur Verhinderung eines unerwarteten Anlaufs STO (STO, Safe Torque Off; früher SH, Sicherer Halt), zum sicheren Stillsetzen SS1 und SS2 und zur sicheren Begrenzung einer Geschwindigkeit SLS (SLS, Safely-Limited Speed; früher SRG, Sicher Reduzierte Geschwindigkeit).

Tabelle 5.1:
Sicherheitsfunktionen aus DIN EN ISO 13849-1

Sicherheitsfunktion	Beispiel für mögliche Anwendung
Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung	Reaktion auf das Auslösen einer Schutzeinrichtung durch STO, SS1 oder SS2 (Tabelle 5.2)
Manuelle Rückstellfunktion	Quittierung beim Verlassen von hintertretbaren Bereichen
Start-/Wiederanlauffunktion	Nur zulässig bei steuernden trennenden Schutzeinrichtungen nach DIN EN ISO 12100-2
Lokale Steuerungsfunktion	Steuern von Maschinenbewegungen von einem Standort innerhalb des Gefahrenbereichs
Mutingfunktion	Zeitweises Unwirksammachen von Schutzeinrichtungen, z.B. beim Materialtransport
Einrichtung mit selbsttätiger Rückstellung (Tippschalter)	Maschinenbewegungen gesteuert von einem Standort innerhalb des Gefahrenbereichs, z.B. beim Einrichten
Zustimmfunktion	Maschinenbewegungen gesteuert von einem Standort innerhalb des Gefahrenbereichs, z.B. beim Einrichten
Verhinderung des unerwarteten Anlaufs	Manueller Eingriff in Gefahrenbereiche
Befreiung und Rettung eingeschlossener Personen	Auseinanderfahren von Walzen
Isolations- und Energieableitungsfunktion	Öffnung eines Hydraulikventils zum Druckabbau
Steuerungsfunktionen und Betriebsartenwahl	Aktivierung von Sicherheitsfunktionen durch Betriebsartenwahlschalter
Funktion zum Stillsetzen im Notfall	Reaktion auf die Betätigung eines Not-Halt-Geräts durch STO oder SS1 (Tabelle 5.2)

Tabelle 5.2:
Sicherheitsfunktionen aus DIN EN 61800-5-2

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

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

- Verwendung in unterschiedlichen Betriebsarten (z.B. Automatikbetrieb, Einrichtbetrieb, Störungsbeseitigung)
- Reaktion(en) beim Ansprechen der Sicherheitsfunktion
- Reaktion(en) beim Erkennen eines Fehlers der Sicherheitsfunktion
- Ansprechzeit
- Häufigkeit der Betätigung
- ggf. eine Priorität, falls mehrere Sicherheitsfunktionen gleichzeitig aktiv sein können
- Festlegung sicherheitsbezogener Parameter, z.B. der maximal zulässigen Geschwindigkeit
- erforderlicher Performance Level PL_r

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

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

Beispiel 1: Sicherheitsfunktion
„Stillsetzen beim Öffnen der Schutztür"

Beim Öffnen der Schutztür hat ein Maschinenbediener Zugang zu einem Gefahrenbereich, in dem fünf Antriebe Bewegungen von Maschinenteilen steuern. Das Öffnen der Schutztür bewirkt ein schnellstmögliches Stillsetzen aller fünf Antriebe. Das zugehörige funktionale Schaltbild ist in Abbildung 5.6 dargestellt.

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

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

Das Resultat kann ein PL sein, der für die Anwendung nicht mehr ausreichend ist, obwohl vielleicht nur die Antriebe 1 und 3 für den Bediener gefahrbringende Bewegungen auslösen und die restlichen Antriebe rein „funktional" stillgesetzt werden. In diesem Fall empfiehlt es sich, für die Sicherheitsfunktion nur die Bewegungen zu berücksichtigen, die tatsächlich eine Gefährdung sind.

Beispiel 2: Sicherheitsfunktion
„Stillsetzen beim Öffnen einer Schutztür"

Eine gefahrbringende Bewegung ist durch einen Zaun abgesichert, der über fünf Schutztüren verfügt. Das Öffnen einer der Türen führt zum Stillsetzen. Im Hinblick auf die spätere Bestimmung des PL ist jede Tür Bestandteil einer eigenen Sicherheitsfunktion SF1 bis SF5, die sich aus folgenden Blöcken[1] zusammensetzt:

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

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

Abbildung 5.6:
Stillsetzen beim Öffnen der Schutztür

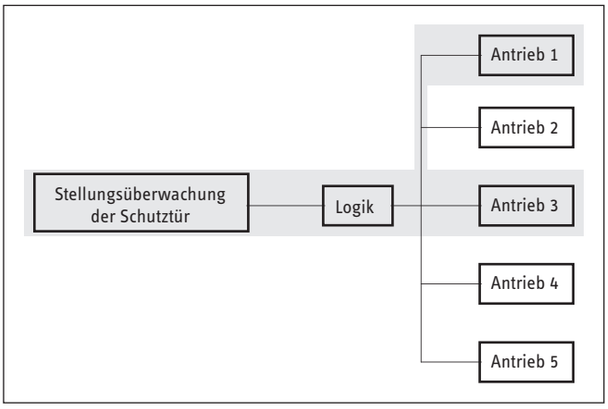
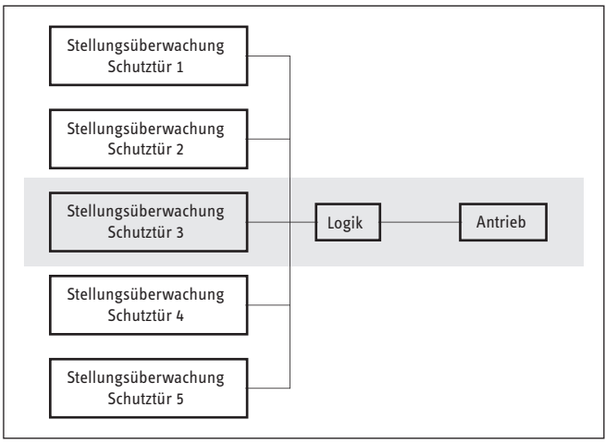


Abbildung 5.7:
Stillsetzen beim Öffnen der Schutztür 3



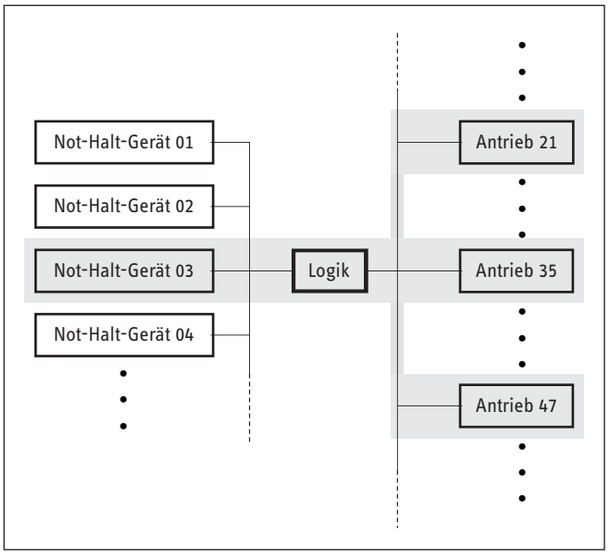
Beispiel 3: Sicherheitsfunktion „Not-Halt einer Gesamtmaschine" (siehe Abschnitt 5.5)

An einer größeren Maschine sind 20 Not-Halt-Geräte installiert, deren Betätigung alle 50 Antriebe schnellstmöglich stillsetzt. Welche Komponenten sind in diesem Fall bei der Realisierung der Sicherheitsfunktion zu berücksichtigen? Es ist nicht vorhersehbar, welches Not-Halt-Gerät zum Auslösen der Sicherheitsfunktion betätigt wird. Da der Bediener immer nur ein Not-Halt-Gerät betätigt, werden die Sicherheitsfunktionen SF1 bis SF20 definiert. Der jeweilige Standort einer gefährdeten Person beim Auslösen des Not-Halts ist nicht bekannt, aber wo auch immer sich diese Person befindet, stellen nicht alle 50 Antriebe eine Gefährdung dar. Daher sollte stellvertretend für alle denkbaren Situationen der ungünstigste Fall betrachtet werden. Dieser ist bestimmt durch den schlechtesten PL, ist also u.a. abhängig von der Anzahl der Antriebe in der Sicherheitskette, die am ungünstigsten Standort gefahrbringende Bewegungen erzeugen, sowie den jeweiligen einzelnen PL. Das zugehörige Blockschaltbild ist in Abbildung 5.8 (siehe Seite 30) dargestellt.

---

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

Abbildung 5.8:
Not-Halt der Gesamtmaschine, ungünstigster Fall



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

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

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

- An welchem Ort befinden sich zum betrachteten Zeitpunkt Personen?
- Welche Bewegungen stellen am Standort der Person(en) Gefährdungen dar?
- Welche Schutzeinrichtungen müssen die Sicherheitsfunktion auslösen? Ggf. sind mehrere alternativ benutzbare Schutzeinrichtungen zu berücksichtigen.

5.4 Bestimmung des erforderlichen Performance Level PL_r

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

5.4.1 Risikograph

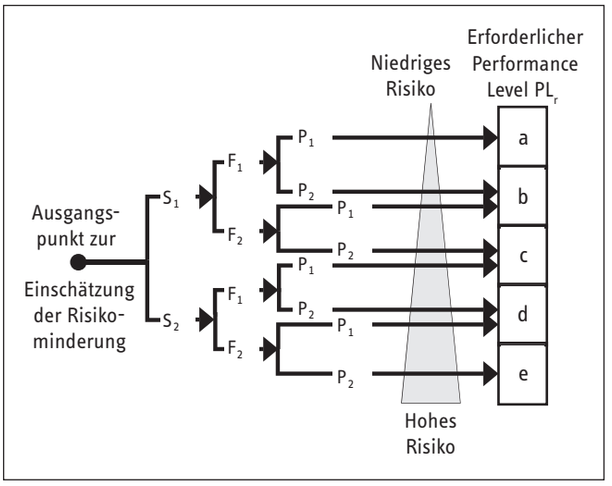
Das Diagramm im Anhang A der Norm führt direkt zum erforderlichen Performance Level PL_r und wird im Folgenden erläutert (siehe Abbildung 5.9). Weitere Beispiele zur Bestimmung des PL_r finden sich in Anhang A.

Beginnend am Ausgangspunkt werden die Risikoparameter[2]

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

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

Abbildung 5.9:
Risikograph zur Bestimmung des PL_r für jede Sicherheitsfunktion



---

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

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

Schwere der Verletzung S1 und S2

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

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

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

Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2

Häufigkeit und Dauer der Gefährdungsexposition werden bewertet mit:

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

Eine feste Grenze zur Auswahl zwischen F1 und F2 kann leider nicht angegeben werden. Die Norm gibt in einer Anmerkung den nicht normativen Hinweis, dass bei Eingriffen, die häufiger als einmal pro Stunde erfolgen, F2 gewählt werden sollte, sonst F1. Dieser Hinweis passt aber in der Regel auf alle in der Praxis vorkommenden Fälle. Bei der Bewertung ist ein durchschnittlicher Wert der Gefährdungsexposition im Verhältnis zur gesamten Nutzungszeit einer Maschine zu berücksichtigen. Eindeutige Fälle liegen jedoch vor, z.B. bei einer manuell beschickten Presse in der Metallbearbeitung, bei der zyklisch zwischen die Werkzeuge der Maschine gegriffen werden muss (F2). Für ein Bearbeitungszentrum hingegen, das einmal jährlich eingerichtet wird und dann automatisch produziert, wird sicherlich F1 gewählt. Bei der Bewertung der Häufigkeit und Dauer ist es nicht zulässig zu unterscheiden, ob dieselbe oder unterschiedliche Personen der Gefährdung ausgesetzt werden.

Möglichkeit zur Vermeidung der Gefährdung P1 und P2

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

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

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

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

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

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

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

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

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

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

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

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

5.5 Ergänzende Schutzmaßnahmen

Die Anforderungen an ergänzende Schutzmaßnahmen sind in DIN EN ISO 12100-2 [3], Abschnitt 5.5, enthalten. Im Hinblick auf die im vorliegenden Report behandelten steuerungstechnischen Fragestellungen sind hierunter insbesondere zu verstehen:

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

Definitionsgemäß handelt es sich hierbei nicht um technische Schutzmaßnahmen, für deren Realisierung ein bestimmter Performance Level erforderlich wäre. Allerdings sollen diese ergänzenden Schutzmaßnahmen dann greifen, wenn technische Schutzmaßnahmen (trennende und/oder nicht trennende Schutzeinrichtungen) versagt haben bzw. durch Manipulation unwirksam gemacht wurden. Besonders in diesen Fällen erwartet man, dass z.B. ein Not-Halt auch funktionsfähig ist. Insofern sind die Anforderungen der DIN EN 60204-1 [20] an Steuerstromkreise und Steuerfunktionen von Maschinen zu berücksichtigen. Im Abschnitt 9.4 „Steuerfunktionen im Fehlerfall“ wird ein angemessenes Niveau der sicherheitstechnischen Leistungsfähigkeit verlangt, das durch die Risikobewertung der Maschine festzulegen ist. Die Anforderungen der DIN EN ISO 13849 gelten letztlich also auch für diese ergänzenden Schutzmaßnahmen. In jedem Falle dürfen ergänzende Schutzmaßnahmen nicht die Funktion und das Niveau von Schutzeinrichtungen beeinflussen.

5.6 Behandlung von Altmaschinen

Unter Altmaschinen sind solche Maschinen zu verstehen, die bereits vor Inkrafttreten der Maschinenrichtlinie in Verkehr gebracht wurden. Die Anforderungen der Richtlinie wurden auf diese Maschinen nicht angewendet. Werden Altmaschinen erweitert, verändert, modernisiert usw., kann dies jedoch erforderlich werden. In solchen Fällen ist zu bewerten, ob eine „wesentliche Veränderung“ vorliegt. Ist dies der Fall, gelten die Anforderungen der EG-Maschinenrichtlinie auch für „alte“ Maschinen, ebenso wie für neue. Dazu gehört u.a. die Anwendung der DIN EN ISO 13849. Bei der Entscheidung, ob eine „wesentliche Veränderung“ vorliegt, hilft ein Diagramm der Berufsgenossenschaft der chemischen Industrie [21].

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

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

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

5.7.1 Festlegung der Grenzen der Maschine

Räumliche Grenzen

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

Zeitliche Grenzen

Je nach Anwendungsfall kann die Maschine über einen Zeitraum von ca. 20 Jahren eingesetzt werden. Durch die Abnutzung von Bauteilen kann sich die benötigte Zeit für das Stillsetzen einer Bewegung verlängern. Die daraus resultierende Überschreitung des Nachlaufwegs muss daher detektiert werden und zu einer Stillsetzung der Maschine führen.

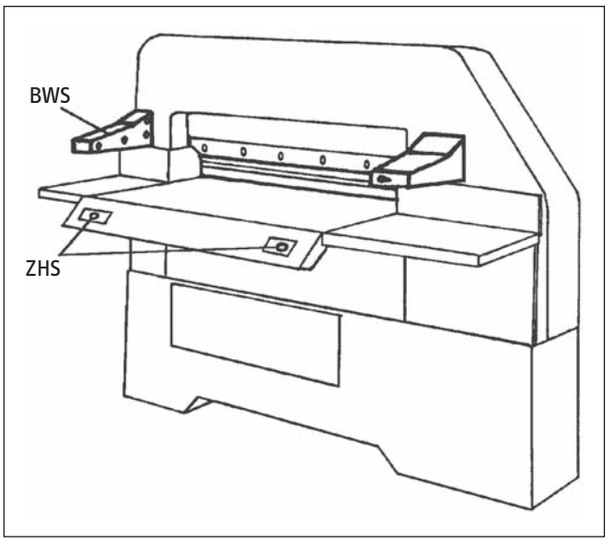
Verwendungsgrenzen

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

Folgende Betriebsarten sind vorgesehen:

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

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



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

5.7.2 Identifizierung der Gefährdungen

Folgende mechanische Gefährdungen sind für eine Planschneidemaschine signifikant:

G1 – Quetschen durch den Pressbalken

G2 – Schneiden durch das Schneidmesser während des Schnittvorgangs

G3 – Schneiden durch das Schneidmesser im Ruhezustand

Risikoeinschätzung

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

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

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

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

Risikobewertung

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

Inhärent sichere Konstruktion

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

Folgende Maßnahmen können jedoch ergriffen werden:

1. Alle Zugänge zum Gefahrenbereich mit Ausnahme der Bedienseite verdecken.
2. Scharfe Kanten und Ecken vermeiden.
3. Für eine angemessene Arbeitsposition und Zugänglichkeit der Bedienteile sorgen.
4. Maschine ergonomisch gestalten.
5. Elektrische Gefährdungen verhindern.
6. Gefährdungen durch die hydraulische Ausrüstung vermeiden.

5.7.3 Notwendige Sicherheitsfunktionen

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

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

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

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

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

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

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

SF7 – Abdeckung des Messers durch den Pressbalken

Eigenschaften der Sicherheitsfunktionen

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

5.7.4 Bestimmung des erforderlichen Performance Level PL_r

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

S2 – ernste, üblicherweise irreversible Verletzung

F2 – dauernder Aufenthalt im Gefahrenbereich

P2 – Vermeidung einer Gefährdungssituation kaum möglich

Entsprechend dem Risikographen in Abbildung 5.9 ergibt sich aus dieser Bewertung ein erforderlicher Performance Level PL_r = e. Abbildung 5.11 zeigt hierzu Dokumentation und Risikograph in der Software SISTEMA für die Sicherheitsfunktion SF1.

