IFA
Institut für Arbeitsschutz
der Deutschen Gesetzlichen
Unfallversicherung

4/2018

IFA Report

Sichere Antriebssteuerungen mit Frequenzumrichtern

Verfasser: Christian Werner, Helmut Zilligen, Burkhard Köhler, Ralf Apfeld
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)

Herausgeber: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Glinkastr. 40
10117 Berlin
Telefon: 030 13001-0
Telefax: 030 13001-9876
Internet: www.dguv.de
E-Mail: info@dguv.de

– 3. Auflage, September 2018 –

Publikationsdatenbank: www.dguv.de/publikationen

ISBN (online): 978-3-86423-220-6
ISSN: 2190-7994

Kurzfassung

Sichere Antriebssteuerungen mit Frequenzumrichtern

Drehzahlgeregelte Antriebe sind an Maschinen Stand der Technik. Genau wie bei ungeregelten Antrieben löst die drehzahlveränderliche Bewegung eines Maschinenteils häufig eine Gefährdung aus, vor der die Bedienpersonen geschützt werden müssen. Die einfachste Lösung zur Vermeidung von Bewegungen bei manuellen Eingriffen in Gefahrstellen ist das (sichere) Abschalten der Antriebsenergie der jeweiligen Motoren. Dies ist jedoch häufig nicht möglich, z. B. wenn zur Störungsbeseitigung, zum Einrichten, im Probebetrieb usw. Eingriffe bei laufender Maschine erforderlich sind. In diesen Fällen ist der Maschinenbetrieb bei aufgehobener Schutzwirkung von Schutzeinrichtungen notwendig. Um trotzdem die Sicherheit der Beschäftigten zu gewährleisten, gibt die Maschinenrichtlinie in Anhang I Abschnitt 1.2.5 die erforderlichen Maßnahmen an. Zur Realisierung der hierfür notwendigen Maschinenfunktionen wurden Sicherheits-Teilfunktionen für Antriebssteuerungen definiert, wie z. B. STO (Sicher abgeschaltetes Moment), SLS (Sicher begrenzte Drehzahl) und SS1 (Sicherer Stopp 1).

Der vorliegende Report behandelt den Einsatz von Antriebssteuergeräten, die abhängig von Applikation und Risiken, Sicherheits-Teilfunktionen in einem bestimmten Performance Level nach DIN EN ISO 13849-1 umsetzen. Die grundlegenden Sicherheits-Teilfunktionen von Antriebssteuerungen und die Anforderungen bei deren Anwendung werden vorgestellt. Die prinzipielle Funktionsweise von Frequenzumrichtern und Gleichstromstellern wird beschrieben und die Umsetzung der Sicherheits-Teilfunktionen erläutert. In Beispielen werden Applikationsschaltungen gezeigt, mit denen unterschiedliche Sicherheitsfunktionen an Maschinen realisiert werden. Die jeweiligen SISTEMA-Dateien zur Quantifizierung dieser Sicherheitsfunktionen stehen zum kostenlosen Download bereit. In den Beispielen finden sowohl Standardfrequenzumrichter Anwendung als auch Frequenzumrichter mit integrierten Sicherheitsfunktionen.

Dieser Report versteht sich als Ergänzung zum IFA Report 2/2017 „Funktionale Sicherheit von Maschinensteuerungen“ und setzt Grundkenntnisse über Kategorien und Performance Level nach DIN EN ISO 13849-1 voraus.

Abstract

Safe drive controls using frequency inverters

Machine drives using closed-loop speed control are state of the art. As on drives without closed-loop speed control, the movement of a machine part at varying speeds frequently gives rise to a hazard against which the machine operators must be protected. The simplest means of preventing movements during manual intervention in danger zones is the (reliable) disconnection of the energy driving the relevant motors. This is however often not possible, for example when intervention is required whilst the machine is running for the purpose of clearing faults, setup, during test operation, etc. Scenarios such as these require the machine to be operated with protective equipment disabled. In order for the operators‘ safety to be assured nonetheless, Annex I, Section 1.2.5 of the Machinery Directive sets out the required measures. Safety sub-functions for drive controls have been defined for implementation of the machine functions required for this purpose. Examples are STO (safe torque off), SLS (safely limited speed) and SS1 (safe stop 1).

This report addresses the use of drive control equipment that implements safety sub-functions at a certain Performance Level according to EN ISO 13849-1 in consideration of the application and risks. The basic safety sub-functions of drive controls and the requirements relating to their use are presented. The principles of operation of frequency inverters and DC converters are described, and implementation of the safety sub-functions are explained. Examples are provided of application circuits by which the various machine safety functions can be implemented. The corresponding SISTEMA files for quantification of these safety functions are available for download free of charge. The examples include both standard frequency inverters and frequency inverters with integral safety functions.

This report supplements IFA Report 2/2017, „Functional safety of machine controls“, and requires a basic understanding of Categories and Performance Levels according to EN ISO 13849-1.

Résumé

Commandes d'entraînement sûres avec convertisseurs de fréquence

La plupart des machines modernes sont équipées d'entraînements dont la vitesse est régulée. Comme pour les entraînements dont la vitesse n'est pas régulée, le déplacement à vitesse variable d'un organe de machine crée souvent un danger, qui nécessite une protection des opérateurs. La solution la plus simple pour empêcher des déplacements d'organes de machine lors d'interventions manuelles dans des zones de danger est la coupure (sûre) de l'alimentation en énergie des moteurs de ces organes de machine. Or, il est fréquent que cela ne soit pas possible, par exemple lorsqu'il faut intervenir sur une machine en fonctionnement pour remédier à des défauts, procéder à des réglages, effectuer des marches d'essai, etc. Dans ces cas, il est nécessaire que la machine continue à fonctionner, bien que les dispositifs de protection soient désactivés. Pour que la sécurité de l'opérateur soit néanmoins garantie, la directive Machines indique, dans l'Annexe I, point 1.2.5, les mesures à prendre. Pour la réalisation des fonctions machine nécessaires à cet effet, des sous-fonctions de sécurité pour commandes d'entraînement ont été définies, telles que STO (Safe Torque Off = suppression sûre du couple), SLS (Safety Limited Speed = limitation sûre de la vitesse) et SS1 (Safe Stop 1 = stop sûr 1).

Ce rapport traite de l'utilisation de dispositifs de commande d'entraînement qui, en fonction de l'application et des risques, met en œuvre des sous-fonctions de sécurité ayant un niveau de performance déterminé, conforme à la norme EN ISO 13849-1. Les sous-fonctions de sécurité de base des commandes d'entraînement et les exigences relatives à leur utilisation sont présentées. Les principes de fonctionnement des convertisseurs de fréquence et des convertisseurs DC-DC sont décrits et la mise en œuvre de la sous-fonction de sécurité est expliquée. Des exemples illustrent les circuits d'application grâce auxquels différentes fonctions de sécurité peuvent être réalisées sur les machines. Les fichiers SISTEMA permettant de quantifier ces différentes fonctions de sécurité peuvent être téléchargés gratuitement. Les exemples comportent aussi bien des convertisseurs de fréquence standard que des convertisseurs de fréquence avec fonctions de sécurité intégrées.

Le présent rapport complète le rapport IFA 2/2017 « Funktionale Sicherheit von Maschinensteuerungen » (Sécurité fonctionnelle des commandes de machines). Il requiert des connaissances de base sur les catégories et niveaux de performance selon la norme EN ISO 13849-1.

Resumen

Accionamientos seguros con convertidores de frecuencia

Los accionamientos con control de velocidad son un estándar técnico en maquinaria. Al igual que en los accionamientos no regulados, un movimiento de velocidad variable de un elemento en una maquinaria suele suponer un riesgo que requiere la consiguiente protección para los operarios. La solución más sencilla para evitar movimientos en las operaciones manuales en puntos de peligro es la desconexión (segura) de la energía de propulsión de los motores en cuestión. Pero con frecuencia no es posible hacerlo, por ejemplo, cuando es necesario realizar operaciones con la maquinaria en marcha para subsanar una avería, realizar ajustes o pruebas, etc. En esos casos, es necesario operar la maquinaria sin accionar los dispositivos de protección. Para aún así poder garantizar la seguridad de los empleados, se aplican las medidas necesarias según la directriz de maquinaria que figura en el anexo I, párrafo 1.2.5. Para implementar las funciones de la máquina necesarias para ello, se han definido funciones parciales de seguridad para los accionamientos como, por ejemplo, la STO (momento de desconexión segura), SLS (velocidad limitada segura) y SS1 (parada segura 1).

El presente informe trata sobre la utilización de accionamientos que, en función de su aplicación y los riesgos, implementan una función subsidiaria de seguridad en un nivel de rendimiento determinado según lo estipulado en la normativa DIN EN ISO 13849-1. Las funciones subsidiarias de seguridad básicas de los accionamientos y los requisitos correspondientes para su aplicación se presentan en dicho informe. En él se describe el funcionamiento básico de los convertidores de frecuencia y los chopper CC, y se explica la aplicación de la función subsidiaria de seguridad. Se muestran ejemplos de conmutación de aplicaciones con los que se introducen diversas funciones de seguridad en las máquinas. Los archivos correspondientes de SISTEMA para cuantificar estas funciones de seguridad se pueden descargar gratuitamente. En los ejemplos se muestra la aplicación tanto de convertidores de frecuencia estándar como también de convertidores de frecuencia con funciones de seguridad integradas.

Este informe se entiende como complemento al IFA Report 2/2017 „Funktionale Sicherheit von Maschinensteuerungen“ (seguridad funcional de controles de maquinaria) y presupone conocimientos básicos sobre las categorías y el nivel de rendimiento según DIN EN ISO 13849-1.

Inhaltsverzeichnis

1 Einleitung

Die Anwendung von Frequenzumrichtern in sicherheitsgerichteten Stromkreisen wurde in der Vergangenheit in zwei Reports (BIA-Report 5/2003 und IFA Report 7/2013) beschrieben. Ausgehend von den Sicherheitsfunktionen wurde anhand von Beispielen der Einsatz von Frequenzumrichtern ohne (PDS, Power Drive Systems) und mit integrierten Sicherheits-Teilfunktionen (PDS(SR), Power Drive Systems Safety Related), erläutert. Basis für den ersten Report war die unter der Maschinenrichtlinie gelistete Norm DIN EN 954-1 [1]. Die umfangreiche Überarbeitung dieser Norm, jetzt als DIN EN ISO 13849-1 [2] vorliegend (Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen), sowie die Herausgabe der DIN EN 61800-5-2 [3] für die Anforderungen an die funktionale Sicherheit von elektrischen Leistungsantriebssystemen mit einstellbarer Drehzahl erforderte eine Überarbeitung und Anpassung des BIA-Report 5/2003. Der überarbeitete Report wurde dann als IFA Report 7/2013[1] veröffentlicht. Die Normen DIN EN ISO 13849-1 [2] und DIN EN 61800-5-2 [3] wurden seit dem letzten Report erneut überarbeitet. Die normativen Änderungen sind in diesen Report eingegangen. Wie im IFA Report 7/2013 wird weiterhin auch die Steuerung von Gleichstromantrieben behandelt.

Auf der Basis der in den letzten Jahren gewonnenen Erkenntnisse bei der Prüfung und Zertifizierung von Produkten sowie bei der Beratung von Herstellern und Fachausschüssen (jetzt Fachbereiche) der Unfallversicherungsträger gibt dieser Report Beispiele und Erläuterungen, um speziell die Gestaltung von drehzahlgeregelten Antrieben nach DIN EN ISO 13849-1 [2] zu erleichtern. Der vorliegende Report versteht sich insofern als Ergänzung zum IFA Report 2/2017 „Funktionale Sicherheit von Maschinensteuerungen“ [4].

Die enthaltenen Beispiele setzen voraus, dass der energielose Zustand einer Antriebssteuerung ein sicherer Zustand für die Maschine ist. Der Abschnitt 5.4 „Stillsetzen und Position halten“ gibt Hinweise für Applikationen, auf die das ggf. nicht zutrifft.

Die Anforderungen an die funktionale Sicherheit von Frequenzumrichtern sind in der Norm DIN EN 61800-5-2 [3] festlegt, die auf DIN EN 61508 [5] basiert. Wo notwendig, wird in diesem Report daher auf die speziellen Zusammenhänge mit der DIN EN 61508 [5] eingegangen. Die Gesamtbetrachtung der Sicherheitsfunktionen erfolgt jedoch immer aus Sicht des Maschinenherstellers; daher wird stets DIN EN ISO 13849-1 [2] herangezogen.

Die Autoren hoffen, dass der vorliegende Report den Konstrukteuren eine konkrete Hilfe für die Umsetzung von Sicherheitsfunktionen mit Antriebssteuerungen gibt.

1 Sichere Antriebssteuerungen mit Frequenzumrichtern (IFA Report 7/2013). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2013

2 Risikominderung

Nach der europäischen Richtlinie 2006/42/EG (Maschinenrichtlinie) [6] ist der Hersteller u. a. verpflichtet, eine Risikobeurteilung vorzunehmen, um alle mit seiner Maschine verbundenen Risiken zu ermitteln. Die Maschine ist unter Berücksichtigung dieser Analyse zu entwerfen und zu bauen. Dabei sind Gefährdungen idealerweise bereits bei der Konstruktion zu vermeiden oder durch konstruktive Maßnahmen zu beseitigen.

Durch die Bauart der Maschine muss gewährleistet sein, dass der Betrieb der Maschine bei bestimmungsgemäßer Verwendung und einer nach vernünftigem Ermessen zu erwartenden Benutzung ohne Gefährdung von Personen erfolgt. Dies trifft auf alle Betriebsarten zu, sodass nicht nur der Automatikbetrieb bei geschlossenen Schutztüren, sondern insbesondere auch alle erforderlichen manuellen Eingriffe berücksichtigt werden müssen.

Um Konstrukteure, Hersteller und andere Interessenten bei der Interpretation der wesentlichen Sicherheitsanforderungen zu unterstützen und um Übereinstimmung mit der europäischen Gesetzgebung in Bezug auf die Sicherheit von Maschinen zu erreichen, wurde u. a. die Norm DIN EN ISO 12100 [7] erarbeitet. Sie enthält allgemeine Gestaltungsleitsätze sowie Festlegungen zur Risikobeurteilung und Risikominderung. Hierdurch soll ein allgemeiner Rahmen und eine Orientierungshilfe vorgelegt werden, um sichere Maschinen herzustellen. Darüber hinaus ist diese Norm eine nützliche Leitlinie, wenn keine maschinenbezogene C-Norm existiert.

Für die Risikominderung gilt die als „Drei-Stufen-Verfahren“ bezeichnete Reihenfolge (DIN EN ISO 12100 [7], Abschnitt 6.1):

- Stufe 1 – Inhärent sichere Konstruktion
- Stufe 2 – Technische Schutzmaßnahmen und/oder ergänzende Schutzmaßnahmen
- Stufe 3 – Benutzerinformation hinsichtlich des Restrisikos

Die Benutzerinformation darf kein Ersatz für die korrekte Anwendung der inhärent sicheren Konstruktion, der technischen Schutzmaßnahmen oder der ergänzenden Schutzmaßnahmen sein.

In der zweiten Stufe des o. g. Verfahrens werden technische und ergänzende Maßnahmen zur Risikominderung herangezogen. Hierzu zählen die in diesem Report behandelten Sicherheitsfunktionen. Für die sicherheitstechnischen Anforderungen an die Realisierung der zugehörigen Steuerungen gilt DIN EN ISO 13849. Diese Norm besteht aus zwei Teilen [2; 8].

Teil 1 stellt Sicherheitsanforderungen und einen Leitfaden für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS, engl.: safety related parts of control systems) bereit, einschließlich der Entwicklung von Software. Für die SRP/CS werden Eigenschaften festgelegt, die zur Ausführung der entsprechenden Sicherheitsfunktionen erforderlich sind. Die Norm ist anzuwenden auf SRP/CS aller Arten von Maschinen, ungeachtet der verwendeten Technologie und Energie (elektrisch, hydraulisch, pneumatisch, mechanisch).

Teil 2 legt das Validierungsverfahren für die Sicherheitsfunktionen von Steuerungen fest, einschließlich der beiden Verfahren Analyse und Prüfung. Das Validierungsverfahren schließt die Betrachtung des Verhaltens von sicherheitsbezogenen Teilen der Steuerung im Fehlerfall ein. Dazu sind für viele Bauteile Listen mit möglichen Fehlern und ggf. konstruktive Bedingungen für deren Ausschluss eingearbeitet. Ergänzend sind die grundlegenden und bewährten Sicherheitsprinzipien aufgeführt.

Für ein und dieselbe Gefahrstelle einer Maschine kann man für die verschiedenen Sicherheitsfunktionen zu unterschiedlichen erforderlichen Performance Levels (PL_r) kommen. Demnach gibt es in der Regel keinen einheitlichen PL_r für alle Sicherheitsfunktionen an einer Gefahrstelle.

Die beiden folgenden Abschnitte gehen auf zwei Spezialfälle bei der Risikominderung durch Sicherheitsfunktionen ein.

2.1 Aktoren in Sicherheitsfunktionen

Sicherheitsfunktionen dienen der Risikominderung an Maschinen. Zur Bewertung der Sicherheitsfunktionen wird DIN EN ISO 13849-1 [2] eingesetzt, deren Anwendungsbereich den sicherheitsbezogenen Teil der Steuerung umfasst. Dieser beginnt beim Sensor, also an der Schnittstelle zum technischen Prozess, beinhaltet die Logik und endet mit dem Leistungssteuerelement (z. B. Motorschütz, Ventil). Der eigentliche Aktor, z. B. der Motor oder der Hydraulikzylinder, liegt außerhalb des Anwendungsbereiches der Norm. Diese Abgrenzung ist sinnvoll, sofern der Ausfall eines Aktors nicht zu einem gefährlichen Zustand führen kann. Wenn an einer Maschine jedoch äußere Kräfte wirken, wie z. B. bei Vertikalachsen, kann der Ausfall eines Aktors (Bremse, Motor) zum Absturz der Last führen und somit zu einer Gefährdung. Die Aktoren sind in solchen Fällen in die Betrachtung der Sicherheitsfunktion mit einzubeziehen und durch zusätzliche sicher-

heitstechnische Maßnahmen zu ertüchtigen. Eine solche Maßnahme könnte beispielsweise ein Rückschlagventil am Hydraulikzylinder oder eine zusätzliche mechanische Bremse sein.

Die Methodik der DIN EN ISO 13849-1 [2] lässt sich auch bei Aktoren anwenden, allerdings müssen ggf. zusätzliche sicherheitsrelevante Eigenschaften (z. B. Festigkeiten) berücksichtigt werden. Das Fachbereichs-Informationsblatt Nr. 005 des Fachbereichs Holz und Metall der Deutschen Gesetzlichen Unfallversicherung (siehe Anhang B, Seite 115 ff.) zeigt speziell zum Thema „Schwerkraftbelastete Achsen“ typische Gefahrensituation auf und beschreibt geeignete Ansätze zur Risikominderung durch steuerungstechnische Maßnahmen.

2.2 Überlagerte Gefährdungen

Von überlagerten Gefährdungen spricht man z. B. dann, wenn eine Person an einem Standort durch mehrere gefahrbringende Bewegungen verletzt werden kann. Bei der Berechnung der möglichen Verletzungswahrscheinlichkeit ist nicht nur eine einzelne Bewegung zu betrachten, vielmehr müssen je nach Maschine bis zu 20 gefahrbringende Bewegungen berücksichtigt werden.

Da alle diese Bewegungen mit einer Ausfallwahrscheinlichkeit belegt sind, addieren sich die Ausfallwahrscheinlichkeiten einer Vielzahl von Bauteilen und der erforderliche Performance Level wird möglicherweise nicht mehr erreicht. Zusammen mit dem Fachbereich Holz und Metall der DGUV hat das IFA einen Lösungsweg beschrieben, der auf der Betrachtung von einzelnen Gefährdungen durch Maschinenteile beruht (Fachbereichs-Informationsblatt Nr. 47). Die regulatorischen Inhalte dieses Informationsblattes wurden in die dritte Normüberarbeitung der DIN EN ISO 13849-1 [2] übernommen. Infolgedessen wurde das Informationsblatt zurückgezogen. Der IFA Report 2/2017 beschreibt in Abschnitt 5.3.2 ein Beispiel für die Berechnung der PFH_D (Probability of a dangerous failure per hour, Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde) bei überlagerten Gefährdungen. Das zurückgezogene Informationsblatt Nr. 47 ist im Anhang J des IFA Reports 2/2017 zu finden.

3 Antriebssteuergeräte als sicherheitsbezogene Teile von Steuerungen

Antriebssteuergeräte, wie z. B. Frequenzumrichter, Servoregler oder Gleichstromsteller verwendet man seit vielen Jahren für die Drehzahlregelung von elektrischen Antrieben in Maschinen. Mit diesen Antrieben sind in der Regel gefahrbringende Bewegungen an den Maschinen verbunden. Trennende oder berührungslos wirkende Schutzeinrichtungen verhindern im Automatikbetrieb den Zugriff zu Gefahrstellen. Für Einricht- und Rüstarbeiten im Gefahrenbereich sind in erster Linie Maßnahmen zur Verhinderung des unerwarteten Anlaufs notwendig, die mit relativ geringem Aufwand, z. B. durch ein Netzschütz in der Energieversorgung des Antriebs oder ein Motorschütz zwischen Antriebssteuergerät und Motor, realisierbar sind. Antriebssteuergeräte mit integrierten Sicherheits-Teilfunktionen verfügen alternativ über eine sogenannte Impulssperre.

Gelegentlich muss jedoch auch bei laufender Maschine und damit bei aufgehobener Schutzwirkung von Schutzeinrichtungen gearbeitet werden. Hierbei sind ersatzweise Sicherheitsmaßnahmen notwendig, die den Bedienpersonen auch in solchen Situationen ausreichenden Schutz bieten. Beispielhaft ist der Einrichtbetrieb an einer Werkzeugmaschine zu nennen, bei dem u. a. Positionen manuell vermessen werden müssen, ohne dabei den Antrieb energielos schalten zu können. Das Abschalten der Antriebsenergie würde zu einem Lageverlust führen, der bei den geforderten Genauigkeiten der Bearbeitung nicht zu tolerieren ist. Der Antrieb muss also während des manuellen Eingriffs in Lageregelung verbleiben. Die Maschinenrichtlinie [6] lässt dies grundsätzlich zu (Anhang I, Abschnitt 1.2.5), allerdings sind in dieser Betriebsart zusätzliche Anforderungen an die Steuerung zu stellen (siehe Abschnitt 4.1 dieses Reports). Darüber hinaus müssen die Sicherheitsfunktionen in einem dem Risiko entsprechenden Performance Level (PL) nach DIN EN ISO 13849-1 [2] realisiert werden.

Anstelle der trennenden Schutzeinrichtungen und eines vom Netz freigeschalteten Motors sind hier andere Maßnahmen notwendig, die für die Bedienperson eine vergleichbare Sicherheit gewährleisten. Dies wird z. B. durch die Anwendung der in DIN EN 61800-5-2 [3] definierten Sicherheits-Teilfunktionen (Tabelle 1, Seite 12) erreicht.

Die in der Norm DIN EN 61800-5-2 [3] definierten Sicherheits-Teilfunktionen stellen eine Art Basis dar. Die Hersteller von PDS(SR) bieten darüber hinaus eine Vielzahl weiterer Sicherheits-Teilfunktionen an. Einige Basisfunktionen werden in Abschnitt 3.1 näher beschrieben.

Die vorstehend genannten Sicherheits-Teilfunktionen sind kein Ersatz für Einrichtungen zum Trennen der elektrischen Ausrüstung vom Netz. Solche Einrichtungen sind zusätzlich erforderlich, um die Ausführung von Arbeiten zu ermöglichen, ohne das Risiko eines elektrischen Schlags oder von Verbrennungen einzugehen.

Tabelle 1:
Sicherheits-Teilfunktionen aus DIN EN 61800-5-2

Abkürzung	Abschnitt der Norm	Bezeichnung englisch	Bezeichnung deutsch	Funktion
STO	4.2.3.2	Safe Torque Off	Sicher abgeschaltetes Drehmoment	Motor erhält keine Energie, die eine Drehbewegung erzeugen kann; Stopp-Kategorie 0 nach DIN EN 60204-1
SS1	4.2.3.3	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	4.2.3.4	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	4.2.4.2	Safe Operating Stop	Sicherer Betriebshalt	Motor steht still und widersteht externen Kräften.
SLA	4.2.4.3	Safely-Limited Acceleration	Sicher begrenzte Beschleunigung	Das Überschreiten eines Beschleunigungsgrenzwerts und/oder der Verzögerung wird verhindert.
SAR	4.2.4.4	Safe Acceleration Range	Sicherer Beschleunigungsbereich	Die Beschleunigung und/oder -verzögerung des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
SLS	4.2.4.5	Safely-Limited Speed	Sicher begrenzte Drehzahl	Das Überschreiten eines festgelegten Grenzwerts der Drehzahl wird verhindert.
SSR	4.2.4.6	Safe Speed Range	Sicherer Drehzahlbereich	Überwachung der Drehzahl des Motors innerhalb spezifizierter Grenzwerte
SLT	4.2.4.7	Safely-Limited Torque	Sicher begrenztes Drehmoment	Das Überschreiten eines Drehmoment-/Kraftgrenzwerts wird verhindert.
STR	4.2.4.8	Safe Torque Range	Sicherer Drehmomentenbereich	Überwachung des Drehmoments oder der festgelegten Kraft des Motors innerhalb spezifizierter Grenzwerte
SLP	4.2.4.9	Safely-Limited Position	Sicher begrenzte Position	Das Überschreiten eines Positionsgrenzwerts wird verhindert.
SLI	4.2.4.10	Safely-Limited Increment	Sicher begrenztes Schrittmaß	Der Motor wird um ein spezifiziertes Schrittmaß verfahren und stoppt anschließend.
SDI	4.2.4.11	Safe Direction	Sichere Bewegungsrichtung	Die Bewegung des Motors in die nicht vorgesehene Richtung um mehr als einen festgelegten Betrag wird verhindert.
SMT	4.2.4.12	Safe Motor Temperature	Sichere Motortemperatur	Das Überschreiten eines Motortemperaturgrenzwerts wird verhindert.
SCA	4.2.4.13	Safe Cam	Sicherer Nocken	Während sich die Motorposition in einem spezifizierten Bereich befindet, wird ein sicheres Ausgangssignal erzeugt.
SSM	4.2.4.14	Safe Speed Monitor	Sichere Drehzahlüberwachung	Während die Motordrehzahl niedriger als ein spezifizierter Wert ist, wird ein sicheres Ausgangssignal erzeugt.
SBC	4.2.5	Safe Brake Control	Sichere Bremsenansteuerung	Sichere Ansteuerung einer externen Bremse

3.1 Beschreibung von Sicherheits-Teilfunktionen

Nach DIN EN ISO 12100-1 [7] wird unter einer Sicherheitsfunktion eine Funktion einer Maschine verstanden, deren Ausfall zur unmittelbaren Erhöhung des Risikos führt. Eine Sicherheitsfunktion in diesem Sinne wird üblicherweise durch die Komponenten Sensor (Eingabegeräte), Logik (Verarbeitungseinheit) und Aktor (Ausgabegeräte) ausgeführt[2] . Die in diesem Report behandelten Antriebssteuergeräte decken dabei den Teil des Aktors ab. Je nach Implementierungsart kann die Logik miteingeschlossen sein. Die Sicherheitsfunktionen des PDS(SR) sind also lediglich ein Teil der vollständigen Sicherheitsfunktion einer Anwendung und werden deshalb als Sicherheits-Teilfunktion bezeichnet.

Die Erkennung von Fehlern spielt eine große Rolle in der Sicherheitstechnik. Speziell beim Einsatz von PDS(SR) sind die unterschiedlichen Reaktionen bei der Fehlererkennung zu berücksichtigen:

- Reaktion auf die Überschreitung von Grenzwerten

  Dies ist die Reaktionsfunktion, die durch die Überschreitung von Grenzwerten während des bestimmungsgemäßen Betriebs der Sicherheitsfunktionen ausgelöst wird.

- Fehlerreaktionsfunktion

  Dies ist die Reaktionsfunktion, die durch Erkennung eines Fehlers innerhalb der Sicherheitsfunktion ausgelöst wird.

In beiden Fällen müssen die möglichen sicheren Zustände für die Anwendung berücksichtigt werden. Wobei auch in Betracht gezogen werden muss, dass Teile des PDS(SR) nicht mehr funktionsfähig sind. Die Benutzerinformation eines PDS(SR) sollte hierüber informieren.

Die Sicherheits-Teilfunktionen lassen eine Einteilung in Stoppfunktionen und Überwachungsfunktionen zweckmäßig erscheinen.

Die folgenden Beschreibungen der Sicherheits-Teilfunktionen enthalten beispielhaft Zeitdiagramme zur Erläuterung des Verhaltens. Dieses Verhalten ist nicht zwangsläufig identisch bei unterschiedlichen PDS(SR). Trotz identischer Bezeichnung und Abkürzung kann es hier Unterschiede geben. Für den Einsatz der Geräte sind daher immer die jeweiligen Betriebsanleitungen zu berücksichtigen.

3.1.1 Stoppfunktionen

Die für Maschinen ebenfalls wichtige Norm zur elektrischen Ausrüstung DIN EN 60204-1 [9] unterscheidet die folgenden drei Kategorien von Stoppfunktionen:

Stopp-Kategorie 0:
Stillsetzen durch sofortiges Unterbrechen der Energiezufuhr zu den Maschinen-Antriebselementen (ungesteuertes Stillsetzen)

Stopp-Kategorie 1:
Ein gesteuertes Stillsetzen, wobei die Energiezufuhr zu den Maschinen-Antriebselementen beibehalten wird, um das Stillsetzen zu erzielen. Die Energiezufuhr wird erst dann unterbrochen, wenn der Stillstand erreicht ist.

Stopp-Kategorie 2:
Ein gesteuertes Stillsetzen, bei dem die Energiezufuhr zu den Maschinen-Antriebselementen beibehalten wird.

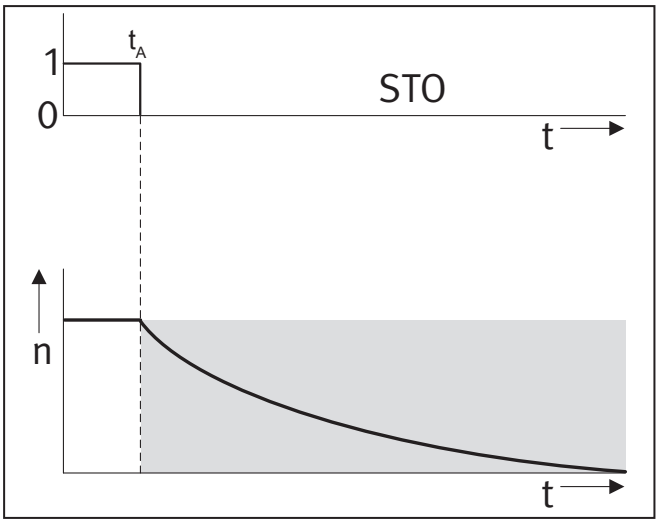
Die in DIN EN 61800-5-2 [3] definierten Stoppfunktionen berücksichtigen diese Stopp-Kategorien und werden in den nachfolgenden Abschnitten beschrieben.

3.1.1.1 Sicher abgeschaltetes Drehmoment (Safe Torque Off, STO)

„Diese Funktion verhindert, dass dem Motor eine kraft-erzeugende Energie zugeführt wird.“

In Abbildung 1 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von STO und der Motordrehzahl gezeigt.

Abbildung 1:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion STO (Safe Torque Off, sicher abgeschaltetes Drehmoment)



2 In DIN EN 61508-4:2011-02 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen“ gibt es hierzu unter Abschnitt 3.5.2 die Definition der „Gesamtsicherheitsfunktion“

Die Sicherheits-Teilfunktion STO entspricht einem ungesteuerten Stillsetzen nach DIN EN 60204-1 [9], Stopp-Kategorie 0. Sie kann angewendet werden, wenn die Abschaltung der Energie zur Verhinderung eines unerwarteten Anlaufs erforderlich ist. Eine Überwachung des Stillstands erfolgt nicht. Sollte die Sicherheits-Teilfunktion STO während des Betriebs aktiviert werden, trudelt der Motor ungebremst aus.

Bei vorhandenen äußeren Kräften (z. B. durch die Schwerkraft bei Vertikalachsen) können zur Risikominderung zusätzliche Maßnahmen erforderlich sein, wie z. B. mechanische Bremsen (siehe auch Abschnitt 5.4).

Elektronische Einrichtungen und Schütze, mit denen die Sicherheits-Teilfunktionen umgesetzt werden können, sind keine geeigneten Komponenten für eine galvanische Trennung. Für den ausreichenden Schutz gegen elektrischen Schlag sind zusätzliche Maßnahmen erforderlich (siehe hierzu auch Abschnitt 5.7).

Geeignete Maßnahmen für ein sicher abgeschaltetes Drehmoment sind z. B. (siehe Abbildung 2)

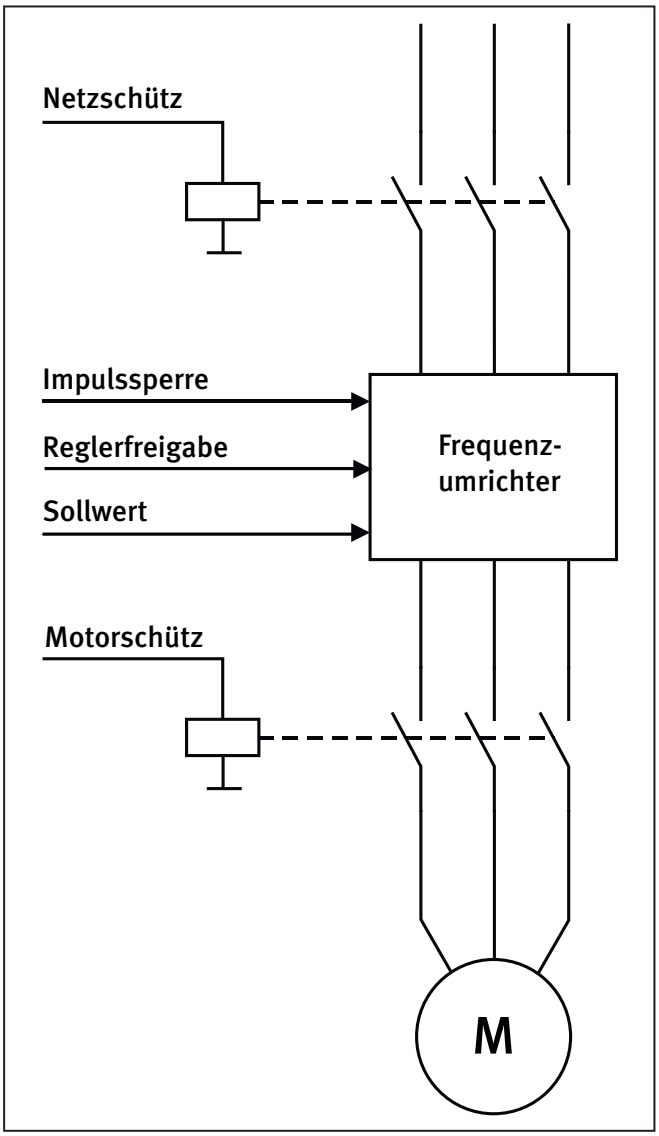
- Schütz zwischen Netz und Antriebssystem (Netzschütz),
- Schütz zwischen Leistungsteil und Antriebsmotor (Motorschütz),
- Impulssperre (Sperren der Ansteuerung der Leistungshalbleiter innerhalb des Frequenzumrichters),
- Reglerfreigabe,
- Sollwertvorgabe.

Je nach Kombination der vorstehenden Maßnahmen lassen sich unterschiedliche PL realisieren.

Anwendungsbeispiele:

- Verhinderung des unerwarteten Anlaufs von gefahrbringenden Bewegungen beim Einrichten, Rüsten und bei der Störungsbeseitigung.
- Beim Öffnen einer Schutztür wird STO aktiviert und der Motor trudelt aus.

Abbildung 2:
Alternative Prinzipien zur Realisierung von STO



3.1.1.2 Sicherer Stopp 1 (Safe Stop 1, SS1)

In DIN EN 61800-5-2 [3] werden die folgenden Varianten des SS1 beschrieben.

„Diese Funktion ist entweder festgelegt als

a) Sicherer Stopp 1 mit gesteuerter Verzögerung SS1-d (engl: safe stop 1 deceleration controlled)

Auslösen und Steuern der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der STO-Funktion (siehe DIN EN 61800-5-2 [3], 4.2.3.2), wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt[3]; oder

b) Sicherer Stopp 1 mit Überwachung der Verzögerungsrampe SS1-r (engl: safe stop 1 ramp monitored)

[3] Den Autoren ist zurzeit kein Produkt mit Lösung a) bekannt.

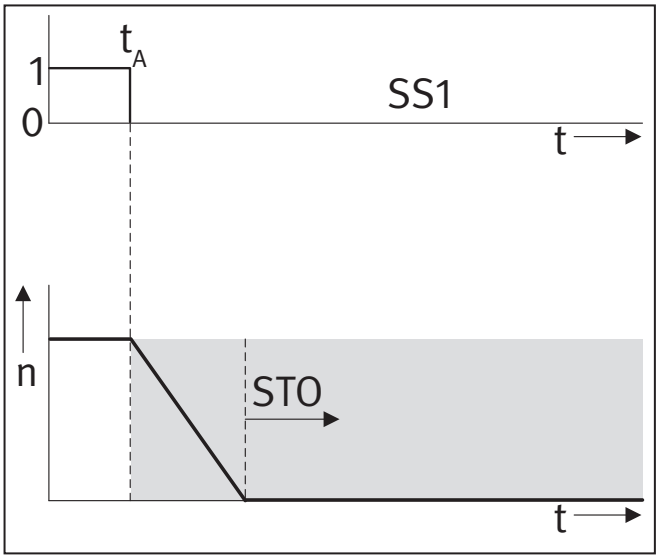
Auslösen und Überwachen der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der STO-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt; oder

c) *Sicherer Stopp 1 mit Zeitsteuerung*
SS1-t (engl: safe stop 1 time controlled)

Auslösen der Motorverzögerung und nach einer anwendungsspezifischen Zeitverzögerung Ausführen der STO-Funktion.“

In Abbildung 3 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SS1 und der Motordrehzahl gezeigt. Die Sicherheits-Teilfunktion SS1 entspricht einem gesteuerten Stillsetzen nach DIN EN 60204-1 [9], Stopp-Kategorie 1. Die „Größe der Motorverzögerung“ beschreibt, mit welchem Maß abgebremst wird.

Abbildung 3:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SS1 (Safe Stop 1, Sicherer Stopp 1)



Bei der Umsetzung der Sicherheits-Teilfunktion SS1-t, bei der nach Ablauf einer Zeitverzögerung die STO-Funktion ausgelöst wird, muss Folgendes beachtet werden: Während der Zeitverzögerung wird die Stillsetzfunktion der Antriebssteuerung nicht überwacht. Sie kann also unbemerkt ausfallen und der Motor könnte bis zum Auslösen der STO-Funktion ungebremst weiterlaufen, im ungünstigsten Fall sogar beschleunigen. Bei der Risikobeurteilung für die Maschine muss dieses Verhalten berücksichtigt werden. Kann ein solches Verhalten aufgrund der zu erwartenden Gefährdung nicht akzeptiert werden, ist die Umsetzung der Sicherheits-Teilfunktion als SS1-t nicht geeignet. Wird dagegen die Sicherheits-Teilfunktion als SS1-r realisiert, mit Überwachung der Bremsrampe (Größe der Motorverzögerung), kann eine fehlerhafte Stillsetzfunktion sehr schnell erkannt werden.

Anwendungsbeispiele:

- Beim Öffnen einer Schutztür wird SS1 ausgelöst und der Motor wird schnellstmöglich stillgesetzt. Anschließend ist der unerwartete Anlauf verhindert, da STO aktiv ist.
- Beim Auftreten von Unwuchten in einer Zuckerzentrifuge muss der Antrieb schnellstmöglich stillgesetzt werden, da sich die tonnenschwere Trommel lösen und außer Kontrolle geraten kann. Es ist zwingend SS1-r erforderlich, da durch einen fehlerhaften Antriebsregler eine Beschleunigung anstelle der Verzögerung nicht ausgeschlossen werden kann. Dies wird durch die Überwachung der Bremsrampe schnell erkannt und als Fehlerreaktion wird STO ausgeführt.

3.1.1.3 Sicherer Stopp 2 (Safe Stop 2, SS2)

In DIN EN 61800-5-2 [3] werden die folgenden Varianten des SS2 beschrieben.

„Diese Funktion ist entweder festgelegt als

a) *Sicherer Stopp 2 mit gesteuerter Verzögerung*
SS2-d (engl: safe stop 2 deceleration controlled)

Auslösen und Steuern der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der SOS-Funktion (siehe DIN EN 61800-5-2 [3], 4.2.4.2), wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt[4]; oder

b) *Sicherer Stopp 2 mit Überwachung der Verzögerungsrampe*
SS2-r (engl: safe stop 2 ramp monitored)

Auslösen und Überwachen der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der SOS-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt, oder

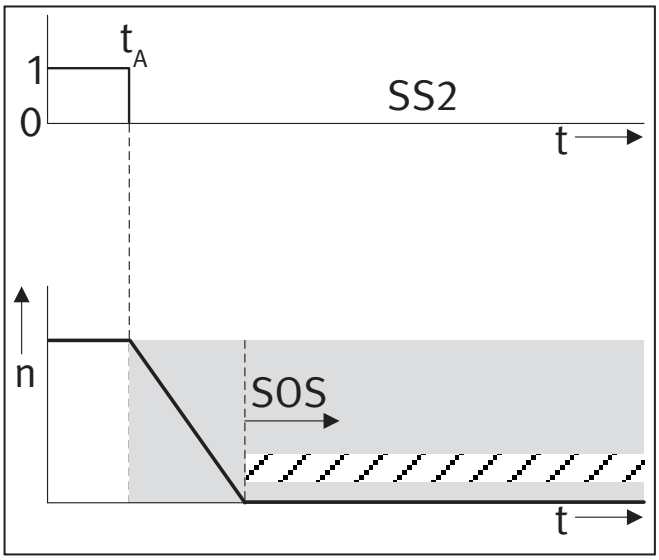
c) *Sicherer Stopp 2 mit Zeitsteuerung*
SS2-t (engl: safe stop 2 time controlled)

Auslösen der Motorverzögerung und nach einer anwendungsspezifischen Zeitverzögerung Ausführen der SOS-Funktion.“

In Abbildung 4 (Seite 16) ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SS2 und der Motordrehzahl gezeigt. Die Sicherheits-Teilfunktion SS2 entspricht einem gesteuerten Stillsetzen nach DIN EN 60204-1 [9], Stopp-Kategorie 2.

[4] Den Autoren ist zurzeit kein Produkt mit Lösung a) bekannt.

Abbildung 4:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SS2 (Safe Stop 2, Sicherer Stopp 2)



Bei der Umsetzung der Sicherheits-Teilfunktion SS2-t, bei der nach Ablauf einer Zeitverzögerung die SOS-Funktion ausgelöst wird, muss Folgendes beachtet werden: Während der Zeitverzögerung wird die Stillsetzfunktion der Antriebssteuerung nicht überwacht. Sie kann also unbemerkt ausfallen und der Motor könnte bis zum Auslösen der SOS-Funktion ungebremst weiterlaufen, im ungünstigsten Fall sogar beschleunigen. Bei der Risikobeurteilung für die Maschine muss dieses Verhalten berücksichtigt werden. Kann ein solches Verhalten aufgrund der zu erwartenden Gefährdung nicht akzeptiert werden, ist die Umsetzung der Sicherheits-Teilfunktion als SS2-t nicht geeignet.

Wird dagegen die Sicherheits-Teilfunktion als SS2-r realisiert, mit Überwachung der Bremsrampe (Größe der Motorverzögerung), kann eine fehlerhafte Stillsetzfunktion sehr schnell erkannt werden.

Anwendungsbeispiele:

- An einer Werkzeugmaschine muss während des Bearbeitungsprozesses eine Messung am Werkstück vorgenommen werden, ohne dass durch Abschalten der Motorregelung eine Positionsveränderung entsteht. Beim Öffnen der Schutztür wird SS2-r ausgelöst. Die gefahrbringende Bewegung wird stillgesetzt und anschließend wird der unerwartete Anlauf durch SOS verhindert.

- Die Last an einer Vertikalachse wird beim Öffnen einer Schutztür stillgesetzt und anschließend durch SOS in Position gehalten. Je nachdem, ob sich Bedienpersonen im Gefahrenbereich aufhalten können, sind weitere Maßnahmen erforderlich (siehe Informationsblatt 005 des Fachbereichs Holz und Metall im Anhang B).

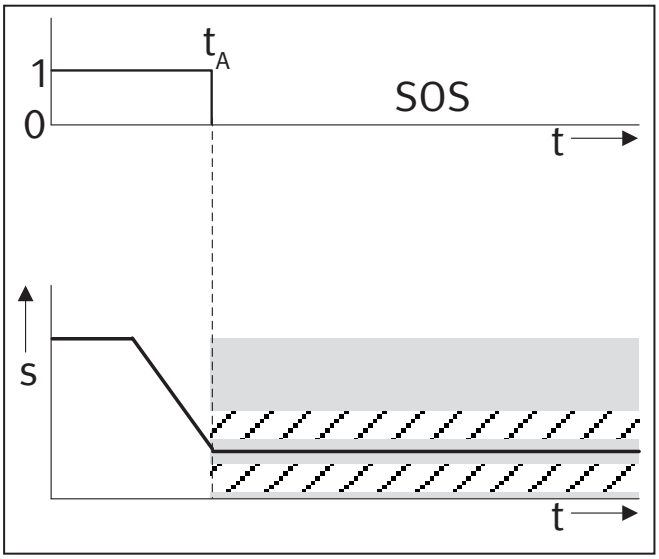
3.1.2 Überwachungsfunktionen

3.1.2.1 Sicherer Betriebshalt (Safe Operating Stop, SOS)

„Diese Funktion verhindert, dass der Motor um mehr als einen festgelegten Betrag von der Halteposition abweicht. Das PDS(SR) liefert dem Motor die Energie, die ermöglicht, dass er dem Angreifen äußerer Kräfte standhält.“ (Abschnitt 4.2.4.2 in [3]).

In Abbildung 5 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SOS und der Motorposition gezeigt.

Abbildung 5:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SOS (Safe Operating Stop, sicherer Betriebshalt)



Ist es erforderlich, das Antriebssystem an einem bestimmten Punkt im Fertigungsprozess zu stoppen, ohne die Position zu verlieren (z. B. Vorschub in einer Werkzeugmaschine), so müssen im Stillstand alle Regelfunktionen erhalten bleiben und gleichzeitig ist der unerwartete Anlauf zu verhindern. Dies wird durch eine sichere Überwachung des Stillstands erreicht, während der Motor in Lageregelung verbleibt. Ein unerwarteter Anlauf wird schnell erkannt. Als Reaktion auf diesen Fehler wird STO aktiviert, sodass eine Gefährdung von Personen vermieden wird. Nach Aufheben von SOS kann die Antriebsbewegung unmittelbar von der Stopp-Position aus fortgesetzt werden.

Anwendungsbeispiele:

- Einrichtbetrieb an Drehautomaten/Bearbeitungszentren,

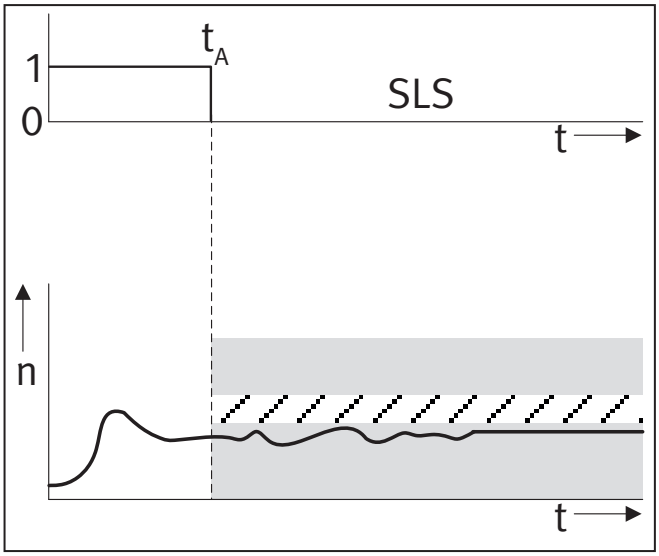
- manuelles Messen während der Bearbeitung.

3.1.2.2 Sicher begrenzte Drehzahl (Safely-Limited Speed, SLS)

„*Diese Funktion verhindert, dass der Motor den festgelegten Grenzwert der Drehzahl überschreitet.*“ (Abschnitt 4.2.4.5 in [3]).

In Abbildung 6 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SLS und der Achsdrehzahl gezeigt.

Abbildung 6:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SLS (Safely-Limited Speed, sicher begrenzte Drehzahl)



Bei dieser Sicherheits-Teilfunktion verhindert eine sichere Überwachung, dass der Antrieb einen vorgegebenen Drehzahlgrenzwert überschreitet. Ein Überschreiten des Grenzwerts wird erkannt und der Antrieb wird sicher stillgesetzt.

Anwendungsbeispiele:

- Einrichtbetrieb an Drehautomaten/Bearbeitungszentren,
- Einfädeln von Material an Kalanderwalzen.

Hinweis:

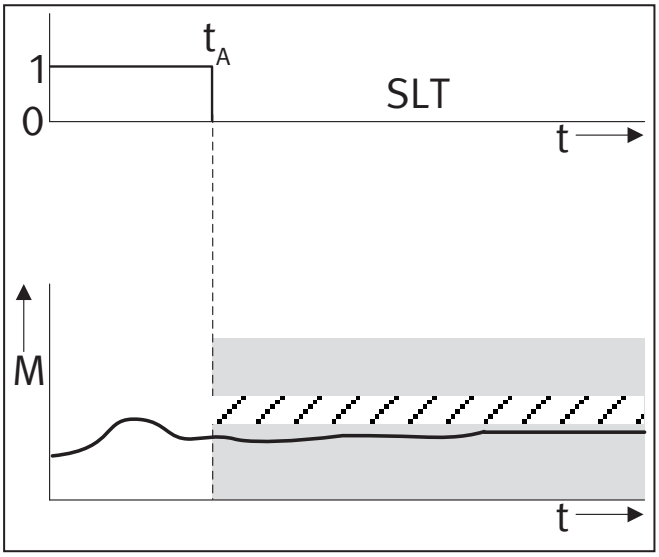
Es existiert keine allgemeine Festlegung für Drehzahlgrenzwerte, die als so sicher angesehen werden, dass Bedienpersonen dadurch nicht gefährdet sind. Je nach Maschine werden unterschiedliche Drehzahlen als sicher angesehen. Das IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz, Kennzahl 330 216 [10], enthält eine Übersicht über entsprechende Festlegungen in maschinenspezifischen Normen (C-Normen).

3.1.2.3 Sicher begrenztes Drehmoment (Safely-Limited Torque, SLT)

„*Diese Funktion verhindert, dass der Motor das festgelegte Drehmoment (oder bei Anwendung eines Linearmotors die festgelegte Kraft) überschreitet.*“ (Abschnitt 4.2.4.7 in [3]).

In Abbildung 7 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SLT und des Motordrehmoments gezeigt.

Abbildung 7:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SLT (Safely-Limited Torque, sicher begrenztes Drehmoment)



Das Schadensausmaß durch eine gefahrbringende Bewegung wird durch SLT verringert. Orientierende Werte hinsichtlich der Einwirkung von Kräften enthält Kapitel 6 der Grenzwerteliste des IFA Reports 3/2017 [11].

Anwendungsbeispiele:

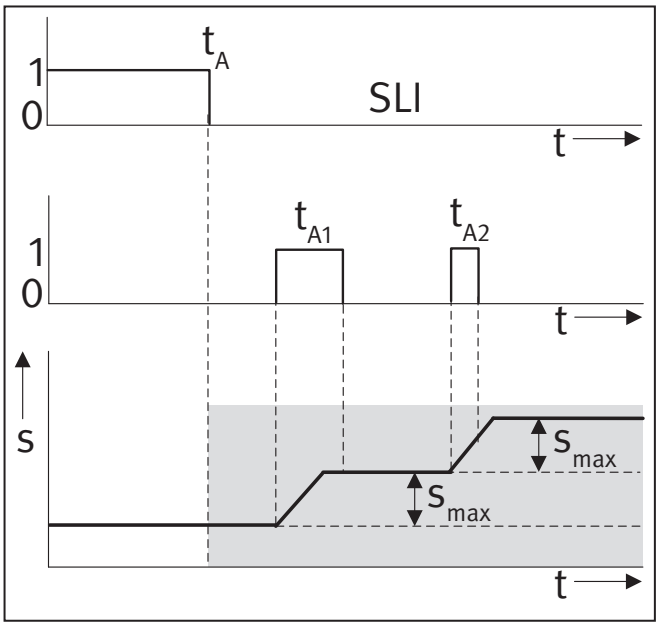
- Kraftbegrenzung an Schließkanten von kraftbetätigten Türen und Toren,
- Verhinderung des Einzugs von Bedienpersonal an Wickelmaschinen.

3.1.2.4 Sicher begrenztes Schrittmaß (Safely-Limited Increment, SLI)

„*Diese Funktion verhindert, dass die Motorwelle (oder die Antriebsvorrichtung, wenn ein Linearmotor verwendet wird) den festgelegten Grenzwert eines Lageschrittmaßes überschreitet.*“ (Abschnitt 4.2.4.10 in [3]).

Abbildung 8 (Seite 18) zeigt das zeitliche Verhalten des Eingangssignals zur Aktivierung von SLI, des Befehls zum Auslösen der Bewegung und des erfolgten Schritts.

Abbildung 8:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SLI (Safely-Limited Increment, sicher begrenztes Schrittmaß)



Bei dieser Sicherheits-Teilfunktion darf der Antrieb nach einem Start-Befehl maximal einen fest vorgegebenen Weg (Schrittmaß) abfahren. Nach Erreichen des Grenzwerts muss ein STO oder ein sicherer Betriebshalt SOS wirksam werden. Ein Überschreiten der Grenzwerte wird erkannt und der Antrieb wird sicher stillgesetzt.

Anwendungsbeispiele:

- Einrichtbetrieb an Drehautomaten/Bearbeitungszentren.
- Wegbegrenztes Tippen an Druckmaschinen.

3.1.2.5 Sicher begrenzte Position (Safely-Limited Position, SLP)

„Diese Funktion verhindert, dass die Motorwelle (oder die Antriebsvorrichtung, wenn ein Linearmotor verwendet wird) die festgelegte(n) Lagebegrenzung(en) überschreitet.“ (Abschnitt 4.2.4.9 in [3]).

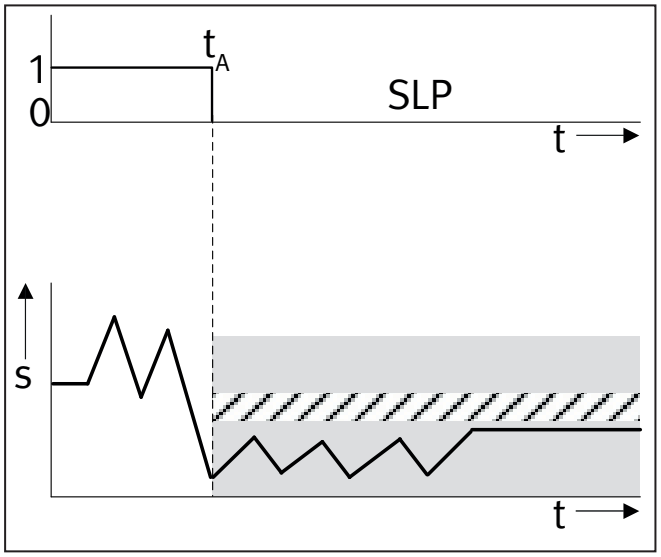
In Abbildung 9 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SLP und der Motorwellenposition gezeigt.

Durch eine sichere Lageüberwachung wird erreicht, dass das Antriebssystem bei Erreichen eines vorgegebenen Absolutlage-Grenzwerts in einen STO oder sicheren Betriebshalt SOS übergeht. Hinsichtlich des Grenzwerts muss der technisch bedingte Nachlauf berücksichtigt werden. Unterhalb des Grenzwerts muss mit unerwarteten Bewegungen des Antriebs gerechnet werden. Das Überschreiten eines Grenzwerts wird erkannt und das Antriebssystem wird sicher stillgesetzt.

Anwendungsbeispiele:

- Bereichsaufteilung an einer Maschine in Fertigungs- und Beschickungsbereich.
- Begrenzung eines Verfahrbereichs (Ersatz von elektromechanischen Endschaltern).
- Begrenzung der Reichweite von Roboterarmen.

Abbildung 9:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SLP (Safely-Limited Position, sicher begrenzte Position)



3.1.2.6 Sicher begrenzte Beschleunigung (Safely-Limited Acceleration, SLA)

„Diese Funktion verhindert, dass der Motor den festgelegten Grenzwert der Beschleunigung und/oder der Verzögerung überschreitet.“ (Abschnitt 4.2.4.3 in [3]).

In Abbildung 10 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SLA und der Motorbeschleunigung gezeigt.

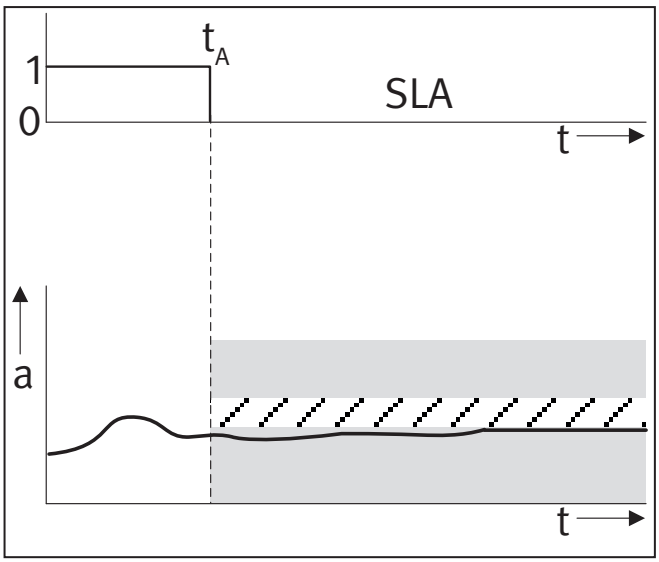
Ein Überschreiten des Beschleunigungs-Grenzwerts wird erkannt und der Antrieb wird sicher stillgesetzt. Der Beschleunigungs-Grenzwert kann positiv und negativ sein, sodass mit dieser Funktion auch das Maß der Verzögerung begrenzt werden kann.

Anwendungsbeispiele:

- Beim Transport offener Flüssigkeitsbehälter wird verhindert, dass durch zu hohe Beschleunigung oder Verzögerung Flüssigkeit austritt.

- Die Beschleunigung bestimmter Schleifscheiben muss begrenzt werden, weil die Scheiben ansonsten durch Trägheitskräfte bersten könnten.

Abbildung 10:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SLA (Safely-Limited Acceleration, sicher begrenzte Beschleunigung)

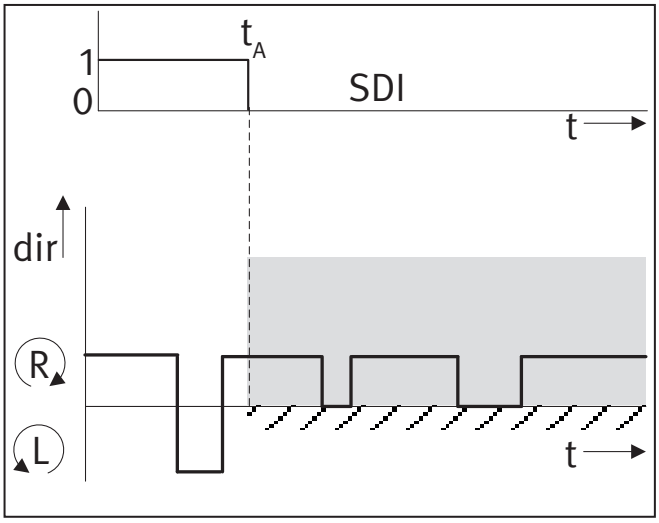


3.1.2.7 *Sichere Bewegungsrichtung (Safe Direction, SDI)*

„*Diese Funktion verhindert, dass sich die Motorwelle um mehr als einen festgelegten Betrag in die nicht vorgesehene Richtung bewegt.*“ (Abschnitt 4.2.4.11 in [3]).

In Abbildung 11 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SDI und der Drehrichtung gezeigt.

Abbildung 11:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SDI (Safe Direction, sichere Bewegungsrichtung)



Eine Bewegung in die unzulässige Richtung wird erkannt und der Antrieb wird sicher stillgesetzt.

Anwendungsbeispiele:

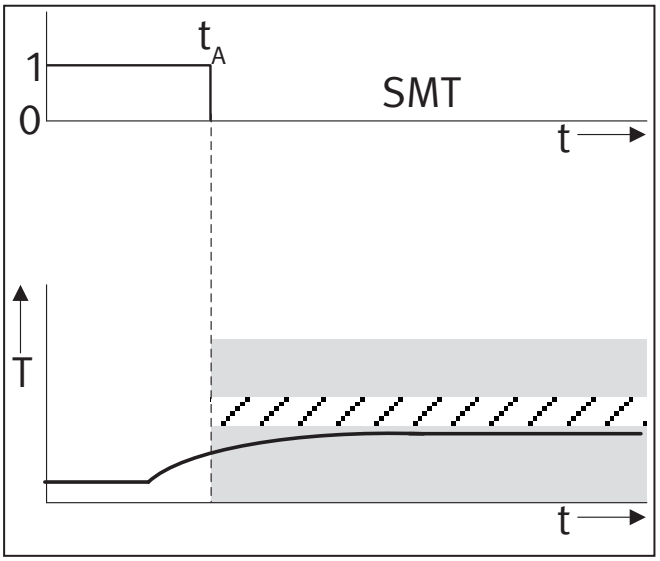
- Es wird verhindert, dass sich Maschinenteile auf die Bedienperson zubewegen.
- Eine Richtungsumkehr von Walzen wird verhindert, da ansonsten Einzugsstellen entstehen können.