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

S1 – leichte, üblicherweise reversible Verletzung

F2 – Zeit der Gefährdungsexposition ist lang

P1 – Vermeidung einer Gefährdungssituation möglich unter bestimmten Bedingungen

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

Abbildung 5.11:
Dokumentation und Risikograph für SF1

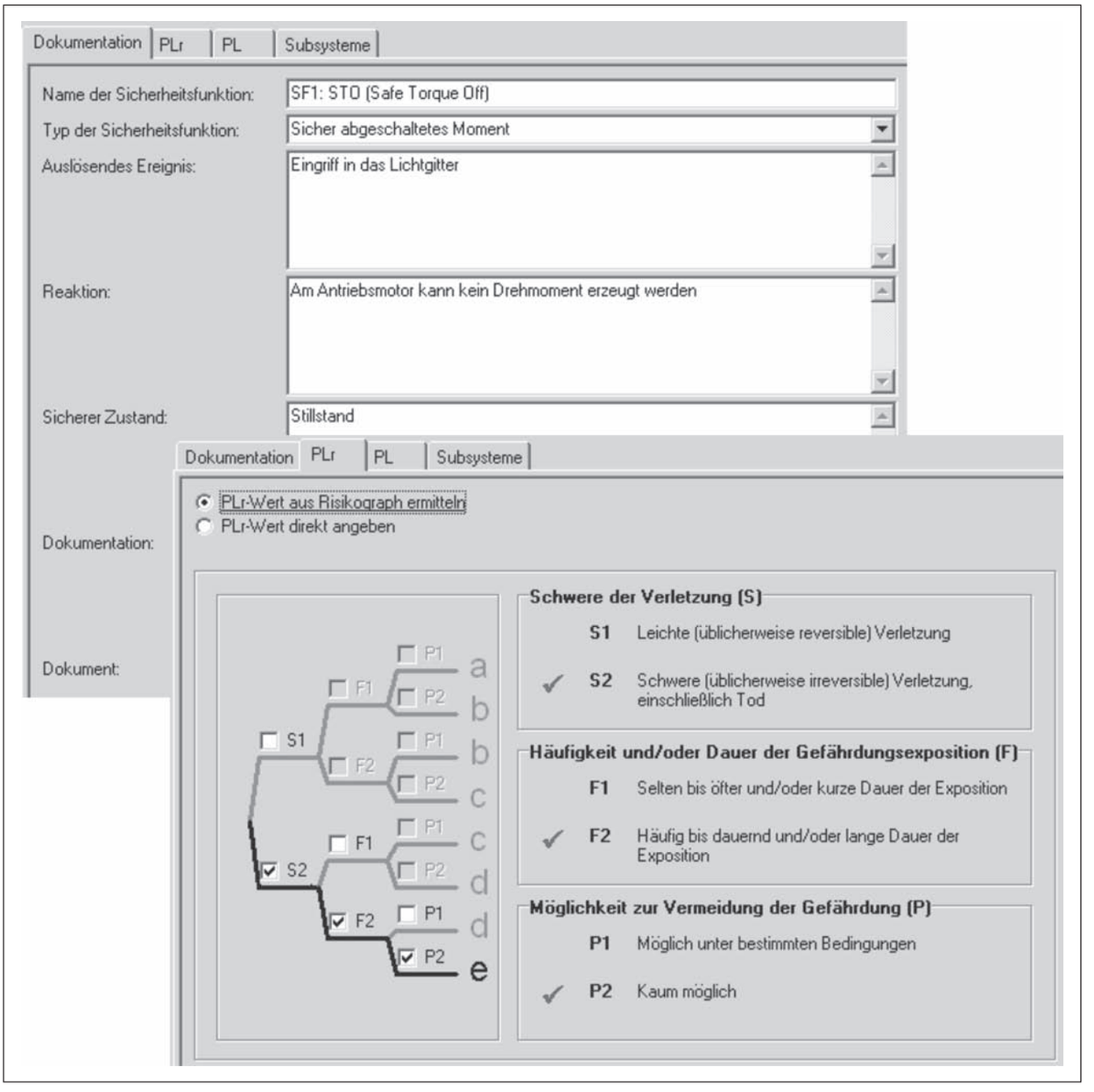
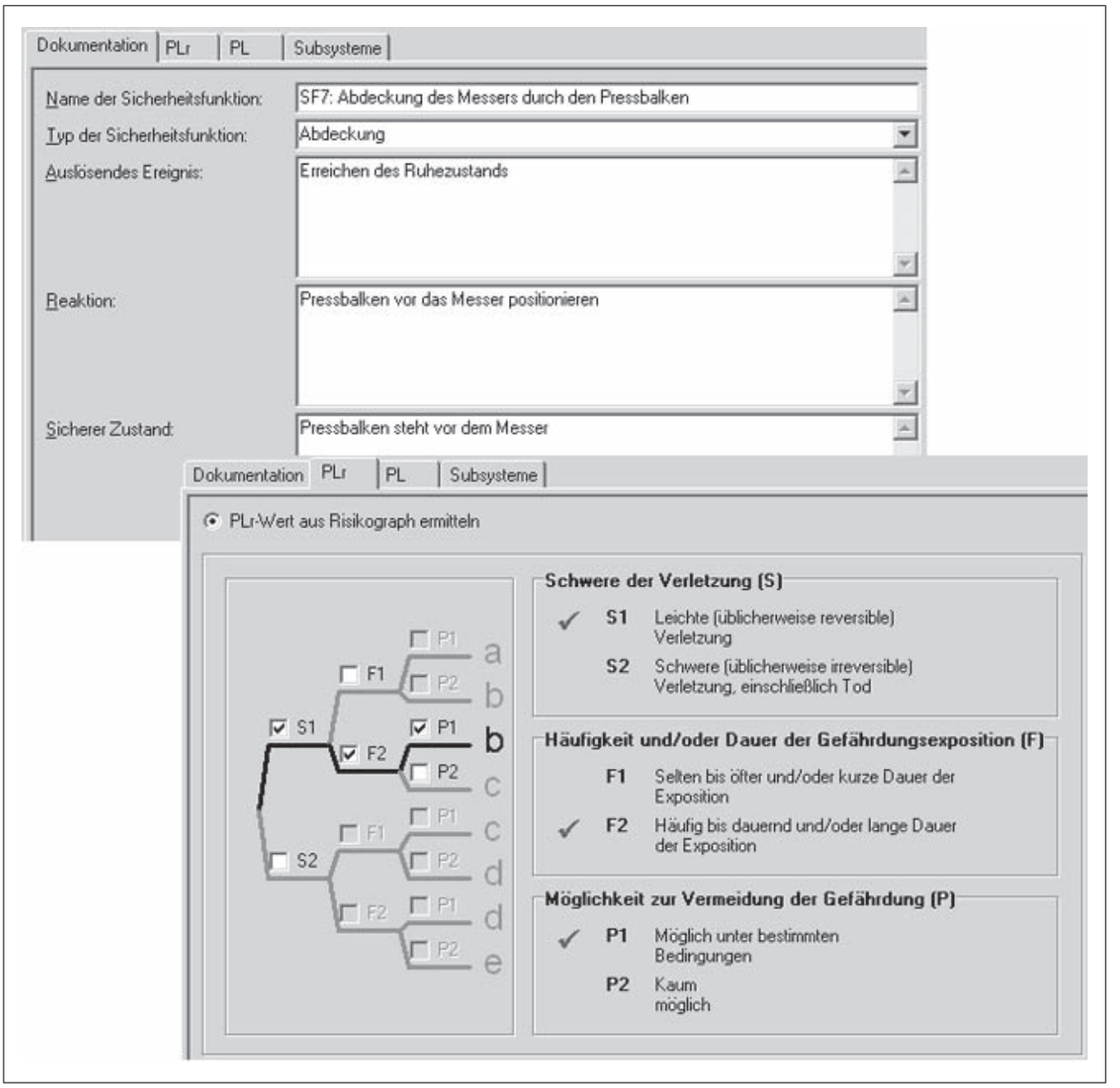


Abbildung 5.12:
Dokumentation und Risikograph für SF7



5.7.5 Ergänzende Schutzmaßnahmen

Folgende Maßnahmen sind erforderlich:

1. Stillsetzen im Notfall

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

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

6 Gestaltung sicherer Steuerungen

6.1 Einleitung

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

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

Tabelle 6.1:
Zuordnung der Ausfallwahrscheinlichkeit zu den Performance Level

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

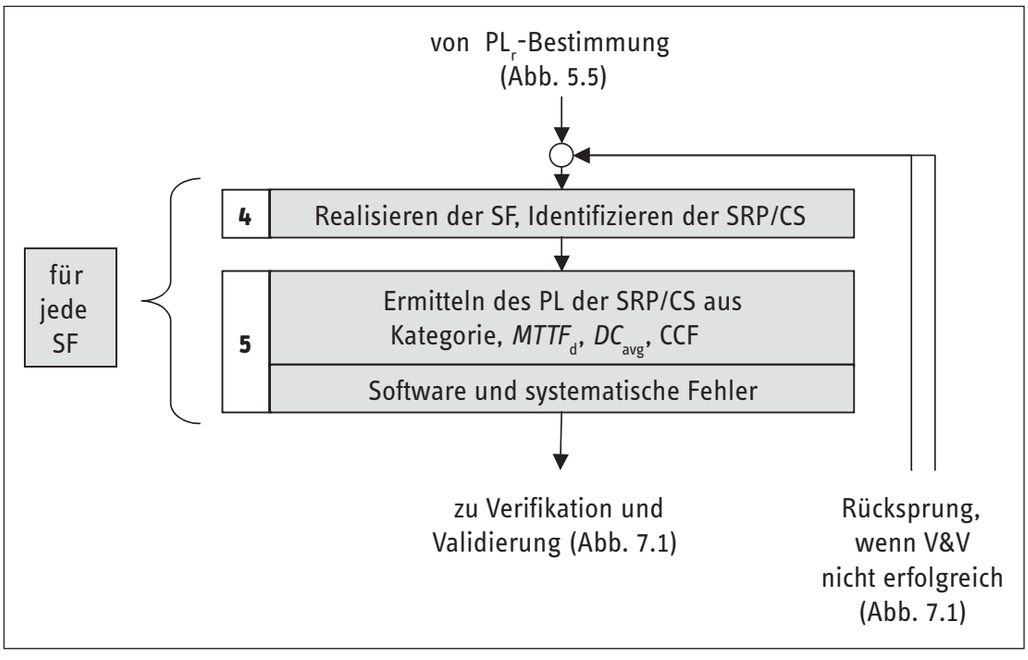


Abbildung 6.1: Ermittlung des erreichten PL in der Realisierungsphase der SRP/CS als Ausschnitt aus dem iterativen Gestaltungsprozess, siehe Abbildung 4.1

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

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

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

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

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

6.1.1 Entwicklungsablauf

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

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

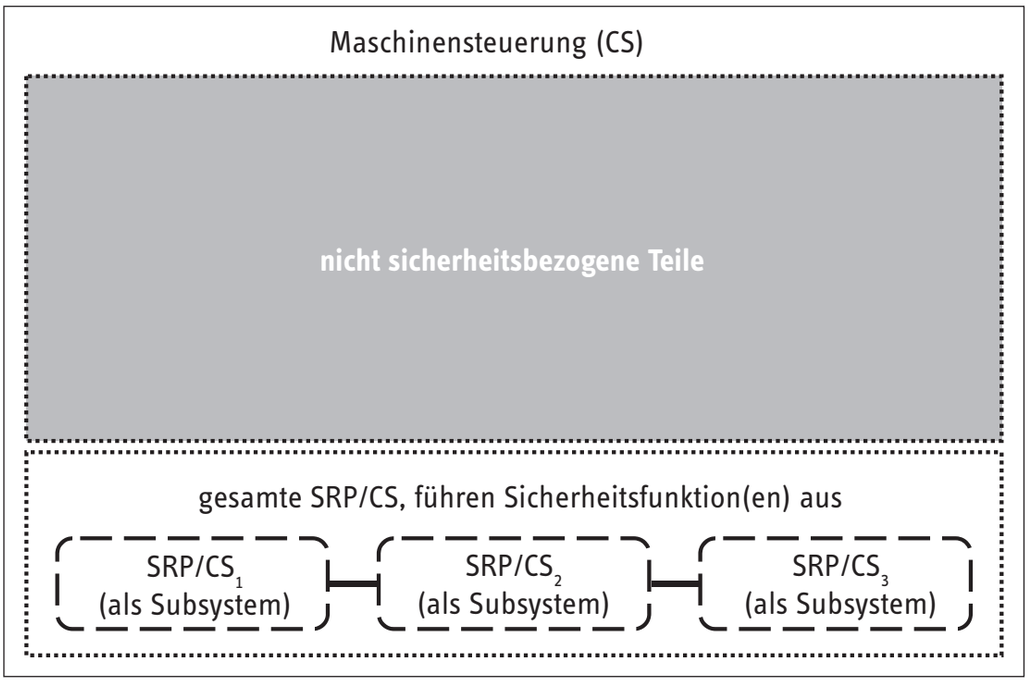
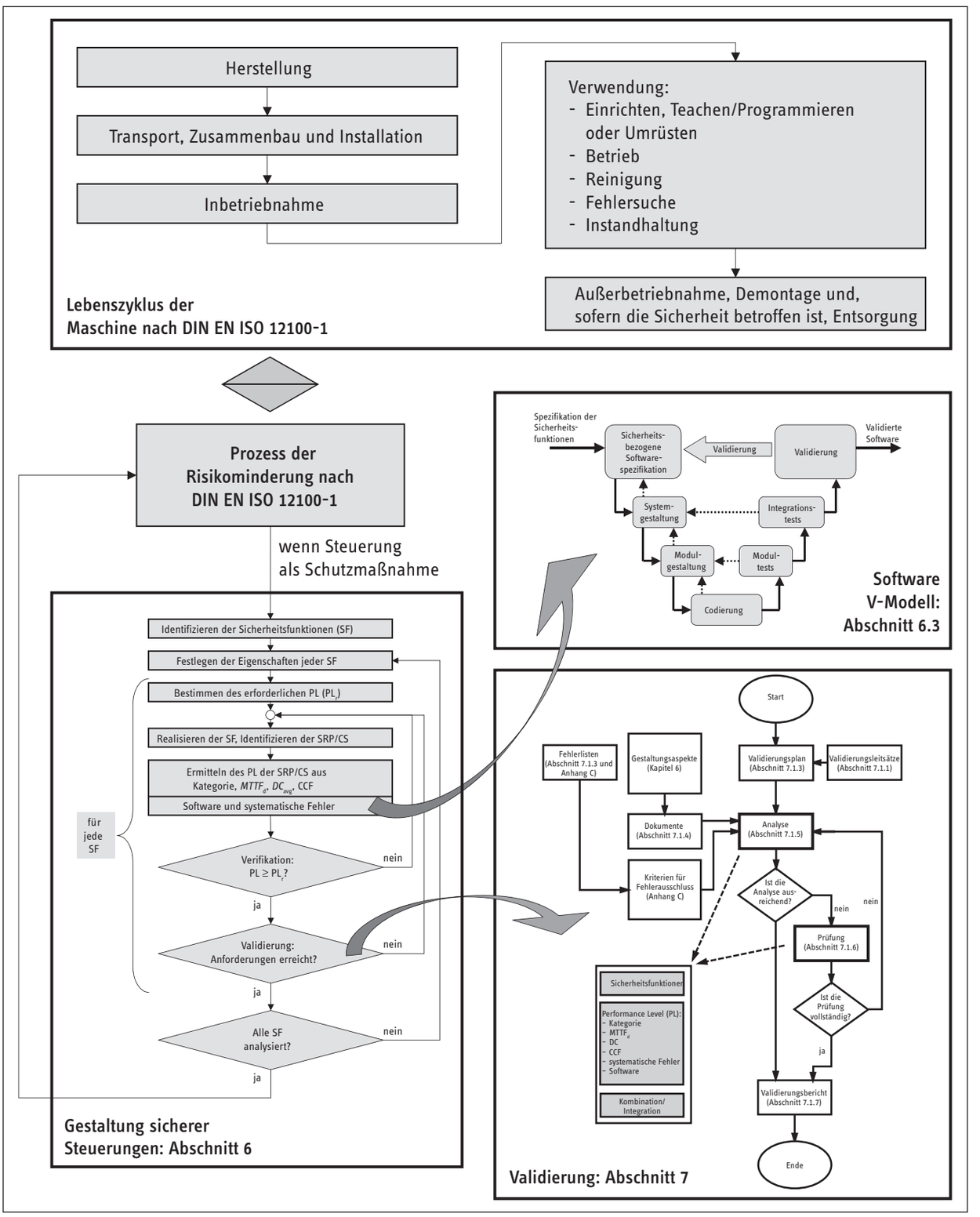


Abbildung 6.2: SRP/CS und Subsysteme innerhalb der Maschinensteuerung

Abbildung 6.3:
Lebenszyklen von Maschine und SRP/CS



Da SRP/CS Teile einer Maschine sind, können Anforderungen in fast jeder Phase des Lebenszyklus der Maschine auch Einfluss auf ein SRP/CS haben. Alle Phasen im Lebenszyklus der Maschine müssen daher bei der Identifikation und Festlegung der Eigenschaften von Sicherheitsfunktionen berücksichtigt werden. Um dies möglichst umfassend und nachprüfbar zu gestalten, werden Sicherheitsfunktionen zunächst spezifiziert. SRP/CS, die nicht speziell für eine Maschinensteuerung entwickelt werden, z.B. ein Lichtgitter oder eine Sicherheits-SPS, bedürfen daher einer besonders genauen Beschreibung ihrer Kenndaten und ihrer Schnittstellen, um eine korrekte Verwendung sicherzustellen.

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

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

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

Mit der Spezifikation ist das erste Dokument im Ablauf der Gestaltung von SRP/CS entstanden. Grundsätzlich hat die Dokumentation einen hohen Stellenwert im Sinne einer nachvollziehbaren Entwicklung. Man sollte beachten, dass ein Produkt unter Umständen von jemand anderem als dem Entwickler weiter gepflegt wird. Details zur erforderlichen Dokumentation im Rahmen des iterativen Gestaltungsprozesses von SRP/CS finden sich im Abschnitt 6.3.8 zu Software und in den Abschnitten 7.1.4 ff. Erwähnt sei an dieser Stelle, dass Dokumente eindeutig identifizierbar sein müssen, eine sogenannte Versionsverwaltung ist also ein Muss. Für die korrekte Umsetzung von Sicherheitsfunktionen wird nicht zuletzt der Inhalt der Benutzerinformationen maßgeblich sein. DIN EN ISO 13849-1 enthält in Kapitel 11 eine Liste der Informationen, die in der Benutzerinformation mindestens enthalten sein müssen. Der Inhalt der herstellerinternen technischen Dokumentation von SRP/CS wird in Kapitel 10 der Norm aufgelistet. Auch der Gesetzgeber erteilt Auflagen zur Dokumentation. Kasten 6.2 (siehe Seite 42) zeigt den Inhalt der erforderlichen technischen Unterlagen für Maschinen aus der zukünftigen (neuen) europäischen Maschinenrichtlinie 2006/42/EG [8], die ab 29. Dezember 2009 anzuwenden ist.

Kasten 6.1:
Allgemeines Gliederungsschema für eine Spezifikation der Sicherheitsanforderungen

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

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

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

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

5 Vorgaben für den SRP/CS-Entwurf
5.1 Zuweisung, durch welche SRP/CS und in welcher Technologie die Sicherheitsfunktion realisiert werden soll, vorgesehene Betriebsmittel
5.2 Auswahl der Kategorie, vorgesehene Architektur (Struktur) als sicherheitsbezogenes Blockdiagramm mit Beschreibung
5.3 Schnittstellenbeschreibung (Prozessschnittstellen, interne Schnittstellen, Bedienerschnittstellen, Bedien- und Anzeigeelemente usw.)
5.4 Einschaltverhalten, Umsetzung des erforderlichen Anlaufverhaltens und Wiederanlaufverhaltens
5.5 Leistungsdaten: Zykluszeiten, Reaktionszeiten usw.
5.6 Verhalten des SRP/CS bei Bauteilausfällen und -fehlern (Erreichen und Aufrechterhalten des sicheren Zustandes) einschließlich Zeitverhalten
5.7 Zu berücksichtigende Ausfallarten von Bauteilen, Baugruppen oder Blöcken und ggf. Begründung für Fehlerausschlüsse
5.8 Konzept zur Umsetzung der Erkennung und Beherrschung von zufälligen und systematischen Ausfällen (Selbsttests, Testschaltungen, Überwachungen, Vergleiche, Plausibilitätsprüfungen, Fehlererkennung durch den Prozess usw.)
5.9 Quantitative Aspekte
5.9.1 Zielwerte für $MTTF_d$ und DC_{avg}
5.9.2 Schalthäufigkeit verschleißbehafteter Bauteile
5.9.3 Häufigkeit von Maßnahmen zur Fehleraufdeckung
5.9.4 Gebrauchsdauer, falls abweichend von der Berechnungsgrundlage der vorgesehenen Architekturen (20 Jahre)
5.10 Betriebs- und Grenzdaten (Betriebs- und Lagertemperaturbereich, Feuchteklasse, IP-Schutzart, Schock-/Vibrations-/EMV-Störfestigkeitswerte, Versorgungsdaten mit Toleranzen usw.) (IP = International Protection, EMV = elektromagnetische Verträglichkeit)
5.11 Anzuwendende Grundnormen für die Konstruktion (zur Ausrüstung, zum Schutz gegen elektrischen Schlag/gefährliche Körperströme, zur Störfestigkeit gegen Umgebungsbedingungen usw.)
5.12 Technische und organisatorische Maßnahmen für einen gesicherten Zugriff auf sicherheitsrelevante Parameter bzw. SRP/CS-Eigenschaften (Manipulationsschutz, Zugangssicherung, Programm-/Datenschutz) und zum Schutz gegen unbefugtes Bedienen (Schlüsselschalter, Code usw.), z.B. bei Sonderbetriebsarten
5.13 Allgemeine technische Voraussetzungen und organisatorische Rahmenbedingungen für die Inbetriebnahme, Prüfung und Abnahme sowie Wartung und Instandhaltung

Kasten 6.2:

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

1. Die technischen Unterlagen umfassen:

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

   b) bei Serienfertigung eine Aufstellung der intern getroffenen Maßnahmen zur Gewährleistung der Übereinstimmung aller gefertigten Maschinen mit den Bestimmungen dieser Richtlinie

6.1.2 Systematische Ausfälle

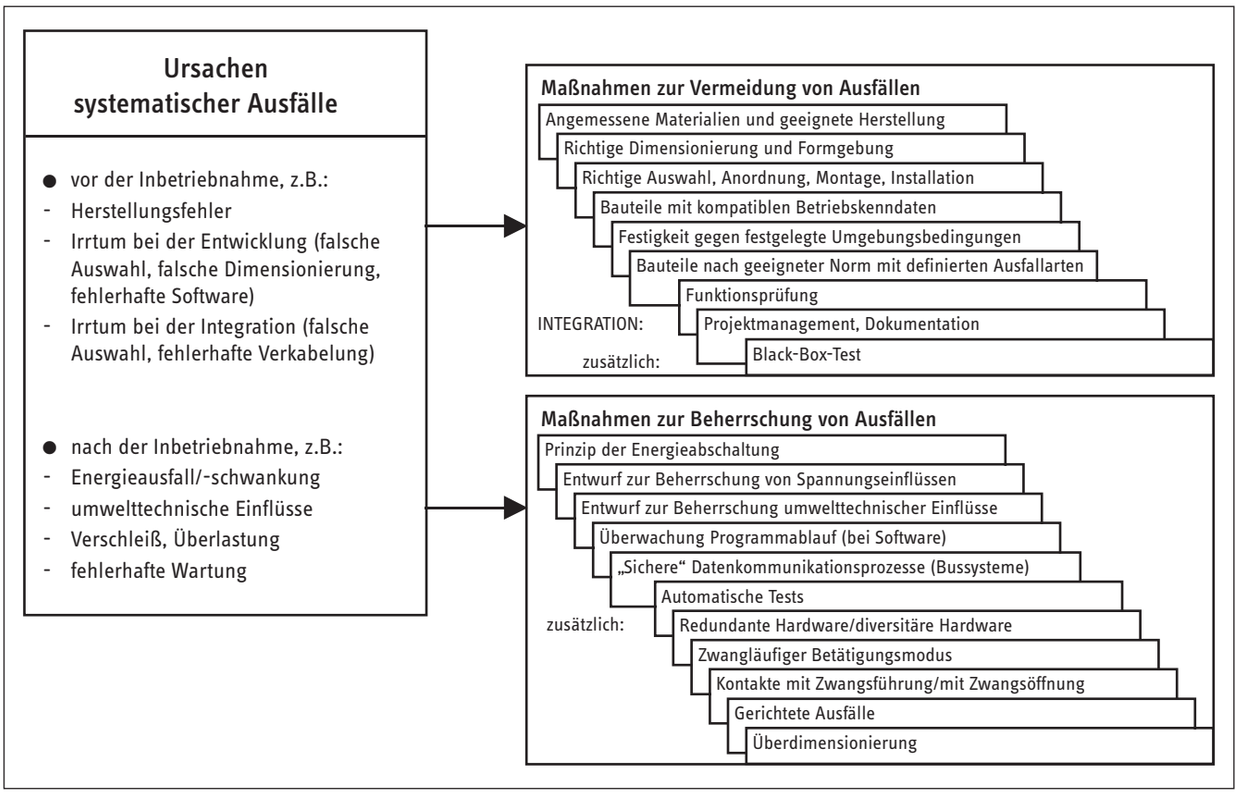
Systematische Ausfälle haben im Gegensatz zu zufälligen Bauteilausfällen Ursachen, die nur durch eine Änderung z.B. der Gestaltung oder des Herstellungsprozesses, der Betriebsverfahren oder der Dokumentation beseitigt werden können. Sie entstehen irgendwann im Laufe des Lebenszyklus eines Produktes,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

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

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

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

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



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

Beispiel 1:
Maßnahmen zur Beherrschung von Auswirkungen eines Energieausfalls

Bei der Gestaltung der sicherheitsbezogenen Teile von Steuerungen sind auch Störungen der Energieversorgung (elektrische Spannung, Luftdruck in der Pneumatik, Hydraulikdruck) zu berücksichtigen (siehe Abschnitt 5.2.8 und Anhang G der Norm). So können z.B. Spannungsausfall, Spannungsschwankungen und Über- bzw. Unterspannung den sicheren Zustand einer Maschine gefährden. Dies trifft insbesondere auf das Hochhalten von Lasten mit elektrischen und hydraulischen Antrieben (Vertikalachsen) zu. Solche Störungen können ihre Ursachen in Bauteilfehlern innerhalb der SRP/CS haben, dann werden ihre Auswirkungen auf den Performance Level in der Verifikation berücksichtigt. Liegen die Ursachen jedoch im Versorgungsnetz begründet oder wurde die Netz-Trenneinrichtung (Hauptschalter) der Maschine betätigt, so entziehen sich diese Vorfälle einer quantitativen Berücksichtigung und können nur als systematische Ausfälle - teilweise sogar als Betriebszustand - betrachtet werden, die vom SRP/CS beherrscht werden müssen, sodass der sichere Zustand erreicht und/oder aufrechterhalten wird. Die Anforderungen auf einen geringeren PL_r zu reduzieren, z.B. weil der Ausfall der Energieversorgung selten vorkommt, ist nicht zulässig, da die für die Risikobeurteilung relevanten Parameter S, F und P durch die Berücksichtigung eines Energieausfalls nicht verändert werden.

Beispiel 2:
Versagen von Pneumatik- bzw. Hydraulikventilen

DIN EN ISO 13849-2, Tabelle B.1 „Grundlegende Sicherheitsprinzipien der Pneumatik“ und Tabelle B.2 „Bewährte Sicherheitsprinzipien der Pneumatik“, legt u.a. fest, dass bei der Konstruktion und Herstellung von pneumatischen Bauteilen auf die *„Anwendung geeigneter Werkstoffe und Herstellungsverfahren“* und *„geeignetes Vermeiden einer Verunreinigung der Druckluft“* geachtet werden muss. Diese Anforderungen beziehen sich vor allem auf die Auswahl der Werkstoffe, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z.B. Spannungen, Haltbarkeit, Reibung, Verschleiß, Korrosion und Temperatur bzw. auf die Berücksichtigung von hoch wirksamer Filtration der Druckluft/Abscheidung von Feststoffen und Wasser. Weiterhin ist in Tabelle C.1 „Grundlegende Sicherheitsprinzipien der Hydraulik“ festgelegt, dass bei der Konstruktion von hydraulischen Bauteilen auch auf die *„richtige Dimensionierung und Formgebung“* geachtet werden muss: Dies bezieht sich z.B. vor allem auf Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Toleranzen und Herstellungsverfahren.

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

- Bei Pneumatikventilen mit Weichdichtungen können die Dichtungen durch chemische Einflüsse der Schmiermittel (Öl mit Additiven in der Druckluft, eingebracht durch Kompressor, Öler oder Initialschmierung) bei längerem Verbleiben in einer Schaltstellung quellen oder der Schmierfilm kann durch die Dichtkantenpressung kollabieren und somit die Haftkraft erhöhen.
- Bei Hydraulikventilen kann bei längerem Verbleiben in einer Schaltstellung sogenanntes Silting auftreten. Hierbei lagern sich während der Haltezeit zwischen den Schaltspielen feine Schmutzpartikeln im Dichtspalt ab und verursachen dadurch ein Klemmen des Ventilschiebers.

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

Beispiel 3:
Trennung sicherheitsbezogener von anderen Funktionen

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

Anschaulich lässt sich diese Anforderung am Beispiel der Erstellung von Anwendungssoftware darstellen. Die weitestgehende Art der Trennung von Standard-Anwendungssoftware und sicherheitsrelevanter Anwendungssoftware (SRASW, siehe Abschnitt 6.3) ist natürlich, diese mit getrennten Programmiersystemen (sogenannte Engineering-Suiten) zu erstellen und auf verschiedenen SPS (Speicherprogrammierbaren Steuerungen) ablaufen zu lassen. Insbesondere aus wirtschaftlichen Gründen wird man jedoch versuchen, die gesamte Anwendungssoftware mit nur einem Programmiersystem und ggf. in einem gemeinsamen Engineering-Ablauf zu erstellen. Dabei sind allerdings eine Vielzahl von Aspekten zu berücksichtigen; z.B. die Anforderung, dass sicherheitsrelevante Variablen, Ergebnisse oder Ausgänge nicht von nicht sicherheitsrelevanten Softwareteilen (Programm, Funktionsbaustein, Funktion/Anweisung u.Ä.) überschrieben werden dürfen. Verknüpfungen beider Welten sind zwar zulässig, jedoch nur unter Einhaltung festgelegter Konventionen. Dabei müssen sicherheitsrelevante Signale und Funktionen immer die Priorität behalten: So ist eine „ODER“-Verknüpfung beispielsweise keinesfalls erlaubt. Inzwischen unterstützen Softwareentwicklungswerkzeuge solche Ansätze und haben vorgegebene Funktionen und automatisch kontrollierende Regeln implementiert (in den Editoren und Compilern). Verknüpfungsfehler, die sich eventuell nur in unvorhersehbaren Betriebssituationen auswirken bzw. mit angemessenem Aufwand zur Abnahme/Inbetriebnahme nicht aufzudecken sind, können so sehr anwenderfreundlich verhindert werden.

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

6.1.3 Ergonomie

Die europäische Maschinenrichtlinie 98/37/EG (MRL) fordert im Anhang I Abschnitt 1.1.2d vom Maschinenhersteller, dass Belästigung, Ermüdung und psychische Belastungen der Maschinenbediener unter Berücksichtigung ergonomischer Prinzipien bereits bei der Konzeption der Maschine auf ein Minimum zu reduzieren sind. Dies gilt daher auch für die Schnittstellen zwischen dem Bediener einer Maschine/Maschinenanlage und den SRP/CS. Darunter fallen sowohl konkrete Schutzeinrichtungen wie z.B. eine Schutztür mit Positionsschalter als auch die Bedienung einer Sicherheitsfunktion, z.B. über Taster oder sogar über eine dafür geeignete Softwareoberfläche eines Displays.

Welche Bedeutung ergonomische Prinzipien für SRP/CS haben und dass nicht immer jede bestimmungsgemäße Verwendung oder vorhersehbare Fehlanwendung von SRP/CS bei der Konstruktion einer Maschine berücksichtigt wird, das zeigt der HVBG-Report „Manipulation von Schutzeinrichtungen an Maschinen“ [22] auf.

DIN EN ISO 13849-1 fordert daher die Verwendung ergonomischer Prinzipien und listet dazu in Abschnitt 4.8 eine Fülle hilfreicher Normen auf. Damit Maschinenkonstrukteure die Gestaltung der Mensch-Maschine-Schnittstelle der SRP/CS überprüfen können, wurde im BGIA die Checkliste „Ergonomische Maschinengestaltung“ entwickelt. Im Oktober 2006 wurden diese Checkliste und weitere Dokumente als BG-Informationen BGI 5048-1 und BGI 5048-2 veröffentlicht [23]. Konkreter behandelt werden u.a. handbediente Stellteile; Tastaturen, Tasten und Eingabegeräte; Displays und Anzeigen; optische Gefahrensignale und die Softwareergonomie von Bedienoberflächen. Eine Konstruktionshilfe bei der nutzergerechten Gestaltung von Bediensystemen für Maschinen bietet z.B. die VDI/VDE-Richtlinie 3850 [24].

6.2 Quantifizierung der Ausfallwahrscheinlichkeit

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

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

6.2.1 Vorgesehene Architekturen...

Die Struktur oder Architektur einer Sicherheitssteuerung bestimmt die Toleranz gegenüber Fehlern (Fehlertoleranz) und stellt das Gerüst dar, auf dem alle anderen quantifizierbaren Aspekte aufbauen, um schließlich den PL der sicherheitsbezogenen Teile von Steuerungen zu bilden. Die Erfahrungen des BGIA mit der Industrie seit 1985 bestätigen, dass es nur wenige Grundtypen von Sicherheitssteuerungen im Maschinenbau gibt, auf die sich der überwiegende Teil aller realisierten Steuerungen zurückführen lässt (bzw. auf Kombinationen dieser Grundtypen, siehe weiter unten): Dies sind das einkanalige ungetestete System mit unterschiedlich zuverlässigen Bauteilen am einen Ende des Spektrums, das im Mittelfeld durch Tests aufgewertet werden kann, und schließlich das zweikanalige hochwertig getestete System am anderen Ende. Systeme mit mehr als zwei Kanälen oder andere „exotische“ Strukturen sind im Maschinenbau extrem selten vertreten und können mit dem vereinfachten Verfahren nur bedingt bewertet werden. Meist reicht es aber selbst bei mehr als zwei Kanälen aus, die beiden zuverlässigsten zu berücksichtigen, um den PL mit dem vereinfachten Verfahren der vorgesehenen Architekturen hinreichend genau abzuschätzen. Daher werden Systeme mit mehr als zwei Kanälen in DIN EN ISO 13849-1 nicht betrachtet. Neben dieser „horizontalen“ Einteilung in verschiedene funktionale oder testende Kanäle ist meist auch eine „vertikale“ Einteilung in eine Sensorebene (Eingabegeräte, Input „I“), eine Verarbeitungsebene (Logik „L“) und eine Aktorebene (Ausgabegeräte, Output „O“) hilfreich.

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

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

6.2.2 ... und Kategorien

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

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

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

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

Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_d$ jedes Kanals	DC_{avg}	CCF
B	SRP/CS(en) und/oder ihre Schutzeinrichtungen sowie ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengebaut und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können. Grundlegende Sicherheitsprinzipien müssen verwendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	überwiegend durch die Auswahl von Bauteilen charakterisiert	niedrig bis mittel	keine	nicht relevant
1	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	überwiegend durch die Auswahl von Bauteilen charakterisiert	hoch	keine	nicht relevant

Tabelle 6.2:
(Fortsetzung)

Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_d$ jedes Kanals	DC_{avg}	CCF
2	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung getestet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Tests führen. Der Verlust der Sicherheitsfunktion wird durch den Test erkannt.	überwiegend durch die Struktur charakterisiert	niedrig bis hoch	niedrig bis mittel	Maßnahmen erforderlich, siehe Anhang F
3	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass: – ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und – wenn immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Sicherheitsfunktion führen.	überwiegend durch die Struktur charakterisiert	niedrig bis hoch	niedrig bis mittel	Maßnahmen erforderlich, siehe Anhang F
4	Die Anforderung von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass: – ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und – der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird. Wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hoher DC_{avg}). Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.	überwiegend durch die Struktur charakterisiert	hoch	hoch einschließlich der Fehleranhäufung	Maßnahmen erforderlich, siehe Anhang F

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

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

6.2.3 Kategorie B

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

- den zu erwartenden Betriebsbeanspruchungen (z.B. Zuverlässigkeit hinsichtlich ihres Schaltvermögens und ihrer Schalthäufigkeit),
- dem Einfluss des im Arbeitsprozess verwendeten Materials (z.B. aggressive chemische Substanzen, Stäube, Späne),
- anderen relevanten äußeren Einflüssen (z.B. mechanischen Erschütterungen, elektromagnetischen Störungen, Unterbrechungen oder Störungen der Energieversorgung)

standhalten können.

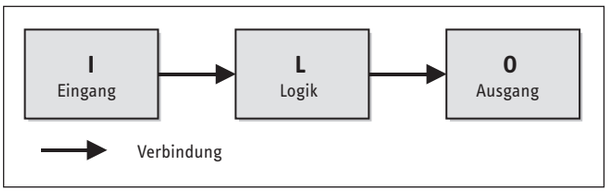
Diese allgemeinen Grundsätze lassen sich in den in Anhang C aufgeführten grundlegenden Sicherheitsprinzipien allgemein, aber auch technologiebezogen, darstellen. Die allgemeinen grundlegenden Sicherheitsprinzipien gelten dabei vollständig für alle Technologien, während die technologiebezogenen Prinzipien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

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

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

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

Abbildung 6.5:
Vorgesehene Architektur für Kategorie B und Kategorie 1



6.2.4 Kategorie 1

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

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

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

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

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

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

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

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

6.2.5 Kategorie 2

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

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

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

- den Betrieb zulassen, wenn keine Fehler erkannt wurden, oder
- einen Ausgang für die Einleitung geeigneter Steuerungsmaßnahmen erzeugen, wenn ein Fehler erkannt wurde. Wann immer möglich, muss dieser Ausgang einen sicheren Zustand einleiten. Dieser muss aufrechterhalten bleiben, bis der Fehler behoben ist. Ist die Einleitung eines sicheren Zustandes nicht möglich (z.B. durch Verschweißen des Kontaktes eines Schaltgliedes), muss der Ausgang die Warnung vor der Gefährdung bereitstellen.