3.1.2.8 *Sichere Motortemperatur (Safe Motor Temperature, SMT)*

„*Diese Funktion verhindert, dass die Motortemperatur(en) (einen) festgelegte(n) obere(n) Grenzwert(e) überschreitet.*“ (Abschnitt 4.2.4.12 in [3]).

In Abbildung 12 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SMT und der Motortemperatur gezeigt.

Abbildung 12:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SMT (Safe Motor Temperature, sichere Motortemperatur)



Eine Temperatur über dem Grenzwert wird erkannt und der Antrieb wird sicher stillgesetzt.

Anwendungsbeispiele:

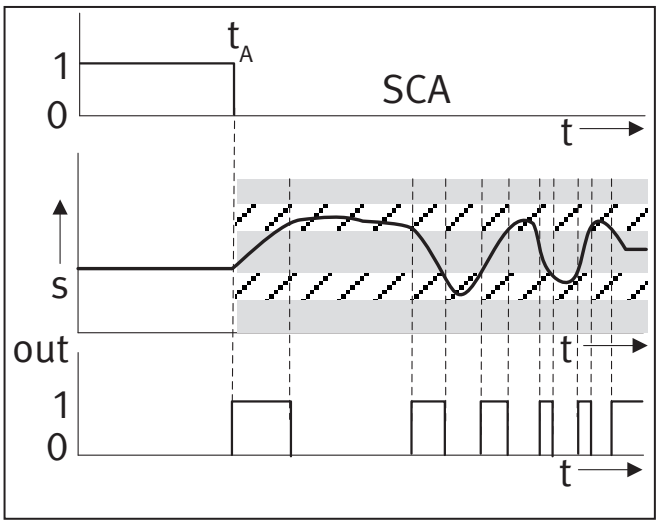
- Für den Einsatz in explosionsgefährdeten Bereichen werden unzulässig hohe Temperaturen am Motor verhindert.
- Brandschutz.

3.1.2.9 Sicherer Nocken (Safe Cam, SCA)

„Diese Funktion liefert ein sicheres Ausgangssignal, um anzuzeigen, ob die Motorwelle innerhalb eines festgelegten Bereiches liegt.“ (Abschnitt 4.2.4.13 in [3]).

In Abbildung 13 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SCA, der Motorposition und des Ausgangssignals gezeigt.

Abbildung 13:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SCA (Safe Cam, sicherer Nocken)



Mithilfe von Parametern wird ein bestimmter Verfahrbereich einer Achse festgelegt. Immer dann, wenn sich die Achse in diesem Bereich befindet, wird ein sicheres Ausgangssignal erzeugt. Das Verlassen des Bereichs hat keinerlei Auswirkungen auf die Funktion innerhalb des PDS(SR), es wird lediglich ein entsprechendes Ausgangssignal gesetzt.

Anwendungsbeispiele:

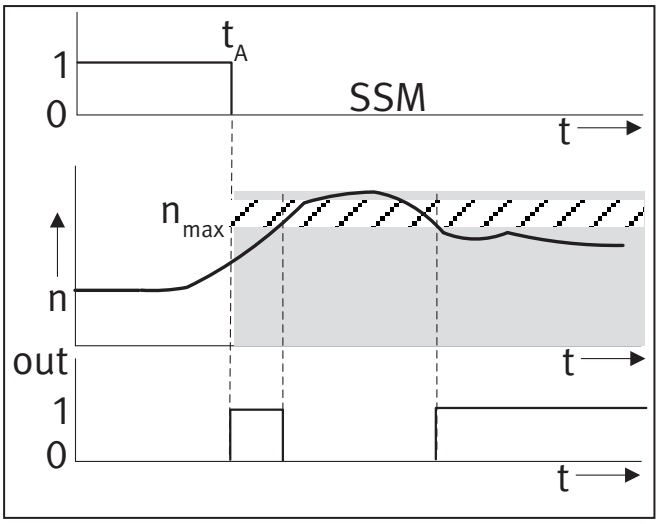
- Die Entsperrung einer Zuhaltung an einer Schutztür wird nur dann erlaubt, wenn sich das Maschinenteil in einem sicheren Bereich befindet. Ggf. ist zusätzlich der unerwartete Anlauf zu verhindern (STO).
- Ersatz von Positionssensoren.
- Lagebegrenzung von Roboterachsen.

3.1.2.10 Sichere Drehzahlüberwachung (Safe Speed Monitor, SSM)

„Diese Funktion liefert ein sicheres Ausgangssignal, um anzuzeigen, ob die Motordrehzahl unterhalb eines festgelegten Grenzwerts liegt.“ (Abschnitt 4.2.4.14 in [3]).

In Abbildung 14 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SSM, der Motordrehzahl und des Ausgangssignals gezeigt.

Abbildung 14:
Beispiel für den zeitlichen Ablauf der Sicherheits-Teilfunktion SSM (Safe Speed Monitor, sichere Drehzahlüberwachung)



Bei aktivierter SSM-Funktion wird dann ein sicheres Ausgangssignal erzeugt, wenn die aktuelle Motordrehzahl unterhalb des Grenzwerts n_{max} liegt. Bei Überschreitung des Grenzwerts wird lediglich das Ausgangssignal zurückgesetzt, es erfolgen keine weiteren Reaktionen innerhalb des PDS(SR).

Anwendungsbeispiel:

- Die Entsperrung einer Zuhaltung an einer Schutztür wird nur dann erlaubt, wenn der Antrieb eine gefährliche Drehzahl unterschreitet.

3.1.3 Ausgangsfunktion – Sichere Bremsenansteuerung (Safe Brake Control, SBC)

„Diese Funktion liefert (ein) sichere(s) Ausgangssignal(e) zur Ansteuerung einer (von) externen Bremse(n).“ (Abschnitt 4.2.5 in [3]).

Auch bei Motoren, die von Frequenzumrichtern angesteuert werden, gibt es teilweise die Notwendigkeit, zusätzliche mechanische Bremsen einzusetzen. Dies trifft insbesondere dann zu, wenn auf einen Motor externe Kräfte einwirken, z. B. die Schwerkraft oder Zugkräfte bei der Bearbeitung von Materialbahnen. Die Ansteuerung dieser Bremsen kann vom PDS(SR) mit der Sicherheits-Teilfunktion SBC erfolgen. Der Zeitpunkt der Ansteuerung ist applikationsspezifisch, z. B. unmittelbar nach erfolgter Stillsetzung, bei Erkennung von Fehlern der Antriebssteuerung, bei NOT-HALT usw.

Anwendungsbeispiele:

- Ansteuerung einer externen Bremse an einer Vertikalachse gleichzeitig mit Aktivierung von STO,
- Ansteuerung einer externen Bremse an einer Vertikalachse bei Spannungsausfall.

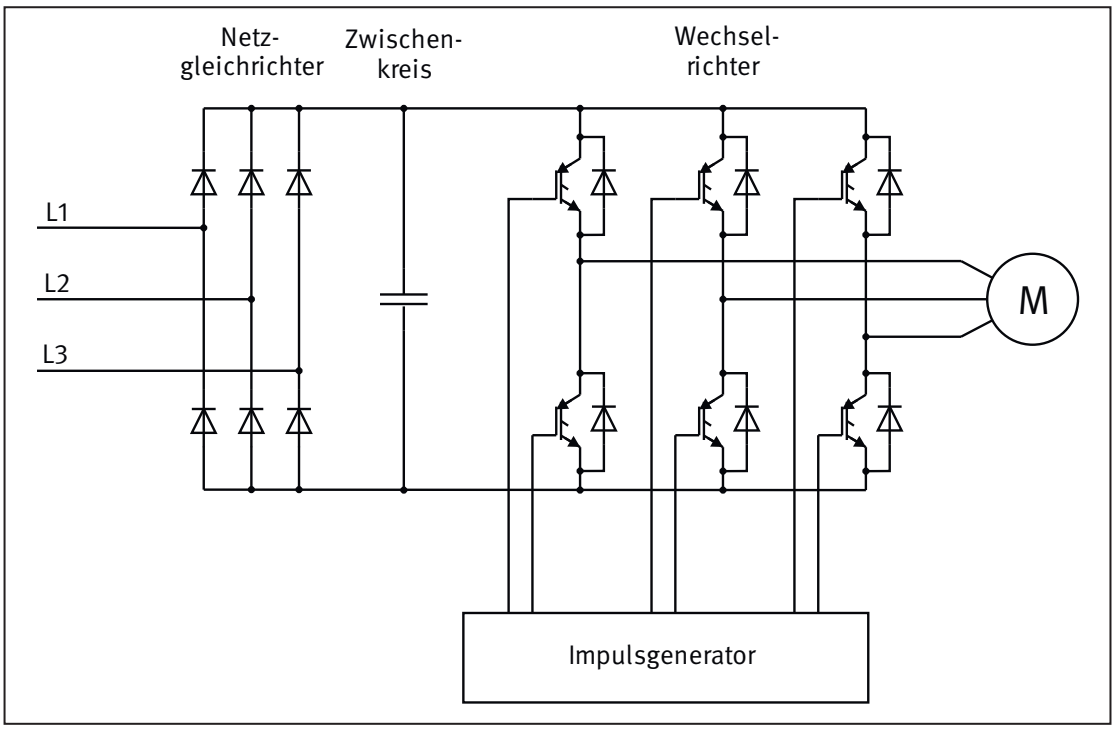
4 Frequenzumrichter und Sicherheitsfunktionen

4.1 Frequenzumrichter ohne integrierte Sicherheits-Teilfunktionen (PDS)

Wurde noch vor wenigen Jahrzehnten der Großteil der drehzahlveränderbaren Antriebe aufgrund der einfachen Regelbarkeit in Gleichstromtechnik ausgeführt, so übernehmen diese Funktion heute überwiegend Drehstromantriebe mit Frequenzumrichtern. Die Entwicklungen im Bereich der Mikroprozessoren und Leistungselektronik haben maßgeblich dazu beigetragen.

Ein Frequenzumrichter besteht, wenn man den prinzipiellen Aufbau betrachtet, aus der Hintereinanderschaltung eines Netzgleichrichters, eines Gleichspannungszwischenkreises und eines Wechselrichters. In Abbildung 15 ist der prinzipielle Aufbau dargestellt.

Abbildung 15:
Prinzipschaltbild eines konventionellen Frequenzumrichters



Der Netzgleichrichter ist ein Brückengleichrichter, der aus der Wechselspannung des Drehstromnetzes eine Gleichspannung erzeugt. Es kommen sowohl ungeregelte als auch geregelte Gleichrichterbrücken zum Einsatz.

Der Gleichspannungszwischenkreis ist in der Regel mit einem Zwischenkreiskondensator versehen, der die Gleichspannung glättet und darüber hinaus als Energiespeicher dient. Teilweise werden auch Induktivitäten als Energiespeicher im Zwischenkreis eingesetzt.

Im Wechselrichter des Frequenzumrichters wird aus der Gleichspannung des Zwischenkreises mithilfe der Leistungshalbleiter (z. B. IGBTs) eine dreiphasige Ausgangsspannung erzeugt, deren Höhe und Frequenz in weiten Bereichen geregelt werden kann. Die Ansteuerung der Leistungshalbleiter zur Erzeugung des Drehfelds erfolgt durch Pulsweitenmodulation (PWM). Die entsprechenden Pulsmuster werden im Mikroprozessor des Umrichters oder in einem separaten Baustein (z. B. FPGA, ASIC) erzeugt.

Je nach Ausführung können Frequenzumrichter nicht nur zum Antreiben, sondern auch zum Abbremsen von Motoren eingesetzt werden. Hierbei findet eine Richtungsumkehr des Energieflusses statt. Zur Umwandlung der kinetischen Energie sind zwei Varianten üblich:

- Die kinetische Energie wird als elektrische Energie über den Zwischenkreis und einen geeigneten Wechselrichter ins Netz zurückgespeist.
- Die kinetische Energie wird vom Zwischenkreis aus über einen Bremswiderstand in thermische Energie umgewandelt.

Sicherheitsfunktionen können mit konventionellen Frequenzumrichtern nur in begrenztem Maße direkt realisiert werden. In aller Regel sind zusätzliche Komponenten

erforderlich. Am Beispiel der Sicherheits-Teilfunktion „Sicher abgeschaltetes Drehmoment“ (Safe Torque Off, STO) kann dies verdeutlicht werden.

Die Aktivierung der Sicherheits-Teilfunktion STO kann beispielsweise über die Reglerfreigabe des Umrichters erfolgen. Durch Wegschalten des Steuersignals an diesem Eingang wird die Erzeugung von Pulsmustern gesperrt. Im Motor kann kein Drehfeld mehr erzeugt werden.

Die Signalverarbeitung erfolgt in diesem Fall einkanalig unter Beteiligung des Mikroprozessors, womit maximal PL b möglich ist. In den meisten Anwendungen an Maschinen werden jedoch höhere PL benötigt, die einkanalig nicht zu realisieren sind. Es ist also ein zweiter unabhängiger Kanal erforderlich. Hierfür bietet sich z. B. die Verwendung eines Netzschützes an (vgl. Abschnitt 3.1.1.1).

4.2 Frequenzumrichter mit integrierten Sicherheits-Teilfunktionen (PDS(SR))

Konventionelle Frequenzumrichter, wie sie in Abschnitt 4.1 beschrieben wurden, sind in erster Linie so konstruiert, dass sie die funktionalen Anforderungen erfüllen und den zu erwartenden Betriebsbeanspruchungen, z. B. Vibrationen, Temperaturen, elektromagnetische Störeinflüsse oder Störungen der Energieversorgung, genügen. Dies wird u. a. durch die Einhaltung der Bestimmungen in der Normenreihe DIN EN 61800 gewährleistet.

Auf der Basis dieser konventionellen Geräte wurden Frequenzumrichter entwickelt, bei denen Sicherheits-Teilfunktionen wie STO oder eine sichere Bewegungsüberwachung bereits integriert sind. Das bringt eine Reihe von Vorteilen mit sich und vereinfacht die Realisierung sicherer Maschinensteuerungen. Darüber hinaus sind einige Anwendungen aufgrund unzulässig langer Reaktionszeiten ohne integrierte Sicherheitstechnik überhaupt nicht möglich.

Um die einzelnen Sicherheits-Teilfunktionen im Frequenzumrichter zu realisieren, werden unterschiedliche Anforderungen an die Komplexität und die Ausführung der Hardware gestellt. Die Sicherheits-Teilfunktion STO kann mit relativ geringem Aufwand in einen Frequenzumrichter integriert werden. Dagegen erfordert beispielsweise die Sicherheits-Teilfunktion SLS eine deutlich komplexere Gestaltung. Im Folgenden soll für die Realisierung von Sicherheits-Teilfunktionen zwischen „Impulssperre“ und „Sicherer Bewegungsüberwachung“ unterschieden werden.

Zunächst soll anhand einer Fehlerbetrachtung gezeigt werden, mit welchen Fehlern bzw. Ausfällen in Frequenzumrichtern zu rechnen ist und welche Auswirkungen diese Fehler auf die Funktion haben. Danach werden geeignete Möglichkeiten zur Realisierung der Sicherheits-Teilfunktion STO vorgestellt.

4.2.1 Fehlerbetrachtung

Die Fehlerbetrachtung entstammt einer Untersuchung des IFA. Dabei wurden folgende, für diese Betrachtung relevante Erkenntnisse gewonnen.

- Das unbeabsichtigte Einschalten, der Verlust der Sperrfähigkeit (Kurzschluss) oder das zu späte Ausschalten eines oder mehrerer Leistungshalbleiter im Wechselrichter während des Betriebs (Motor wird angetrieben) führt zum Kurzschluss des Zwischenkreises und infolgedessen zum Ansprechen von Sicherungen oder zur Zerstörung weiterer Halbleiter. In jedem Fall macht sich der Fehler durch Betriebshemmung bemerkbar. Treten die genannten Fehler während des Bremsens auf, muss mit dem Ausfall der elektrogeneratorischen Bremsung gerechnet werden.

- Der Verlust der Sperrfähigkeit (Kurzschluss) eines oder mehrerer Leistungshalbleiter in der Gleichrichterbrücke des Netzgleichrichters führt zum Kurzschluss von mindestens zwei Phasen des speisenden Drehstromnetzes. Die Folge ist das Ansprechen von Sicherungen oder die Zerstörung weiterer Leistungshalbleiter. In jedem Fall macht sich der Fehler durch Betriebshemmung bemerkbar.

- Der Verlust der Leitfähigkeit (Unterbrechung) eines oder mehrerer Leistungshalbleiter im Wechselrichter führt dazu, dass am Ausgang die zur Verfügung stehende Leistung gemindert ist. Das erzeugte Drehmoment sinkt sowohl beim Antreiben als auch beim Bremsen ab oder entfällt völlig.

- Der Verlust der Leitfähigkeit (Unterbrechung) eines oder mehrerer Leistungshalbleiter in der Gleichrichterbrücke des Netzgleichrichters führt dazu, dass die am Ausgang der Gleichrichterbrücke bzw. im Zwischenkreis zur Verfügung stehende Leistung gemindert ist. Das erzeugte Drehmoment sinkt sowohl beim Antreiben als auch beim Bremsen ab oder entfällt völlig.

- Die zum Erzeugen eines Drehfelds erforderlichen Pulsmuster sind sehr komplex. Sie können ausschließlich mithilfe aufwendiger elektronischer Schaltungen erzeugt werden. Das zufällige Entstehen eines geeigneten Impulsmusters, z. B. aufgrund einer Beeinflussung durch elektromagnetische Störungen oder durch Bauteilfehler im Leistungsteil, wie sie zuvor beschrieben wurden, kann ausgeschlossen werden.

Mit Bauteilausfällen oder einer Beeinflussung der Signal- bzw. Steuereingänge des Frequenzumrichters, die jede denkbare, unbeabsichtigte oder fehlerhafte Ansteuerung

der Impulsmustererzeugung zur Folge hat, muss jedoch gerechnet werden. Dies kann zu spontanen und unerwarteten Fehlfunktionen führen, wie beispielsweise unerwartetem Anlauf, Drehzahlerhöhung und ggf. Abbruch des Bremsvorgangs mit Weiter- oder Hochlauf des Antriebs. Zur Vermeidung gefahrbringender Situationen sind besondere, dem jeweiligen Risiko angepasste Maßnahmen erforderlich.

4.2.2 Impulssperre

Wird durch einen geeigneten zusätzlichen Schaltungsteil im Frequenzumrichter sicher verhindert, dass die Leistungshalbleiter des Wechselrichters mit Impulsmustern angesteuert werden, so ist dies eine Möglichkeit, die Sicherheits-Teilfunktion STO zu realisieren. Im Wechselrichter kann kein Drehfeld mehr erzeugt werden, folglich auch kein Drehmoment im Motor. Mit der Sicherheits-Teilfunktion STO kann der Schutz vor unerwartetem Anlauf des Motors umgesetzt werden.

Eine geeignete Stelle für eine solche Schaltung bietet sich an den Übertragungselementen für die Impulsmuster, die zwischen dem Mikroprozessor und dem Wechselrichter für eine galvanische Trennung sorgen. Unabhängig davon, ob hierfür Übertrager oder Optokoppler verwendet werden, ist das Prinzip das Gleiche.

Bei Verwendung von Optokopplern sperrt man die Übertragung der Impulsmuster, indem die Versorgungsspannung für die Optokoppler abgeschaltet wird (Abbildung 16). Sobald an den Anoden der Optokoppler keine Spannung anliegt, können keine Signale mehr übertragen werden, selbst wenn der Mikroprozessor Impulsmuster generiert und damit die Optokoppler ansteuert.

Kombiniert man diese Impulssperre beispielsweise mit dem Wegschalten der Reglerfreigabe, so wird zweikanalig verhindert, dass der Wechselrichter mit geeigneten Impulsmustern angesteuert wird. Verbunden mit einer entsprechenden Fehlererkennung (siehe Abschnitt 4.2.3) lässt sich eine sicherheitsrelevante Schaltung in Kategorie 3 oder 4 nach DIN EN ISO 13849-1 [2] realisieren.

Eine andere Möglichkeit, die Anforderungen der Kategorie 3 oder 4 im Hinblick auf die Einfehlersicherheit zu erfüllen, bietet die sinnvolle Aufteilung der IGBTs in zwei Gruppen. Dabei werden jeweils die drei Optokoppler der oberen IGBTs und die drei Optokoppler der unteren IGBTs zu einem Abschaltpfad zusammengefasst (Abbildung 17).

Hierbei bedient man sich der Tatsache, dass immer eine entsprechende Kombination der oberen und der unteren IGBTs angesteuert werden muss, um einen Stromfluss bzw. ein Drehfeld im Motor zu erzeugen. Das bedeutet im Umkehrschluss, dass im Fehlerfall die Abschaltung eines der beiden Kanäle ausreicht, um die Ausführung der Sicherheits-Teilfunktion STO zu gewährleisten.

Abbildung 16:
Unterbrechung der Versorgungsspannung für die Optokoppler

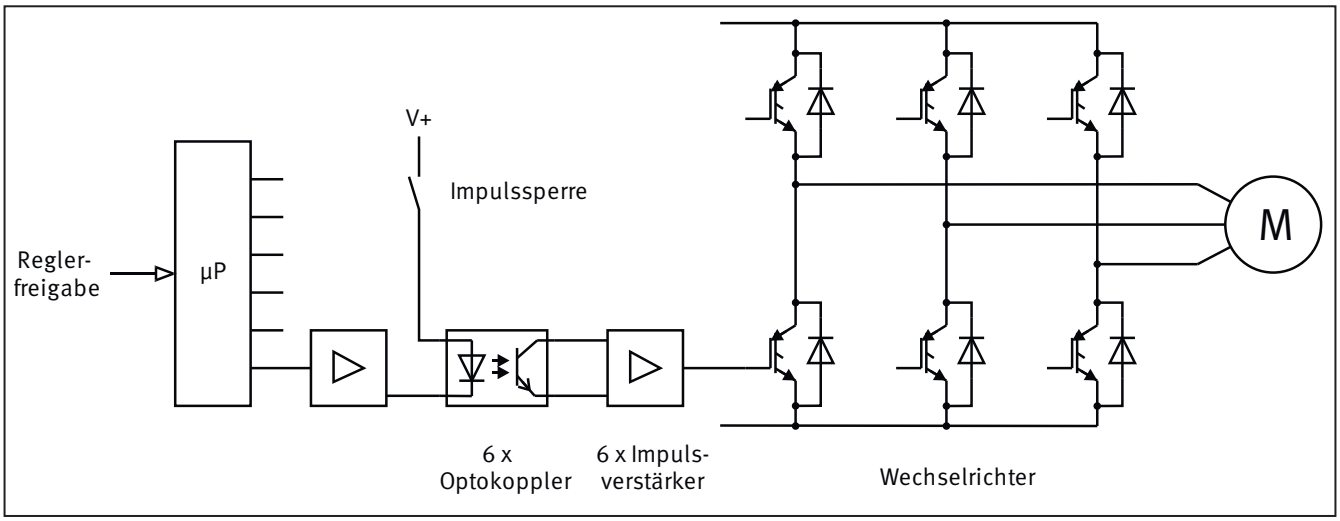
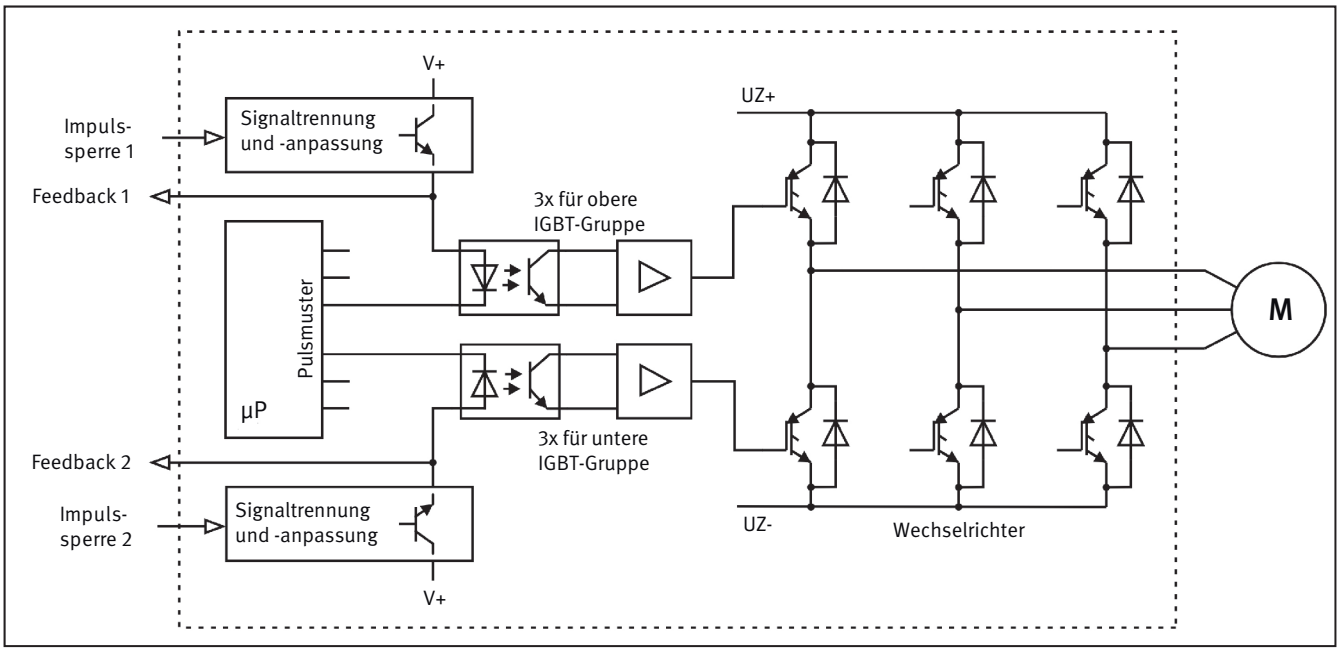


Abbildung 17:
Aufteilung in zwei IGBT-Gruppen



Neben den gezeigten Beispielen zur Implementierung der Sicherheits-Teilfunktion STO in einem Frequenzumrichter sind noch weitere Möglichkeiten denkbar, auf die hier aber nicht eingegangen werden soll.

Hinweise:

Die Impulssperre kann zufällige Bauteilfehler im Leistungskreis nicht verhindern. Es kann daher beim gleichzeitigen Auftreten von zwei bestimmten Fehlern im Leistungsteil zu einer ruckartigen Bewegung am Motor kommen, die maximal 180° pro Polpaarzahl betragen kann. Ein Anlauf des Motors ist jedoch nicht möglich. Im konkreten Anwendungsfall muss geprüft werden, ob die mögliche Ruckbewegung der Motorwelle zu einer gefahrbringenden Maschinenbewegung führen kann.

Durch die Impulssperre findet keine galvanische Trennung des Motors vom Netz statt, dadurch kann sowohl am Frequenzumrichter als auch an den Motorklemmen nach wie vor Spannung anliegen. Für Wartungs- und Reparaturarbeiten ist deshalb zusätzlich ein geeigneter Schalter mit Trennfunktion erforderlich.

4.2.3 Fehlererkennung

Die Abschaltpfade in einem Frequenzumrichter, unabhängig davon, ob es sich um Impulssperre oder Reglerfreigabe handelt, können im Fehlerfall versagen. Durch geeignete Maßnahmen ist aber eine Fehlererkennung möglich.

Je nach Ausführung des Frequenzumrichters erfolgt die Fehlererkennung innerhalb des Geräts oder muss durch externe Maßnahmen ausgeführt werden.

Bei der internen Fehlererkennung ist keine zusätzliche Beschaltung des Frequenzumrichters erforderlich: Die Fehlererkennung und die erforderliche sicherheitsgerichtete Reaktion (in der Regel das Verhindern weiterer Bewegungen) erfolgen unabhängig von der äußeren Beschaltung durch Maßnahmen im Frequenzumrichter selbst.

Im anderen Fall müssen externe Komponenten diese Aufgabe übernehmen. Dies kann beispielsweise durch eine SPS geschehen, die bereits vorhanden ist und Steuerungsaufgaben in der Maschine erfüllt, oder durch ein Sicherheitsschaltgerät (z. B. Schutztürwächter), von dem aus auch die Sicherheits-Teilfunktion im Frequenzumrichter aktiviert wird. Zu diesem Zweck müssen entsprechende Rückmeldesignale aus dem Frequenzumrichter nach außen geführt werden. Diese Feedbacksignale müssen Aufschluss über den Zustand des jeweiligen Abschaltpfades geben. Der Hersteller des Frequenzumrichters legt in der Benutzerinformation entsprechende Anforderungen für die Ausführung der Maßnahmen fest. Die Einhaltung dieser Herstelleranweisung ist zwingend erforderlich für das Erreichen des angegebenen PL und der PFH.

Werden keine besonderen Maßnahmen zum Testen der Abschaltpfade getroffen, dann kann eine Fehleraufdeckung immer nur bei Anforderung der Sicherheitsfunktion stattfinden. Je nach Anwendung reicht das aber unter Umständen nicht aus, um den geforderten PFH und PL zu erreichen. Die Zeitabstände zwischen den Anforderungen könnten zu groß sein.

In solchen Fällen sind Diagnosetests erforderlich, bei denen die Sicherheitsfunktion in regelmäßigen Abständen getestet wird. Dabei sind die Tests so zu gestalten,

dass es möglich ist, Fehler oder Ausfälle in den einzelnen Abschaltpfaden aufdecken zu können.

Diese Diagnosetests müssen unabhängig vom Willen des Maschinenpersonals durchgeführt werden. Zumindest die Anforderung der Tests muss fest in der Maschinensteuerung implementiert werden. Sollten die Tests nicht nach der erforderlichen Zeit durchgeführt werden, muss die Maschinensteuerung den weiteren Betrieb der Maschine verhindern. Die Maschine darf erst wieder freigegeben werden, nachdem die Diagnosetests erfolgreich absolviert wurden.

Gemäß DIN EN 61800-5-2 [3], Abschnitt 6.2.2.1.4 können für redundante Teile eines PDS(SR), die nicht geprüft werden können, ohne die Anwendung, in der das PDS(SR) (Maschine oder Anlage) eingesetzt wird, zu unterbrechen, und wenn keine vertretbare technische Lösung umgesetzt werden kann, die folgenden längsten Diagnoseprüf-Intervalle als annehmbar angesehen werden:

- eine Prüfung je Jahr für SIL 2, PL d/Kategorie 3,
- eine Prüfung alle drei Monate für SIL 3, PL e/Kategorie 3,
- eine Prüfung täglich für SIL 3, PL e/Kategorie 4.