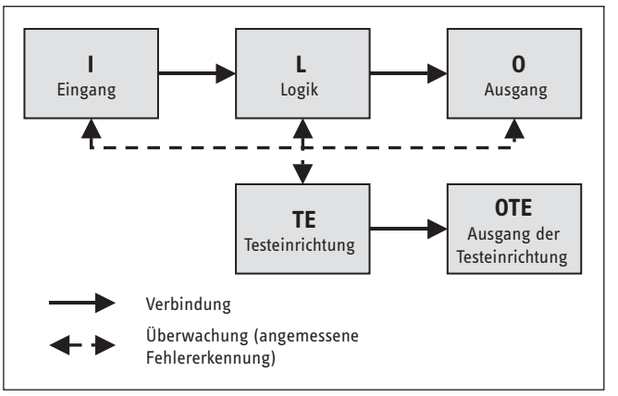
Für die vorgesehene Architektur der Kategorie 2 (Abbildung 6.6) berücksichtigt die Berechnung der $MTTF_d$ und DC_{avg} nur die Blöcke des Funktionskanals (d.h. I, L und O) und nur indirekt die $MTTF_d$ der Blöcke des Testkanals (d.h. TE und OTE). Für die $MTTF_d$ des Funktionskanals sind Werte von niedrig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

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

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

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

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



6.2.6 Kategorie 3

Zusätzlich zu den Anforderungen für Kategorie B (z.B. Verwendung grundlegender Sicherheitsprinzipien) müssen SRP/CS der Kategorie 3 bewährte Sicherheitsprinzipien verwenden und so gestaltet werden, dass ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion führt. Wann immer in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

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

Die Forderung nach Einfehlersicherheit bedeutet nicht zwangsweise eine Realisierung als zweikanaliges System, da z.B. auch einkanalige Teile ohne gefahrbringendes Ausfallpotenzial (fehlersicheres Design) sicher gegen Einzelfehler sein können. Dasselbe gilt für Systeme mit hochwertiger Überwachung, die durch einen eigenen Abschaltpfad eine Fehlerreaktion so schnell einleiten, dass ein gefährlicher Zustand vermieden wird. Trotzdem werden Kategorie-3-Systeme überwiegend zweikanalig realisiert, weshalb auch die zugehörige vorgesehene Architektur entsprechend gewählt wurde (Abbildung 6.7, siehe Seite 50). Eine rein „logische Zweikanaligkeit“, z.B. durch redundante Software auf einkanaliger Hardware, wird allerdings in der Regel nicht einfehlersicher gegen Hardwareausfälle sein.

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

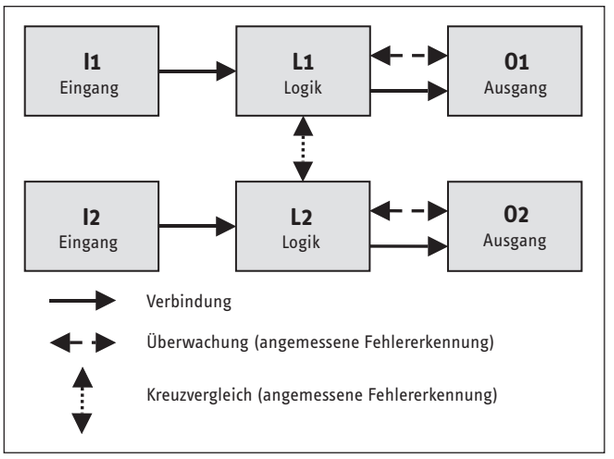
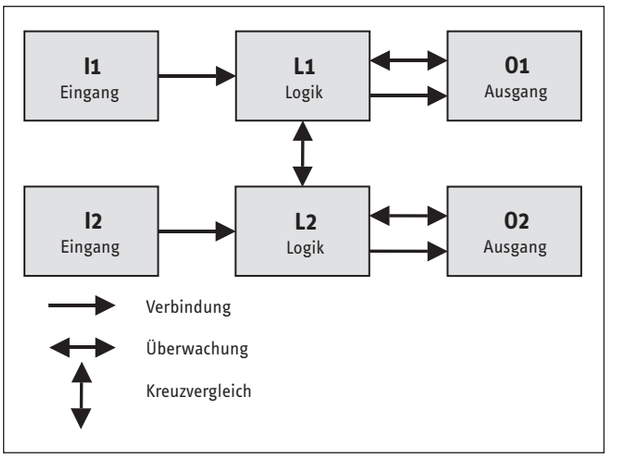


Abbildung 6.8:
Vorgesehene Architektur für Kategorie 4



6.2.7 Kategorie 4

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

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

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

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

6.2.8 Blöcke und Kanäle

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

- Die Blöcke sollen in abstrakter Form alle Steuerungselemente abbilden, die sich auf die Ausführung der Sicherheitsfunktion beziehen.
- Wird die Sicherheitsfunktion in mehreren redundanten Kanälen ausgeführt, sollen diese in separaten Blöcken dargestellt werden. Dies spiegelt die Tatsache wider, dass bei Ausfall eines Blocks die Ausführung der Sicherheitsfunktion durch die Blöcke des anderen Kanals nicht beeinträchtigt wird.
- Die Aufteilung der Blöcke innerhalb eines Kanals ist eher willkürlich; zwar schlägt DIN EN ISO 13849-1 pro Kanal drei Blöcke vor (Eingangsebene I, Logikebene L und Ausgangsebene O), dies ist aber mehr als Verständnishilfe gedacht. Weder die genaue Grenze zwischen I, L und O noch die Anzahl der Blöcke in einem Kanal haben signifikante Auswirkungen auf die in Form des PL berechnete Ausfallwahrscheinlichkeit.
- Für jede sicherheitsrelevante Hardwareeinheit soll die Blockzugehörigkeit eindeutig festgelegt sein (z.B. als Stückliste). Dies erlaubt die Berechnung der mittleren Zeit bis zum gefahrbringenden Ausfall ($MTTF_d$) des Blocks, basierend auf der $MTTF_d$ der Hardwareeinheiten, die zu diesem Block gehören (z.B. durch die Ausfalleffektanalyse FMEA oder das „Parts Count“-Verfahren, siehe 6.2.13).
- Nur rein zu Testzwecken verwendete Hardwareeinheiten, deren Ausfall die Ausführung der Sicherheitsfunktion in den verschiedenen Kanälen nicht direkt beeinträchtigen kann, können als separate Blöcke eines zusätzlichen Testkanals zusammengefasst werden.

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

6.2.9 Sicherheitsbezogenes Blockdiagramm

Das sicherheitsbezogene Blockdiagramm ist dem bekannteren Zuverlässigkeitsblockdiagramm [25] entlehnt. Gemeinsam ist beiden das Prinzip, dass die (Sicherheits-)Funktion so lange ausgeübt werden kann, wie von links nach rechts entlang der funktionalen Verbindungslinien eine Kette nicht gefährlich ausgefallener Blöcke besteht. Das sicherheitsbezogene Blockdiagramm stellt aber zusätzlich Testmechanismen dar, z.B. den Kreuzvergleich redundanter Kanäle oder Tests durch separate Testeinheiten. Ein allgemeines Beispiel eines sicherheitsbezogenen Blockdiagramms ist in Abbildung 6.9 gezeigt.

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

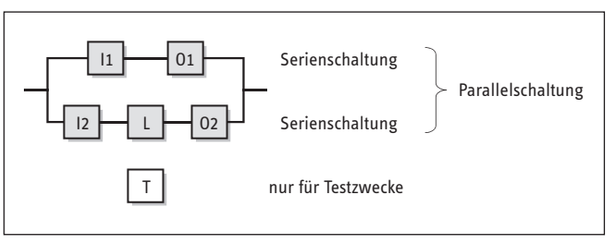
- Die Serienschaltung von Blöcken als sogenannter „Kanal" (z.B. I, L und O) bringt zum Ausdruck, dass der Ausfall eines Blocks zu einem Ausfall der gesamten Kette führen kann. Fällt z.B. eine Hardwareeinheit in einem Kanal gefährlich aus, kann der gesamte Kanal die Sicherheitsfunktion nicht weiter ausführen.

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

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

Die Definition der Blöcke und Kanäle geht einher mit der Bestimmung der Kategorie und ist der erste Schritt bei der quantitativen Bestimmung des PL. Dazu werden weitere Kennwerte benötigt: die Bewertung der Bauteilzuverlässigkeit ($MTTF_d$), der Tests (DC_{avg}) und der Relevanz von Ausfällen infolge gemeinsamer Ursache (CCF).

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



6.2.10 Fehlerbetrachtungen und Fehlerausschluss

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

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

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

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

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

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

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

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

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

Fehlerausschlüsse sind bei entsprechenden Voraussetzungen auch für Komponenten möglich, z.B. für die elektrischen Öffnerkontakte und die mechanische Betätigung von elektromechanischen Positionsschaltern oder Not-Halt-Geräten. Für diese Komponenten ist bei Fehlerausschluss keine Berücksichtigung von Ausfallraten ($MTTF_d$) und Überwachungsmaßnahmen *(DC)* notwendig.

6.2.11 Mittlere Zeit bis zum gefahrbringenden Ausfall – $MTTF_d$

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

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

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

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

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

6.2.12 Datenquellen für Einzelbauteile

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

6.2.13 FMEA versus „Parts Count"-Verfahren

Sind die $MTTF_d$-Werte aller sicherheitsrelevanten Bauteile zusammengetragen, helfen einige simple Regeln, daraus den $MTTF_d$-Kennwert der Steuerung zu berechnen. Dabei gibt es verschiedene Methoden – aufwendig durch eine genaue Ausfalleffektanalyse FMEA (Failure Modes and Effects Analysis) oder schnell und einfach nach dem „Parts Count"-Verfahren mit ein paar Abschätzungen zur sicheren Seite. Dies beginnt schon bei dem kleinen Unterschied zwischen *MTTF* und $MTTF_d$: Wie groß ist der gefährliche Anteil der Ausfälle eines bestimmten Bauelements? In einer aufwendigen FMEA können alle denkbaren Ausfallarten aufgelistet, jeweils als „ungefährlich" oder „gefahrbringend" bewertet und in der anteiligen Häufigkeit ihres Auftretens geschätzt werden. Da die Auswirkungen eines Bauteilausfalls auf den Block über die sichere oder unsichere Ausfallrichtung entscheiden, sind unter Umständen detaillierte Analysen des von einem Ausfall hervorgerufenen Effekts nötig. Dafür entpuppen sich vielleicht mehr Ausfallarten als „sicher" als bei einer vereinfachten Bewertung, wie DIN EN ISO 13849-1 sie vorschlägt: Beim „Parts Count"-Verfahren wird mit einem konservativen Ansatz pauschal davon ausgegangen, dass sich ungefährliche und gefahrbringende Anteile die Waage halten. Daher wird die $MTTF_d$ hier immer als doppelt so groß angenommen wie die *MTTF* – sofern keine genaueren Informationen vorliegen. Grundlage ist wieder das Prinzip des statistischen Mittels, d.h. eine zu günstige Bewertung eines Bauelements wird durch eine zu pessimistische eines anderen Bauelements wettgemacht. Es ist durchaus möglich, das „Parts Count"-Verfahren und eine FMEA zu kombinieren. Dort, wo die Werte allein durch „Parts Count" zu einer ausreichend kleinen *PFH* führen, muss keine FMEA vorgenommen werden. Gelingt es jedoch nicht, dann ist insbesondere an den Bauteilen, die schlechtere $MTTF_d$-Werte aufweisen, eine Untersuchung der Ausfallrichtungen hilfreich, z.B. durch eine partielle FMEA. Weitere Erläuterungen zu diesem Thema finden sich in Anhang B.

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

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

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

Tabelle 6.3:
Klasseneinteilung der $MTTF_d$ jedes Kanals

$MTTF_d$ für jeden Kanal	
Bezeichnung	Bereich
nicht angemessen	0 Jahre ≤ $MTTF_d$ < 3 Jahre
niedrig	3 Jahre ≤ $MTTF_d$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_d$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_d$ ≤ 100 Jahre
nicht zulässig	100 Jahre < $MTTF_d$

Weniger als drei Jahre mittlere (nicht garantierte!) Lebensdauer wird für Komponenten der Sicherheitstechnik als nicht angemessen betrachtet. Mehr als 100 Jahre dürfen nicht in Rechnung gestellt werden, um die Bauteilzuverlässigkeit gegenüber den anderen wichtigen Einflussgrößen wie Struktur oder Tests nicht überzubewerten. Ergeben sich tatsächlich für einen Kanal weniger als drei Jahre, sollten die Bauteile durch solche mit höherer Zuverlässigkeit ausgetauscht werden, da sonst noch nicht einmal PL a erreicht werden kann. Mehr als 100 Jahre mittlere Lebensdauer sind nicht unüblich, tragen aber wegen der „Kappung" nicht mehr zum PL bei, da in der Bauteilzuverlässigkeit bereits der Höchstwert von 100 Jahren in Rechnung gestellt wird.
Sind mehrere Kanäle an einer Steuerung beteiligt, so ist zunächst nicht klar, welcher Wert stellvertretend für das ganze System herangezogen werden soll. Natürlich könnte man hier vorsichtigerweise den kleineren Wert nehmen, zu immer noch sicheren, aber besseren Ergebnissen führt allerdings folgende Mittelungsformel (C1 und C2 bezeichnen hierbei die beiden Kanäle, die symmetrisiert werden):

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

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

6.2.14 Diagnosedeckungsgrad von Test- und Überwachungsmaßnahmen – *DC*

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

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

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

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

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

- Die Erkennung eines gefahrbringenden Ausfalls ist nur der Anfang. Zum erfolgreichen Abschluss eines Tests ist die Einleitung eines sicheren Zustands, aus dem heraus keine Gefährdung mehr besteht, erforderlich. Dazu gehört ein wirksamer Abschaltpfad, was z.B. bei einkanalig getesteten Systemen (Kategorie 2) dazu führt, dass ein zweites Abschaltelement vorhanden sein muss. Dieses ist nötig, um den sicheren Zustand einzuleiten bzw. aufrechtzuerhalten, wenn der Test ein Versagen des regulären Abschaltelements (Block „O“ im sicherheitsbezogenen Blockdiagramm) festgestellt hat.
- Sowohl das Auslösen eines Tests, dessen Ausführung als auch die erforderliche Abschaltung sollten bevorzugt automatisch von SRP/CS durchgeführt werden. Nur in Ausnahmefällen erscheint es angeraten, hier auf eine manuelle Intervention, z.B. des Maschinenbedieners, angewiesen zu sein. Denn die Praxis zeigt leider oft, dass die erforderlichen Maßnahmen aus Bequemlichkeit, wegen Arbeitsdrucks oder fehlerhafter Information bzw. Organisation nicht ausreichend umgesetzt werden. Hier sind ein hoher organisatorischer Aufwand und Disziplin nötig, um manuelle Tests wirksam umzusetzen. Gleichwohl berücksichtigt die Bestimmung des *DC* für zweikanalige Systeme Fehleraufdeckung bei Anforderung der Sicherheitsfunktion, d.h., es werden nicht nur automatisch ausgelöste Tests in programmierbarer Elektronik betrachtet. Gerade bei elektromechanischen Bauteilen, z.B. Relais oder Schützen, kann eine Erkennung des Fehlers „Nichtabfall“ üblicherweise nur bei Anforderung der Sicherheitsfunktion erfolgen. Für die Fehleraufdeckung bei Anforderung muss die Häufigkeit der Anforderung der Sicherheitsfunktion berücksichtigt werden.
- Ein weiterer Aspekt ist die Frage nach der notwendigen Testhäufigkeit. Ein Test, der zu selten ausgeführt wird, wird unter Umständen durch das Eintreten eines Gefährdungsereignisses überholt und bietet damit nur trügerische Sicherheit. Als Faustregel gilt: Die Testhäufigkeit konkurriert immer mit anderen Häufigkeiten, daher kann eine ausreichende Häufigkeit nicht generell genannt werden. In zweikanaligen Systemen der Kategorien 3 und 4 steht die Testhäufigkeit in Konkurrenz zur Häufigkeit des Auftretens eines zweiten gefahrbringenden Ausfalls. Denn erst, wenn der zweite Kanal ausfällt, bevor ein Test den Ausfall des ersten bemerkt hat, besteht die Gefahr der Nichtausführung der Sicherheitsfunktion – Kategorie-4-Systeme tolerieren gemäß Definition sogar die Anhäufung unerkannter Fehler. In zweikanaligen Systemen hat sich ein Test einmal pro Schicht in der Praxis bewährt. Anders ist es beim einkanalig getesteten System der Kategorie 2: Hier muss der Test erfolgreich sein, bevor die nächste Anforderung der Sicherheitsfunktion – also eine potenzielle Gefährdung – erfolgt. Hier steht die Testhäufigkeit also in Konkurrenz zur Häufigkeit der Anforderung der Sicherheitsfunktion. In beiden Fällen wird ein Faktor von 100 als ausreichend angesehen, also eine mindestens 100-mal höhere Testrate als die gefahrbringende Ausfallrate λ_d (= $1/MTTF_d$) bzw. als die mittlere Anforderungsrate der Sicherheitsfunktion. Bis hinunter zu einem Faktor von 25 ergibt sich demgegenüber eine maximale Erhöhung der Ausfallwahrscheinlichkeit von ca. 10 %. Darunter ist es wesentlich von der Synchronisation von Anforderung und Testung abhängig, ob die Testung überhaupt zur Geltung kommt. Falls in einkanalig getesteten Systemen allerdings die Tests so schnell ausgeführt werden, dass der sichere Zustand erreicht wird, bevor es zu einer Gefährdung kommt, dann werden keine Bedingungen an die Testhäufigkeit gestellt.

- Ein weiterer Punkt ist die Zuverlässigkeit der Testeinrichtung selbst: Grundsätzlich sollte gelten, dass die Testeinrichtung nicht vor der von ihr überwachten Komponente ausfallen sollte. Andererseits ist es aber auch nicht effektiv, viel mehr in die Zuverlässigkeit der Testeinrichtung zu investieren als in die Sicherheitseinrichtungen, die die eigentliche Sicherheitsfunktion ausführen. DIN EN ISO 13849-1 hält sich daher mit Anforderungen an die Zuverlässigkeit der Testeinrichtungen zurück. Bei den Kategorien 3 und 4 wird auf die Einfehlertoleranz vertraut, da inklusive des Ausfalls der Testeinrichtung insgesamt drei gefahrbringende Ausfälle notwendig sind, bevor die Sicherheitsfunktion nicht mehr ausgeführt wird. Dass dieser Fall unbemerkt auftreten kann, wird als extrem unwahrscheinlich und daher nicht entscheidend angesehen. Bei Kategorie 2 gibt es zumindest bei der vereinfachten PL-Bestimmung anhand des Säulendiagramms eine Nebenbedingung, die bei der Berechnung der „Kategorie-2-Säulen" zugrunde gelegt wurde: Hier sollte die gefahrbringende Ausfallrate der Testeinrichtung nicht mehr als doppelt so hoch sein wie die gefahrbringende Ausfallrate der davon überwachten Komponenten - im Zweifel lässt sich dieser Vergleich kanalweise durchführen, sodass der $MTTF_d$-Wert des gesamten Testkanals nicht kleiner sein sollte als der halbe $MTTF_d$-Wert des Funktionskanals.

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

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

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

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

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

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

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

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

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

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

6.2.15 Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache – CCF

Der letzte Parameter, der bei der vereinfachten Quantifizierung der Ausfallwahrscheinlichkeit eine Rolle spielt, betrifft Ausfälle infolge einer gemeinsamen Ursache CCF (Common Cause Failure). Dabei handelt es sich um korrelierte gefahrbringende Ausfälle, z.B. in beiden Kanälen eines redundanten SRP/CS, die auf eine einzige Ursache zurückzuführen sind. Beispiele hierfür sind ungünstige Umgebungsbedingungen oder Überbelastungen, die beim Entwurf der Steuerung nicht ausreichend berücksichtigt wurden. Bei unzureichender Trennung der Kanäle kann es dann zu gefahrbringenden Folgefehlern kommen, die die beabsichtigte Einfehlertoleranz außer Kraft setzen. Die Relevanz dieser Effekte in einem konkreten System lässt sich nur schwer quantitativ abschätzen (siehe auch Anhang F). Im Anhang D der DIN EN 61508-6 [27] wird dazu das sogenannte Beta-Faktor-Modell bemüht, das die Ausfälle gemeinsamer Ursache als β mal λ_d ins Verhältnis setzt zur gefahrbringenden Ausfallrate eines Kanals λ_d. Ohne eine genaue FMEA kann β für reale SRP/CS allerdings bestenfalls geschätzt werden. DIN EN ISO 13849-1 bietet dazu eine Checkliste aus acht wichtigen Gegenmaßnahmen an, die mit 5 bis 25 Punkten bewertet werden:

- physikalische Trennung der Signalpfade unterschiedlicher Kanäle (15 Punkte)

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

- Schutz gegen mögliche Überbelastungen (15 Punkte) und Verwendung bewährter Bauteile (5 Punkte)
- Ausfalleffektanalyse in der Entwicklung zur Aufdeckung potenzieller Ausfälle infolge gemeinsamer Ursache (5 Punkte)
- Schulung der Konstrukteure/Monteure hinsichtlich CCF und ihrer Vermeidung (5 Punkte)
- Schutz vor durch Verunreinigung (mechanische und fluidische Systeme) bzw. elektromagnetische Beeinflussung (elektrische Systeme) ausgelöste Ausfälle infolge gemeinsamer Ursache (25 Punkte)
- Schutz vor durch ungünstige Umgebungsbedingungen ausgelöste Ausfälle infolge gemeinsamer Ursache (10 Punkte)

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

6.2.16 Vereinfachte PL-Bestimmung durch das Säulendiagramm

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

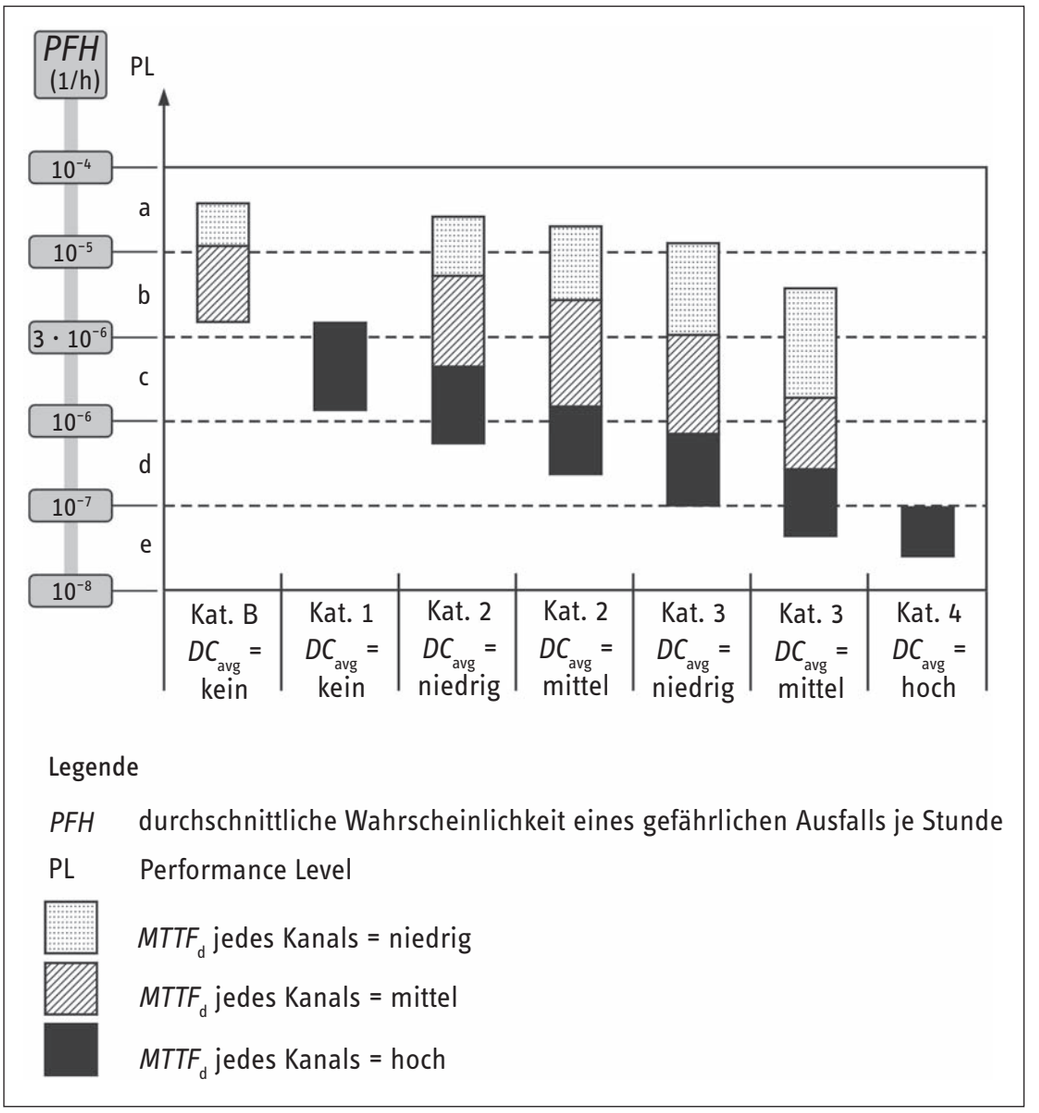


Abbildung 6.10: Säulendiagramm zur vereinfachten PL-Bestimmung aus der Kategorie (inklusive Maßnahmen gegen CCF), dem DC_{avg} und der $MTTF_d$

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

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

- Als Gebrauchsdauer der SRP/CS wurden 20 Jahre unterstellt, innerhalb derer die Bauteilzuverlässigkeiten durch konstante Ausfallraten beschrieben bzw. angenähert werden können. Durch Verwendung stark verschleißbehafteter Bauteile (siehe T_{10d}-Wert in Anhang D) oder aus anderen Gründen kann die tatsächliche Gebrauchsdauer die angenommenen 20 Jahre unterschreiten. Dann ist durch vorsorglichen Austausch der betroffenen Bauteile oder der betroffenen SRP/CS die Anwendung des Säulendiagramms zu rechtfertigen. Dem Anwender sind diese Informationen in geeigneter Form mitzuteilen, zum Beispiel über die Benutzerinformationen und durch Kennzeichnung auf den SRP/CS.

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

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

- Mit Kategorie B kann maximal PL = b erreicht werden.

- Mit Kategorie 1 kann maximal PL = c erreicht werden.

- Mit Kategorie 2 kann maximal PL = d erreicht werden.

- Mit Kategorie 3 oder 4 ist auch PL = e erreichbar.

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

6.2.17 Bussysteme als „Verbindungsmittel“

Die einzelnen Blöcke Eingabeeinheit, Logik und Ausgabeeinheit einer vorgesehenen Architektur müssen nicht nur logisch, sondern auch physikalisch miteinander verbunden werden. Dazu definiert die Norm sogenannte „Verbindungsmittel“, die als Teil der SRP/CS betrachtet werden. Der Name Verbindungsmittel erscheint zunächst aus der Sicht eines Experten der Elektro- oder Fluidtechnik merkwürdig, ist aber der Oberbegriff für elektrische sowie fluidtechnische Leitungen und sogar für mechanische Stößel usw. Somit gelten alle Anforderungen der Norm auch für diese „Verbindungsmittel“. Unter dem Aspekt der Fehlerbetrachtung ist also z.B. ein Leitungskurzschluss ein anzunehmender Fehler. Wie aber sieht es mit dem Einsatz von Bussystemen zur Übertragung von sicherheitsrelevanten Informationen aus? Natürlich kann es nicht Gegenstand der Norm sein, ein solch komplexes Thema detailliert zu beleuchten, zumal es bereits berufsgenossenschaftliche Prüfgrundsätze (GS-ET-26 [28]) und eine Norm (DIN EN 61784-3 [29]) zu diesem Thema gibt. Bussysteme, die den in diesen Publikationen beschriebenen Anforderungen genügen, lassen sich ohne Weiteres auch unter dem Dach der DIN EN ISO 13849-1 einsetzen. Auf dem Markt gibt es bereits mehrere Bussysteme, die für den sicherheitstechnischen Einsatz geeignet sind.

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

Werten hinzugerechnet werden. Umfassende Informationen zu Bussystemen für die Übertragung sicherheitsrelevanter Informationen gibt z.B. [30].

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

6.3 Entwicklung sicherheitsbezogener Software

„Der Programmierer einer Software, der jahrelange Erfahrung hat, macht selbstverständlich keine Fehler mehr", diese oder ähnliche Aussagen sind oft zu hören. Dabei ist gerade diese Selbstüberschätzung der größte Fehler, den man machen kann. Software ist in der Regel kompliziert und deshalb gibt es auch im Gegensatz zur Hardware zunehmend mehr Versagen durch Softwarefehler. Wie oft wundert sich der „Power-User" am PC, dass ein Peripheriegerät nicht mehr funktioniert, wie oft war es dann ein Teil der Software, der sich mit einem anderen, z.B. Treiber, nicht verträgt? Dagegen sind Hardwarefehler eher selten. Normale, das heißt einfache Software für einfache Funktionen hat nach [31] etwa 25 Fehler pro 1 000 Programmzeilen. Gute Software hat nach [31] etwa zwei bis drei Fehler pro 1 000 Programmzeilen und die Software im Space-Shuttle hat (laut NASA) weniger als einen Fehler pro 10 000 Zeilen. Was bedeutet das in der Praxis: Ein Mobiltelefon hat bis zu 200 000 Programmzeilen und damit bis zu 600 Softwarefehler. Ein PC-Betriebssystem hat 27 Millionen Programmzeilen und damit bis zu 50 000 Fehler, das Space-Shuttle bis zu 300 Fehler und die Software für das Verteidigungssystem SDI bis zu 10 000 Fehler. Diese Programmfehler „schlummern" in den Produkten und werden sich unter bestimmten Bedingungen und in bestimmten Situationen auf die Funktion auswirken. Wie keine zweite Technologie übernimmt Software eine höhere Verantwortung als je zuvor und damit also auch ihr Programmierer.

Als eine der wesentlichen Neuerungen in der Revision der DIN EN ISO 13849-1 wurden die schon im Anwendungsbereich der DIN EN 954-1 einbezogenen programmierbaren SRP/CS erstmals mit Anforderungen an die Software und deren Entwicklung ausgestattet. Um es vorweg deutlich herauszustellen: Die Anforderungen in Abschnitt 4.6 der Norm ermöglichen es, sicherheitsbezogene Software für alle SRP/CS im Maschinensektor und für alle erforderlichen Performance Level von a bis e zu entwickeln. Dieser Abschnitt richtet sich in erster Linie an Anwendungsprogrammierer, die Sicherheitsfunktionen für eine Maschine, z.B. in einer applikationsorientierten Sprache auf einer speicherprogrammierbaren Steuerung (SPS), entwickeln. Für Entwickler von SRESW (Safety-Related Embedded Software – sicherheitsbezogene eingebettete Software), also Firmware oder Softwarewerkzeuge für elektronische Sicherheitskomponenten, ist dagegen der Neuigkeitswert dieser Anforderungen in DIN EN ISO 13849-1 nicht so hoch. Solche „Embedded Software"-Entwicklungen für die meist zertifizierten Komponenten unterliegen oft auch den sehr komplexen Anforderungen der für IEC-Normen zur Funktionalen Sicherheit verbindlichen Sicherheitsgrundnorm DIN EN bzw. IEC 61508-3 [32] (und aller weiteren sieben Teile).

Die Grundgedanken dieses Abschnitts können auf beide Softwaretypen bezogen werden. Einzelne Anforderungen werden aber eher für Anwendungsprogrammierer von SRASW (Safety-Related Application Software – sicherheitsbezogene Anwender-Software) konkretisiert. Dahingegen zeigt das Beispiel der Steuerung einer Planschneidemaschine in Abschnitt 6.5 die Entwicklung einer SRESW.

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

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

6.3.1 Software ohne Fehler ...

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

Um eine gute Qualität sicherheitsbezogener Software zu erreichen, ist es nahe liegend, entsprechende aktuelle und bewährte Entwicklungsmodelle des „Software Engineering" aufzugreifen. Für sicherheitsbezogene Systeme wird dabei meist auf das sogenannte „V-Modell" referenziert [32]. Da das aus der Literatur bekannte V-Modell eher für sehr komplexe Software zum Einsatz kommt, wird dieses Entwicklungsmodell in DIN EN ISO 13849-1, Abschnitt 4.6.1, nur in einer vereinfachten Form (Abbildung 6.11) gefordert. Diese wird für die Bedingungen der sicherheitsbezogenen SRP/CS im Maschinensektor und dort speziell für die Entwicklung von SRASW als praxisgerecht und zielführend bewertet. Das eigentliche Ziel dabei ist es, lesbare, verständliche, testbare und wartbare Software zu erhalten. Diese Anforderungen werden von einem Programmierer, der üblicherweise nicht sicherheitsrelevante Software erstellt, als mühsam empfunden, geben ihm aber andererseits die Bestätigung, die Software hinreichend gut entwickelt zu haben.

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

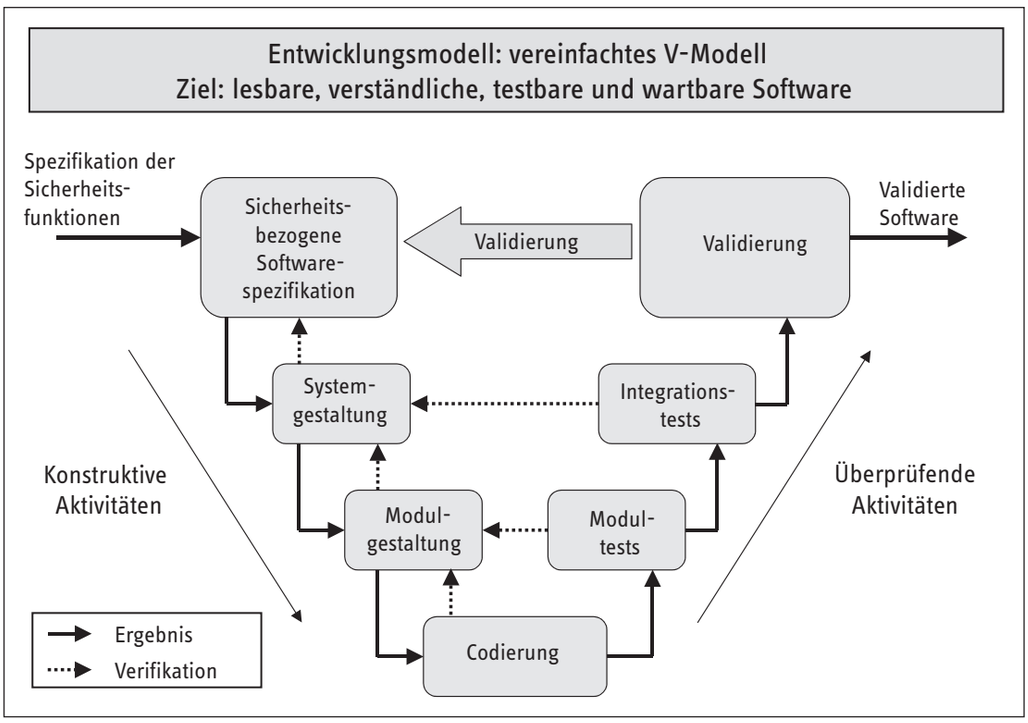


Abbildung 6.11: Vereinfachtes V-Modell für die Entwicklung sicherheitsbezogener Software

Ergebnis

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

Verifikation

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

Validierung

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

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

6.3.2 Schnittstelle zur Gesamtsicherheit: Softwarespezifikation

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

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

dargestellt.

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

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

Die gesamte Sicherheit einer Maschine bzw. Maschinenanlage wird durch alle sicherheitsbezogenen Teile der Steuerung und deren Funktionen (Komponenten aller Technologien, Elektronik, Software) gewährleistet. Hier ist also eine Beschreibung der Sicherheit für die Maschine bzw. Maschinenanlage in Form einer Spezifikation notwendig. Das Dokument muss nicht Hunderte von Seiten umfassen, sondern kann sich durchaus in verständlicher

Form auf das Wesentliche beschränken. Nach den Festlegungen zur Gesamtheit der Maschine bzw. Maschinenanlage wird es eine Teilmenge von Arbeiten für den Programmierer geben. Die Softwarespezifikation ist damit Teil des Gesamtkonzepts und folglich als „Vertrag“ mit einem „Unterauftragnehmer“, dem Programmierer, zu bewerten.

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

6.3.3 System- und Modulgestaltung für das „sicherheitsbezogene Pflichtenheft“

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

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

6.3.4 Endlich programmieren

Nun freut sich der Programmierer: Endlich geht es zur eigentlichen Codierung. Im Sinne der Fehlervermeidung sind hierbei drei Dinge zu beachten:

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

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

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

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

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

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

6.3.6 Struktur der normativen Anforderungen

Nachdem der Entwicklungsprozess skizziert ist, werden normative Anforderungen an die Software selbst, an die benutzten Entwicklungswerkzeuge sowie an die Entwicklungsaktivitäten beschrieben. Diese Anforderungen tragen ebenfalls zur Fehlervermeidung bei. Der dazu erforderliche Aufwand soll - ähnlich wie bei der Hardware der programmierbaren SRP/CS – der jeweils notwendigen Risikominderung entsprechend angemessen sein. Daher werden die Anforderungen bzw. deren Wirksamkeit mit zunehmendem PL_r sinnvoll gesteigert. DIN EN ISO 13849-1 nennt aber keine Minimalanforderungen, die für jede Software - unabhängig vom PL - notwendig wären.

Abbildung 6.12 zeigt, dass es sowohl bei SRASW als auch bei SRESW für alle PL zunächst ein geeignetes Bündel von Basismaßnahmen gibt. Diese Basismaßnahmen genügen für die Entwicklung von Software für PL a oder b. Für Software, die in SRP/CS für PL c bis e eingesetzt wird, gelten neben den Basismaßnahmen zusätzliche fehlervermeidende Maßnahmen. Letztere sind für PL c mit geringerer Wirksamkeit, für PL d mit mittlerer Wirksamkeit und für PL e mit höherer Wirksamkeit gefordert. Unabhängig davon, ob die Software nur in einem oder in beiden Kanälen einer beliebigen Kategorie mitwirkt: Als Maßstab für die Anforderungen gilt immer der PL_r der realisierten Sicherheitsfunktion(en).