Unter bestimmten Umständen können Fehler in einem Abschaltpfad auch über den technischen Prozess erkannt werden. Dies ist beispielsweise dann möglich, wenn ein Abschaltpfad, wie z. B. die Reglerfreigabe, nicht ausschließlich der Aktivierung der Sicherheitsfunktion dient, sondern auch betriebsmäßig zum funktionalen Starten und Stoppen des Motors verwendet wird. Ein Defekt in diesem Pfad würde sich dann beim Stoppen durch ein fehlerhaftes Betriebsverhalten der Maschine bemerkbar machen, vorausgesetzt, es wird nicht gleichzeitig auch ein anderes Signal, wie z. B. der Sollwert, auf Drehzahl Null gesetzt.

4.2.4 Sichere Bewegungsüberwachung

Mit Ausnahme der Sicherheits-Teilfunktion STO, und je nach Umsetzung auch SS1-t, erfordern alle anderen Sicherheits-Teilfunktionen komplexe Berechnungen von Drehzahlen, Positionen, Rampen usw. und werden daher mit entsprechend aufwendigen Rechnersteuerungen realisiert. Die Anforderungen an diese Antriebssteuerungen führen in der Regel zu zweikanaligen Rechnerstrukturen, die die Anforderungen von Kategorie 3 oder Kategorie 4 nach DIN EN ISO 13849-1 [2] erfüllen. Abbildung 18 (siehe Seite 28) zeigt das Konzept einer derartigen zweikanaligen Steuerung.

Die Messung der Motordrehzahl oder der Achslagepositionen geschieht in Abbildung 18 über zwei unabhängige motorseitige Geber[5]. Die in den Gebern erzeugten Signale werden in Rechner 1 bzw. Rechner 2 ausgewertet. Die Überwachungen von Geschwindigkeit, Stillstand, Endlagen, Nocken usw. erfolgen also zweikanalig. Alle Eingänge, die z. B. für die Anwahl der sicherheitsrelevanten Maschinenfunktionen wie sicherer Betriebshalt (SOS) oder sicher begrenzte Geschwindigkeit (SLS) benötigt werden, sind ebenfalls redundant ausgeführt. Der Block „Impulssperre“ in Abbildung 18 führt den STO zweikanalig aus und ist entsprechend dem Prinzip in Abschnitt 4.2.2 aufgebaut. Im Fehlerfall verfügen also Rechner 1 und Rechner 2 über jeweils einen unabhängigen Abschaltpfad.

Um Fehler in der Steuerung und der Sensorik zu erkennen, führen die beiden Rechner neben eigenen Selbsttests u. a. einen kreuzweisen Datenvergleich durch, bei dem sicherheitsrelevante Daten gegenseitig miteinander verglichen werden. Eingänge und Ausgänge werden ebenfalls getestet. Die Testungen haben Einfluss auf die Wahrscheinlichkeit für einen gefährlichen Ausfall pro Stunde (PFH_D). Je nachdem, wie gut die Fehleraufdeckung der Tests (Diagnostic Coverage, DC) ist und wie häufig die Testungen erfolgen, wird für die Sicherheitsfunktion(en) die PFH_D verbessert.

Fehlerreaktionen und Fehlerreaktionszeiten geben die Hersteller in der Betriebsanleitung an; sie müssen für die jeweilige Applikation geeignet sein (siehe Abschnitt 5.6).

[5] Die Anzahl der zu verwendenden Geber ist abhängig von der Sicherheitsfunktion und dem erforderlichen PL bzw. SIL. Sie kann ggf. durch zusätzliche Maßnahmen zur Erkennung von Geberfehlern reduziert werden. Einige Hersteller haben alternative Methoden zum Einsatz eines Gebers in die Rechnersteuerungen implementiert (siehe Kapitel 7).

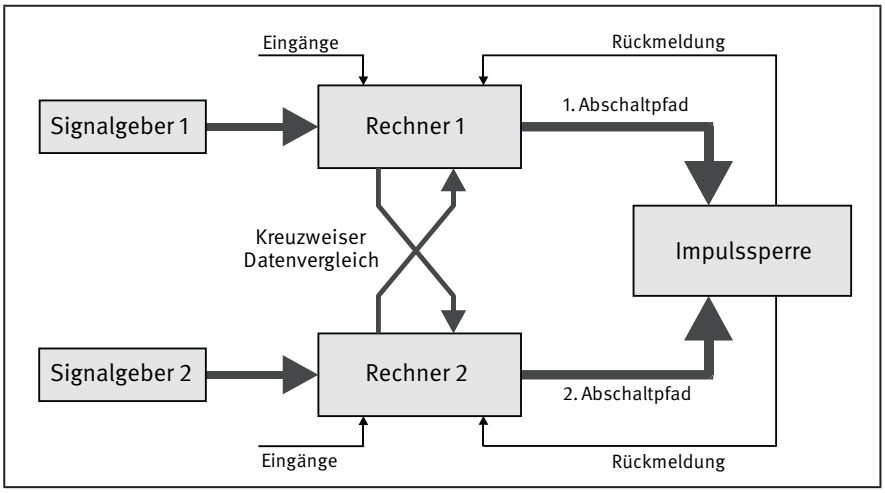


Abbildung 18:
Sichere Bewegungsüberwachung

4.3 Antriebssteuerung – Integrierte oder externe Sicherheit?

Grundsätzlich ist es möglich, Sicherheitsfunktionen bei Verwendung rein funktionaler Antriebssteuerungen durch das Hinzufügen zusätzlicher externer Komponenten zu realisieren. Hierzu enthält dieser Report entsprechende Beispiele (siehe Anhang A). Eine integrierte Lösung mit einem PDS(SR) bietet jedoch Vorteile und je nach Applikation kann die Leistungsfähigkeit einer externen Lösung auch unzureichend sein. Abbildung 19 zeigt beispielhaft die beiden Lösungskonzepte für die Sicherheits-Teilfunktion „Sicher begrenzte Geschwindigkeit“ (SLS). Die Motordrehzahl wird auf einen bestimmten Grenzwert hin überwacht. Bei Überschreitung dieser Drehzahl, also im Fehlerfall, wird die Sicherheits-Teilfunktion „Sicher abgeschaltetes Drehmoment“ (STO) aktiviert.

Verwendet man beispielsweise hoch dynamische Motoren mit sehr hohen Beschleunigungen und Drehzahlen, so können die Abschaltzeiten im externen Überwachungspfad unter Umständen so hoch sein, dass im Fehlerfall eine Gefährdung nicht rechtzeitig vermieden werden kann. Integrierte Lösungen haben deutlich geringere Fehlererkennungs- und Reaktionszeiten und könnten die Anforderungen erfüllen.

Aber auch dann, wenn externe Lösungen für die entsprechenden Aufgaben geeignet sein sollten, können sie erhebliche Nachteile mit sich bringen. Wird beispielsweise der unerwartete Anlauf durch ein Netzschütz verhindert, so muss beim erneuten Einschalten zunächst der Zwischenkreis im Frequenzumrichter neu geladen werden, bevor eine Bewegung des Motors möglich ist. Dies führt zu eventuell unerwünschten Verzögerungszeiten. Zudem haben insbesondere ältere Frequenzumrichter teilweise sehr hohe Einschaltströme, die das Netzschütz extrem belasten können. Dies kann zum frühzeitigen Verschleißen der Kontakte führen. Wird zusätzlich eine ungeeignete Schaltung verwendet, besteht die Gefahr, dass dieser Fehler nicht erkannt wird und dadurch Gefährdungen entstehen.

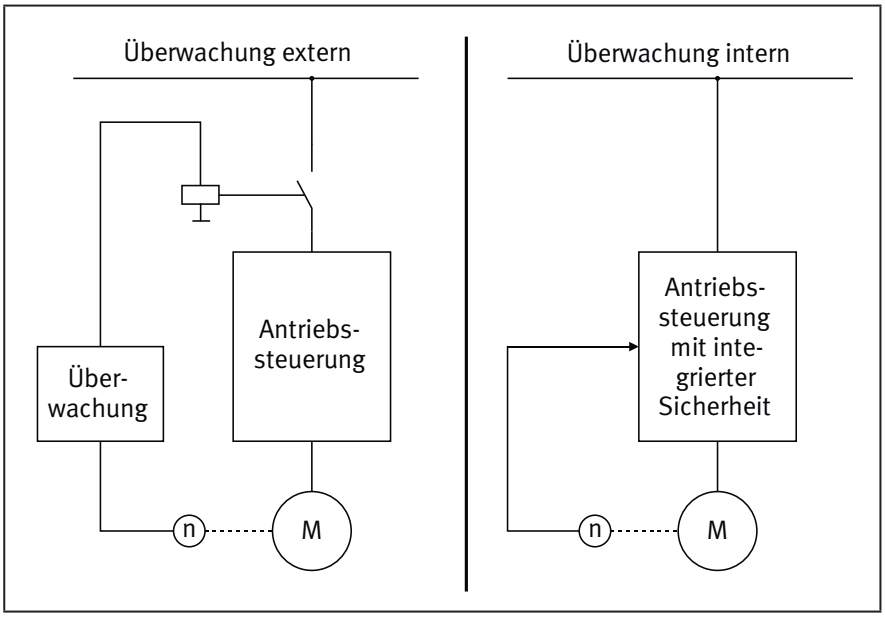


Abbildung 19:
SLS mit externer Überwachung und als integrierte Lösung

Ein weiterer Vorteil der integrierten Lösung ist in dem geringeren Hardwareaufwand zu sehen. Es werden weniger Komponenten benötigt und der Verdrahtungsaufwand reduziert sich deutlich. Hinzu kommt, dass gerade bei Antrieben mit hoher Leistung alleine das Netzschütz schon ein nicht zu unterschätzender Kostenfaktor ist.

Darüber hinaus ist die Projektierung integrierter Lösungen deutlich einfacher. Es gibt weniger Schnittstellen zu betrachten und die Maßnahmen zur Fehleraufdeckung der externen Komponenten entfallen.

Der Frequenzumrichter ist Teil der gesamten Sicherheitsfunktion an der Maschine und muss bei der Quantifizierung mit berücksichtigt werden. Ein PDS(SR) wird als gekapseltes Subsystem berücksichtigt, für das der Hersteller alle erforderlichen Daten (PL und PFH) angibt. $MTTF_D$, DC, CCF und Angaben zur Software des Umrichters sind nicht erforderlich. Die integrierte Lösung vereinfacht also auch die Berechnung der PFH für die Sicherheitsfunktion.

5 Sicherheitsfunktionen in der Anwendung

5.1 PL, PFH und SIL

Frequenzumrichter mit integrierten Sicherheits-Teilfunktionen (PDS(SR)) sind Sicherheitsbauteile und Logikeinheiten für Sicherheitsfunktionen gemäß Anhang IV der Maschinenrichtlinie 2006/42/EG [6], für deren Einsatz Angaben zu den sicherheitsrelevanten Eigenschaften erforderlich sind. Das PDS(SR) wird zur Realisierung einer (oder mehrerer) Sicherheits-Teilfunktion(en) eingesetzt, mit deren Hilfe eine Risikominderung an einer Maschine erreicht werden soll. Das erforderliche Maß dieser Risikominderung ist durch die Risikoanalyse an der jeweiligen Gefahrenstelle bestimmt worden und wird durch den PL_r ausgedrückt. Um beurteilen zu können, ob ein PDS(SR) eingesetzt werden kann, muss der PL (oder SIL für den Einsatz nach DIN EN 62061 [12]) für die integrierten Sicherheits-Teilfunktionen bekannt sein. Weiterhin wird für die gesamte Sicherheitsfunktion an der Maschine die PFH berechnet, die sich durch die Kombination aller beteiligten Bauteile ergibt. Der Anwender muss daher auch für die integrierten Sicherheits-Teilfunktionen des PDS(SR) die jeweiligen PFH-Werte kennen. Die PFH kann für unterschiedliche Sicherheits-Teilfunktionen auch unterschiedliche Werte annehmen, da hier ggf. unterschiedliche Bauteile des PDS(SR) verwendet werden. Werden mehrere Sicherheits-Teilfunktionen eines PDS(SR) gleichzeitig verwendet, so ist prinzipiell die Addition der einzelnen PFH-Werte möglich. Allerdings verwenden die Sicherheits-Teilfunktionen in der Regel größtenteils identische Hardware, sodass bei dieser Addition die Ausfallrate vieler Bauteile mehrfach berücksichtigt wird. Die Hersteller der PDS(SR) geben daher häufig auch PFH-Werte für die Kombination von integrierten Sicherheits-Teilfunktionen an.

Eine Angabe von $MTTF_D$ und DC ist für PDS(SR) nicht erforderlich, da diese Werte bereits bei der Ermittlung von PL und PFH berücksichtigt wurden. Ebenso ist die Angabe der realisierten Kategorie nicht erforderlich für die Anwendung des Frequenzumrichters, allerdings verlangt die Norm DIN EN ISO 13849-1 im Abschnitt „Benutzerinformation“ diese Angabe, weiterhin enthalten einige C-Normen Anforderungen an die Kategorie.

5.2 Betriebsartenwahl

Zur Änderung von Steuerungsabläufen oder Arbeitsverfahren werden an Maschinen Betriebsartenwahlschalter eingesetzt. Gelangen unterschiedliche Schutzmaßnahmen zur Anwendung, so muss ein in jeder Stellung abschließbarer Betriebsartenwahlschalter vorhanden sein. Dabei muss jede Stellung des Wahlschalters deutlich erkennbar sein und darf nur einer Steuer- oder Betriebsart entsprechen (siehe Maschinenrichtinie [6] Anhang I, Abschnitt 1.2.5). Die gewählte Steuerungs- und Betriebsart muss allen anderen Steuerungs- und Betriebsfunktionen außer NOT-HALT übergeordnet sein.

Der Wahlschalter kann durch andere Wahleinrichtungen ersetzt werden, z. B. eine Eingabeeinheit mit Zugriffscode, der die Nutzung bestimmter Funktionen der Maschine auf bestimmte Personenkreise beschränkt. Dabei ist jedoch zu beachten, dass die Anforderungen an die hierfür eingesetzten sicherheitsrelevanten Stromkreise vergleichbar sicher sein müssen.

Erfordern bestimmte Arbeiten einen Betrieb der Maschine bei aufgehobener Schutzwirkung der Schutzeinrichtungen, z. B. für Einrichtbetrieb oder Störungsbeseitigung, so sind der entsprechenden Wahlschalterstellung gleichzeitig folgende Steuerungsvorgaben zuzuordnen:

- Alle anderen Steuerungs- oder Betriebsarten sind nicht möglich. Das bedeutet ein Außer-Funktion-Setzen und Verhindern aller anderen Betriebsarten/Steuerungsarten.
- Es sind nur Bewegungen möglich, solange die entsprechenden Befehlseinrichtungen betätigt werden (Befehlseinrichtungen mit selbsttätiger Rückstellung wie Tippschaltung, Freigabesteuerung).
- Der Betrieb gefährlicher Funktionen ist nur unter geringeren Risikobedingungen möglich (z. B. begrenzte Geschwindigkeit, reduzierte Leistung, Schrittbetrieb, Begrenzung des Bewegungsbereichs) und unter Ausschaltung von Gefährdungen, die sich aus Befehlsverkettungen ergeben.
- Der Betrieb gefährlicher Funktionen durch absichtliche oder unabsichtliche Einwirkung auf die Sensoren der Maschine ist nicht möglich.

Die Festlegungen nach DIN EN 60204-1 [9], Abschnitt 9.2.7 ergänzen diese Steuerungsvorgaben. Zu nennen ist die

- Verwendung einer tragbaren Bedienstation mit NOT-HALT-Befehlsgerät.

Die Betriebsartenwahl bzw. die Umschaltung von Betriebsarten darf keine Maschinenbewegungen automatisch starten. Dazu muss eine getrennte Betätigung der Startsteuerung vorgenommen werden. Der Start von Bewegungen muss stets bewusst eingeleitet werden.

Können die oben angegebenen Steuerungsvorgaben nicht gleichzeitig erfüllt werden, muss der Steuerungs- oder Betriebsartenwahlschalter andere Schutzmaßnahmen

aktivieren. Diese müssen so gestaltet sein, dass ein sicherer Arbeitsbereich gewährleistet ist.

Eine eindeutige Anzeige der gewählten Betriebsart muss vorgesehen sein, z. B. durch die Kennzeichnung der Stellung eines Betriebsartenwahlschalters, Verwendung von Leuchtmeldern oder eine Bildschirmdarstellung. Werden elektrische Anzeigen verwendet, sollten diese mit einer Prüfeinrichtung ausgestattet sein.

Bei den vorstehenden Steuerungsvorgaben handelt es sich um Sicherheitsfunktionen, Anforderungen an die Konstruktion und ggf. weitere organisatorische Maßnahmen. Mit dem Betriebsartenwahlschalter werden also je nach Betriebsart die jeweiligen Sicherheits-Teilfunktionen aktiviert oder deaktiviert. Bauteilfehler in der Betriebsartenwahl könnten somit dazu führen, dass erforderliche Sicherheits-Teilfunktionen nicht wirksam sind. Derartige Fehler erhöhen das Risiko an einer Maschine und müssen daher betrachtet werden.

Es stellt sich die Frage, ob der steuerungstechnische Anteil der Betriebsartenwahl zu jeder an der Maschine realisierten Sicherheitsfunktion hinzugezählt werden muss oder ob die Betriebsartenwahl als eigenständige Sicherheitsfunktion betrachtet werden kann. Analog zur Vorgehensweise bei den überlagerten Gefährdungen, bei denen einzelne Maschinenteile betrachtet werden, wird die Betriebsartenwahl als eigene Sicherheitsfunktion angesehen. Damit wird auch vermieden, dass die Betriebsartenwahl in jeder einzelnen Sicherheitsfunktion zusätzlich die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde PFH_D (probability of a dangerous failure per hour) erhöht.

5.2.1 Gleichzeitig ausgeführte Sicherheits-Teilfunktionen

Bei einigen Betriebsarten an Maschinen wird die erforderliche Risikominderung durch ein Zusammenwirken mehrerer Maßnahmen, u. a. auch durch mehrere gleichzeitig ausgeführte Sicherheits-Teilfunktionen, erreicht. Dies trifft insbesondere auf Betriebsarten zu, bei denen eine Maschine bei geöffneter trennender Schutzeinrichtung betrieben werden muss, z. B. für das Einrichten oder die Störungsbeseitigung. In diesen Fällen sind häufig Sicherheits-Teilfunktionen zur Begrenzung der Drehzahl (SLS) und für den Tipp- bzw. Freigabebetrieb gleichzeitig aktiv. Die erforderlichen PL_r für diese Sicherheits-Teilfunktionen, die das Risiko der gleichen gefahrbringenden Bewegung reduzieren sollen, werden jeweils durch eine Risikoanalyse ermittelt. Hierbei kann die Ausführung der ersten Sicherheits-Teilfunktion das Risiko der gefahrbringenden Bewegung bereits soweit mindern, sodass die Risikoanalyse über die verbliebene Gefährdung für die zweite Sicherheits-Teilfunktion u. U. zu einem geringeren PL_r führt (siehe [4], Anhang A, Beispiel 4). Eine wechselseitige Reduzierung des PL_r durch die Sicherheits-Teilfunktionen darf nicht erfolgen, weil dann die gesamte Risikominderung unzureichend wäre. Dies kann durch eine iterative Anwendung des Risikographen verhindert werden. Im o. g. Beispiel wurde zunächst der PL_r für SF 2 (Sicher begrenzte Drehzahl) bestimmt. Beim Tippbetrieb in SF 3 kann dann unterstellt werden, dass durch die Drehzahlbegrenzung von SF 2 die Maschinenbewegungen für die Bedienperson überschaubar sind und sie gefahrbringenden Bewegungen ausweichen kann (Risikoparameter P1 statt P2). Durch die gleichzeitige Ausführung von SF 2 und SF 3 ergibt sich also PL_r = c anstatt PL_r = d für SF 3[6].

Siehe auch Sistema-Kochbuch 6 Abschnitt 4.3.

5.2.2 Sicherheitsfunktion Betriebsartenwahl

Aufgrund der Vorgaben der Maschinenrichtlinie zur Betriebsartenwahl ist zu verhindern, dass ein Betrieb in einer nicht gewählten Betriebsart erfolgt. Dies erfolgt in der Regel so, dass sicherheitstechnisch die für die jeweilige Betriebsart erforderlichen Schutzeinrichtungen aktiviert und ggf. unbeabsichtigte Bewegungen einzelner Maschinenteile verhindert werden. Gleichzeitig erfolgt funktional die Sperrung anderer Betriebsarten über die Maschinensteuerung.

Im Folgenden werden übliche Bedienelemente zur Betriebsartenwahl genannt.

a) Nockenbetätigte Wahlschalter

   Schalter mit zwangläufigem Betätigungsmodus (direktöffnend) gelten als bewährte Bauteile, wenn sie DIN EN 60947-5-1 [13], Anhang K entsprechen. Eine Einstufung in Kategorie 1 nach DIN EN ISO 13849 ist daher gegeben.

b) Nockenbetätigte Schalter mit weiteren Fehlerausschlüssen

   Sind bei Schaltern mit zwangläufigem Betätigungsmodus zusätzlich die Fehlerausschlüsse

   - Kurzschluss von benachbarten Kontakten, die voneinander isoliert sind, und
   - gleichzeitiger Kurzschluss zwischen den drei Klemmen von Wechselkontakten

   gemäß Tabelle D.8 der DIN EN ISO 13849-2 [8] möglich, müssen diese Bauteilfehler nicht angenommen

[6] Wird eine Sicherheitsfunktion in mehreren Betriebsarten eingesetzt, können sich aufgrund unterschiedlicher Risiken auch unterschiedliche PL_r ergeben. Die Realisierung der Sicherheitsfunktion muss im höchsten PL_r erfolgen.

werden. Der Nachweis kann zum Beispiel durch eine Failure Mode and Effects Analysis (FMEA) erfolgen. Dadurch sind auch höhere Kategorien als Kategorie 1 möglich (siehe hierzu auch Beispiel 8 im Anhang A).

c) Sonstige elektromechanische Schalter

Für die Fehlerbetrachtung ist u. a. eine FMEA durchzuführen.

d) Betriebsartenwahl über elektronische Betriebsmittel (z. B. Tastatur, Transponder)

Für die Fehlerbetrachtung ist u. a. eine FMEA durchzuführen (siehe hierzu IFA Report 2/2017 [4], I.3).

5.2.3 Sicherheitsfunktion Tippschaltung

Als Befehlsgeräte für die Tippschaltung dienen üblicherweise handelsübliche federrückstellende Drucktaster. Durch die Einhaltung des Ruhestromprinzips wird erreicht, dass beim Loslassen des Stellteils des Befehlgerätes die Bewegung stillgesetzt wird. Besondere Anforderungen an die Konstruktion der Drucktaster bestehen nicht, obwohl im Fehlerfall (z. B. bei Federbruch) das Öffnen der Kontakte beim Loslassen des Drucktasters versagen kann. Für die Quantifizierung der Sicherheitsfunktion Tippschaltung ist die Kenntnis des B_{10D}-Werts der Drucktaster erforderlich. Üblicherweise gibt der Bauteilhersteller diesen Wert an; alternativ enthält DIN EN ISO 13849-1 [2] entsprechende Angaben. Hiermit kann die Sicherheitsfunktion für den Tippbetrieb quantifiziert werden.

Sofern nicht maschinenspezifische Festlegungen in C-Normen getroffen sind, muss eine Risikoanalyse ergeben, ob zusätzliche Maßnahmen, wie z. B. eine Freigabesteuerung oder ein NOT-HALT-Befehlsgerät in der Nähe des Tipptasters, erforderlich sind (siehe hierzu IFA Report 2/2017 [4], D.2.5.6).

5.2.4 Sicherheitsfunktion Freigabesteuerung (Zustimmungseinrichtung)

Freigabesteuerungen (Zustimmungseinrichtungen) müssen in der Weise gestaltet sein, dass sie gefahrbringende Maschinenfunktionen nur dann zulassen, wenn deren Befehlsgeräte (Zustimmungsschalter) in einer bestimmten Stufe („Zustimmfunktion“) betätigt werden. Mit der Freigabesteuerung alleine dürfen keine gefahrbringenden Bewegungen eingeleitet werden. Die Geräte müssen so ausgesucht bzw. angeordnet werden, dass die Möglichkeit einer Umgehung minimiert ist.

Es sind zweistufige und dreistufige Zustimmungsschalter verfügbar. Bei der dreistufigen Ausführung löst das Durchdrücken in die dritte Stufe („Aus-Funktion“) ein dem „Stillsetzen im Notfall“ vergleichbares Signal aus. Dadurch ist die Bedienperson in Gefahrensituationen in der Lage, durch Loslassen oder Durchdrücken, z. B. durch Verkrampfen, die Bewegung sicher stillzusetzen.

Die Freigabesteuerung ist eine Sicherheitsfunktion und die für die Berechnung der PFH erforderlichen Angaben stellt der Bauteilhersteller bereit. Es wird empfohlen, Zustimmungseinrichtungen/Zustimmungsschalter einzusetzen, die den Prüfgrundsatz GS-ET-22 von DGUV Test [14] erfüllen (zur Modellierung siehe IFA Report 2/2017, Abschnitt D.2.5.5). Falls zweistufige Befehlsgeräte zum Einsatz gelangen, ist zusätzlich die Anordnung eines NOT-HALT-Befehlsgerätes in der Nähe des Zustimmungsschalters erforderlich.

5.2.5 Geringere Risikobedingungen

Ist es z. B. erforderlich, dass Personen im Gefahrenbereich Einstellarbeiten vornehmen (Einrichtbetrieb), so muss das Verletzungsrisiko minimiert werden. Beispielsweise sind unerwartete Bewegungen zu verhindern (STO, SOS) oder so zu reduzieren (SLS, SLA), dass der Bediener das Bewegungsverhalten von Maschinenteilen einschätzen kann. Hierzu gehört auch, den Bewegungsbereich von Achsen einzuschränken (SLP, SDI) und möglichst nur eine einzige Achse zu verfahren. Weiterhin können Leistungsbegrenzungen (SLT) und ein Schrittbetrieb (SLI) erforderlich sein. Darüber hinaus müssen Gefährdungen, die sich aus Befehlsverkettungen ergeben, ausgeschlossen sein, damit an der Maschine keine automatischen (Teil-) Abläufe ausgeführt werden.

Werden diese Anforderungen mit steuerungstechnischen Mitteln realisiert, so sind dies Sicherheits-Teilfunktionen, die nach DIN EN ISO 13849-1 [2] auszulegen sind.

5.2.6 Einwirkung auf die Sensoren der Maschine

Für den automatischen Ablauf an Maschinen werden in der Regel Sensoren eingesetzt, die z. B. Positionen von Werkstücken erfassen. Basierend auf diesen Sensorsignalen startet eine SPS im Automatikbetrieb dann ggf. den nächsten Fertigungsschritt – es wird also eine Bewegung eingeleitet. Durch Arbeiten an der Maschine bei geöffneten Schutzeinrichtungen kann es zu einer Auslösung von Sensorsignalen kommen. In dieser Situation würde die Einleitung der Bewegung eines Maschinenteils möglicherweise die Bedienperson gefährden, was zu verhindern ist. Die Maschinenrichtlinie [6] enthält daher die Steuerungsvorgabe „Einwirkungen auf die Sensoren der Maschine darf nicht zu einer Gefahr führen“. Der entsprechende Nachweis geschieht sinnvollerweise durch Analyse des Schaltplans oder durch eine Überprüfung an der Maschine durch gezielte Einwirkung auf die Sensoren (z. B. Betätigung oder Umschaltung von Positionsschaltern). Hierbei ist ggf. in den Kategorien 3 bzw. 4 die

erforderliche Einfehlersicherheit bzw. Fehlerhäufung von unerkannten Fehlern zu berücksichtigen. Das Ergebnis der Analyse/Prüfung ist zu dokumentieren, z. B. im Rahmen der Validierung der Sicherheitsfunktionen der Maschine.

5.2.7 Verwendung einer tragbaren Bedienstation

Bei der Steuerungsvorgabe „Verwendung einer tragbaren Bedienstation“ handelt es sich um eine Forderung an die Ausrüstung der Maschine. In der Benutzerinformation ist eine Angabe zur bestimmungsgemäßen Verwendung erforderlich.

Die tragbare Bedienstation ist üblicherweise mit NOT-HALT-Befehlsgerät, Tippschalter und/oder Zustimmungsschalter ausgerüstet.

5.3 Stillsetzen im Notfall

Den Anforderungen der Maschinenrichtlinie 2006/42/EG [6], Anhang I entsprechend, muss jede Maschine (bis auf Ausnahmen) mit einem oder mehreren NOT-HALT-Befehlsgeräten ausgerüstet sein, die eine unmittelbar drohende oder eintretende Gefahr vermeiden können.

Die NOT-HALT-Funktion wird durch eine einzelne menschliche Handlung über das Betätigen des NOT-HALT-Befehlsgeräts ausgelöst. Der gefahrbringende Vorgang muss daraufhin möglichst schnell zum Stillstand gebracht werden, ohne dass dadurch zusätzliche Gefährdungen entstehen.

Um im Notfall eine Maschine oder Anlage schnellstmöglich stillsetzen zu können, muss die NOT-HALT-Funktion unabhängig von der Betriebsart jederzeit verfügbar und betriebsbereit sein. Das bedeutet auch, dass die NOT-HALT-Einrichtung in keiner Betriebsart außer Funktion gesetzt werden darf. Sie ist somit allen anderen Betriebsarten, Betriebszuständen und Sicherheitsfunktionen übergeordnet. Dabei ist zu beachten, dass es sich beim NOT-HALT um eine ergänzende Schutzmaßnahme handelt, die zusätzlich zur möglichst inhärent sicheren Konstruktion und zu anderen technischen Schutzmaßnahmen bzw. Sicherheitsfunktionen getroffen wird, aber nicht an deren Stelle treten darf.

Der Steuerbefehl, der durch Betätigen des NOT-HALT-Befehlsgeräts ausgelöst wird, bleibt solange wirksam, bis das Befehlsgerät wieder zurückgestellt ist. Ein solcher Steuerbefehl kann beispielsweise die Aktivierung der Sicherheits-Teilfunktion STO in den Antrieben sein.

Das manuelle Rückstellen (Entriegeln) des NOT-HALT-Befehlsgeräts darf allerdings keinen Wiederanlauf auslösen und nur an dem Ort möglich sein, an dem der Befehl zum Stillsetzen im Notfall erfolgt ist. Damit wird erreicht, dass vom Ort der Rückstellung aus geprüft werden kann, ob der zugehörige Gefahrenbereich wieder „frei“ ist.

Abhängig von der Risikobeurteilung muss die NOT-HALT-Funktion entweder in Stopp-Kategorie 0 oder Stopp-Kategorie 1 gemäß DIN EN 60204-1 [9] ausgeführt werden. Für jede Maschine muss im Einzelnen beurteilt werden, ob es die richtige Maßnahme ist, wenn die Energiezufuhr zu den Maschinenantrieben unverzüglich unterbrochen wird (STO) und die Motoren austrudeln oder so gesteuert wird, dass die gefahrbringenden Bewegungen so schnell wie möglich zum Stillstand kommen (SS1).