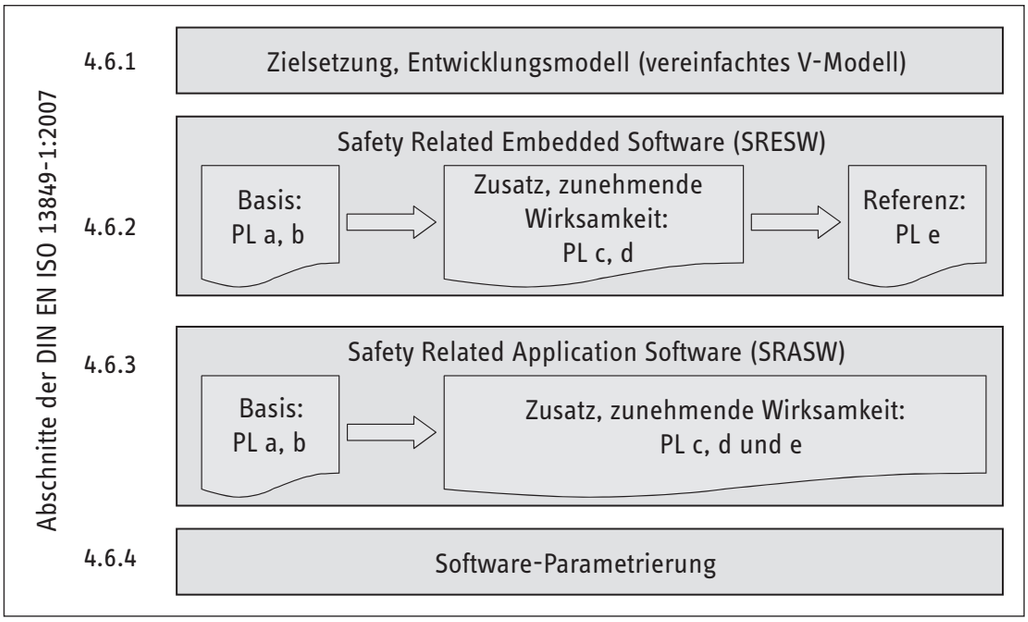


Abbildung 6.12: Abstufung der Anforderungen an sicherheitsbezogene Software

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

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

- Redundante SRP/CS, von denen nur ein Kanal programmierbar ist: Obwohl die programmierbare Elektronik nur einen Kanal darstellt, entspricht die Gesamtstruktur der Kategorie 3 oder 4. Mit diesen Strukturen werden häufig Sicherheitsfunktionen höherer PL_r wie z.B. d oder e realisiert. Dementsprechend gelten die Anforderungen des höchsten PL_r auch für die Software dieses einen Kanals (siehe auch Abschnitt 6.3.10).

- Verwendung von Standard-SPS: Die Schaltungsbeispiele in diesem BGIA-Report (siehe Kapitel 8, Seite 85 ff.) demonstrieren, dass sicherheitsbezogene Steuerungen prinzipiell auch mit Standard-SPS aufgebaut werden können. Es dürfte nur bei PL e sehr schwer sein, für die Hardware der SPS den erforderlichen hohen Diagnosedeckungsgrad *DC* (mindestens 99 %) zu erreichen – sofern diese Diagnose durch die SRASW realisiert werden muss. Für PL a bis d werden die Anforderungen an die Standard-SPS im Abschnitt 6.3.10 beschrieben. Zusätzlich muss der Anwendungsprogrammierer die Anforderungen zur Fehlervermeidung bei SRASW (Abschnitte 4.6.1 und 4.6.3 der Norm) entsprechend des PL_r erfüllen.

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

6.3.7 Passende Softwarewerkzeuge

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

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

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

- Geeignete Programmiersprachen:
  Für SRASW werden applikationsorientierte Sprachen, z.B. gemäß DIN EN 61131-3 [33], empfohlen. Selbst diese Sprachen sind bereits über das notwendige Maß hinaus sehr umfangreich und enthalten teilweise fehlerträchtige Konstrukte. Daher sollte der Programmierer die Syntax nur eingeschränkt einsetzen. Entsprechende Sprachteilmengen werden meist durch das Werkzeug vorgegeben.

- Programmierrichtlinien:
  Zur Codierung der Softwarefunktionen sind geeignete Programmierrichtlinien zu beachten [34; 35]. Dies sollten bestehende und akzeptierte Regeln einer anerkannten Organisation sein. Alternativ kann ein Unternehmen selbst passende Programmierregeln aufstellen, sofern diese praktisch oder theoretisch fundiert sind. Programmierrichtlinien regeln die Benutzung kritischer Sprachkonstrukte, den Umfang und die Schnittstelle von Softwarefunktionen, die Formatierung und Kommentierung des Codes, symbolische Namen von Funktionen und Variablen usw.

Diese Werkzeuge und Richtlinien sollten im Gestaltungsdokument vorgegeben werden.

6.3.8 Ungeliebt, aber wichtig: Dokumentation und Konfigurationsmanagement

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

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

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

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

6.3.9 Software ist ständig im Fluss: Modifikation

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

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

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

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

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

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

6.3.10 Anforderungen an die Software von Standardkomponenten in SRP/CS

Sicherheitsbezogene Steuerungen werden oft auch mit Standardkomponenten für den industriellen Anwendungsbereich realisiert. Da die Norm Anforderungen an die Realisierung von SRESW und SRASW formuliert, sind diese auch in Bezug auf elektronische programmierbare Standardkomponenten zu erfüllen. Im Vergleich zu geprüften Sicherheitskomponenten ergeben sich jedoch Einschränkungen. Folgende Kategorien bzw. Performance Level (PL) können durch elektronische programmierbare Standardkomponenten nicht beansprucht werden:

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

Anforderungen an SRESW

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

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

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

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

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

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

Tabelle 6.5:
Anforderungen an die SRESW von Standardkomponenten

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

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

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

Anforderungen an SRASW

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

6.4 Kombination von SRP/CS als Subsysteme

Bisher war in diesem Kapitel nur die Rede von einer kompletten Steuerung als SRP/CS, die sich als Ganzes auf eine Kategorie bzw. vorgesehene Architektur mit einem entsprechenden Performance Level abbilden lässt. Die Sicherheitsfunktion wird von einer solchen Steuerung, beginnend bei einem auslösenden Ereignis bis zum Erreichen des sicheren Zustands, vollständig alleine ausgeführt. In der Realität ist es aber oft notwendig, verschiedene SRP/CS als Subsysteme hintereinander zu schalten, die jeweils in Teilen die Sicherheitsfunktion ausführen. Solche Subsysteme können in unterschiedlichen Technologien aufgebaut sein und/oder verschiedene Kategorien bzw. Performance Level realisieren. Häufig werden etwa unterschiedliche Technologien in der Sensor- bzw. Logikebene (z.B. Elektronik in Kategorie 3) gegenüber der Antriebsebene (z.B. Hydraulik in Kategorie 1) verwendet, oder zugekaufte Geräte werden verkettet, z.B. Lichtgitter, elektronische Steuerung und pneumatische Ventilebene wie in Abbildung 6.13 dargestellt. Einer der großen Vorteile des PL-Konzepts gegenüber den Kategorien ist es, dass nun ein Verfahren existiert, um Subsysteme verschiedener Kategorien, aber ähnlichen Performance Level zu einem Gesamtsystem gemischter Kategorien, aber mit definiertem Gesamt-PL kombinieren zu können. In der Praxis können verschiedene Konstellationen auftreten, deren Behandlung im Folgenden näher erläutert wird:

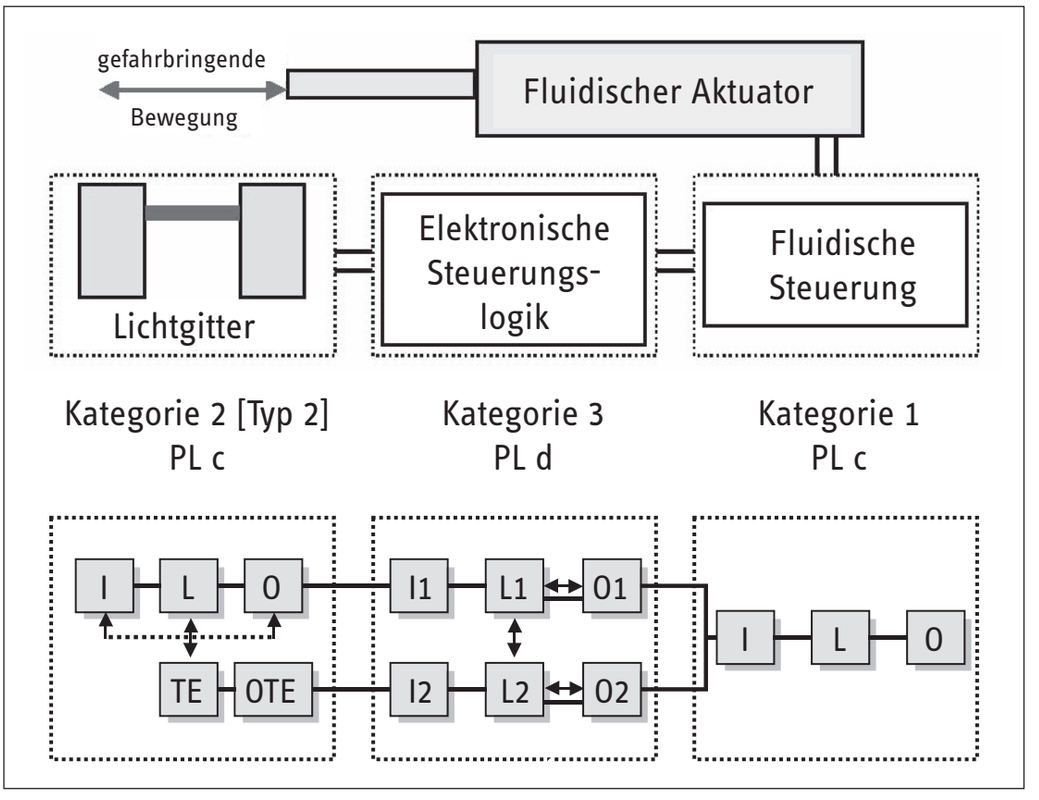


Abbildung 6.13: Reihenschaltung von Subsystemen zur Realisierung einer Sicherheitsfunktion

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

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

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

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

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

Eine Kette ist immer nur so stark wie ihr schwächstes Glied: Diese Regel gilt für die Verknüpfung von Steuerungsteilen sowohl unterschiedlicher Kategorien als auch unterschiedlicher Performance Level. Wie die Praxis schon oft gezeigt hat, ist eine hydraulische Steuerung der Kategorie 1 wegen der hohen $MTTF_d$ der Komponenten unter Umständen vergleichbar sicher wie eine elektronische der Kategorie 3 mit mittlerem DC_{avg} und niedriger $MTTF_d$. Da Zu- und Abschläge zur Kategorie durch $MTTF_d$ und DC_{avg} im PL bereits berücksichtigt sind, orientiert sich der PL für die Zusammenschaltung an der Häufigkeit des niedrigsten PL in der Serienschaltung und nicht an der niedrigsten Einzelkategorie. Mit der Anzahl der Steuerungselemente steigt auch die Gesamt-Ausfallwahrscheinlichkeit, daher kann der PL der Reihenschaltung gegenüber dem niedrigsten Subsystem-PL noch um eine Stufe verringert sein, wenn z.B. davon mehr als drei Elemente hintereinander geschaltet werden. Als grobe Abschätzung des erreichten Gesamt-PL auf der Basis der Subsystem-PL lässt sich folgendes Verfahren der DIN EN ISO 13849-1 verwenden:

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

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

- Aus $PL_{niedrig}$ und $N_{niedrig}$ lässt sich dann nach Tabelle 6.6 der Gesamt-PL bestimmen.

Tabelle 6.6:
Vereinfachte PL-Bestimmung für in Reihe geschaltete Subsysteme

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

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

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

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

mit

N = Zahl der an der Sicherheitsfunktion beteiligten Subsysteme

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

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

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

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

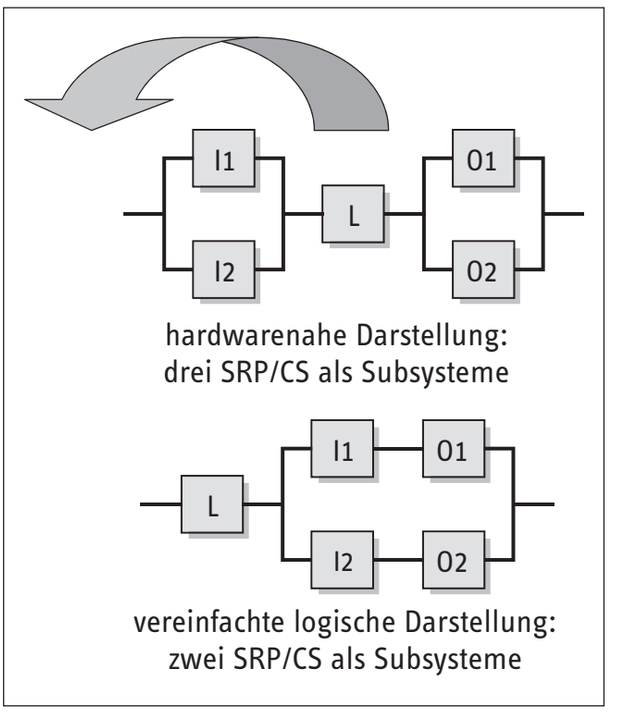
Bei hintereinander geschalteten zweikanaligen Systemen können bei der Addition der Subsystem-PFH-Werte geringe Rechenfehler zur unsicheren Seite auftreten. Streng genommen müssten die beiden Ausgänge des ersten Subsystems zusätzlich über Kreuz in die Eingänge des zweiten Subsystems eingelesen und verglichen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

Mit den bisher beschriebenen Regeln lassen sich Subsysteme bereits viel flexibler kombinieren, als dies vor der Revision der DIN EN ISO 13849-1 auf der Basis der Kategorien möglich war. Diese Subsysteme können sehr unterschiedlicher Natur sein, z.B. hinsichtlich Technologie oder Kategorie, aber auch nach anderen Normen für sicherheitsbezogene Teile von Maschinensteuerungen entwickelt, die sich statt auf einen PL auf einen SIL beziehen (vgl. Abbildung 3.2).

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

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

Abbildung 6.14:
Gemischte Subsysteme lassen sich im sicherheitsbezogenen Blockschaltbild umsortieren



Einen weiteren Spezialfall stellt die Integration von bereits mit einem PL (oder SIL) oder einer durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde versehenen Subsystemen als Block in einem SRP/CS dar. Hier kann als grobe Regel ohne Ansehen der inneren Struktur des Subsystems der Kehrwert der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde als Block-$MTTF_d$ angesetzt werden. Da alle unter Umständen intern realisierten Diagnosemaßnahmen des Subsystems bereits in der Ausfallwahrscheinlichkeit berücksichtigt sind, können für die *DC* des Blocks nur zusätzliche, von außen auf das Subsystem wirkende Diagnosemaßnahmen herangezogen werden.

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

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

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

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

6.5.1 Sicherheitsfunktionen

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

Sicherheitsfunktion (SF2):

- Ortsbindung der Hände des Bedieners außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung

6.5.2 Realisierung

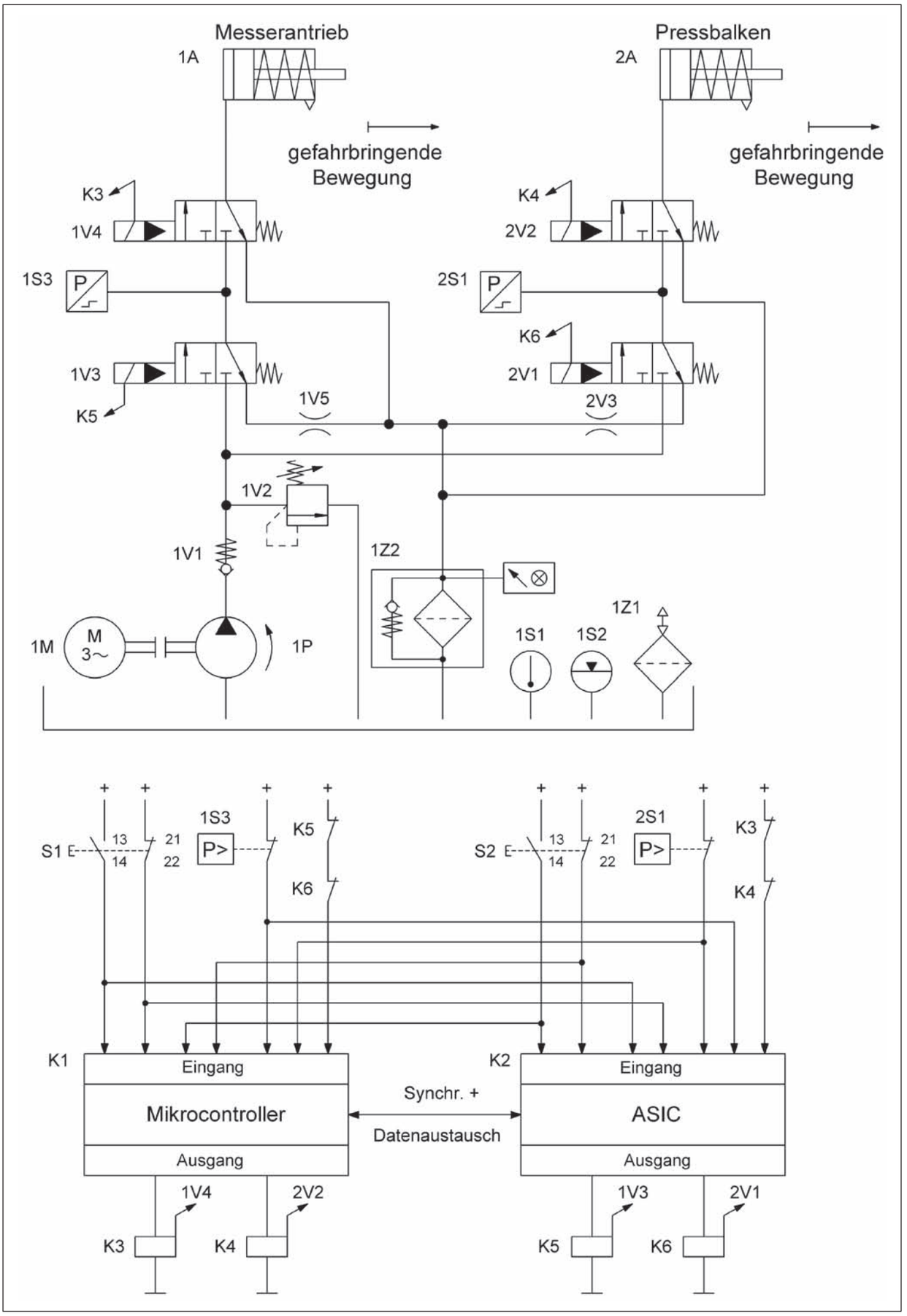
Realisiert als Zweihandschaltung lässt sich diese Sicherheitsfunktion folgendermaßen beschreiben: Beim Loslassen mindestens eines der beiden Stellteile S1 und S2 wird die gefahrbringende Bewegung von Pressbalken und Messer unterbrochen und sowohl Messer als auch Pressbalken kehren durch Federkraft in ihre Ausgangslage zurück. Ein Neustart wird solange verhindert, bis beide Stellteile losgelassen wurden und ein neuer Zyklus durch die Zweihandschaltung eingeleitet wird. Zur Ortsbindung der Hände werden zwei Stellteile verwendet, die zum Start der Maschine synchron betätigt werden müssen (für Details, z.B. zur Manipulationssicherheit, siehe DIN EN 574). Die elektrischen Signale müssen zeitlich und logisch ausgewertet werden, wozu sich z.B. eine programmierbare Elektronik anbietet, die in der Regel auch die Bewegung des Pressbalkens und Messers steuert. Diese werden hier wegen der erforderlichen hohen Kräfte hydraulisch angetrieben. Im Sinne des Kapitels 5 (siehe Abschnitt 5.3.2) enthält die Sicherheitsfunktion beide Aktoren – Pressbalken und Messer –, da sie sich an derselben Gefahrenstelle befinden. Abbildung 6.15 (siehe Seite 68) zeigt in einem elektrohydraulischen Prinzipschaltplan, wie die sicherheitsrelevanten Steuerungsteile konkret realisiert werden. Die hier wie auch im Kapitel 8 gewählte Darstellung als Prinzipschaltplan muss aus Gründen der Übersichtlichkeit natürlich viele Details unterschlagen. Neben dem Großteil der funktionalen Steuerungsteile, die für ein prozessgerechtes Funktionieren der Maschine notwendig sind, werden auch sicherheitsrelevante Details wie Schutzbeschaltungen (Sicherungen, EMV) oder „Peripherie“ (Energieversorgung, Takt usw. für den Logikteil) ausgelassen. Wegen der notwendigen Einfehlersicherheit bzw. Toleranz gegenüber Anhäufung unerkannter Fehler sind in der Praxis z.B. auch Entkopplungselemente zwischen den verbundenen Eingängen beider Logikkanäle erforderlich, damit ein fehlerhafter Eingang eines Kanals nicht auch den anderen Kanal stört. Es ist daher wichtig zu verstehen, dass ein solcher Prinzipschaltplan keine direkte Vorlage zum Nachbau ist, sondern die sicherheitstechnische Struktur illustrieren soll.