Bei dieser Beurteilung spielt die Zeit zwischen der Auslösung des NOT-HALT-Befehls – wie auch beim Ansprechen einer Schutzeinrichtung – und dem Stillstand des Antriebs eine entscheidende Rolle. Diese Zeit bezeichnet man als Nachlaufzeit. Bei einer Vielzahl von Maschinen, z. B. bei Pressen oder Kalanderwalzen, ist die Einhaltung eines Grenzwerts für die Nachlaufzeit erforderlich. Daher beschreiben einige C-Normen Anforderungen an die Bremsung.

Um eine Maschine im Notfall möglichst schnell zum Stillstand zu bringen, kann das gesteuerte Stillsetzen durch die Antriebssteuerung erfolgen. Dabei kommt die Sicherheits-Teilfunktion SS1 zur Anwendung, die in unterschiedlichen Ausführungen realisiert werden kann (siehe Abschnitt 3.1.1.2). Die SS1-Funktion mit überwachter Bremsrampe und anschließender Aktivierung der STO-Funktion bietet gegenüber der Variante mit Aktivierung der STO-Funktion nach einer eingestellten Verzögerungszeit allerdings den Vorteil, dass schneller auf Fehler während des Stillsetzvorgangs reagiert wird.

Maschinen, bei denen der NOT-HALT realisiert ist, müssen zusätzlich über geeignete Maßnahmen des elektrischen Berührungsschutzes verfügen, sodass ein NOT-AUS nicht erforderlich ist. Weiterhin ist zu berücksichtigen, dass die endgültige Abschaltung der Energie nach dem Stillsetzen nicht gleichzeitig eine Trennung von der Energieversorgung bedeutet. So verhindert die Impulssperre im Frequenzumrichter zwar die Erzeugung eines Drehfelds im Motor, trotzdem können aber hohe Spannungen an den Motorklemmen anliegen. Auch wenn Netz- oder Motorschütze eingesetzt werden, ist eine ausreichende Trennung von der Energieversorgung nur dann gegeben, wenn der Kontaktabstand der Schütze ausreichend ist. In der Regel sind Schütze für die Netztrennung nicht geeignet (siehe hierzu auch Abschnitt 5.7 dieses Reports).

Für das Freischalten zum Arbeiten an der elektrischen Ausrüstung ist der NOT-HALT also ungeeignet. Auch beim NOT-AUS ist das Freischalten nicht zwangsläufig gewährleistet, denn häufig wird diese Maßnahme für den Notfall zwar NOT-AUS genannt, aber tatsächlich realisiert wurde NOT-HALT. Die Verwendung der Begriffe NOT-AUS und NOT-

HALT wurde 2005 in DIN EN 60204-1 [9] eingeführt, hat sich aber noch nicht vollständig durchgesetzt.

5.4 Stillsetzen und Position halten

5.4.1 Stillsetzen von Lasten

Das Abbremsen einer Bewegung ist dann eine Sicherheitsfunktion und nach DIN EN ISO 13849-1 [2] zu bewerten, wenn die Risikobeurteilung eine Gefährdung durch die austrudelnde Bewegung aufzeigt und zur Risikominderung ein schnelles Stillsetzen durch eine Bremsung des Antriebs erfolgen soll. Dies ist beispielsweise bei gefahrbringenden Bewegungen mit Nachlauf der Fall, die nicht mit zugehaltenen Schutztüren bis zum Erreichen des Stillstands gesichert sind. An diesen Maschinen kann ggf. die Gefahrenstelle erreicht werden, bevor die Bewegung zum Stillstand gekommen ist.

Bauteile für das Stillsetzen

Für nicht schwerkraftbelastete Achsen, angetrieben durch Asynchronmotoren, sind im Allgemeinen gebräuchlich:

- Gegenstrombremsung,
- Gleichstrombremsung,
- Widerstandsbremsung.

Drehzahlgeregelte Antriebe werden meist über Frequenzumrichter angesteuert, die in der Regel nicht nur zum Antreiben, sondern auch zum gesteuerten Stillsetzen von Motoren geeignet sind. Die kinetische Energie, die beim Abbremsen im Frequenzumrichter entsteht, wird entweder ins Stromnetz zurückgespeist oder in einem Bremswiderstand in Wärme umgewandelt.

Mit mechanischen Bremsen kann entweder ein Stillsetzen von Bewegungen realisiert werden (Betriebsbremse) oder es wird eine bereits stillgesetzte Last in Position gehalten (Haltebremse). Die Bremskraft der Bremse wird in der Regel durch Federn bereitgestellt. Das Öffnen erfolgt elektrisch, pneumatisch oder hydraulisch. Durch dieses Konzept ist die Bremswirkung auch im energielosen Zustand vorhanden (Ruhestromprinzip).

Anforderungen an das Stillsetzen von drehzahlgeregelten Antrieben

Bei der Risikobeurteilung an der Maschine ergeben sich bestimmte Anforderungen an die Sicherheitsfunktion „Stillsetzen“. Insbesondere muss entsprechend dem erforderlichen PL_r sowohl das Verhalten der Steuerung im Fehlerfall und bei Spannungsausfall betrachtet werden als auch die sich hieraus ergebenden zusätzlichen Gefährdungen. Entsprechend DIN EN ISO 12100 [7], Abschnitt 5.4 b) sind beim Stillsetzen mit Frequenzumrichtern u. a. diese zwei Betriebszustände zu berücksichtigen:

- Normalbetrieb

  Die Maschine führt die vorgesehene Funktion zum gesteuerten Stillsetzen aus. Der Frequenzumrichter bremst bei Anforderung die gefahrbringende Bewegung ab und schaltet den Motor momentenfrei (SS1) oder er bremst ab und hält anschließend die Position (SS2).

- Gestörter Betrieb

  Ausfall der Energieversorgung oder Ausfall des Frequenzumrichters aufgrund eines Fehlers. Die Abbremsung der Last durch den Frequenzumrichter geschieht nur mit verringertem Bremsmoment, überhaupt nicht oder es erfolgt fehlerhaft eine Beschleunigung.

Im gestörten Betrieb kann es also zu erhöhten Nachlaufzeiten kommen. Da der Leistungsteil bei allen bekannten Antriebssteuerungen mit Frequenzumrichtern einkanalig realisiert ist, führt ein Fehler sofort zum Ausfall oder einer verminderten Leistung der Bremsfunktion. Das gilt sowohl für herkömmliche Frequenzumrichter als auch für Frequenzumrichter mit den integrierten Sicherheits-Teilfunktionen SS1 bzw. SS2, bei denen nach Auftreten eines Fehlers das Abschalten des Antriebs (STO) erfolgt; ein gesteuertes Stillsetzen ist also nicht mehr möglich (siehe Abschnitt 3.1.1.2 bzw. 3.1.1.3). Hier muss für die jeweilige Applikation entschieden werden, ob das Verhalten akzeptabel ist. Inakzeptabel ist es z. B. für die Abbremsung von Kalanderwalzen. Sind Personen nahe der Einzugsstelle tätig, kommt es wesentlich auf die Verfügbarkeit der Bremsfunktion an.

Je nachdem, welcher PL_r für die Funktion des sicheren Stillsetzens erreicht werden muss, sind zusätzlich zur Abbremsung mit Frequenzumrichtern weitere Maßnahmen erforderlich, z. B. durch den Einsatz einer mechanischen Betriebsbremse (linear oder rotatorisch) oder eine Bremsung durch Gleichstromaufschaltung.

Hinweis:

Einige Frequenzumrichter bzw. Servoregler versorgen ihre Steuerelektronik aus dem Zwischenkreis und sind dadurch in der Lage, trotz eines Energieausfalls eine Bewegung gesteuert stillzusetzen (siehe Abschnitt 5.5.1).

5.4.2 Hochhalten von Lasten (Vertikalachsen)

Schwerkraftbelastete Achsen müssen sowohl im Betrieb als auch bei Energieausfall in Position gehalten werden, wenn Personen in den Gefahrenbereich eingreifen können. Dazu sind in der Regel zumindest Haltebremsen erforderlich, die bei Energieausfall das unbeabsichtigte Herabsinken der Last verhindern. Als Beispiel sind pressenähnliche Maschinen mit Servoantrieben anzuführen,

deren Gefahrenbereich über einen Lichtvorhang als Schutzeinrichtung gesichert ist. Bei diesen Maschinen ist sowohl ein gesteuertes Stillsetzen durch die Antriebssteuerung als auch der Einsatz von Haltebremsen erforderlich.

Entsprechend DIN EN ISO 12100 [7], Abschnitt 5.4 b) sind bei Vertikalachsen u. a. diese zwei Betriebszustände zu berücksichtigen:

Normalbetrieb:

Die Maschine führt die vorgesehene Funktion aus:

a) nach dem gesteuerten Stillsetzen durch den Frequenzumrichter übernimmt dieser auch das sichere Hochhalten (SS2) oder

b) nach dem gesteuerten Stillsetzen durch den Frequenzumrichter (SS1) wird eine Haltebremse angesteuert (SBC), die die Position der Last hält.

Gestörter Betrieb:

Durch einen Ausfall der Energieversorgung oder Ausfall des Frequenzumrichters aufgrund eines Fehlers ist das Hochhalten einer Last durch den Frequenzumrichter nicht möglich.

Im gestörten Betrieb muss das Stillsetzen und Hochhalten durch eine mechanische Bremse erfolgen (z. B. Federdruckbremse mit Not-Stopp-Eigenschaft, siehe [15]).

Auch bei der Projektierung der Maßnahmen zum Stillsetzen im Notfall (NOT-HALT) ist die spezielle Situation bei Vertikalachsen zu berücksichtigen. Entsprechend DIN EN 60204-1 [9], Abschnitt 9.2.3.4.2 ist die Ausführung des NOT-HALT grundsätzlich nur in Stopp-Kategorie 0 oder Stopp-Kategorie 1 zulässig. Es wird also immer die Antriebsenergie abgeschaltet, sodass mechanische Bremsen unabdingbar sind.

Anforderungen an das Hochhalten

Bei der Risikobeurteilung an der Maschine ergeben sich bestimmte Anforderungen an die Sicherheitsfunktion „Hochhalten“. Zur Ermittlung des erforderlichen PL_r und zu möglichen Schutzmaßnahmen finden sich im Fachbereichs-Informationsblatt 005 „Schwerkraftbelastete Achsen“ (siehe Anhang B) detaillierte Hinweise. Zusätzlich können die Anmerkungen im Abschnitt 5.5 „Ausfall der Energieversorgung“ berücksichtigt werden.

5.4.3 Mechanische Bremsen als Bauteile für Sicherheitsfunktionen

Haltebremsen, die der Hersteller zum sicheren Hochhalten von Lasten anbietet, sind Sicherheitsbauteile nach Maschinenrichtlinie [6], Artikel 2 Nr. c), sofern sie gesondert in Verkehr gebracht werden. Dasselbe gilt auch für Betriebsbremsen, die zur Reduzierung von Nachlaufzeiten gefahrbringender Bewegungen vorgesehen sind. In diesen Fällen stellt der Bremsenhersteller eine Konformitätserklärung aus und gibt in der Betriebsanleitung Hinweise für den sicheren Einsatz der Bremse. Falls Standardbauteile eingesetzt werden, liegt es allein beim Maschinenhersteller, die entsprechenden Sicherheitsfunktionen korrekt zu realisieren [16].

Anforderungen an mechanische Bremsen in Sicherheitsfunktionen sind bislang nur für „Notfallbremsen mit Haltebremsfunktion für lineare Bewegungen“ verfügbar (siehe Prüfgrundsatz DGUV Test GS-MF-28/04.2015 [15]).

Neben konstruktiven Anforderungen sind Prüfungen zum Nachweis der mechanischen Lebensdauer festgelegt. Hierbei müssen 1 000 000 Schaltspiele mit statischer Last und 2 000 Schaltspiele mit dynamischer Last nachgewiesen werden.

Bei rotatorischen Bremsen für Werkzeugmaschinen werden meist 5 000 000 Schaltspiele gefordert.

Hinweis:

Häufig wird eine Federdruckbremse eingesetzt. Die Bremskraft wird durch mehrere Bremsfedern erzeugt. Sie wirkt als Anpresskraft des Reibbelags gegen die Bremsscheibe. Ein plötzliches Komplettversagen der Federdruckbremse wird aufgrund der Konstruktion in der Regel nicht angenommen.

Neben einer geeigneten Konstruktion der Bremse sind ab Kategorie 2 nach DIN EN ISO 13849-1 [2] fehlererkennende Maßnahmen in der Anwendung erforderlich. Die Funktion von Bremsen kann durch statische und dynamische Tests überprüft werden. Das IFA empfiehlt folgendes Vorgehen:

a) Statischer Test der Bremse

Die mechanische Bremse wird durch einen regelmäßigen Test auf Funktionsfähigkeit überprüft. Dabei wird die Bremse vom Antriebsmotor mit dem 1,3-Fachen des maximalen Lastmoments beaufschlagt. Falls die Position der Last im vorgegebenen Bereich gehalten wird, ist die ordnungsgemäße Funktion der Bremse gegeben. Falls die vorgegebene Position verlassen wird, muss die Bremse entsprechend der Betriebsanleitung überprüft oder ggf. ausgetauscht werden.

b) Dynamischer Test der Bremse

Der dynamische Bremsentest erfolgt in regelmäßigen Abständen unter definierten Bedingungen für Geschwindigkeit und Masse. Der zeitliche Testabstand

ist abhängig von den Einsatz- und Umgebungsbedingungen, darf jedoch maximal ein Jahr betragen.

Kurz vor Einleitung des Bremsvorgangs durch die mechanische Bremse wird der Antriebsmotor durch die Steuerung momentenfrei geschaltet. Die mechanische Bremse wird zum Einfallen gebracht. Nachlaufweg sowie Nachlaufzeit sind zu ermitteln und mit den zulässigen Werten zu vergleichen. Wird ein zulässiger Wert überschritten, muss ein Weiterbetrieb der Maschine unterbunden werden. Die mechanische Bremse ist ggf. auszutauschen.

Hinweis:

Der dynamische Test soll sicherstellen, dass sich der Nachlauf beim Bremsvorgang während der Betriebszeit nicht unzulässig verlängert (z. B. durch Verhärtung der Bremsbeläge). Trotz erfolgreich bestandenem statischen Bremsentest ist ein geringfügig vergrößerter Nachlauf möglich. Dies ergibt sich u. a. aus unterschiedlichen physikalischen Eigenschaften beim dynamischen Bremsen gegenüber dem statischen Halten. Der Test selbst darf nicht zu einer Gefährdung führen. Zwischen den dynamischen Tests kann es zu einer Verlängerung des Nachlaufs kommen. Zeigt die Risikobeurteilung auf, dass dies nicht tolerierbar ist, sind zusätzliche Maßnahmen erforderlich.

5.5 Ausfall der Energieversorgung

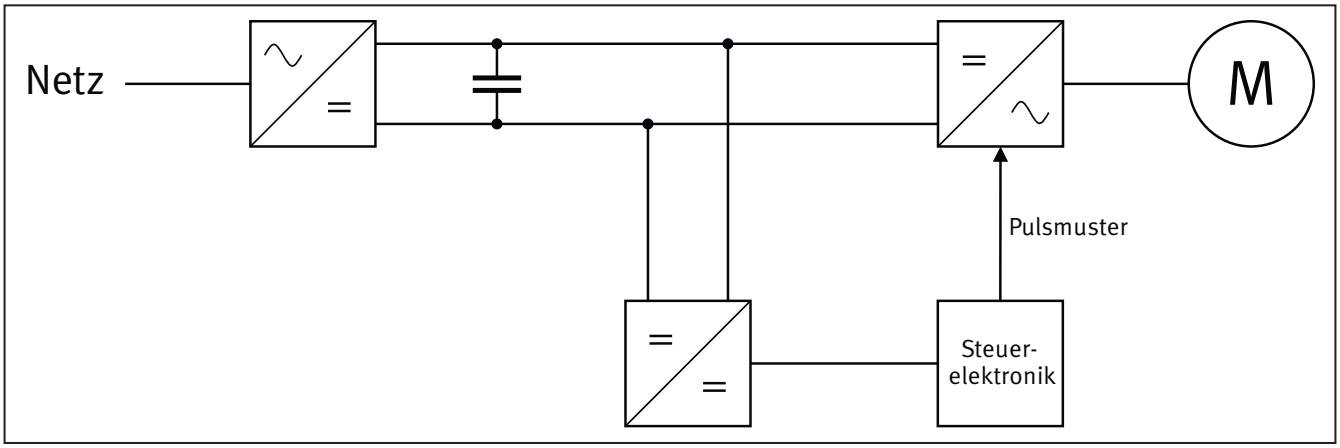
Ein Ausfall der Energieversorgung kann sich jederzeit ereignen. Dieser Zustand muss bei der Projektierung eines Frequenzumrichters für eine Maschinensteuerung berücksichtigt werden und stellt keinen Fehlerfall dar (DIN EN ISO 12100 [7], Abschnitt 5.4b „Mögliche Betriebszustände der Maschine: Störung der Energieversorgung“, DIN EN ISO 13849-1 [2], Abschnitt 5.2.8 „Schwankungen, Verlust und Wiederkehr der Energiequellen“). Bei der Risikoanalyse einer Maschine ist der Spannungsausfall zu berücksichtigen und insbesondere das zeitliche Verhalten von Sicherheitsfunktionen zu betrachten. Falls ein schnellstmögliches Stillsetzen (SS1 oder SS2) notwendig, aber durch den Frequenzumrichter nicht mehr möglich ist, können z. B. zusätzlich mechanische Bremsen eingesetzt werden. Dies gilt in jedem Fall auch bei Vertikalachsen.

Die Konsequenzen eines Spannungsausfalls auf einen Frequenzumrichter und seine Möglichkeiten, in dieser Situation ein Drehmoment im Motor oder eine Kraft im Linearmotor zu erzeugen, hängen vom internen Aufbau des Geräts ab. Es kommt darauf an, woher die Steuerelektronik des Frequenzumrichters ihre Spannungsversorgung erhält. Dabei muss unterschieden werden zwischen Frequenzumrichtern, bei denen die Steuerelektronik aus dem Gleichspannungszwischenkreis versorgt wird (siehe Abschnitt 5.5.1), und solchen, bei denen die Speisung der Steuerelektronik aus dem Versorgungsnetz (siehe Abschnitt 5.5.2) erfolgt.

5.5.1 Versorgung der Steuerelektronik aus dem Gleichspannungszwischenkreis

Bei dieser Bauform erhält die Steuerelektronik über einen DC/DC-Wandler ihre Spannungsversorgung aus dem Gleichspannungszwischenkreis (Abbildung 20).

Abbildung 20:
Spannungsversorgung der Steuerelektronik aus dem Gleichspannungszwischenkreis



Zum Zeitpunkt eines Spannungsausfalls ist der Gleichspannungszwischenkreis zumindest teilweise geladen. Erhält die Steuerelektronik hieraus ihre Versorgungsspannung, so ist sie noch in der Lage, die Pulsmuster für die Ansteuerung der IGBTs (englisch: insulated-gate bipolar transistor, Bipolartransistor mit isolierter Gate-Elektrode) im Leistungsteil des Frequenzumrichters zu erzeugen. Damit kann ein Drehmoment im Motor generiert werden. In vielen Anwendungen soll der Motor bei Spannungsausfall schnellstmöglich stillgesetzt werden. Dies ist aufgrund des geladenen Gleichspannungszwischenkreises noch für eine gewisse Zeit möglich, zumal Frequenzumrichter je nach Bauart auch in der Lage sind, aus der kinetischen Energie des Motors beim Bremsen Energie zurückzuge-

winnen und in den Gleichspannungszwischenkreis einzuspeisen. In vielen Fällen ist damit ein sicheres Stillsetzen noch möglich. Ist dies für die Sicherheit einer Applikation erforderlich, muss eine Analyse des Zeitverhaltens durchgeführt werden. Bei Vertikalachsen muss am Ende des Stillsetzvorgangs eine mechanische Vorrichtung den sicheren Zustand aufrechterhalten. Dies könnte durch das Einfallen einer mechanischen Bremse erfolgen, die durch die Sicherheits-Teilfunktion SBC angesteuert wird.

Eine Rückspeisung der Energie ins Versorgungsnetz ist bei Spannungsausfall ggf. nicht mehr möglich. Die kinetische Energie aus dem Bremsvorgang muss daher auch bei rückspeisefähigen Frequenzumrichtern in Bremswiderständen verbraucht werden. Ansonsten wäre ein gesteuertes Stillsetzen wegen Überladung des Gleichspannungszwischenkreises nicht mehr vollständig möglich.

5.5.2 Versorgung der Steuerelektronik aus dem Versorgungsnetz

Bei dieser Bauform erhält die Steuerelektronik über ein Netzteil ihre Betriebsspannung aus dem Versorgungsnetz (Abbildung 21). Üblich ist auch die Versorgung aus einem separaten 24-V-Netz, das jedoch bei Netzausfall ebenfalls versagt, sofern keine unterbrechungsfreie Spannungsversorgung (USV) eingesetzt wird.

Fällt die Netzversorgung aus, steht auch an der Steuerelektronik keine Versorgungsspannung mehr zur Verfügung und es können keine Pulsmuster für den Leistungsteil des Frequenzumrichters erzeugt werden. Der Motor kann kein Drehmoment mehr aufbringen, weder ist ein gesteuertes Stillsetzen noch das Hochhalten einer Last möglich. Der Motor trudelt aus bzw. bei Vertikalachsen stürzt die Last ab. Dieses Verhalten weisen auch Frequenzumrichter mit den integrierten Sicherheits-Teilfunktionen SS1, SS2 und SOS auf. Sofern hierdurch an einer Maschine Gefährdungen bestehen, sind zusätzliche Maßnahmen erforderlich, z. B. der Einsatz mechanischer Bremsen. Die Ansteuerung der Bremse kann durch die Sicherheits-Teilfunktion SBC erfolgen.

5.5.3 Berücksichtigung des Energieausfalls in Sicherheitsfunktionen nach DIN EN ISO 13849-1

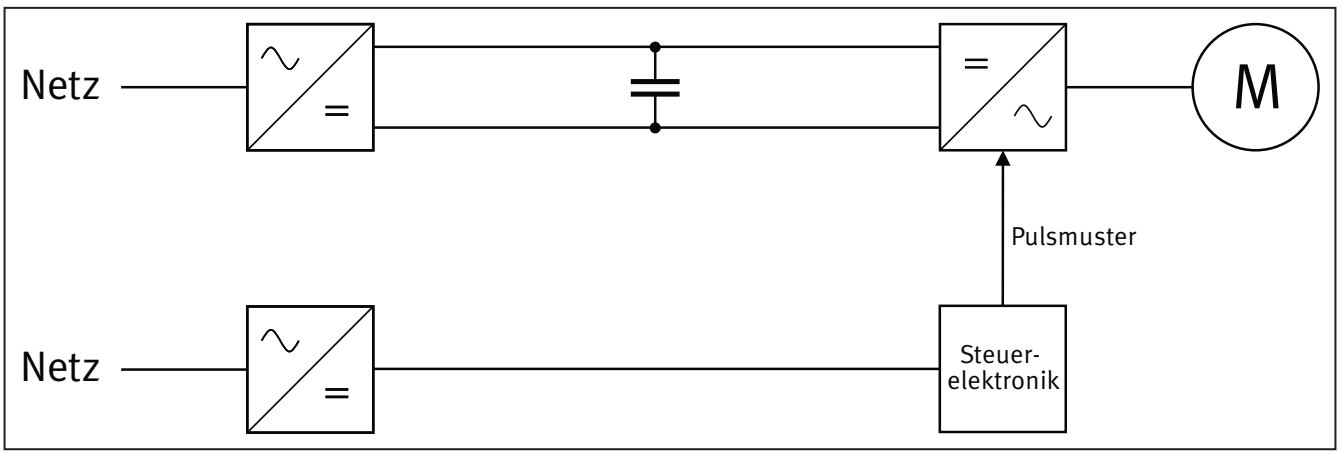
Speziell bei Vertikalachsen kann es vorkommen, dass für die Betriebszustände „Versorgungsspannung vorhanden“ und „Versorgungsspannung nicht vorhanden“ teilweise unterschiedliche Bauteile verwendet werden, um den sicheren Zustand der Maschine aufrechtzuerhalten. Damit können sich auch unterschiedliche Kategorien, PL und in jedem Fall unterschiedliche PFH_D-Werte ergeben. Die Norm schlägt seit ihrer dritten Ausgabe für diesen Fall vor, jeweils unterschiedliche Sicherheitsfunktionen vorzusehen:

a) mit verfügbarer Energie und

b) ohne verfügbare Energie.

Geht man davon aus, dass die Energieversorgung in der Regel vorhanden ist, kann sich für beide Sicherheitsfunktionen eine unterschiedliche Bewertung der Risikoparameter nach DIN EN ISO 13849-1 [2] ergeben. Dies erlaubt in Einzelfällen, je nach konkreten Risikoparametern, Sicherheitsfunktionen ohne verfügbare Energie mit einem geringeren PL_r zu realisieren.

Abbildung 21:
Spannungsversorgung der Steuerelektronik aus dem Versorgungsnetz

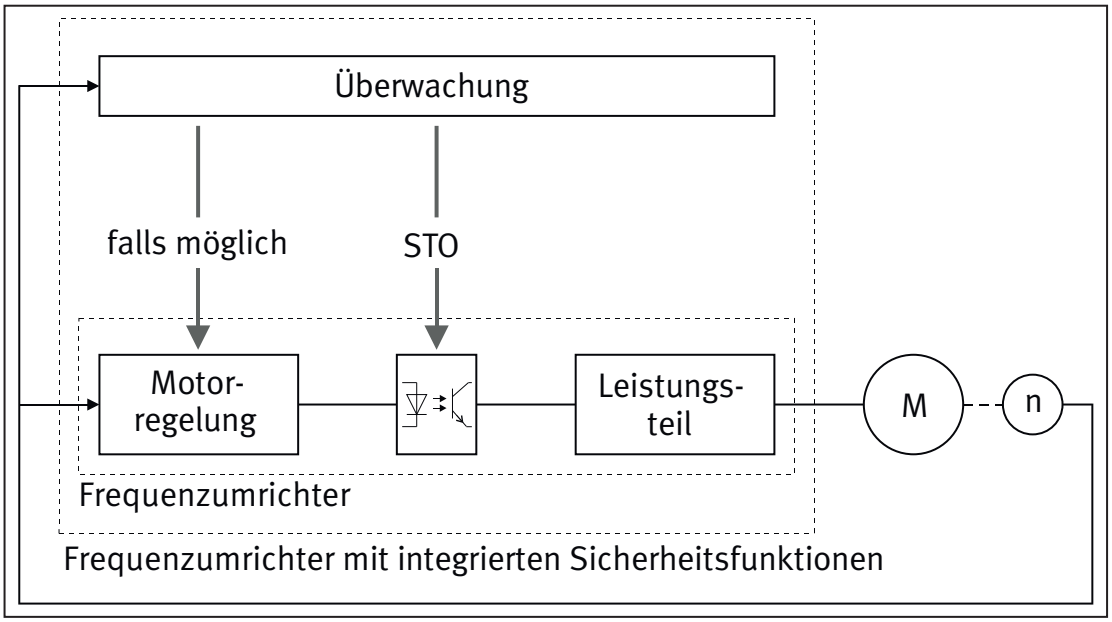


5.6 Anwendungsgrenzen von Sicherheits-Teilfunktionen

Sicherheits-Teilfunktionen, abgesehen von STO, sind in der Regel reine Überwachungsfunktionen. Hierbei wird der Motor einkanalig und ohne sicherheitstechnische Ertüchtigung angesteuert (siehe Frequenzumrichter in Abbildung 22). Eine zusätzliche Überwachungseinrichtung kontrolliert die Motorbewegungen und greift dann in die Motoransteuerung ein, wenn es zu einer Verletzung von eingestellten Grenzwerten kommt oder wenn festgestellt wird, dass der die Sicherheits-Teilfunktion ausführende Teil der Steuerung selbst einen Fehler aufweist.

Man geht bei Maschinen grundsätzlich davon aus, dass der energielose Zustand ein sicherer Zustand ist. Es wird kein Wert auf die Verfügbarkeit einer Motorsteuerung gelegt. Entsprechend sind im Fehlerfall die Reaktionen auf das Stillsetzen von Bewegungen ausgerichtet. Wird z. B. eine Überschreitung der maximal zulässigen Drehzahl festgestellt (Sicherheits-Teilfunktion SLS), so wird ein Stillsetzen eingeleitet. Ob noch ein gesteuertes Stillsetzen oder nur ein Austrudeln möglich ist, hängt davon ab, welche Funktionen im Frequenzumrichter noch verfügbar sind. Sofern die Motorregelung noch fehlerfrei arbeitet und der Leistungsteil keine Störung aufweist, kann schnellstmöglich stillgesetzt werden. Liegt allerdings ein Fehler der Motorregelung im Frequenzumrichter vor, so wird der Motor nicht mehr das erforderliche Bremsmoment aufbringen können. Die Fehlerursache ist oftmals nicht bekannt, sodass in den meisten Fällen nichts Anderes übrig bleibt, als im Fehlerfall die Sicherheits-Teilfunktion STO zu aktivieren und den Motor austrudeln zu lassen. Bei der Festlegung der notwendigen Sicherheitsfunktionen für eine Maschine ist dieses mögliche Verhalten zu berücksichtigen und ggf. sind zusätzliche Maßnahmen zu ergreifen. Falls z. B. bei Ausfall von SS1 oder SS2 eine verlängerte Zeit zum Stillsetzen nicht toleriert werden kann oder bei Versagen von SOS vertikale Lasten abstürzen können, ist eventuell eine mechanische Bremse erforderlich.

Abbildung 22:
Frequenzumrichter + Überwachung + Impulssperre = Frequenzumrichter mit integrierten Sicherheits-Teilfunktionen



Diese Problematik besteht bei allen bekannten Frequenzumrichtern mit integrierten Sicherheits-Teilfunktionen. Eine Redundanz im Steuerungs- und Leistungsteil zur Sicherstellung der Verfügbarkeit wurde nach Kenntnis der Autoren bisher nicht realisiert. Selbst wenn diese verfügbar wäre, müsste trotzdem eine Lösung für den Spannungsausfall gefunden werden.

Bei vielen Sicherheits-Teilfunktionen ist eine Festlegung von Parametern erforderlich, die das Verhalten der Sicherheits-Teilfunktion bestimmen. Hierbei ist insbesondere das Zeitverhalten zu berücksichtigen. Ein Fehler muss erst einmal erkannt werden, bevor eine geeignete Reaktion eingeleitet und bis zur Herstellung des sicheren Zustands ausgeführt werden kann.