6.5.3 Funktionsbeschreibung

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

Abbildung 6.15:

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



Funktionsbeschreibung:

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

6.5.4 Sicherheitsbezogenes Blockdiagramm

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

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

Bemerkungen:

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

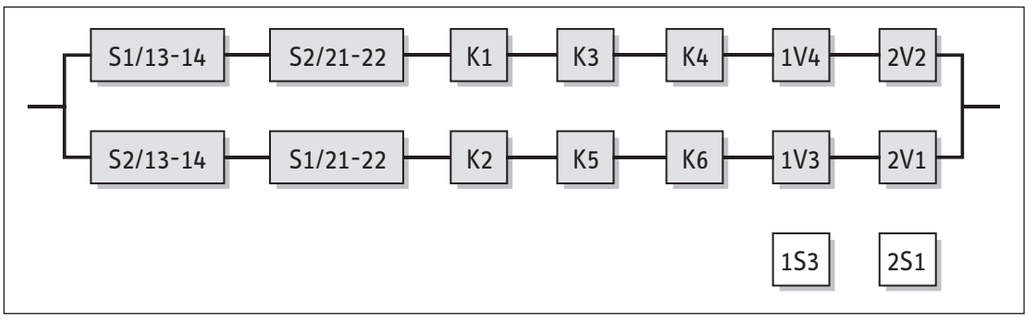


Abbildung 6.16: Sicherheitsbezogenes Blockdiagramm zum SRP/CS für die ausgewählte Sicherheitsfunktion SF2 an der Planschneidemaschine

6.5.5 Eingangsgrößen zur quantitativen Bewertung des erreichten PL

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

Berechnung der Ausfallwahrscheinlichkeit:

- $MTTF_d$: Bei 240 Arbeitstagen/Jahr, 8 Arbeitsstunden/Tag und 80 Sekunden Zykluszeit beträgt n_{op} 86 400 Zyklen/Jahr. Für S1 und S2 sowie K3 bis K6 ergibt sich bei einem B_{10d}-Wert von 2 000 000 Zyklen [H] eine $MTTF_d$ von 232 Jahren. Für den Mikrocontroller alleine wird eine $MTTF_d$ von 1 142 Jahren ermittelt [D]. Der gleiche Wert wird auch für den ASIC eingesetzt [D]. Zusammen mit der zugehörigen Beschaltung ergibt sich für die Blöcke K1 und K2 jeweils eine $MTTF_d$ von 806 Jahren. Für die Ventile 1V3, 1V4, 2V1 und 2V2 wird eine $MTTF_d$ von jeweils 150 Jahren [N] angenommen. Diese Werte ergeben eine $MTTF_d$ jedes Kanals von 31,4 Jahren („hoch").
- DC_{avg}: Nach DIN EN ISO 13849-1, Anhang E, ergeben sich als DC-Werte für S1/S2: 99 % (Kreuzvergleich von Eingangssignalen ohne dynamischen Test mit häufigem Signalwechsel), für K1/K2: 90 % (Selbsttest durch Software und Kreuzvergleich), für K3 bis K6: 99 % (direkte Überwachung über zwangsgeführte Kontakte), für 1V3/2V1: 99 % (indirekte Überwachung durch den Drucksensor) und für 1V4/2V2: 99 % (indirekte Überwachung durch die Funktion und Messung einer geänderten Druckabfallzeit). Diese Werte ergeben einen DC_{avg} von 98,6 % („hoch").

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (31,4 Jahre) und DC_{avg} = 98,6 %, im Toleranzbereich von „hoch". Damit ergibt sich eine durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls von $9{,}7 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Um die $MTTF_d$-Ermittlung zu erläutern, sei zunächst der Block „K1" vorgestellt: Obwohl das Prinzipschaltbild (Abbildung 6.15) nur den Mikrocontroller zeigt, umfasst dieser Block weitere Elemente, die für die praktische Funktion notwendig sind (z.B. Schwingquarz). Alle Elemente, deren gefahrbringender Ausfall die Ausführung der Sicherheitsfunktion im betroffenen Kanal verhindern könnte, sind zu berücksichtigen. Dies sind in der Regel alle Elemente im sicherheitskritischen Signalpfad, z.B. zur Entkopplung, Rücklesung, zum EMV-Schutz oder Schutz vor Überspannungen. Diese Elemente sind meist im Sinne der grundlegenden und bewährten Sicherheitsprinzipien oder zum Erreichen des DC notwendig. Abbildung B.2 (siehe Seite 207) zeigt diese Herangehensweise anhand eines weiteren einfachen Beispiels. Als einfaches tabellarisches Verfahren zur Ermittlung der Block-$MTTF_d$ auf der Basis der Element-$MTTF_d$ bietet sich das „Parts Count"-Verfahren an, das in Tabelle 6.7 gezeigt wird (Abbildung B.3 auf Seite 209 zeigt im Vergleich das Vorgehen bei einer Ausfalleffektanalyse).

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

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

Die in der zweiten Spalte genannten Ausfallraten der Elemente wurden mithilfe der **D**atensammlung SN 29500 [35] ermittelt, was unter „Berechnung der Ausfallwahrscheinlichkeit“ durch das Kürzel „[D]“ gekennzeichnet wird (siehe Abschnitt 7.6). Die Validierung wird in der Fortsetzung dieses Beispiels in Abschnitt 7.6 näher beschrieben. Da gleiche Elemente mehrfach auftreten können (dritte Spalte), wird in der vierten Spalte die Gesamtausfallrate für jeden Elementtyp errechnet. Durch die globale Näherung, dass nur die Hälfte der Ausfälle gefahrbringend ist, ergibt sich der halbierte Wert in Spalte 5. Durch einfache Summation ergibt sich schließlich die Gesamtrate gefahrbringender Ausfälle für den Block K1. Spalte 6 zeigt die zugehörigen $MTTF_d$-Werte in Jahren, die sich als Kehrwerte der gefahrbringenden Ausfallraten (aus Spalte 5, nach Umrechnung von Stunden in Jahre) ergeben. Für den Block K1 beträgt dieser Wert gerundet 806 Jahre. Da die verwendete Datenbank für den Mikrocontroller und den ASIC gleiche Ausfallraten nennt und die Beschaltung ähnlich ist, gilt für den Block K2 der gleiche $MTTF_d$-Wert von 806 Jahren.

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

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

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

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

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

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

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

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

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

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

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

Die im grauen Kasten auf Seite 70 oben genannten Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) sind weitgehend selbsterklärend, dennoch wird die Validierung in Kapitel 7 näher erläutert. Zusätzlich wirkt im elektrischen Subsystem die Maßnahme „Diversität“ und im hydraulischen Subsystem die Maßnahme „Verwendung bewährter Bauteile“, siehe Anhang F. Mit der Erfüllung der Anforderungen an CCF, DC_{avg} „hoch“ und $MTTF_d$ „hoch“ werden auch die quantitativen Anforderungen für Kategorie 4 erfüllt.

6.5.6 Mehrere Wege zur quantitativen PL-Bestimmung

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

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

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

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

6.5.7 Systematische Ausfälle

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

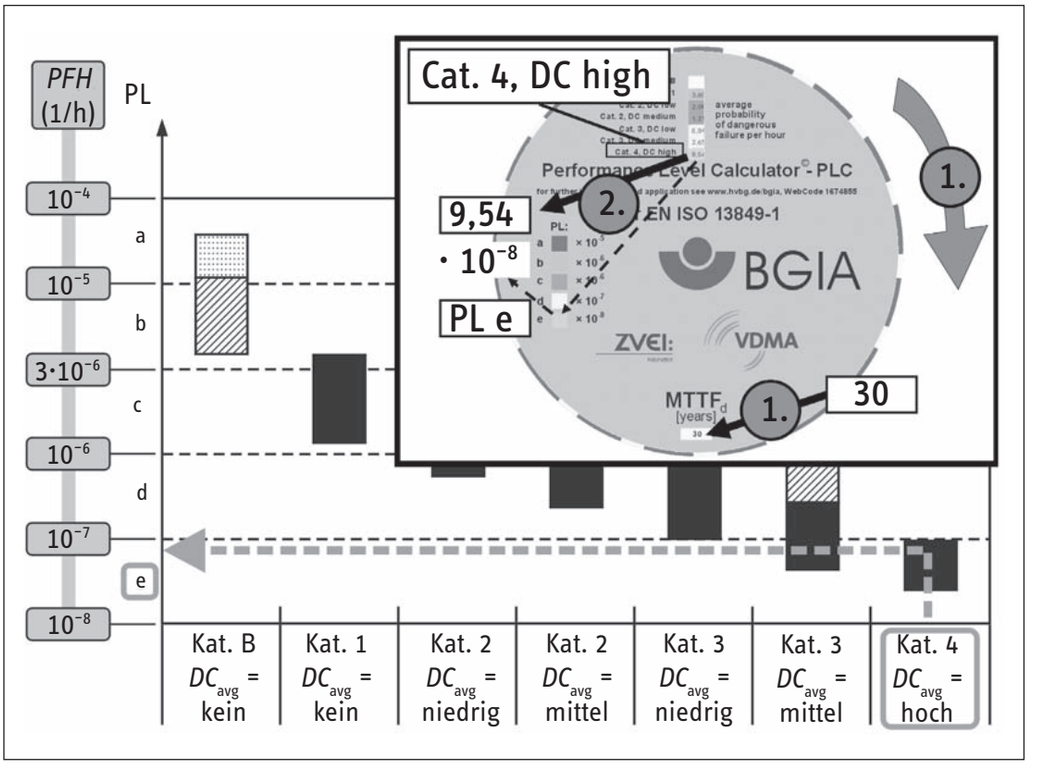


Abbildung 6.17: PL-Bestimmung mithilfe des Säulendiagramms

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

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

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

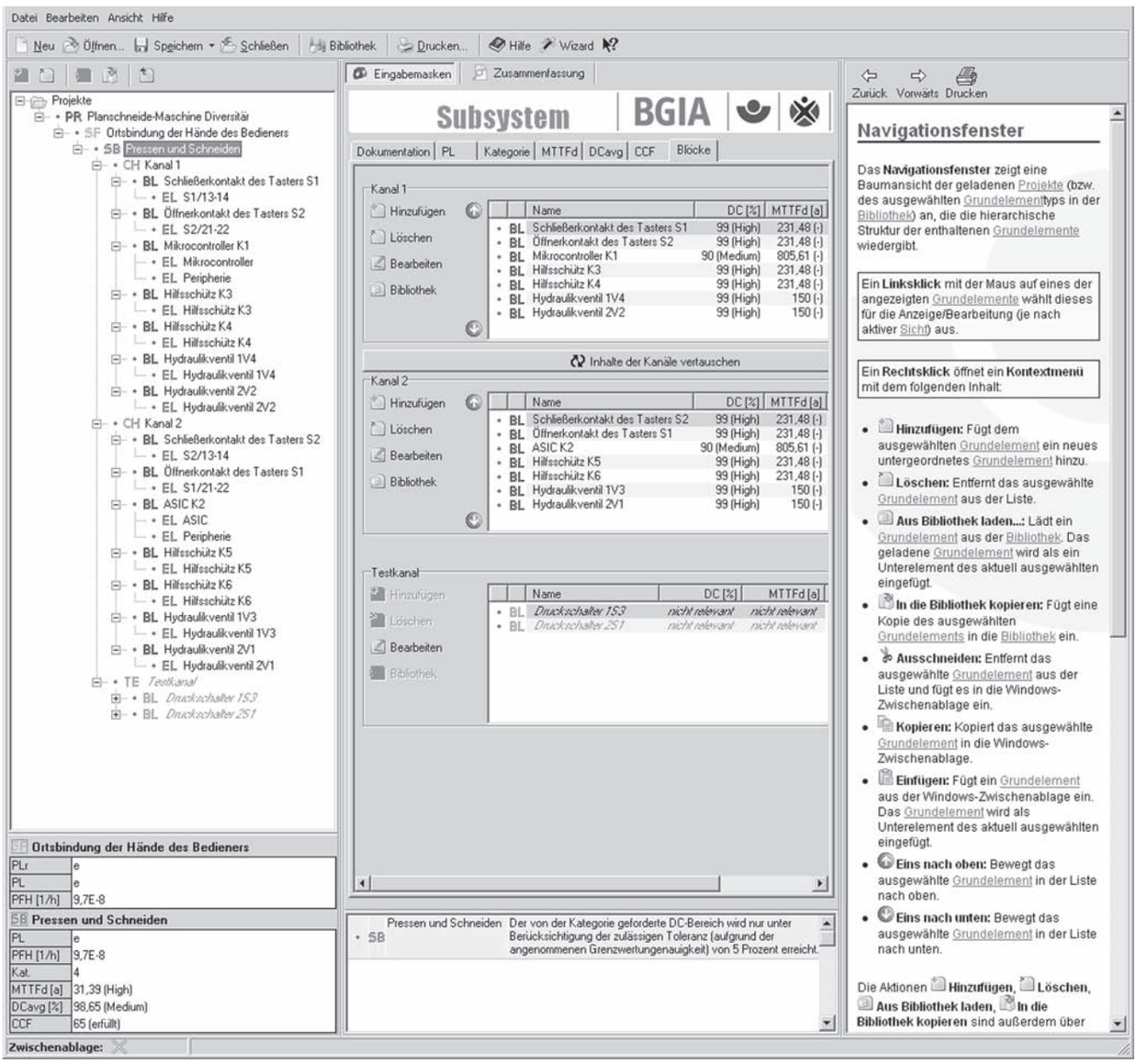
- Verwendung von Hilfsschützen mit zwangsgeführten Kontakten; durch das Rücklesen entsprechender Kontakte können gefährliche Ausfälle der Hilfsschütze und unter Umständen anderer Schaltungsteile erkannt werden.

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

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

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

Abbildung 6.18:
PL-Bestimmung mithilfe von SISTEMA



- Fehlervermeidende Maßnahmen bei der ASIC-Entwicklung gemäß ASIC-Entwicklungs-Lebenszyklus des Normentwurfs DIN IEC 61508-2:2006. In diesem Normentwurf ist für die Entwicklung eines ASICs ein V-Modell in Anlehnung an das aus der Softwareentwicklung bekannte V-Modell vorgesehen.

6.5.8 Ergonomische Aspekte

In diesem Beispiel gibt es eine sicherheitsrelevante Schnittstelle zwischen dem Benutzer und der Steuerung: die Zweihandschaltung (ZHS) mit den Stellteilen S1 und S2. Hier sind einige ergonomische Aspekte zu berücksichtigen, damit keine Person während der geplanten Verwendung und vernünftigerweise vorhersehbaren Fehlanwendung unmittelbar oder auf Dauer durch Fehlbelastungen gefährdet wird. Diese Benutzerschnittstellen können für die meisten Maschinen mit den BG-Informationen 5048 „Ergonomische Maschinengestaltung", Teile 1 und 2 [23], überprüft werden. Folgende Aspekte sind dabei u.a. zu betrachten:

- Höhe und Orientierung der Stellteile in Bezug auf den Bediener
- Greif- und Beinraum bei der üblicherweise stehenden Bedienung
- mit der Bedienaufgabe abgestimmte Anordnung und gute Erreichbarkeit außerhalb des Gefahrenraums
- Beobachtbarkeit des Schneidevorgangs vom Ort der ZHS aus
- Mindestabmessungen und Form der Stellteile (ergonomische Gestaltung unter Beachtung der Vorgaben nach DIN EN 574)
- leichte Betätigung mit geringen Kräften, aber unbeabsichtigtes Betätigen durch konstruktive Maßnahmen verhindern
- widerstandsfähige Gestaltung sowie geeignete Kennzeichnung und Farbgebung der Taster
- Gestaltung der ZHS, die eine Manipulation und damit Umgehung der Ortsbindung verhindert

6.5.9 Anforderungen an die Software, speziell SRESW

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

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

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

Die Gestaltung der Softwarearchitektur und der erforderlichen Softwaremodule und Funktionen zur Realisierung der oben beschriebenen Software werden in einem weiteren Dokument, dem Pflichtenheft zur System- und Modulgestaltung, zusammengefasst. Für die Fehlervermeidung während des gesamten Lebenszyklus sind die geeignete Modularisierung und in diesem Fall auch eine deutliche Abgrenzung der SRESW zur nicht sicherheitsbezogenen Software besonders wichtig. Wo für das Verständnis notwendig, sind Aufbau und Ablauf der Software grafisch dargestellt. Ergänzt werden Vorgaben über die einzusetzende Programmiersprache, hier ANSI C mit compilerspezifischen Spracherweiterungen, und die Entwicklungswerkzeuge, z.B. Compiler, Versionsverwaltung, Konfigurationsmanagement; alle bereits mit langjähriger positiver Erfahrung im Einsatz. Ebenso werden die Programmierrichtlinien und Methoden zur toolgestützten statischen Analyse für die Verifikation der Codierung festgelegt. Die Planung von Modul- und Integrationstest wird ebenfalls schon in diesem Dokument festgeschrieben. Nach einem erneuten Review z.B. durch den „Entwicklungsleiter Software" wird das Pflichtenheft als Vorgabe für die Codierung freigegeben. In diesem Review wird auch verifiziert, ob die Anforderungen der Softwarespezifikation erfüllt sind.

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

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

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

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

6.5.10 Kombination von SRP/CS

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

6.5.11 Weitere Erläuterungen

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

Weiterführende Literatur

- DIN EN 1010-3: Sicherheit von Maschinen - Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen - Teil 3: Schneidmaschinen (12.02). Beuth, Berlin 2002
- DIN IEC 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (Normentwurf). Beuth, Berlin 2006
- DIN EN 574: Sicherheit von Maschinen - Zweihandschaltungen - Funktionelle Aspekte; Gestaltungsleitsätze (02.97). Beuth, Berlin 1997

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

7 Verifikation und Validierung

Verifikation und Validierung bezeichnen qualitätssichernde Maßnahmen zur Vermeidung von Fehlern während des Entwurfes und der Realisierung sicherheitsbezogener Teile von Steuerungen (SRP/CS), die Sicherheitsfunktionen ausführen. Besonders Teil 2 der DIN EN ISO 13849 [7] beschäftigt sich ausgiebig mit diesem Thema.