In Abbildung 23 ist beispielhaft der Zeitablauf für die Sicherheits-Teilfunktion SLP dargestellt. Zum Zeitpunkt t_0 wird der eingestellte Maximalwert für die Position einer Achse überfahren. Die Überwachung erkennt bei t_1 die Überschreitung und aktiviert STO. Der Antrieb trudelt aus und kommt bei t_2 zum Stillstand. Im Zeitraum t_0 bis t_2 hat sich die Achse noch bewegt und ist in den nicht zulässigen Bereich eingedrungen. Um dies zu verhindern, muss das Zeitverhalten für die Ausführung der Sicherheits-Teilfunktion berücksichtigt und der Grenzwert entsprechend

niedriger eingestellt werden, sodass der zulässige Bereich nicht verlassen wird.

Die Sicherheits-Teilfunktion STO ist keine Überwachungsfunktion. Sie stellt lediglich sicher, dass die funktionale Ansteuerung des Motors unterbrochen wird, sodass im Motor kein Drehfeld aufgebaut werden kann. Aber auch diese Funktion hat ihre Grenzen. So kann STO nicht verhindern, dass im Stillstand bei einem Fehler im Leistungsteil ein kurzzeitiges Rucken des Motors erfolgt. Das Ausmaß des Ruckens ist abhängig von der Polpaarzahl des Motors und ggf. einer Getriebestufe. STO verhindert jedoch, dass es zu einer Drehbewegung kommt. In Applikationen mit STO ist zu prüfen, ob das Rucken im Fehlerfall toleriert werden kann. Sollte das nicht der Fall sein, ist ggf. zusätzlich eine mechanische Bremse vorzusehen. Dies ist z. B. an einer Fräsmaschine mit von Hand einzuspannendem Fräswerkzeug der Fall. Hier können auch geringe Motorbewegungen zu Finger- und Handverletzungen führen.

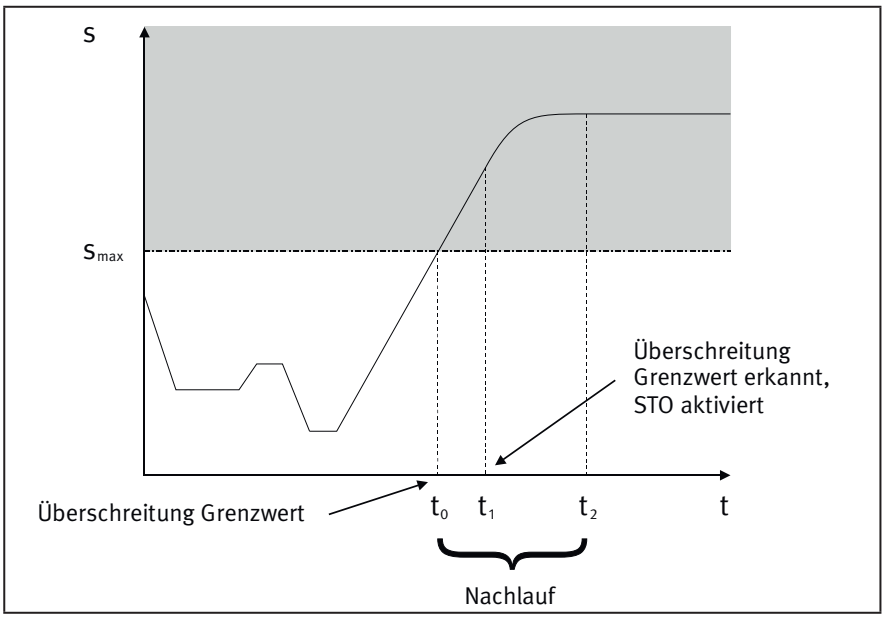


Abbildung 23: Weg/Zeit-Diagramm der Sicherheits-Teilfunktion SLP (Sicher begrenzte Position)

Alle Sicherheits-Teilfunktionen haben also ihre individuellen Einsatzgrenzen und ggf. auch unterschiedliche Reaktionen im Fehlerfall. Hierzu macht der Hersteller des PDS(SR) Angaben in der Betriebsanleitung. Bei der Projektierung einer Antriebssteuerung mit integrierten Sicherheits-Teilfunktionen ist u. a. zu beachten:

- Welche Reaktion erfolgt bei Verletzung eines Grenzwerts?
- Welche Reaktion erfolgt bei Erkennung eines Fehlers in dem Teil der Steuerung, der die Sicherheits-Teilfunktion ausführt?
- Welche Reaktionszeit ist bis zur Herstellung des sicheren Zustands zu berücksichtigen?
- Welche Gefährdung ergibt sich dadurch in der Applikation?
- Sind zusätzliche Maßnahmen erforderlich (z. B. mechanische Bremse, größerer Abstand zwischen Lichtgitter und Gefahrenstelle)?

5.7 Trennung von den Energiequellen bei Reparatur- und Wartungsarbeiten

In den vorangegangenen Abschnitten wurden eine Reihe von Sicherheitsfunktionen und Teil-Sicherheitsfunktionen beschrieben, die unter Verwendung von Antriebssteuergeräten und anderen sicherheitsrelevanten Teilen von Steuerungen realisiert werden, ohne dass dabei der Antrieb von der Versorgungsenergie getrennt werden muss.

Diese Sicherheitsfunktionen sind allerdings nicht für alle Anwendungsfälle und Betriebsarten der Maschine geeignet. Insbesondere für Instandhaltungsarbeiten ist eine Trennung von den Energiequellen erforderlich.

5.7.1 Anforderungen aus der Maschinenrichtlinie

Die Maschinenrichtlinie 2006/42/EG [6] stellt in Anhang I, Abschn. 1.6.3 „Trennung von den Energiequellen“, folgende Forderungen auf:

- *„Die Maschine muss mit Einrichtungen ausgestattet sein, mit denen sie von jeder einzelnen Energiequelle getrennt werden kann. Diese Einrichtungen sind klar zu kennzeichnen. Sie müssen abschließbar sein, falls eine Wiedereinschaltung eine Gefahr für Personen*

verursachen kann. Die Trenneinrichtung muss auch abschließbar sein, wenn das Bedienungspersonal die permanente Unterbrechung der Energiezufuhr nicht von jeder Zugangsstelle aus überwachen kann."

- *„Bei elektrisch betriebenen Maschinen, die über eine Steckverbindung angeschlossen sind, genügt die Trennung der Steckverbindung, sofern dass Bedienungspersonal die permanente Trennung der Steckverbindung von jeder Zugangsstelle aus überwachen kann."*

- *„Die Restenergie oder die gespeicherte Energie, die nach der Unterbrechung der Energiezufuhr noch vorhanden sein kann, muss ohne Risiko für Personen abgeleitet werden können."*

- *„Abweichend von den vorstehenden Anforderungen ist es zulässig, dass bestimmte Kreise nicht von ihrer Energiequelle getrennt werden, z. B. um Teile in ihrer Position zu halten, um Daten zu sichern oder um die Beleuchtung innen liegender Teile zu ermöglichen. In diesem Fall müssen besondere Vorkehrungen getroffen werden, um die Sicherheit des Bedienungspersonals zu gewährleisten."*

Der „Leitfaden für die Anwendung der Maschinenrichtline 2006/42/EG" [17] gibt dazu noch erläuternde Hinweise.

Dem Leitfaden zufolge soll mit den Anforderungen im ersten Absatz von Abschnitt 1.6.3 [6] erreicht werden, dass die Maschine während der Reparatur- und Wartungsarbeiten in einem sicheren Zustand gehalten wird. Die Personen, die Wartungsarbeiten bei stillgesetzter Maschine ausführen, müssen die Maschine vor Beginn der Arbeiten von den Energiequellen trennen können, damit gefährliche Zwischenfälle (z. B. unerwarteter Anlauf) vermieden werden. Das gilt unabhängig davon, ob diese Zwischenfälle auf Fehler in der Maschine, auf Handlungen Dritter (welche die Anwesenheit von Wartungspersonal nicht wahrnehmen) oder auf versehentliche Maßnahmen des Wartungspersonals selbst zurückzuführen sind.

Kann das Wartungspersonal nicht auf einfache Weise überprüfen, ob die Trenneinrichtungen in der Trennstellung bleiben, müssen die Trenneinrichtungen in der Trennstellung abgeschlossen werden können. Sind mehrere Personen gleichzeitig an den Wartungsarbeiten beteiligt, müssen alle beteiligten Mitglieder des Wartungspersonals für die Dauer der Wartungsarbeiten ihr Schloss an der Trenneinrichtung anbringen können.

Der zweite Absatz gilt in erster Linie für handgehaltene kraftbetätigte Werkzeuge oder transportable Maschinen, bei denen die Bedienperson von jedem für ihn zugänglichen Punkt aus überprüfen kann, ob die Stromversorgung angeschlossen ist.

Die gespeicherte Energie, von der in Absatz 3 die Rede ist, kann beispielsweise als kinetische Energie (Trägheit bewegter oder rotierender Massen), elektrische Energie (in Zwischenkreis-Kondensatoren), Druckenergie (in fluidtechnischen Systemen) oder als potenzielle Energie (in gespannten Federn oder schwerkraftbelasteten beweglichen Maschinenteilen) vorliegen.

Zu den in Absatz 4 genannten Stromkreisen, die nicht von der Energiequelle getrennt werden müssen, können auch solche gezählt werden, die für den Betrieb von Werkzeugen oder die Abfuhr gefährlicher Stoffe erforderlich sind. Die Sicherheit der Bedienperson kann in solchen Fällen beispielsweise durch Sperrung des Zugangs zu den betreffenden Energiekreisen oder durch geeignete Warnanzeigen oder Warneinrichtungen gewährleistet werden.

Die Betriebsanleitung des Herstellers oder das Handbuch zur Instandhaltung muss Angaben zur Trennung der Energiequellen, zum Abschließen der Trenneinrichtung, zur Ableitung der Restenergien, sowie zur Überprüfung des sicheren Maschinenzustands enthalten (siehe Leitfaden zur Maschinenrichtlinie [17] § 272: Anmerkungen zu Nummer 1.7.4.2, Buchstabe s).

Eine gesonderte Anforderung zum Trennen von Batterien an mobilen Maschinen ist in der Maschinenrichtlinie [6], Anhang I, Abschn. 3.5.1 festgelegt.

5.7.2 Anforderungen aus DIN EN 60204-1

Die Norm DIN EN 60204-1 [9] enthält zur elektrischen Ausrüstung von Maschinen die entsprechenden Spezifikationen für die zuverlässige Trennung von der Energieversorgung.

Gemäß Abschnitt 5.3.1 in [10] muss eine Netz-Trenneinrichtung vorgesehen werden für:

- *jeden Netzanschluss zu einer oder mehreren Maschinen,*

- *für jede Bordstromstromversorgung.*

Wenn erforderlich, muss die Netztrenneinrichtung die elektrische Ausrüstung der Maschine von der Stromversorgung trennen (z. B. für Arbeiten an der Maschine, einschließlich der Arbeiten an der elektrischen Ausrüstung).

Abhängig von den Arbeiten, die im Rahmen der Instandhaltung durchzuführen sind, unterscheidet die Norm DIN EN 60204-1 [9] zwischen:

a) Ausschalteinrichtungen zur Verhinderung von unerwartetem Anlauf (Abschnitt 5.4)

b) Einrichtungen zum Trennen der elektrischen Ausrüstung (Abschnitt 5.5)

Basierend auf den Anforderungen in den Abschnitten 5.4 und 5.5 kann die folgende Übersicht abgeleitet werden.

a) Verhinderung eines unerwarteten Anlaufs	b) Trennen der elektrischen Ausrüstung
Geräte und Einrichtungen **mit** Trennereigenschaften • Alle Arbeiten, die im Rahmen der Instandhaltung erforderlich sind (Wartung, Störungsbeseitigung, Reparaturen).	Geräte und Einrichtungen **mit** Trennereigenschaften • Alle Arbeiten, die im Rahmen der Instandhaltung erforderlich sind (Wartung, Störungsbeseitigung, Reparaturen).
Geräte und Einrichtungen **ohne** Trennereigenschaften • Inspektionen, • Einstellungen, • Arbeiten an der elektrischen Ausrüstung, wenn: – keine Gefährdung durch elektrischen Schlag und Verbrennung besteht; – die Ausschalteinrichtung während der Arbeiten wirksam bleibt; – die Arbeit von geringem Umfang ist (z. B. Auswechseln einer steckbaren Einheit ohne Eingriff in die bestehende Verdrahtung).	Geräte und Einrichtungen **ohne** Trennereigenschaften • Nicht zulässig

Die zulässigen Geräte und Einrichtungen für a) und b) sowie die Anforderungen an Eignung, Zugänglichkeit, Kennzeichnung und Verhinderung des Wiedereinschaltens, sind DIN EN 60204-1 [9], Abschnitte 5.3 bis 5.6 zu entnehmen.

Fazit:

Wie DIN EN 60204-1 [9] zeigt, sind Ausschalteinrichtungen zur Verhinderung von unerwartetem Anlauf ohne Trennereigenschaften nur für geringfügige Arbeiten unter bestimmten Voraussetzungen zulässig. Erlaubt sind beispielsweise Inspektions- und Einstellarbeiten. Arbeiten an der elektrischen Ausrüstung sind nur dann zulässig, wenn keine Gefährdungen durch elektrischen Schlag oder Verbrennungsgefahr durch Lichtbögen bestehen und die Ausschalteinrichtung stets wirksam bleibt.

Dies gilt auch, wenn für den sicherheitsbezogenen Teil der Steuerung bzw. die Sicherheitsfunktion, ein höherer Performance Level nach DIN EN ISO 13849 eingehalten wird, wie zum Beispiel PL d.

Für alle weitergehenden Arbeiten wie Reparaturen und Störungsbeseitigung sind Geräte und Einrichtungen mit Trennereigenschaften erforderlich.

Es wird darauf hingewiesen, dass herkömmliche Schütze im Allgemeinen keine Trennereigenschaften aufweisen.

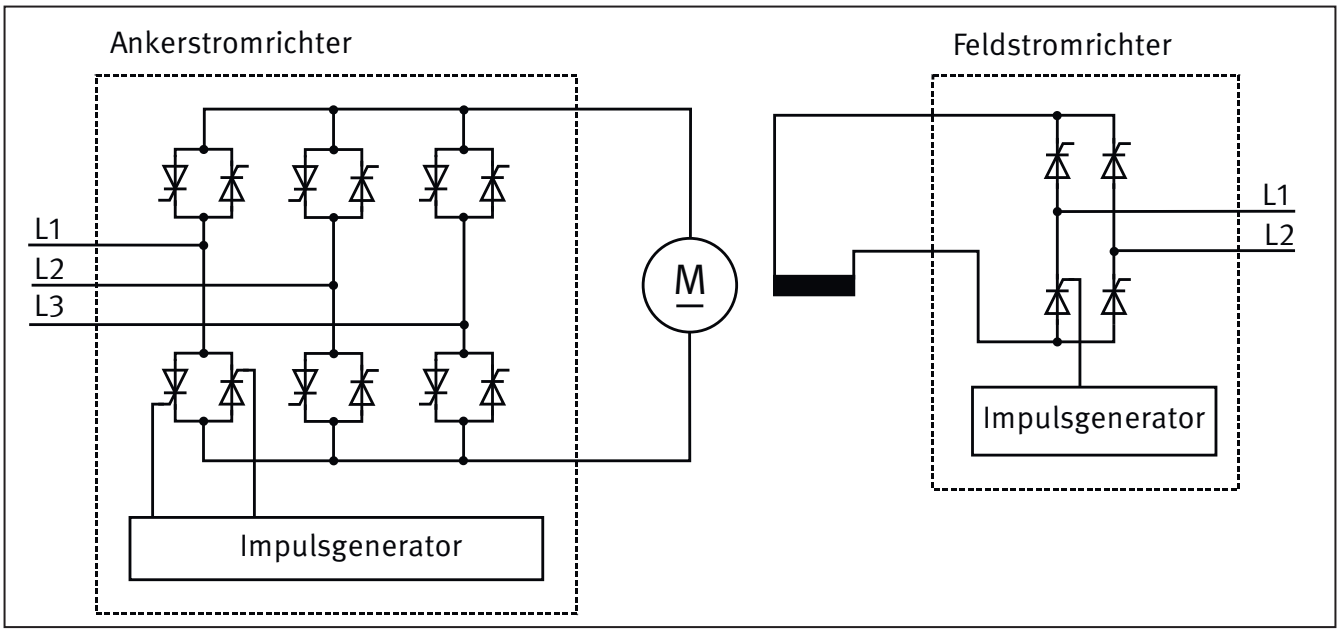
6 Sicherheitsfunktionen bei Gleichstromantrieben

Wie bereits erwähnt, wurde noch vor wenigen Jahrzehnten der Großteil der drehzahlveränderbaren Antriebe aufgrund der einfachen Regelbarkeit in Gleichstromtechnik ausgeführt. Heute übernehmen fast ausschließlich Drehstromantriebe mit Frequenzumrichtern oder Servoreglern diese Funktion. Dieser Report beschäftigt sich aus diesem Grund auch größtenteils mit Sicherheitsfunktionen, die in Verbindung mit Antriebssteuerungen für Drehstrommotoren realisiert werden.

Allerdings dürfen die Gleichstromantriebe nicht gänzlich außer Acht gelassen werden, denn in einigen Anwendungsbereichen, insbesondere in der Schwerindustrie (z. B. Walzwerke), sind sie nach wie vor im Einsatz. Nachfolgend wird am Beispiel eines fremderregten Gleichstrommotors das Prinzip der Drehzahlsteuerung kurz erläutert.

Der Motor besteht aus einem feststehenden Teil (Stator) und einem drehbaren Teil (Rotor) – auch Anker genannt. Das Magnetfeld des Stators wird mit dem Strom aus dem Feldstromrichter erzeugt, der Anker bezieht seine Energie aus dem Ankerstromrichter. Die Drehzahl des Motors kann bis zur Nenndrehzahl über die Ankerspannung verstellt werden. Bei gleichbleibender Belastung bewirkt eine Erhöhung der Ankerspannung eine entsprechende Geschwindigkeitszunahme. Die Ankerspannung wird in diesem Beispiel im Ankerstromrichter mittels einer Drehstrom-Thyristorbrücke aus der Netzspannung erzeugt. Die Höhe der Gleichspannung wird über eine Phasenanschnittsteuerung eingestellt, deren Zündimpulse der Impulsgenerator erzeugt. Damit der Antrieb in beiden Drehrichtungen betrieben werden kann, sind zwei Drehstrom-Thyristorbrücken gegenparallel geschaltet (Abbildung 24).

Abbildung 24:
Prinzipieller Aufbau einer Antriebssteuerung für fremderregte Gleichstrommotoren



Um die Drehzahl der Maschine über die Nenndrehzahl hinaus zu erhöhen, ist eine Abschwächung des Erregerfeldes erforderlich, was durch Reduzierung des Stromes in der Erregerwicklung erreicht werden kann. Die entsprechende Schaltung hierfür ist in dem separaten Feldstromrichter enthalten.

Die Integration von Sicherheits-Teilfunktionen in Antriebssteuerungen für Gleichstrommotoren ist prinzipiell ähnlich wie für Drehstrommotoren. Ein großer Unterschied besteht jedoch für die Sicherheits-Teilfunktion STO.

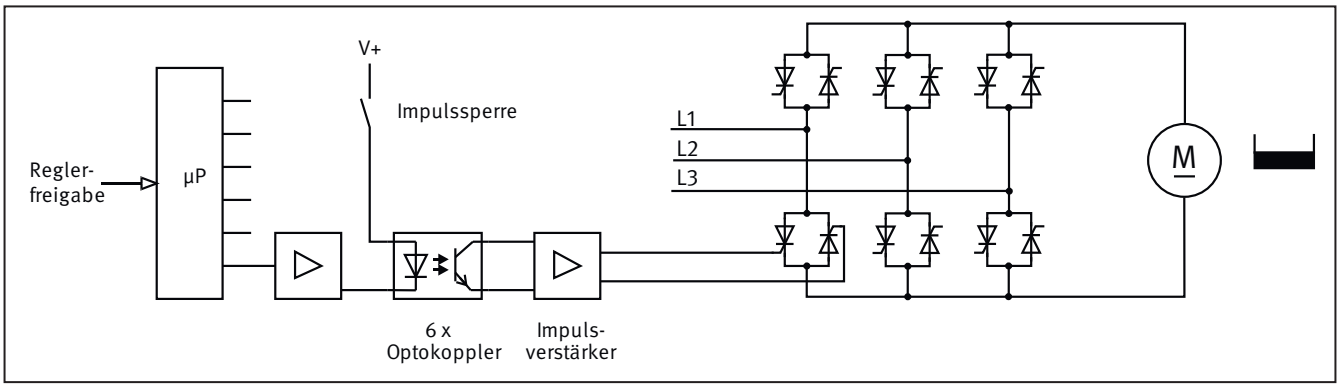
Um die Sicherheits-Teilfunktion STO zu realisieren, muss der Aufbau eines Drehmoments im Motor verhindert werden. Dies kann u. a. dadurch erreicht werden, dass der Stromfluss im Anker unterbunden wird. Eine Möglichkeit hierfür ist beispielsweise die Verwendung eines Netzschützes, mit dem die Energieversorgung zum Anker des Motors abgeschaltet wird. Die Verwendung von Leistungsschaltgeräten ist allerdings aus verschiedenen Gründen nicht immer sinnvoll (siehe Abschnitt 4.3). Es bringt Vorteile, die Sicherheits-Teilfunktion in die Antriebssteuerung zu integrieren. Als geeignete Maßnahme zur Implementierung der Sicherheits-Teilfunktion STO in einer Antriebssteuerung für Drehstrommotoren wurde die Impulssperre beschrieben. Durch Abschaltung der Versorgungsspannung für die Übertragungselemente (z. B. Optokoppler) wird die Ansteuerung der Leistungshalbleiter gesperrt.

In Abbildung 25 ist dieses Konzept beispielhaft für den Ankerstromrichter eines Gleichstrommotors dargestellt.

Anders als bei Drehstromantrieben, für die man komplexe Pulsmuster benötigt, um ein Drehfeld zu erzeugen, braucht der Gleichstrommotor lediglich einen Gleichstrom zur Erzeugung eines Drehmoments. Das bedingt eine andere Fehlerbetrachtung bezüglich der Sicherheits-Teilfunktion STO und stellt den entscheidenden Unterschied zu den Drehstromantrieben dar. Während man bei Drehstromantrieben davon ausgehen kann, dass bei sicher gesperrter Impulsübertragung im Motor kein Drehfeld aufgrund von zufälligen Bauteilfehlern in der Endstufe entstehen kann – und damit auch kein Drehmoment –, verhält sich das beim Stromrichter für Gleichstrommotoren anders. So kann es aufgrund von Fehlern in den Leistungsthyristoren trotz Impulssperre (und evtl. abgeschalteter Reglerfreigabe) zu einem Stromfluss kommen, wenn beispielsweise durch einen Ausfall infolge gemeinsamer Ursache (Common Cause Failure, CCF) zwei „passende“ Thyristoren ein Diodenverhalten aufweisen. Durch diesen Fehler fließt ein Ankerstrom, der Gleichstrommotor kann ein Drehmoment aufbauen und die Motorwelle dreht sich. Der hier angenommene Fehler der Leistungsthyristoren kann zwar auch im Leistungsteil für den Drehstrommotor auftreten. Es kann dadurch aber nur zu einem Rucken der Motorwelle und nicht zu einer Drehbewegung kommen, da kein Drehfeld aufgebaut werden kann.

In Anwendungen, bei denen die Einfehlersicherheit erfüllt sein muss (Kategorie 3 und 4), ist die Impulssperre im Ankerstromrichter als alleinige Maßnahme nicht ausreichend. Für diese Kategorien wird ein zusätzlicher Abschaltpfad benötigt, selbst wenn die Impulssperre zweikanalig bzw. einfehlersicher ausgeführt ist. Ein solcher zusätzlicher Abschaltpfad könnte beispielsweise ein Netzschütz oder ein Leistungsschalter im Ankerstromkreis sein.

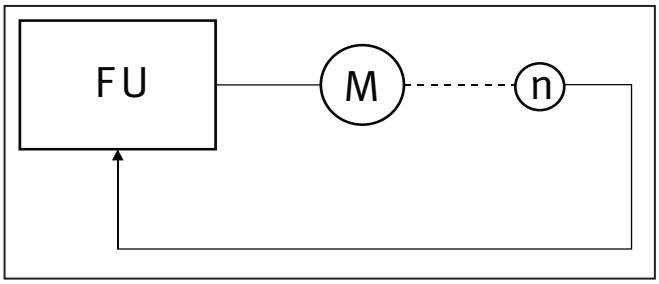
Abbildung 25:
Impulssperre im Ankerstromrichter



7 Positionsgeber in Sicherheitsfunktionen

Für die Kommutierung und Regelung eines Motors benötigt der Frequenzumrichter bzw. Servoregler die aktuelle Position, die üblicherweise ein Drehgeber oder Lineargeber bereitstellt[7]. Damit kann ein geschlossener Regelkreis aufgebaut werden, der z. B. für Positionieraufgaben eingesetzt wird (siehe Abbildung 26).

Abbildung 26:
Geschlossener Regelkreis



Geber lassen sich grob in Inkrementalgeber und Absolutwertgeber unterteilen. Inkrementalgeber stellen Relativinformationen über den Drehwinkel einer Achse oder die Position einer linearen Bewegung zur Verfügung. Je nach Erfordernis der zu realisierenden Sicherheits-Teilfunktion kann eine angeschlossene Antriebssteuerung hieraus u. a. Drehzahl/Geschwindigkeit (SLS, Sicher begrenzte Geschwindigkeit) und/oder Beschleunigung (SLA, Sicher begrenzte Beschleunigung) ermitteln. In diesen Fällen ist die Kenntnis der absoluten Position nicht erforderlich.

Sollen jedoch in einer Maschine z. B. Quetschstellen mit Sicherheitsfunktionen abgesichert werden, dürfen bestimmte Maschinenteile den zulässigen Verfahrbereich nicht verlassen. Dies kann mit der Sicherheits-Teilfunktion SLP (Sicher begrenzte Position) erfolgen und hierfür ist die Kenntnis der absoluten Lage erforderlich. Inkrementalgeber müssen nach dem Einschalten zunächst sicher referenziert werden. Dies erfolgt in der Regel durch das Anfahren einer definierten Position in der Maschine, die mit einem zusätzlichen Positionssensor versehen ist. Nachdem der Referenzpunkt angefahren wurde, kann dann in der Antriebssteuerung durch Addition oder Subtraktion von Inkrementen die Absolutposition berechnet werden.

Einfacher ist der Einsatz von Absolutwertgebern. Hier steht direkt ein digitales Positionssignal zur Verfügung, ein Referenzieren kann entfallen. Bei der Ausführung als Drehgeber sind Singleturn- und Multiturngeber zu unterscheiden. Beim Singleturngeber ist nur innerhalb einer Umdrehung der Geberwelle eine eindeutige Absolutposition zu erhalten, während ein Multiturngeber zusätzlich ein Signal über die Anzahl der zurückgelegten Umdrehungen bereithält, sodass auch bei mehreren Umdrehungen ein eindeutiger Absolutwert zur Verfügung steht.

Die Anforderungen der Sicherheitstechnik an die Geber hängen wesentlich von der zu realisierenden Sicherheitsfunktion und natürlich von dem für den Einsatzfall ermittelten PL_r ab.

Am Markt werden sehr unterschiedliche Geber angeboten. Beim Zusammenspiel mit dem angeschlossenen Frequenzumrichter oder Servoregler ist insbesondere die Schnittstelle zwischen diesen beiden Bauteilen von Bedeutung. Weit verbreitet sind:

- Inkrementalgeber mit Rechtecksignalen,
- Inkrementalgeber mit Sinus/Cosinus-Signalen,
- Inkremental- und Absolutgeber mit Bus-Schnittstellen.

Für sicherheitstechnische Anwendungen wird inzwischen eine Vielzahl von sicheren Gebern angeboten. Die Hersteller geben hierbei an, bis zu welchem PL oder SIL das Bauteil eingesetzt werden kann. Auch bei sicheren Gebern können Bauteilfehler auftreten, die zu einem gefährlichen Ausfall einer Sicherheitsfunktion führen; es sind also fehlererkennende Maßnahmen notwendig. Dies ist vielfach nicht im Geber selbst möglich, sondern muss im angeschlossenen Frequenzumrichter oder Servoregler erfolgen. Die Geberhersteller beschreiben in der Betriebsanleitung die erforderlichen Maßnahmen, um den entsprechenden PL bzw. SIL erfüllen zu können. Bei Sinus/Cosinus-Gebern wird oft die Überprüfung auf $\sin^2 + \cos^2 = 1$ verwendet.

Kritisch ist der sogenannte Geberwellenbruch. Hierunter ist zu verstehen, dass sich die Kopplung der Geberwelle an die Motorwelle löst oder dass die mechanische Befestigung des Gebers fehlerhaft ist und sich der gesamte Geber mit der Motorwelle mitdrehen kann. Je nach Sicherheitsfunktion kann hierdurch ein unentdeckter gefährlicher Fehler entstehen. Dies führt zu Einschränkungen insbesondere beim Einsatz an schwerkraftbelasteten Vertikalachsen. Als Lösung bietet sich der Einsatz von Gebern an, bei denen der Hersteller eine mechanische Überdimensionierung vorgenommen hat, sodass der Geberwellenbruch ausgeschlossen werden kann (siehe [3], Tabelle D.8).

7 Es gibt auch Frequenzumrichter, die die notwendigen Positionsinformationen von internen Signalen ableiten und daher keine externen Geber benötigen. Jedoch lassen sich hiermit nicht alle Sicherheits-Teilfunktionen realisieren.

Hinweis:

Die Realisierung von PL e/SIL 3 unter Anwendung von Fehlerausschlüssen wird generell kritisch gesehen (siehe DIN ISO/TR 23849 [18], Abschnitt 7.2.2.3). Die hier zu betrachtenden mechanischen Bauteile des Gebers sind jedoch mit einem derart hohen Faktor überdimensioniert, dass die Fehlerausschlüsse auch in PL e/SIL 3 zulässig sind.

Sollen bei einer Anwendung keine sicheren Geber eingesetzt werden, so ist prinzipiell der Aufbau von Sicherheitsfunktionen auch mit nicht sicherheitstechnisch ertüchtigten Gebern möglich. Einige Hersteller von PDS(SR) ermöglichen den Einsatz solcher Geber durch eine geeignete Fehlererkennung in der sicheren Steuerung (siehe Betriebsanleitung des PDS(SR)). In jedem anderen Fall liegt es jedoch in der Verantwortung des Maschinenherstellers, den Nachweis zu erbringen, dass der geforderte PL/SIL erfüllt wird (siehe [16] und [19]). Unter anderem müssen dazu mittels einer FMEA für alle an der Signalerzeugung und -verarbeitung beteiligten Bauteile die möglichen Ausfallarten und deren Auswirkung auf die Sicherheitsfunktion untersucht werden (siehe „Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit“ [20]). Die hierzu nötigen Informationen und Kenntnisse liegen dem Anwender des Gebers in der Regel nicht vor, sodass in diesem Fall Unterstützung durch den Geberhersteller erforderlich ist.