Die Verifikation umfasst die Analysen und Prüfungen für SRP/CS bzw. deren Teilaspekte, die feststellen, ob die erzielten Resultate einer Entwicklungsphase bzw. eines Entwicklungsabschnittes den Vorgaben für diese Phase entsprechen, also z.B. ob das Schaltungslayout dem Schaltungsentwurf entspricht.

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

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

7.1 Ablauf

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

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

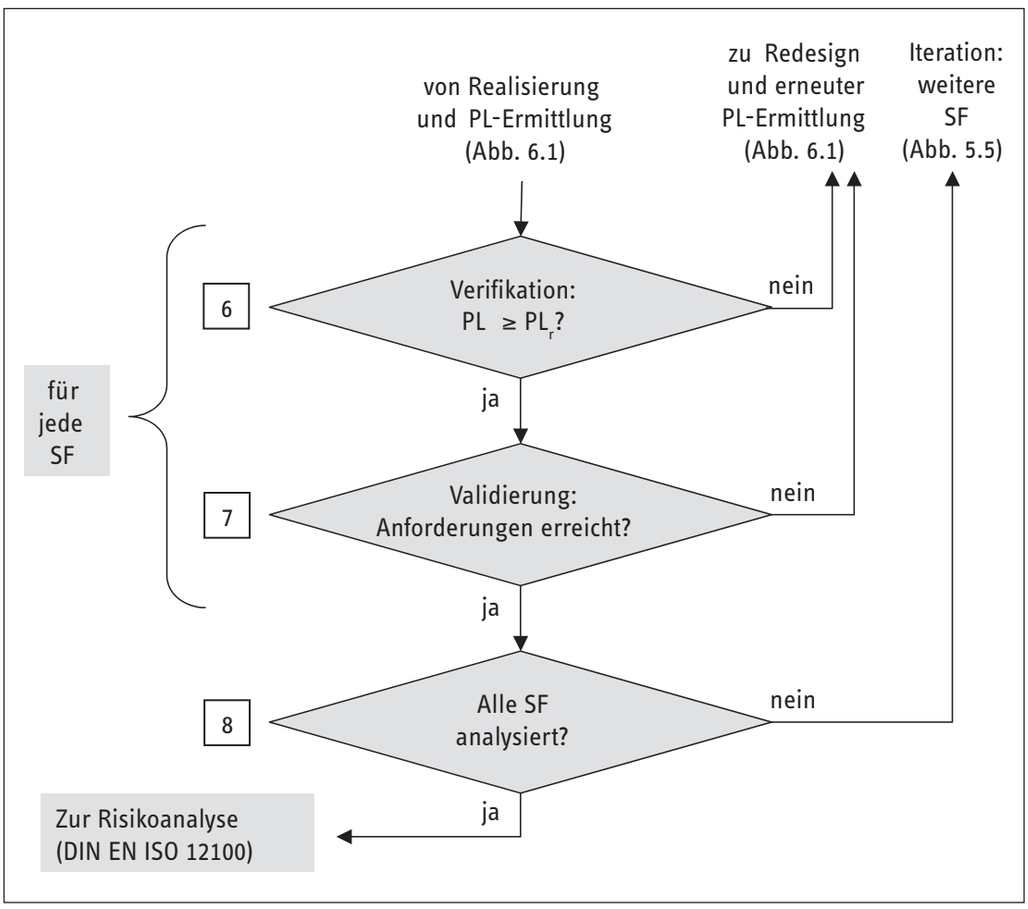


Abbildung 7.1: V&V-Aktivitäten; Ausschnitt aus Abbildung 4.1

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

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

7.1.1 Leitsätze für die Verifikation und Validierung

Verifikation und Validierung sollen die Konformität der Gestaltung der SRP/CS mit der Maschinenrichtlinie sicherstellen.
Da DIN EN ISO 13849-1 als Sicherheitsnorm für Maschinensteuerungen unter der Maschinenrichtlinie gelistet ist, müssen die V&V-Aktivitäten zeigen, dass jedes sicherheitsbezogene Teil und jede seiner ausgeführten Sicherheitsfunktionen die Anforderungen der DIN EN ISO 13849-1 erfüllt, sofern die Vermutungswirkung der Norm beansprucht werden soll. Diese Aktivitäten sollten so früh wie möglich während der Entwicklung begonnen werden, sodass Fehler rechtzeitig erkannt und behoben werden können. Die Prüfungen sollten nach Möglichkeit von Personen durchgeführt werden, die nicht in den Gestaltungsprozess der sicherheitsbezogenen Teile einbezogen sind, d.h. unabhängig von Entwurf und Realisierung sind. Dies können andere Personen, andere Abteilungen oder andere Stellen sein, die der Konstruktionsabteilung hierarchisch nicht unterstehen. Der Grad der Unabhängigkeit sollte dabei dem Risiko, also dem erforderlichen Performance Level PL_r, angemessen sein.

Verifikation und Validierung können durch alleinige Analyse oder durch eine Kombination aus Analyse und Prüfung erfolgen.

7.1.2 Verifikations- und Validierungsplan

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

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

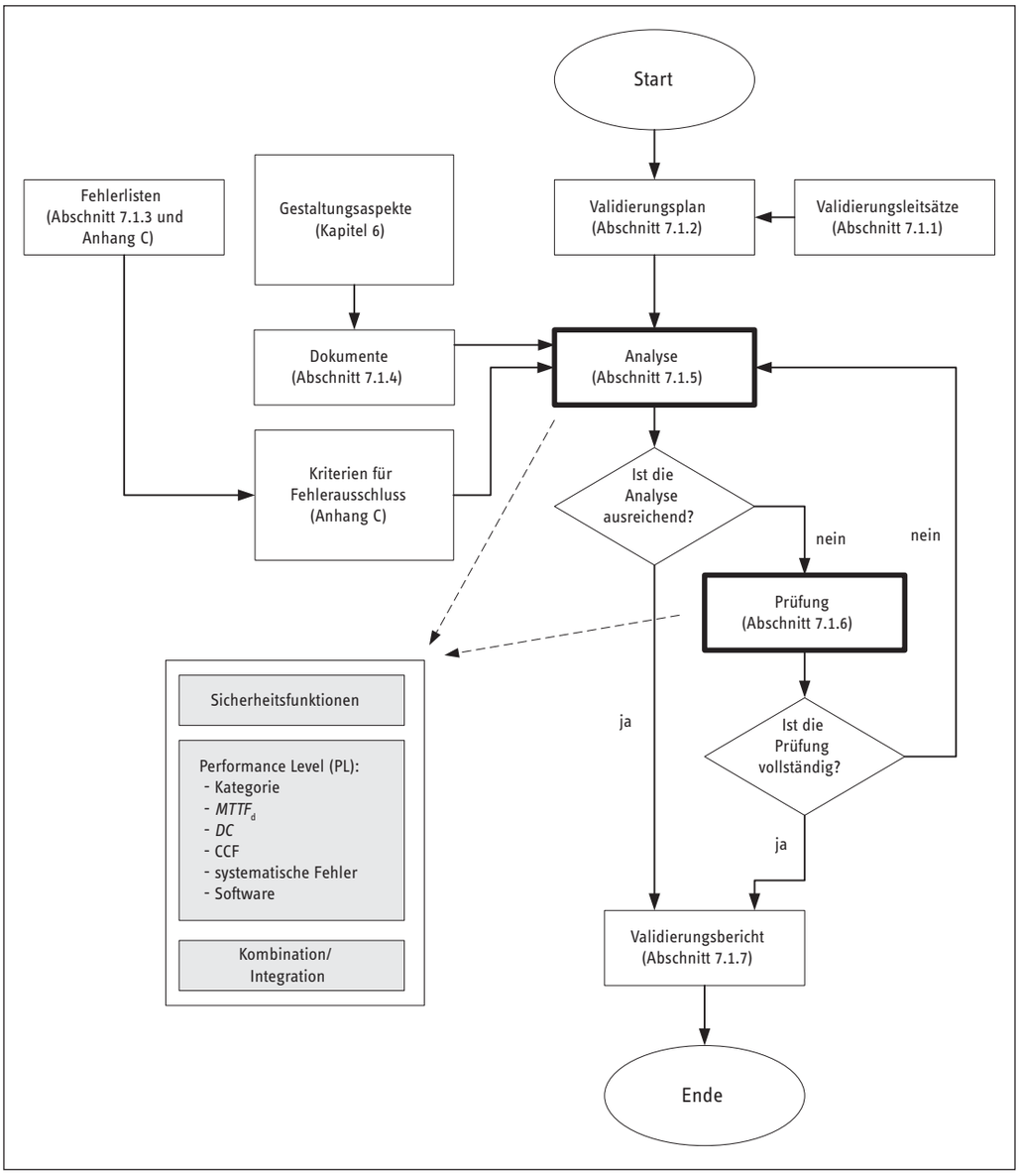


Abbildung 7.2: Übersicht zum Verifikations- und Validierungsablauf nach DIN EN ISO 13849-2

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

7.1.3 Fehlerlisten

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

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

7.1.4 Dokumente

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

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

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

7.1.5 Analyse

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

7.1.6 Prüfung

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

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

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

7.1.7 Dokumentation der V&V-Aktivitäten

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

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

7.2 Validieren der Sicherheitsfunktion

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

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

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

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

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

7.3 Validieren des PL der SRP/CS

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

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

7.3.1 Validieren der Kategorie

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

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

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

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

Diese Teilprüfungen sollten durch folgende Analysen ergänzt werden:

- Struktur-/Signalpfadanalyse
- Inspektion zur Einhaltung grundlegender Sicherheitsprinzipien
- Inspektion zur Umsetzung bewährter Sicherheitsprinzipien (ab Kategorie 1)
- Inspektion zum Einsatz bewährter Bauteile (nur Kategorie 1)

- Bewertung der in Fehlerlisten individuell ergänzten zu betrachtenden Fehler und zulässiger Fehlerausschlüsse, einschließlich deren hinreichender Begründung

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

7.3.2 Validieren der $MTTF_d$-Werte

Die zur Bestimmung des PL herangezogenen $MTTF_d$-Werte sollten mindestens auf ihre Plausibilität überprüft werden. Dazu zählt typischerweise die Beurteilung, ob geeignete Quellenangaben zur Herkunft der Werte benannt werden. Bei den dominanten Bauteilen und stichprobenartig bei allen anderen Bauteilen ist es ratsam, auch die genaue Begründung der Werte nachzuvollziehen. Dazu können u.a. die in Abschnitt 6.2.12 und Anhang D genannten Datenquellen herangezogen werden.

7.3.3 Validieren der DC-Werte

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

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

7.3.4 Validieren der Maßnahmen gegen CCF

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

7.3.5 Verifizieren und Validieren der Maßnahmen gegen systematische Ausfälle

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

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

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

- Analyse zur Implementierung der Programmlaufüberwachung

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

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

7.3.6 Validieren der Software

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

Für die Entwicklung von sicherheitsbezogener Software ist mit Ausnahme der unten beschriebenen Embedded-Lösung im PL e das vereinfachte „V-Modell“ anzuwenden (siehe Abbildung 6.11). Die letzte Entwicklungsaktivität hierbei ist die Softwarevalidierung. Zu prüfen ist, ob die Anforderungen der sicherheitsbezogenen Softwarespezifikation an das funktionale Verhalten sowie die Leistungskriterien (z.B. zeitbezogene Vorgaben) korrekt umgesetzt wurden. Die Validierung betrachtet hier keine „Interna“ der Software mehr, sondern das „externe“ Verhalten am Ausgang der kompletten, auf die Hardware integrierten Software bei Änderungen an deren Eingängen. Die Software wird dabei als „Black box“ betrachtet, die Validierung hierzu ist der sogenannte Black-Box-Test.

Bei sicherheitsrelevanter Anwendungssoftware (SRASW) müssen „I/O-Tests“ sicherstellen, dass die sicherheitsbezogenen Eingangs- und Ausgangssignale korrekt verwendet werden. Für PL d und e wird bei der Validierung auch eine erweiterte Testfallausführung auf der Basis von Grenzwertanalysen empfohlen. Hierbei wird auch die Reaktion auf vorher analytisch bestimmte und im Test durchgeführte Fehlerfälle beobachtet, um so die Fehlererkennung und -beherrschung durch die Software zu testen. Einzelne Softwarefunktionen, die als Sicherheits-Funktionsbausteine bereits zertifiziert oder qualitätsgesichert validiert wurden, müssen nicht nochmals geprüft werden. Allerdings ist die bereits erfolgte Validierung zu belegen. Sobald aber mehrere dieser Sicherheits-Funktionsbausteine projektspezifisch zusammengeschaltet werden, ist die resultierende gesamte Sicherheitsfunktion zu validieren.

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

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

7.3.7 Kontrolle der Abschätzung des PL

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

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

7.4 Prüfen der Benutzerinformation

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

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

7.5 Validieren der Kombination und Integration von SRP/CS

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

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

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

Begleitend zur allgemeinen Beschreibung der Verifikation und Validierung von Sicherheitsfunktionen werden in diesem Abschnitt die V&V-Aktivitäten am praktischen Beispiel einer Planschneidemaschine, das schon in den Abschnitten 5.7 und 6.5 beschrieben wurde, erläutert.

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

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

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

Fehlerlisten

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

Dokumente

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

Dokumentation

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

Validieren der Sicherheitsfunktion

Zur Überprüfung der funktionalen Anforderungen an die Sicherheitsfunktion wird ein Funktionstest durchgeführt, ergänzt um einen erweiterten Funktionstest, um das Verhalten der Sicherheitsfunktion bei seltenen oder nicht festgelegten Eingaben zu überprüfen. Ein Beispiel für einen solchen Test wäre die Überprüfung der Reaktion der SRP/CS, wenn eine weitere Person in den Gefahrenbereich durch eine dort vorhandene BWS (Lichtgitter) eingreift, während ein Mitarbeiter gerade die Zweihandschaltung bedient. Leistungstests zu funktionalen Aspekten werden durchgeführt. Dazu zählt die Überprüfung der nach der Norm DIN EN 574 [37] einzuhaltenden Zeit für eine synchrone Betätigung. Nur wenn beide Stellteile S1 und S2 in einem Zeitabschnitt ≤ 0,5 Sekunden betätigt werden, dürfen Ausgangssignale zur Ansteuerung des Pressbalkens und des Messers erzeugt werden. Die vorgenannten Prüfungen und die Analysen der spezifizierten sicherheitstechnischen Eigenschaften wurden mit positivem Ergebnis abgeschlossen.

Validieren des PL der SRP/CS

- Validieren der Kategorie

Unter Einbeziehung der Entwicklungsunterlagen finden an einem Prototypen Tests zum Verhalten im Fehlerfall statt. Dies geschieht durch gezielten Einbau von Fehlern. Die Reaktion der SRP/CS auf die eingebauten Fehler sollte den spezifizierten Reaktionen entsprechen. Zunächst wird durch Analyse und dann durch Prüfung getestet, was geschieht, wenn z.B. einzelne Hilfsschütze nicht mehr in der Lage sind, Schaltbefehle auszuführen, oder wie die SRP/CS reagieren, wenn einer der beiden Stellteile S1 oder S2 zeitverzögert oder gar nicht betätigt wird. Die Sicherheitsfunktion bei Einbringung eines einzelnen Fehlers in die SRP/CS muss stets gewährleistet sein. Ein einzelner Fehler muss bei oder vor der nächsten Ausführung der Sicherheitsfunktion erkannt werden. Kann der Fehler nicht erkannt werden, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.

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

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

- Validieren der $MTTF_d$-Werte

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

Konstruktive Merkmale

- Die Anforderungen von Kategorie B, grundlegende und bewährte Sicherheitsprinzipien, werden eingehalten. Durch diversitär redundante Verarbeitungskanäle (Mikrocontroller und ASIC) führt ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion und systematische Fehler werden weitgehend vermieden.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung aller elektrischen Signale, auch die der Drucksensoren, erfolgt in einer mehrkanaligen Steuerung.
- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1.
- K3 bis K6 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L [38]. Die zugehörigen Öffner-Kontakte zur Überwachung der Schließer-Kontakte werden im jeweiligen Nachbarkanal überwacht.
- Alle Signal führenden Anschlussleitungen sind entweder getrennt oder gegen mechanische Beschädigung geschützt verlegt.
- Die Programmierung der Software (SRESW) erfolgt entsprechend den Anforderungen für PL d (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.
- Fehlervermeidende Maßnahmen bei der ASIC-Entwicklung sind gemäß ASIC-Entwicklungs-Lebenszyklus (V-Modell) des Normentwurfs DIN IEC 61508-2:2006 [39] durchgeführt.

- Validieren der DC-Werte

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

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

- Validieren der Maßnahmen gegen CCF

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

- Verifizieren und Validieren der Maßnahmen gegen systematische Ausfälle

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

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

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

Um die Beständigkeit der SRP/CS gegen die festgelegten Umgebungsbedingungen zu zeigen, finden Prüfungen unter allen erwarteten und vorhersehbar widrigen Bedingungen für u.a. Temperatur, Feuchte und elektromagnetische Beeinflussung statt. Dies ist ein Beispiel für eine Maßnahme zur Vermeidung systematischer Ausfälle.

- Validieren der Software

Die Verifikation der Software wird ausführlich in Abschnitt 6.3 beschrieben. An dieser Stelle wird ergänzend die Validierung der Software durchgeführt, d.h. die Prüfung der Funktion und auch der Reaktionszeiten der auf der Hardware integrierten Software. Geprüft wird mit funktionalen Tests und einem erweiterten Funktionstest, bei dem einerseits die sicherheitsrelevanten Eingangssignale korrekt zu sicherheitsrelevanten Ausgangssignalen verarbeitet werden müssen und andererseits Testfälle mit eingebauten Fehlern ausgeführt werden, um die spezifizierten Fehlerreaktionen der Firmware des Mikrocontrollers K1 zu validieren.

- Kontrolle der Abschätzung des PL

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

Prüfen der Benutzerinformation

Die Benutzerinformation muss zu Belangen der SRP/CS auf folgende Punkte erfolgreich überprüft werden: Beschreibung der bestimmungsgemäßen Verwendung; Angabe von Informationen zum PL und der Kategorie (einschl. datierter Verweisung auf die Norm); Erläuterung aller Betriebsarten; Beschreibung der Schutzeinrichtungen und Sicherheitsfunktionen mit Ansprechzeiten, Umgebungsbedingungen für den Betrieb und Schnittstellen nach außen; Informationen und technische Daten zum Transport, zur sicheren Montage, Inbetriebnahme und Instandhaltung.

Validieren der Kombination und Integration von SRP/CS

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

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

Die hier für SF2 gezeigten V&V-Aktivitäten werden für alle vom SRP/CS ausgeführten Sicherheitsfunktionen (SF1 bis SF7) durchgeführt. Der Mehraufwand ist allerdings gering, da viele Sicherheitsfunktionen auf dieselbe Hardware zurückgreifen. Die Analysen und Prüfungen müssen zeigen, dass die umgesetzten Sicherheitsfunktionen korrekt realisiert wurden. Nach Betrachtung aller Sicherheitsfunktionen ist die Bewertung nach DIN EN ISO 13849 Teil 1 und Teil 2 abgeschlossen.