Neben der Überprüfung auf $\sin^2 + \cos^2 = 1$ gibt es weitere Möglichkeiten zur Erkennung von Geberfehlern, z. B. indem der Geber in den Regelkreis Frequenzumrichter/Motor einbezogen wird. Fehlerhafte Gebersignale werden in der Regel dazu führen, dass ein falscher Wert für die Motorposition vorliegt und daher eine korrekte Kommutierung des Motors nicht mehr möglich ist. Dies führt zu einer Betriebsstörung und damit zu einer Aufdeckung des Fehlers über den technischen Prozess. Allerdings ist zu beachten, dass moderne Regelalgorithmen auch bei angeschlossenem Geber zeitweise im geberlosen Betrieb arbeiten können, sodass in diesem Fall eine schnelle Fehlererkennung an der Maschine nicht sichergestellt ist.

Signalauswertung von sicheren Sinus-/Cosinus-Gebern

Werden Geber zusammen mit sicheren Frequenzumrichtern, Drehzahlüberwachungsgeräten oder Stillstandswächtern eingesetzt, so stellt sich die Frage der Signalauswertung für den Anwender nicht. In diesen Fällen beschreiben die Anwendungshinweise für diese Bauteile die korrekte Verbindung von Geber und Auswertegerät sowie ggf. die Einstellung von Parametern. Die Signalauswertung erfolgt in den Auswertegeräten entsprechend dem angegebenen PL bzw. SIL. Wenn jedoch eigene Schaltungen entwickelt werden, ist Folgendes zu berücksichtigten.

Sinus-/Cosinus-Geber liefern am Ausgang zwei Signale, eben das Sinussignal und das Cosinussignal. Werden diese beiden Signale unabhängig voneinander ausgewertet und sind innerhalb des Gebers die erforderlichen Fehlerausschlüsse nachweisbar, so könnte im Geber und im Auswertegerät eine durchgängige Zweikanaligkeit vorliegen. Dies ist von Bedeutung, wenn Kategorie 3 oder 4 nach DIN EN ISO 13849-1 [2] erreicht werden soll. Diese Zweikanaligkeit geht jedoch dann verloren, wenn für die Realisierung einer Sicherheitsfunktion sowohl das Sinus- als auch das Cosinus-Signal verwendet werden. Dies ist z. B. dann der Fall, wenn für die Sicherheitsfunktion die absolute Position gebildet wird (aus Sinus UND Cosinus muss hierfür die Drehrichtung/Bewegungsrichtung ermittelt werden), die Hardware im Auswertegerät Quadraturdecoder-ICs verwendet (siehe [19]) oder aus Sinus UND Cosinus durch Interpolation Zwischenwerte gebildet werden. Je nach erforderlichem PL ist dann ggf. ein zweiter Kanal, z. B. durch Einsatz eines weiteren Gebers, hinzuzuziehen.

8 Konfigurationsprüfung

Das Systemverhalten jeder Antriebssteuerung wird über einstellbare Parameter an die jeweilige Applikation angepasst. Dabei werden z. B. maximal zulässige Geschwindigkeitswerte oder Grenzen für das Zeitverhalten beim Stillsetzen eines Antriebs festgelegt. Unabhängig davon, ob Sicherheits-Teilfunktionen unter Verwendung von Steuerungen mit integrierter Sicherheit oder mit externen Überwachungseinrichtungen realisiert werden, muss eine Überprüfung der Einstellungen erfolgen. Ziel ist es, ein korrektes Systemverhalten (Zeit, Weg, Drehzahl usw.) nachzuweisen und damit ggf. Projektierungs- oder auch Eingabefehler aufzudecken.

Übertragungsfehler, z. B. auf dem Weg vom unsicheren PC in den sicheren Parameterspeicher, werden zum Zeitpunkt der Konfigurationsprüfung nicht unterstellt. Für den Ablauf zur Einstellung von Parametern gelten spezifische Anforderungen. Diese sind in DIN EN ISO 13849-1 [2], Abschnitt 4.6.4 beschrieben. In der Konfigurationsprüfung geht es vielmehr um die Aufdeckung von ungeeignet festgelegten Parametern, die aber fehlerfrei in der sicheren Steuerung abgelegt sind. Als Fehlerquelle sind u. a. möglich:

- ungeeignet festgelegte Grenzwerte für Drehzahl, Abbremsung, Verzögerungszeiten, Position etc.
- Parameter sind prinzipiell korrekt gewählt, aber für bestimmte Maschinenzustände ungeeignet
- Eingabefehler bei der Parametrierung
- Prioritätskonflikte mit anderen Sicherheits-Teilfunktionen
- je nach Betriebsart unterschiedliche Anforderungen an die Parametrierung

Eine Konfigurationsprüfung ist nach der Inbetriebnahme einer Maschine erforderlich und nachdem Änderungen an der Hardware oder Software der Maschine vorgenommen wurden. Dies gilt auch für Änderungen, die durch Datenfernübertragung vorgenommen wurden.

Der Antriebshersteller muss in der Anwenderdokumentation eine Anleitung zur Durchführung einer Konfigurationsprüfung bereitstellen, z. B. in Form einer Checkliste. Die Durchführung der Prüfung erfolgt durch autorisiertes Personal und muss in geeigneter Weise protokolliert werden.

Die Durchführung der Konfigurationsprüfung sollte stets auch das Verhalten bei Energieausfall und beim Auftreten von Fehlern innerhalb der Sicherheitsfunktion betrachten.

Bei Serienmaschinen kann darauf verzichtet werden, die Konfigurationsprüfung für alle Maschinen durchzuführen, wenn eine vollständige Konfigurationsprüfung an einer Mustermaschine durchgeführt wurde und die Daten der sicherheitsrelevanten Parameter gegen Veränderung gesichert in die Serienmaschinen übertragen werden oder sichergestellt ist, dass die Sicherheits-Teilfunktionen in allen Geräten wie vorgesehen konfiguriert werden.

Literatur

[1] DIN EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (3/1997). Beuth, Berlin 1997

[2] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (6/2016). Beuth, Berlin 2016

[3] DIN EN 61800-5-2 (VDE 0160-150-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (11/2017). Beuth, Berlin 2017

[4] *Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Borowski, T.; Büllesbach, K.-H.; Dorra, M.; Foermer-Schaefer, H.-G.; Uppenkamp, J.; Lohmaier, O.; Heimann, K.-D.; Köhler, B.; Zilligen, H.; Otto, S.; Rempel, P.; Reuß, G.*: Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849. IFA Report 2/2017. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2017. http://publikationen.dguv.de/dguv/pdf/10002/rep0217.pdf

[5] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer elektronischer programmierbarer elektronischer Systeme – Teil 0 (2005) bis Teil 7 (2/2011). Beuth, Berlin 2011

[6] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung) mit Berichtigung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG vom 09.06.2006. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32006L0042&from=DE

[7] DIN EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung. Beuth, Berlin 2010

[8] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (2/2013). Beuth, Berlin 2013

[9] DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (6/2007). Beuth, Berlin 2007

[10] *Apfeld, R.; Portmann, M.*: Festlegen von Maximalgeschwindigkeiten für manuelle Eingriffe an laufender Maschine (Kennzahl 330 216). In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitzplatz. 2. Lfg. XII/2011. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. Erich Schmidt, Berlin – Losebl.-Ausg. 2. Aufl. 2003. www.ifa-handbuchdigital.de/330216

[11] Grenzwerteliste 2017 – Sicherheit und Gesundheitsschutz am Arbeitsplatz. IFA Report 3/2017. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2017. www.dguv.de/ifa/grenzwerteliste

[12] DIN EN 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (5/2016). Beuth, Berlin 2016

[13] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (3/2018). Beuth, Berlin 2018

[14] Grundsätze für die Prüfung und Zertifizierung von Elektromechanischen Zustimmungsschaltern und Zustimmungseinrichtungen (GS-ET-22). Ausg. 7/2016. Hrsg.: Fachausschuss Elektrotechnik, Prüf- und Zertifizierungsstelle im DGUV Test, Köln. www.bgetem.de, Webcode 12204269

[15] Prüfgrundsatz für Notfallbremsen mit Haltefunktion für lineare Bewegungen (GS-MF-28). Ausg. 04/2015. Hrsg.: Prüf- und Zertifizierungsstelle Maschinen und Fertigungsautomation im DGUV Test, Mainz 2015. www.dguv.de/dguv-test/prod-pruef-zert/pruefgrundsaetze-erfahrung/pruefgrundsaetze/maschinen/index.jsp

[16] *Bömer, T.; Schaefer, M.*: Unterschiede bei der Verwendung von fertigen Sicherheitsbauteilen und Standardbauteilen für die Realisierung von Sicherheitsfunktionen an Maschinen. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2011. http://publikationen.dguv.de/dguv/pdf/10002/standardkomponenten.pdf

[17] Leitfaden für die Anwendung der Maschinenrichtline 2006/42/EG. 2. Aufl. 2010. Hrsg.: Bundesministerium für Arbeit und Soziales (BMAS), Berlin. www.bmas.de/SharedDocs/Downloads/DE/Thema-Arbeitsschutz/leitlinie-mrl-2006-42-eg.html

[18] DIN ISO/TR 23849: Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen (12/2014). Beuth, Berlin 2014

[19] Brauchen sichere Antriebssteuerungen auch sichere Positionsgeber? Aktualisierung 2017. www.dguv.de/medien/ifa/de/pub/rep/pdf/reports2013/ifar0713/positionsgeber_ifa.pdf

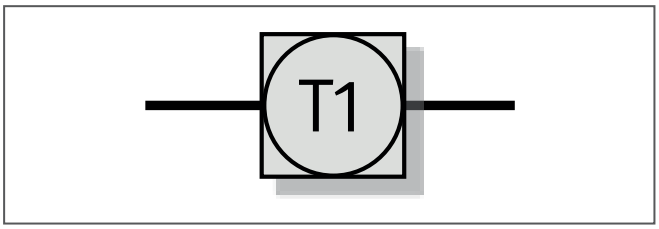
[20] Prüfgrundsatz GS-IFA-M21. Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015. www.dguv.de, Webcode d11973 (hier steht auch das Tool „Statische Analyse“ zur Verfügung)

Anhang A:
Schaltungsbeispiele mit Frequenzumrichtern

Um den praktischen Einsatz von Frequenzumrichtern zu verdeutlichen, wurden die folgenden Schaltungsbeispiele zusammengestellt. Die Beispiele entstammen der langjährigen Erfahrung bei der Beratung und Prüfung hinsichtlich sicherheitsbezogener Maschinensteuerungen, ohne auf herstellerspezifische Realisierungsvorschläge einzugehen. Teilweise sind aus Vereinfachungsgründen die Steuerungseinrichtungen zur Realisierung der Steuerungsvorgaben (Betriebsartenwahlschalter, Tippschalter ...) nicht vollständig dargestellt.

Die in den Berechnungen verwendeten $MTTF_D$-Werte sind als Herstellerwerte (Kennzeichnung „[H]“ für Hersteller), typische Werte aus Datenbanken (Kennzeichnung „[D]“ für Datenbank) oder als Werte aus der Norm DIN EN ISO 13849-1 (Kennzeichnung „[N]“ für Norm) und für angenommene Werte mit [G] markiert.

Wie auch bei den im IFA Report 2/2017 benutzten Symbolen in der Darstellung der sicherheitsbezogenen Blockdiagramme wird in den folgenden Schaltungsbeispielen auch das gekapselte Subsystem verwendet:



Als gekapselte Subsysteme werden Sicherheitsbauteile bezeichnet, für die der Hersteller PL (oder SIL) und PFH angibt. Diese Angaben sind für die Berücksichtigung in Sicherheitsfunktionen ausreichend. Der Einfluss von Kategorie, grundlegenden sowie bewährten Prinzipien, $MTTF_D$, DC, CCF und den Maßnahmen zu systematischen Ausfällen, einschließlich Software, ist bereits berücksichtigt worden. Bei der Quantifizierung mit SISTEMA ist nur die Eingabe von PL und PFH erforderlich (siehe auch SISTEMA-Kochbuch 1, Abschnitt 4.5).

Mithilfe der Tabelle A.1 kann gezielt ein Schaltungsbeispiel ausgesucht werden, in dem eine bestimmte Sicherheitsfunktion in einem bestimmten PL realisiert wurde.

Tabelle A.1:
Übersicht über die Schaltungsbeispiele

Stichwort	Schaltungsbeispiel mit		
	PL c	PL d	PL e
Schutztürüberwachung, STO	1, 2, 8	3, 6, 7, 8, 9, 10, 15	12
Überwachung Parkposition	1, 2		
SLS		4, 8, 9	
Freigabesteuerung	8, 9	4	
Not-Halt		5, 11	
SS1		5, 9, 10	
Zuhaltung		7, 11	
Betriebsartenwahl		8, 9	
Manuelle Rückstellung		10	
Sichere Bewegungssteuerung		11	
Kraftbetriebene Tür		13	
Vertikalachse hochhalten	14 (Spannungsausfall)	14	
Gleichstromantrieb, STO		15	
Sicherer Walzenstopp		16	

Beispiel 1: Stillsetzen bei Verlassen der sicheren Parkposition einer Achse bei geöffneter Schutztür – PL c

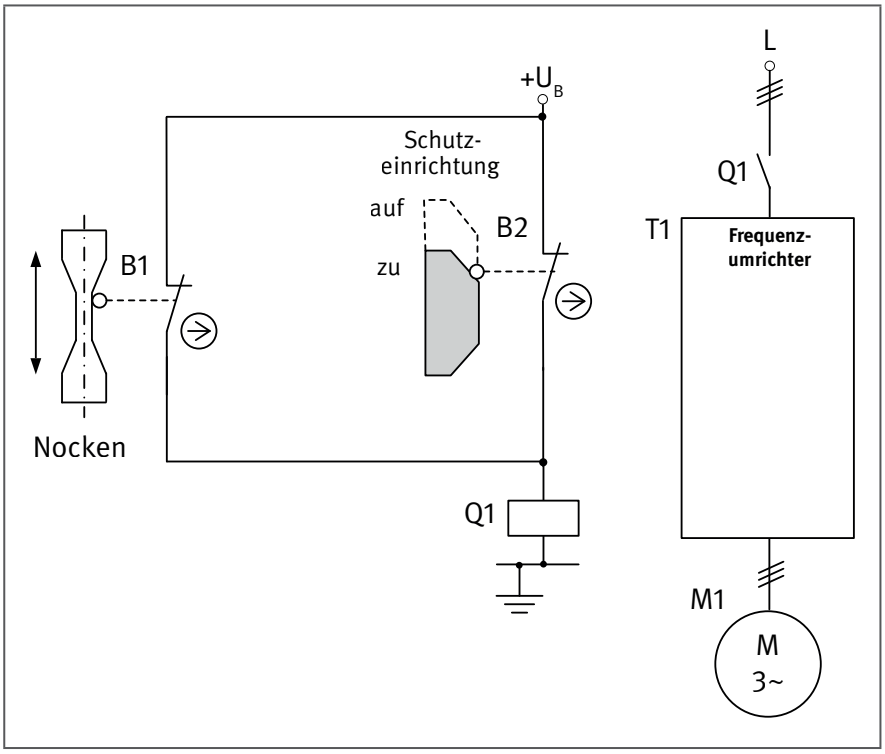


Abbildung A.1:
Kombinierte Stellungsüberwachung einer Achse mithilfe eines Nockenschalters

Sicherheitsfunktion

- SF 1: Verlässt die Achse bei geöffneter Schutztür die sichere Parkposition oder wird die Schutztür bei unsicherer Achsposition geöffnet, so wird der Motor momentenlos geschaltet (STO).

Funktionsbeschreibung

- Vor dem manuellen Eingriff wird die Antriebsachse auf eine sichere Parkposition gefahren, in der der Positionsschalter B1 nicht betätigt wird. Der geschlossene Öffnerkontakt von B1 überbrückt den Positionsschalter B2, der die Stellung der Schutztür überwacht.
- Bei fehlerhaftem Anlaufen des Antriebs wird B1 betätigt und damit die Überbrückung von B2 aufgehoben. Bei geöffneter Schutztür erfolgt ein ungesteuertes Stillsetzen durch Abfall des Netzschützes Q1 (Stopp-Kategorie 0 nach DIN EN 60204-1).
- Wird die Schutztür geöffnet, während die Achse sich außerhalb der sicheren Parkposition befindet, erfolgt ebenfalls ein ungesteuertes Stillsetzen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen. Im vorliegenden Beispiel werden als grundlegendes Sicherheitsprinzip u. a. das Ruhestromprinzip und die Erdung des Steuerstromkreises verwendet. Als bewährtes Sicherheitsprinzip wird u. a. die Überdimensionierung der Kontaktbelastung von B1, B2 und Q1 angewendet. Der Frequenzumrichter ist mit einer Vorladeschaltung für den Zwischenkreis ausgestattet.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen.

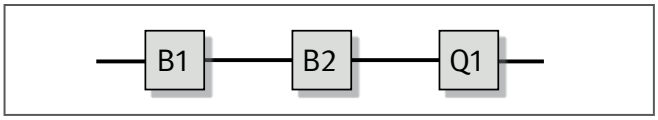


Abbildung A.2:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 1

- Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und befestigt sein. Die Positionsschalter sind bewährte Bauteile nach DIN EN ISO 13849-2, Tabelle D.3 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K. Die Positionsschalter und deren Betätigungselemente sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden.
- Das Schütz Q1 ist ein bewährtes Bauteil und erfüllt die Anforderungen der DIN EN 60947-4-1.
- Bei dem Frequenzumrichter T1 handelt es sich um ein handelsübliches Produkt ohne integrierte Sicherheits-Teilfunktionen. Bei unterbrochener Energiezufuhr zum Frequenzumrichter kann der Motor kein Drehmoment erzeugen.

Bemerkungen:

- Bei hintertretbaren Bereichen ist zusätzlich eine Quittierungsmöglichkeit vorzusehen, die nach Verlassen des Gefahrenbereichs und Schließen der Schutztür betätigt wird. Vom Ort der Quittierung aus muss der Gefahrenbereich einsehbar sein.
- Alternativ zu B1 kann auch ein Stillstandswächter eingesetzt werden, der mindestens den PL c erfüllt.
- Bei Verzicht auf B1 wird beim Öffnen der Schutztür der Frequenzumrichter T1 direkt vom Netz geschaltet (sicher abgeschaltetes Moment, STO).
- Das Zeitverhalten der Stillsetzung beim STO (Austrudeln) darf nicht zu Gefährdungen führen.

Berechnung der Ausfallwahrscheinlichkeit

- Für B1 und B2 mit zwangsöffnendem elektrischem Kontakt und separatem Betätiger wird jeweils ein B_{10d}-Wert von 2 000 000 Schaltspielen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 10 Minuten ergibt sich n_{op} = 35 040 Zyklen/Jahr und $MTTF_D$ = 571 Jahre.
- Das Schütz Q1 weist bei induktiver Last (AC3) einen B_{10}-Wert von 1 300 000 Schaltspiele [H] auf. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich ein B_{10d}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} ergibt sich für Q1 eine $MTTF_D$ von 742 Jahren.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Für SF 1 ergibt sich folgende Bewertung: Die Steuerung entspricht Kategorie 1 mit hoher $MTTF_D$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Beispiel 2: Stillsetzen bei Verlassen der sicheren Parkposition bei geöffneter Schutztür – PL c

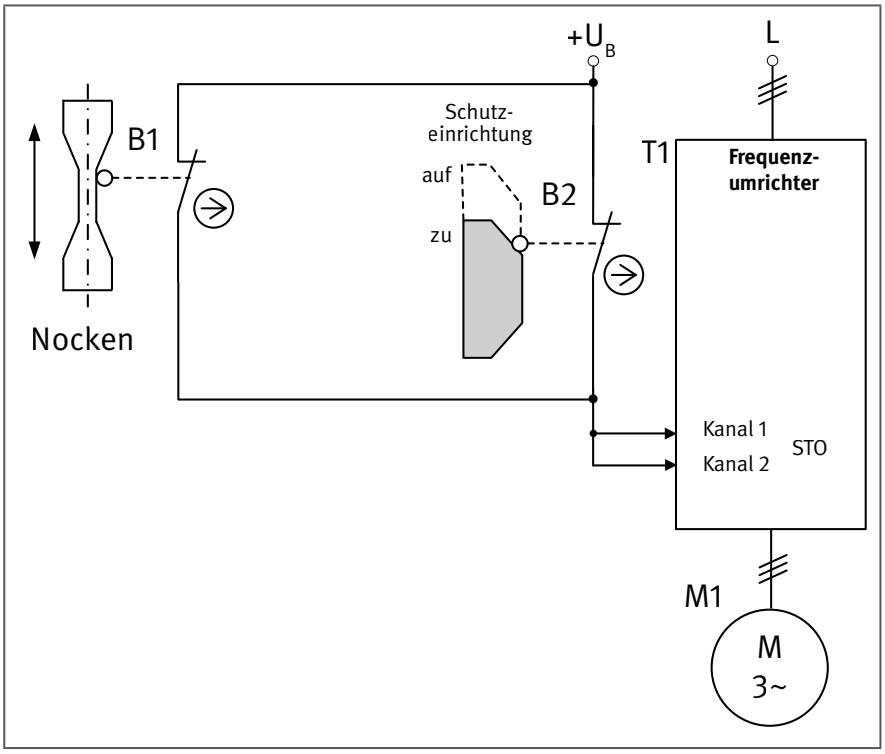


Abbildung A.3:
Kombinierte Stellungsüberwachung einer Schutztür und Positionsüberwachung einer Achse mithilfe eines Nockenschalters

Sicherheitsfunktion

- SF 1: Verlässt die Achse bei geöffneter Schutztür die sichere Parkposition oder wird die Schutztür bei unsicherer Achsposition geöffnet, so wird der Motor momentenlos geschaltet (STO).

Funktionsbeschreibung

- Vor dem manuellen Eingriff wird die Antriebsachse auf eine sichere Parkposition gefahren, in der der Positionsschalter B1 nicht betätigt wird. Der geschlossene Öffnerkontakt von B1 überbrückt den Positionsschalter B2, der die Stellung der Schutztür überwacht.
- Bei fehlerhaftem Anlaufen des Antriebs wird B1 betätigt und damit die Überbrückung von B2 aufgehoben. Bei geöffneter Schutztür erfolgt ein ungesteuertes Stillsetzen durch Aktivierung von STO im Frequenzumrichter T1 (Stopp-Kategorie 0 nach DIN EN 60204-1).
- Wird die Schutztür geöffnet, während die Achse sich außerhalb der sicheren Parkposition befindet, erfolgt ebenfalls ein ungesteuertes Stillsetzen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen. Im vorliegenden Beispiel werden als grundlegendes Sicherheitsprinzip u. a. das Ruhestromprinzip und die Erdung des Steuerstromkreises verwendet. Als bewährtes Sicherheitsprinzip wird u. a. die Überdimensionierung der Kontaktbelastung von B1 und B2 angewendet.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen.

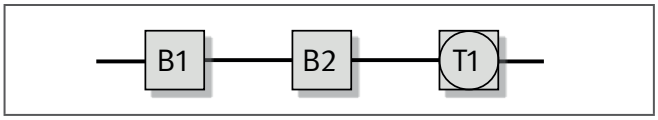


Abbildung A.4:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 2

- Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und befestigt sein. Die Positionsschalter sind bewährte Bauteile nach DIN EN ISO 13849-2, Tabelle D.3 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K. Die Positionsschalter und deren Betätigungselemente sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden.
- Der Frequenzumrichter T1 verfügt über die integrierte Sicherheits-Teilfunktion STO.

Bemerkungen:

- Bei hintertretbaren Bereichen ist zusätzlich eine Quittierungsmöglichkeit vorzusehen, die nach Verlassen des Gefahrenbereichs und Schließen der Schutztür betätigt wird. Vom Ort der Quittierung aus muss der Gefahrenbereich einsehbar sein.
- Alternativ zu B1 kann auch ein Stillstandswächter eingesetzt werden, der mindestens den PL c erfüllt.
- Bei Verzicht auf B1 wird beim Öffnen der Schutztür der Frequenzumrichter T1 direkt vom Netz geschaltet (sicher abgeschaltetes Moment, STO).
- Das Zeitverhalten der Stillsetzung beim STO (Austrudeln) darf nicht zu Gefährdungen führen.

Berechnung der Ausfallwahrscheinlichkeit

- Für B1 und B2 mit zwangsöffnendem elektrischem Kontakt und separatem Betätiger wird jeweils ein B_{10D}-Wert von 2 000 000 Schaltspielen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 10 Minuten ergibt sich ein n_{op} = 35 040 Zyklen/Jahr und eine $MTTF_D$ = 571 Jahre.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Für den Frequenzumrichter T1 gibt der Hersteller Kategorie 3, PL d, SIL2 und PFH = $3{,}2 \cdot 10^{-7}$/Stunde an.
- Für SF 1 ergibt sich folgende Bewertung: Die Kombination der Subsysteme ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}1 \cdot 10^{-6}$/Stunde + $3{,}2 \cdot 10^{-7}$/Stunde = $1{,}5 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Beispiel 3: Das Öffnen einer beweglich trennenden Schutzeinrichtung führt zum STO des Antriebs – PL d

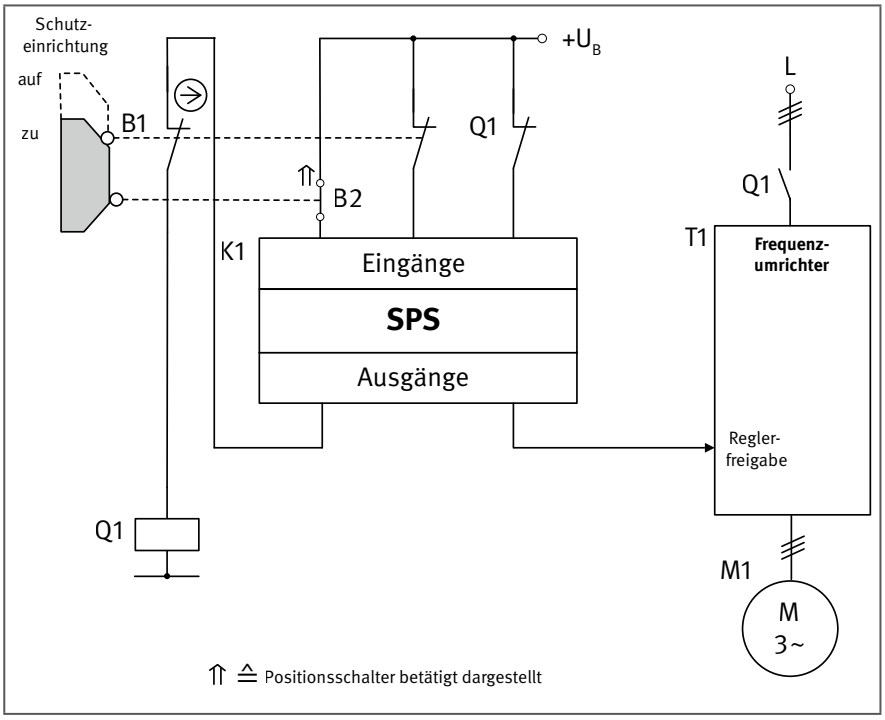


Abbildung A.5:
Prinzipschaltbild der Stellungs-
überwachung

Sicherheitsfunktion

- SF 1: Das Öffnen der Schutzeinrichtung führt zum STO des Antriebs.

Funktionsbeschreibung

- Beim Öffnen der Schutzeinrichtung unterbricht B1 die Ansteuerung des Netzschützes Q1, so dass dieses abfällt.
- Die SPS K1 überwacht die Schaltstellung von B2 und schaltet beim Öffnen des Kontakts die Reglerfreigabe des Frequenzumrichters T1 ab.
- Darüber hinaus führt die SPS K1 einen Vergleich der Signale von B1 und B2 sowie eine Überwachung des Meldekontakts von Q1 durch. Im Fehlerfall wird der weitere Betrieb durch Rücknahme der Reglerfreigabe des Frequenzumrichters T1 verhindert.
- Die Reglerfreigabe in diesem Beispiel verfügt über kein Rückmeldesignal, das zur Fehlererkennung genutzt werden kann. Eine Fehlererkennung ist über den technischen Prozess möglich, sofern Motorbewegungen ausschließlich über die Reglerfreigabe freigegeben werden und ein Fehler über eine Störung des Maschinenablaufs aufgedeckt wird. Alternativ kann eine Fehleraufdeckung über einen zusätzlichen Testzyklus erfolgen (siehe hierzu Abschnitt 4.2.3 „Fehlererkennung“).
- Fehler in der SPS werden ebenfalls über den technischen Prozess aufgedeckt.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Steuerstromkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.

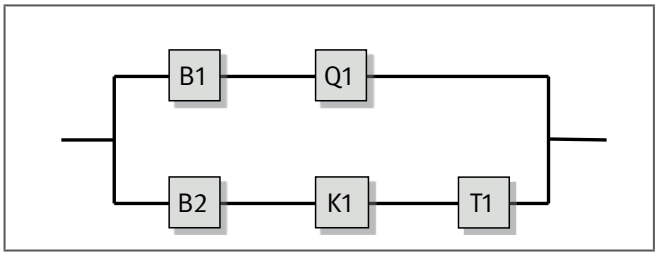


Abbildung A.6:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 3

- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.

- Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden. Der Positionsschalter B1 ist ein bewährtes Bauteil nach DIN EN ISO 13849-2, Tabelle D.3 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K.

- Das Netzschütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F. Die Rücklesung dieses Hilfskontakts von Q1 ermöglicht eine Aussage über die Schaltstellung der Hauptkontakte des Schützes.

- Bei dem Frequenzumrichter T1 handelt es sich um ein Standardgerät ohne integrierte Sicherheits-Teilfunktionen mit Vorladung des Zwischenkreises.

- Die Standardkomponenten K1 (SPS) und T1 (Frequenzumrichter) werden entsprechend den Hinweisen in Abschnitt 4.6.2 (Anforderungen an SRESW) der DIN EN ISO 13849-1 eingesetzt.

- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL c (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 9.3.4 des IFA Reports 2/2016.

Berechnung der Ausfallwahrscheinlichkeit

- Für B1 mit zwangsöffnendem elektrischem Kontakt und separatem Betätiger wird ein B_{10D}-Wert von 2 000 000 Schaltspielen [H] angegeben. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 30 Minuten ergibt sich ein n_{op} = 7 680 Zyklen/Jahr und eine $MTTF_D$ = 2 604 Jahren.

- Für den Positionsschalter B2 wird ein B_{10d} von 1 000 000 Schaltspielen [H] angegeben. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 30 Minuten ergibt sich n_{op} = 7 680 Zyklen/Jahr und eine $MTTF_D$ von 1 302 Jahren.

- Für das Netzschütz Q1 wird ein B_{10d}-Wert von 400 000 Schaltspielen [H] angegeben. Mit n_{op} = 7 680 Zyklen/Jahr ergibt sich eine $MTTF_D$ von 521 Jahren.

- Sowohl für die SPS K1 als auch für den Frequenzumrichter T1 wird eine $MTTF_D$ von 30 Jahren [H] angegeben.

- DC-Wert = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung beider Schaltzustände in der SPS K1.

- Für das Netzschütz Q1 kann ein DC-Wert von 99 % angegeben werden, da stets eine direkte Überwachung des Spiegelkontakts in der SPS K1 erfolgt.

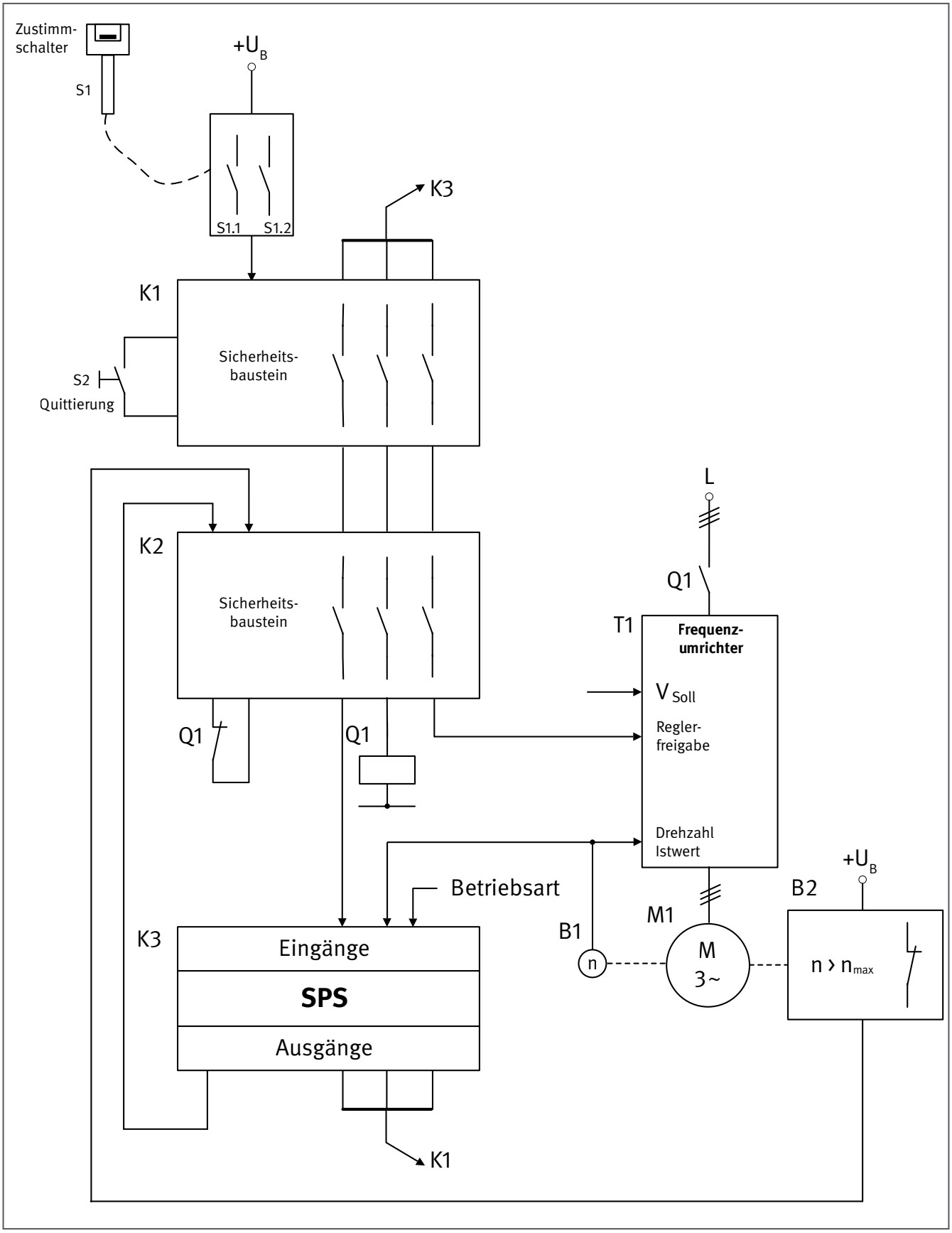
- Der DC-Wert für die SPS K1 und die Reglerfreigabe im Frequenzumrichter T1 wird mit jeweils 60 % (Fehlererkennung über den technischen Prozess) angesetzt.

- Es werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (80 Punkte): Trennung (15), Unterschiedliche Technologien (20), Verwendung bewährter Bauteile (5), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25).

- Für SF 1 ergibt sich folgende Bewertung: Die Kombination der Subsysteme ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}8 \cdot 10^{-7}$ 1/Stunde. Dies entspricht PL d.

Beispiel 4: Einrichtbetrieb mit begrenzter Geschwindigkeit und Zustimmungsschalter – PL d

Abbildung A.7:
Einrichtbetrieb mit begrenzter Geschwindigkeit und Zustimmungsschalter – Kaskadierung von Sicherheitsbausteinen



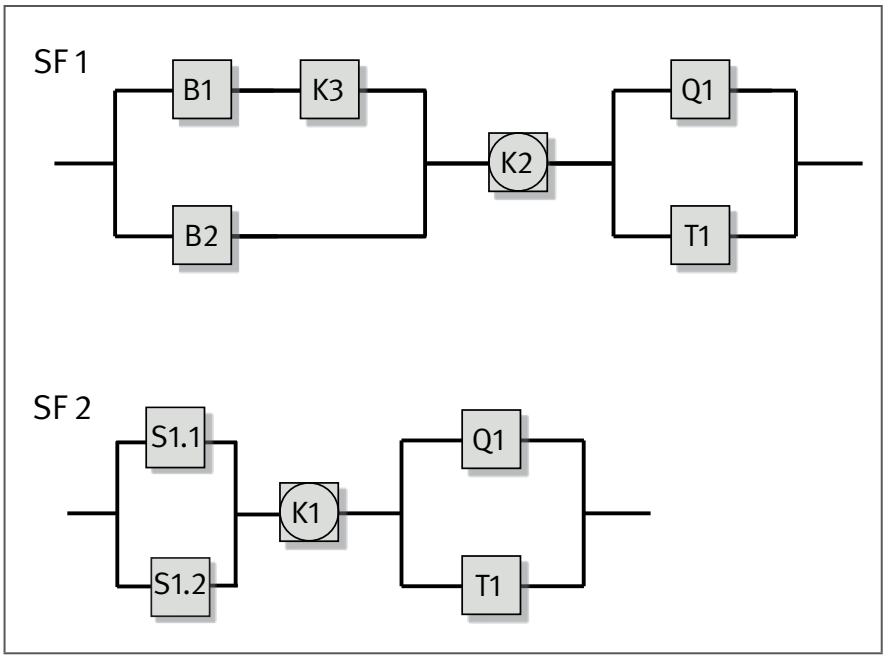


Abbildung A.8:
Sicherheitsbezogene Blockdiagramme zu Beispiel 4

Sicherheitsfunktionen

- SF 1: Sicher begrenzte Geschwindigkeit (SLS) im Einrichtbetrieb; Überdrehzahl führt zum STO des Antriebs.
- SF 2: Beim Loslassen des Zustimmungsschalters wird STO ausgelöst.

Funktionsbeschreibung

- Mit diesem Teil der Steuerung wird in der Betriebsart „Einrichten“ die Sicherheits-Teilfunktion „Sicher begrenzte Geschwindigkeit“ (SLS) realisiert. Überdrehzahl führt zum ungesteuerten Stillsetzen mittels STO.
- Bewegungen des Antriebs werden in dieser Betriebsart durch Betätigen des Zustimmungsschalters S1 ermöglicht. Sie werden verhindert, wenn S1 nicht betätigt wird. Die Signale des Zustimmungsschalters S1 wirken auf den Sicherheitsbaustein K1.
- Auf die Darstellung der Betriebsartenwahl wurde aus Gründen der Übersichtlichkeit verzichtet.
- Die Drehzahlüberwachung erfolgt zweikanalig. Bei einem Kanal erfolgt die Signalverarbeitung über den Drehgeber B1 und die SPS K3. Der zweite Kanal wird mittels Drehzahlwächter B2 realisiert. Die Ausgänge der beiden Kanäle wirken auf den Sicherheitsbaustein K2.
- Die Sicherheitsbausteine K1 und K2 sind kaskadiert. Das Öffnen der Freigabepfade eines der beiden Sicherheitsbausteine führt zur Abschaltung des Antriebs mittels STO.
- Der STO erfolgt zweikanalig durch Sperrung der Reglerfreigabe des Frequenzumrichters T1 und durch Unterbrechung der Netzversorgung mittels Netzschütz Q1.
- Durch Kaskadierung der Sicherheitsbausteine können weitere Schutzeinrichtungen und Befehlsgeräte eingebunden werden, um die Sicherheits-Teilfunktion STO auszulösen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung, Vorladung des Frequenzumrichter-Zwischenkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.

- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.

- Das Netzschütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F. Die Rücklesung dieses Hilfskontakts ermöglicht eine Aussage über die Schaltstellung der Hauptkontakte des Schützes Q1.

- Frequenzumrichter T1 und SPS K3 sind Standardgeräte ohne integrierte Sicherheits-Teilfunktionen. Sie werden entsprechend den Hinweisen in Abschnitt 4.6.2 (Anforderungen an SRESW) der DIN EN ISO 13849-1 eingesetzt.

- Die Drehzahlerfassung ist diversitär ausgeführt. Bei B1 handelt es sich um einen sin/cos-Geber, der an die SPS K3 angeschlossen ist. B2 ist ein Drehzahlwächter mit integriertem Schaltkontakt. Die Anbringung von Drehgeber und Drehzahlwächter muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler z. B. Geberwellenbruch ausgeschlossen ist.

- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL c (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 9.3.4 des IFA Reports 2/2016.

- Die Stillsetzzeit (Nachlaufzeit) bei STO nach einer Geschwindigkeitsüberschreitung mit maximal möglicher Beschleunigung darf nicht zu Gefährdungen führen.

- Der Zustimmungsschalter S1 ist zweistufig ausgeführt. Er verfügt über jeweils zwei Schließerkontakte. Bei dem Zustimmungsschalter handelt sich um eine Ausführung mit zwei Signalkanälen. Der Zustimmungsschalter S1 erfüllt die Anforderungen in DIN EN 60204-1, Abschnitt 10.9.

Bemerkung:

Der Zustimmungsschalter S1 und die sicher begrenzte Geschwindigkeit (Drehzahl) in Verbindung mit dem Betriebsartenwahlschalter etc. sind Steuerungsvorgaben gemäß Maschinenrichtlinie 2006/42/EG, Anhang 1, Abschnitt 1.2.5.

Berechnung der Ausfallwahrscheinlichkeit

- Die Sicherheitsbausteine K1 und K2 erfüllen die Anforderungen für Kategorie 3, PL d und SIL2. Die PFH beträgt jeweils $2{,}3 \cdot 10^{-9}$/Stunde [H].

- Für den Drehgeber B1 wird die $MTTF_D$ zu 132 Jahren [H] angegeben.

- Für den Drehzahlwächter B2 gibt der Hersteller $MTTF_D$ = 60 Jahre [H] an.

- Das Schütz Q1 hat einen B_{10d}-Wert von 1 000 000 Schaltspielen [H]. Bei 250 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} = 4 000 Zyklen/Jahr und $MTTF_D$ = 2 500 Jahre.

- Für die Standard-SPS K3 wird eine $MTTF_D$ = 30 Jahre angenommen [G].

- Der Frequenzumrichter T1 verfügt über keine integrierten Sicherheits-Teilfunktionen. Da keine Herstellerangaben zur $MTTF_D$ vorliegen, werden in einer konservativen Abschätzung zehn Jahre für die Berechnung [N] (siehe hierzu DIN EN ISO 13849-1, Abschnitt 4.5.2) eingesetzt.

- Der zweistufige Zustimmungsschalter S1 entspricht GS-ET-22 und die Anzahl der Betätigungszyklen ist kleiner als 100 000. Nach IFA Report 2/2017, Tabelle D.7 beträgt B_{10D} für das Loslassen jeweils für einen Kanal 100 000 Zyklen. Für die Betätigungsanzahl von 200 Zyklen/Jahr ergibt sich $MTTF_D$ zu 5 000 Jahre.

- Der DC-Wert für den Zustimmungsschalter S1 wird für die Schließer-Kontakte S1.1/S1.2 mit 99 % angenommen, da der Sicherheitsbaustein K1 eine Plausibiltätsprüfung durchführt.

- Der DC-Wert für den Drehgeber B1 wird mit 60 % angenommen, da der Geber auch für die funktionale Steuerung der Maschine benötigt und daher über den technischen Prozess getestet wird.

- Für das Schütz Q1 kann ein DC-Wert von 99 % angegeben werden, da eine Rücklesung des Spiegelkontakts durch den Sicherheitsbaustein K1 erfolgt (direkte Überwachung).

- Der Drehzahlwächter B2 wird einmal jährlich auf ordnungsgemäße Funktion bei der Wiederholungsprüfung der Maschine geprüft. Hierfür wird ebenfalls ein DC-Wert von 60 % angenommen. Gemäß der CO-ORDINATION OF NOTIFIED BODIES, Maschinenrichtlinie 2006/42/EC + Amendment, Recommendation for use CNB/M/11.050_R_E [1] ist zur Fehleraufdeckung für Sicherheitsfunktionen der Kategorie 3, PL d ein Testintervall für automatische oder manuelle funktionale Tests von längstens zwölf Monaten festgelegt.

- Der DC-Wert für die SPS K3 wird aufgrund der Fehlererkennung durch den technischen Prozess auf 60 % angesetzt. Für den Frequenzumrichter T1 wird der DC-Wert mit 60 % abgeschätzt, da die funktionale Stillsetzung des Motors ausschließlich durch Wegnahme der Reglerfreigabe erfolgt und ein Fehler durch den technischen Prozess erkannt wird.

- Für das Subsystem B1/B2/K3 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (80 Punkte): Trennung (15), unterschiedliche Technologien (20), Schutz gegen Überspannung usw. (15), Ausfalleffektanalyse (5) und Schutz gegen Umgebungseinflüsse (25).

- Für das Subsystem Q1/T1 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (90 Punkte): Trennung (15), unterschiedliche Technologien (20), Schutz gegen Überspannung usw. (15), Ausfalleffektanalyse (5) und Schutz gegen Umgebungseinflüsse (25 + 10).

- Für die Sicherheitsfunktion SF 1 „Sicher begrenzte Geschwindigkeit (SLS) im Einrichtbetrieb; Überdrehzahl führt zum STO des Antriebs“ ergibt sich folgende Bewertung: Die Subsysteme Drehzahlerfassung und -auswertung (B1, B2, K3) und Abschaltpfade (Q1, T1) entsprechen Kategorie 3 und PL d. In Kombination mit dem gekapselten Subsystem Sicherheitsbaustein K2 ergibt sich für SF 1 eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 5{,}5 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 2 „Beim Loslassen des Zustimmungsschalters S1 wird STO ausgelöst“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme Zustimmungsschalter (S1), Sicherheitsbaustein (K1) und Abschaltpfade (Q1, T1) ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}1 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Literatur:

[1] CO-ORDINATION OF NOTIFIED BODIES, Maschinenrichtlinie 2006/42/EC + Amendment, Recommendation for use CNB/M/11.050_R_E. http://ec.europa.eu/docsroom/documents/25221

Beispiel 5: Stillsetzen im Notfall – PL d

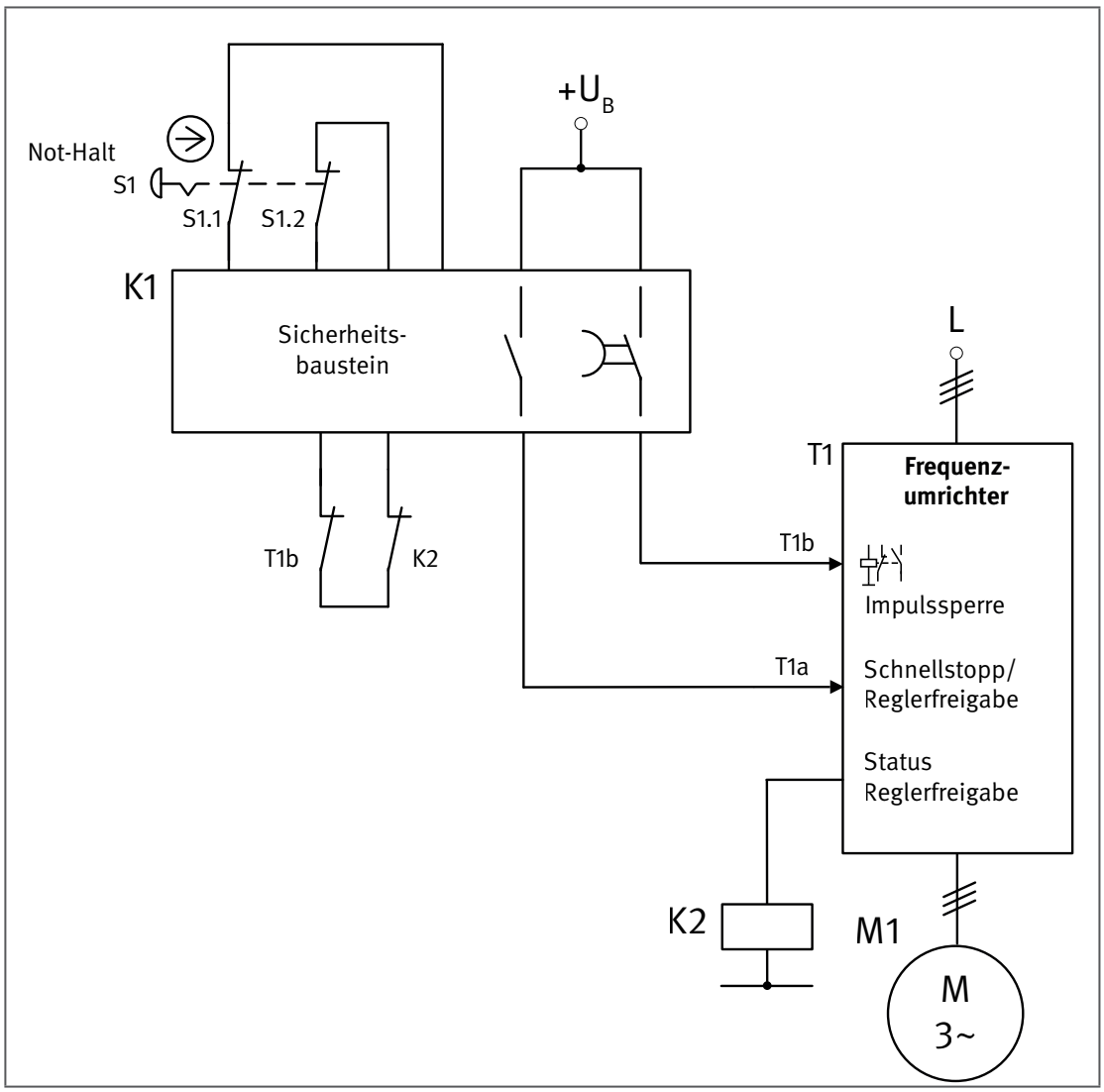


Abbildung A.9: Prinzipschaltbild der Antriebs-steuerung

Sicherheitsfunktion

- SF 1: Schnellstmögliches Stillsetzen bei Not-Halt (SS1-t)

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch Betätigen des Not-Halt-Geräts S1 schnellstmöglich stillgesetzt. Die Auswertung der redundanten Kontakte S1.1/S1.2 erfolgt im Sicherheitsbaustein K1.
- Über den unverzögerten Schaltkontakt des Sicherheitsbausteins K1 wird im Frequenzumrichter T1 die Schnellstopp-Funktion mit anschließender Rücknahme der Reglerfreigabe aktiviert, wodurch der Antrieb schnellstmöglich zum Stillstand gebracht wird. Nach einer für diese Applikation geeignet parametrierten Zeit wird über den verzögerten Schaltkontakt von K1 die Impulssperre des Frequenzumrichters T1 aktiviert und der Antrieb momentenfrei geschaltet. Die Verzögerungszeit in K1 wird so gewählt, dass der Frequenzumrichter T1 gerade ausreichend Zeit hat, den Antrieb gesteuert stillzusetzen.
- Die Kontakte des Not-Halt-Geräts S1 sind redundant ausgeführt und werden zusammen mit der Verdrahtung durch den Sicherheitsbaustein K1 überwacht. Die beiden Abschaltpfade im Frequenzumrichter T1 verfügen über Rückmeldesignale, die direkt bzw. über ein Koppelglied K2 in den Freigabekreis von K1 eingebunden sind. Fehler im Frequenzumrichter T1 machen sich somit vor dem nächsten Start des Antriebs bemerkbar.

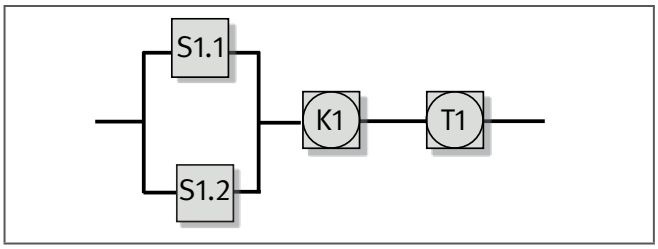


Abbildung A.10:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 5

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung, Vorladung des Frequenzumrichter-Zwischenkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.
- Das Not-Halt-Gerät S1 erfüllt die Anforderungen der DIN EN ISO 13850 und ist mit zwangsöffnenden Kontakten S1.1/S1.2 entsprechend DIN EN 60947-5-1, Anhang K ausgestattet.
- Der Sicherheitsbaustein K1 verfügt über unverzögerte und verzögerte Freigabepfade und erfüllt die Anforderungen für Kategorie 3 und PL d.
- T1 ist ein Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO. Die Sicherheits-Teilfunktion wird zweikanalig über die Eingänge Schnellstopp/Reglerfreigabe (T1a) und Impulssperre (T1b) realisiert. Durch die Kombination mit einem geeigneten Sicherheitsbaustein wird die Sicherheits-Teilfunktion SS1 realisiert. Die Schnellstopp-Funktion wird in diesem Beispiel bei Wegnahme der Reglerfreigabe aktiviert.
- Beide Abschaltpfade des Frequenzumrichters T1 werden vom Sicherheitsbaustein K1 überwacht. Das Relais der Impulssperre T1b verfügt zur Fehleraufdeckung über einen zwangsgeführten Öffner-Kontakt und der Status der Reglerfreigabe T1a wird über das Koppelglied K2 erfasst.
- Es ist zu beachten, dass die Schnellstoppfunktion des Frequenzumrichters T1 rein funktional erfolgt, also nicht sicherheitstechnisch ertüchtigt ist. Falls gleichzeitig zur Betätigung des Not-Halt-Geräts ein Fehler in T1 auftritt, könnte das schnellstmögliche Stillsetzen völlig ausbleiben oder die Verzögerung geringer sein. Im ungünstigsten Fall wäre sogar eine Beschleunigung des Motors denkbar, die erst nach Ablauf der Verzögerungszeit in K1 durch das Einlegen der Impulssperre beendet wird und dann zum Austrudeln des Motors führt. Die in diesem Beispiel beschriebene Lösung wird vielfach eingesetzt und kann als Stand der Technik beschrieben werden. Falls das beschriebene Fehlverhalten trotz der geringen Wahrscheinlichkeit des Auftretens nicht akzeptiert werden kann (Beispiel: SS1 bei Auftreten von Unwuchten in Zuckerzentrifugen), sind andere Realisierungen erforderlich, z. B. mit einer Überwachung der Bremsrampe und dem zusätzlichen Einsatz von mechanischen Bremsen.

Berechnung der Ausfallwahrscheinlichkeit

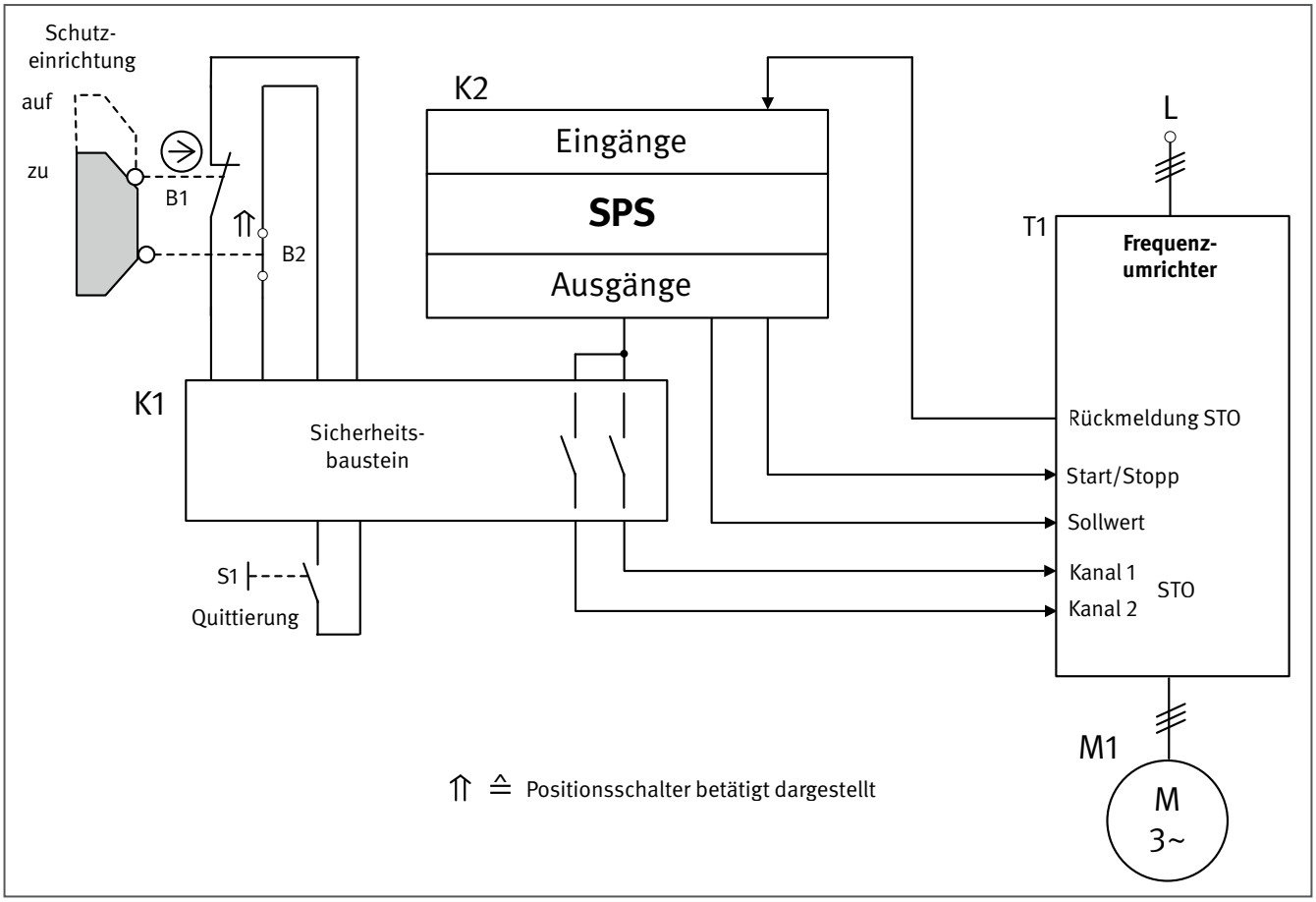
- Für das Not-Halt-Gerät S1 und die Kontakte S1.1 und S1.2 kann gemäß DIN EN ISO 13849-2, Tabelle D.8 und IFA Report 2/2017, Tabelle D.6 jeweils ein B_{10D} von 100 000 Schaltspielen [N] angenommen werden. Bei einem n_{op} von 120 Schaltspielen im Jahr ergibt sich für die Konfiguration ein PFH_D von $2{,}5 \cdot 10^{-8}$/Stunde. Aufgrund der Plausibilitätsprüfung des Sicherheitsbausteins K1 wird ein DC-Wert von 99 % zugeordnet.
- Der Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 3, PL d und SIL 2. Die PFH_D beträgt $3{,}2 \cdot 10^{-7}$/Stunde [H].

- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO. Er erfüllt die Anforderungen für Kategorie 3, PL d und SIL 2. Die PFH_D beträgt $3{,}2 \cdot 10^{-7}$/Stunde [H]. Diese Angaben für T1 sind nur dann gültig, wenn die Vorgaben des Herstellers zur Fehleraufdeckung durch externe Komponenten berücksichtigt und entsprechend der Betriebsanleitung umgesetzt werden.

- Für die Sicherheitsfunktion SF 1 „Schnellstmögliches Stillsetzen bei Not-Halt (SS1-t)“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme S1.1/S1.2, K1 und T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 6{,}6 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 6: Sicherheitsbezogene Stoppfunktion STO, eingeleitet durch eine beweglich trennende Schutzeinrichtung mit Positionsschaltern – PL d

Abbildung A.11:
STO eines Frequenzumrichters



Sicherheitsfunktion

- SF 1: Das Öffnen der beweglich trennenden Schutzeinrichtung führt zum STO des Frequenzumrichterantriebs.

Funktionsbeschreibung

- Der Frequenzumrichterantrieb wird funktional durch die SPS K2 gesteuert. Sie gibt dem Frequenzumrichter T1 den Sollwert vor, schaltet die beiden STO-Eingänge und kann den Antrieb starten und stoppen. Die SPS K2 ist jedoch nicht an der Sicherheitsfunktion beteiligt.

- Die Absicherung der Gefahrenstelle erfolgt durch eine beweglich trennende Schutzeinrichtung. Das Öffnen der Schutzeinrichtung wird durch die Positionsschalter B1 und B2 erfasst und in einem Sicherheitsbaustein K1 ausgewertet. Über die Freigabepfade von K1 werden im Frequenzumrichter T1 die STO-Eingänge unabhängig von der SPS K2 abgeschaltet. Im Antrieb wird dadurch die Generierung eines Drehfeldes sicher verhindert.

- Fehler in den Positionsschaltern B1 und B2 werden durch den Plausibilitätsvergleich im Sicherheitsbaustein K1 aufgedeckt. Der Frequenzumrichter T1 ist intern mit einer Überwachungsfunktion des STO ausgerüstet. Diese verhindert im Fehlerfall einen erneuten Start des Antriebs. Eine entsprechende Fehlermeldung wird an die SPS K2 gegeben.

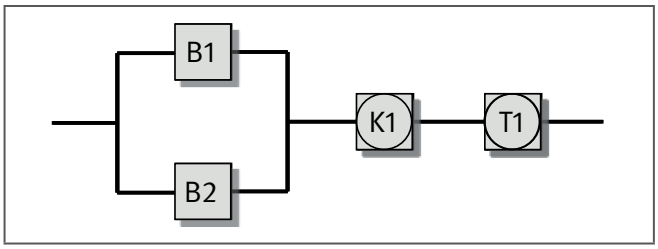


Abbildung A.12:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 6

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Steuerstromkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.
- Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden. Der Positionsschalter B1 ist ein bewährtes Bauteil nach DIN EN ISO 13849-2, Tabelle D.3 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K.
- Der Sicherheitsbaustein erfüllt die Anforderungen der Kategorie 4 und PL e.
- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO. Es werden die Anforderungen der Kategorie 3 und PL d erfüllt.

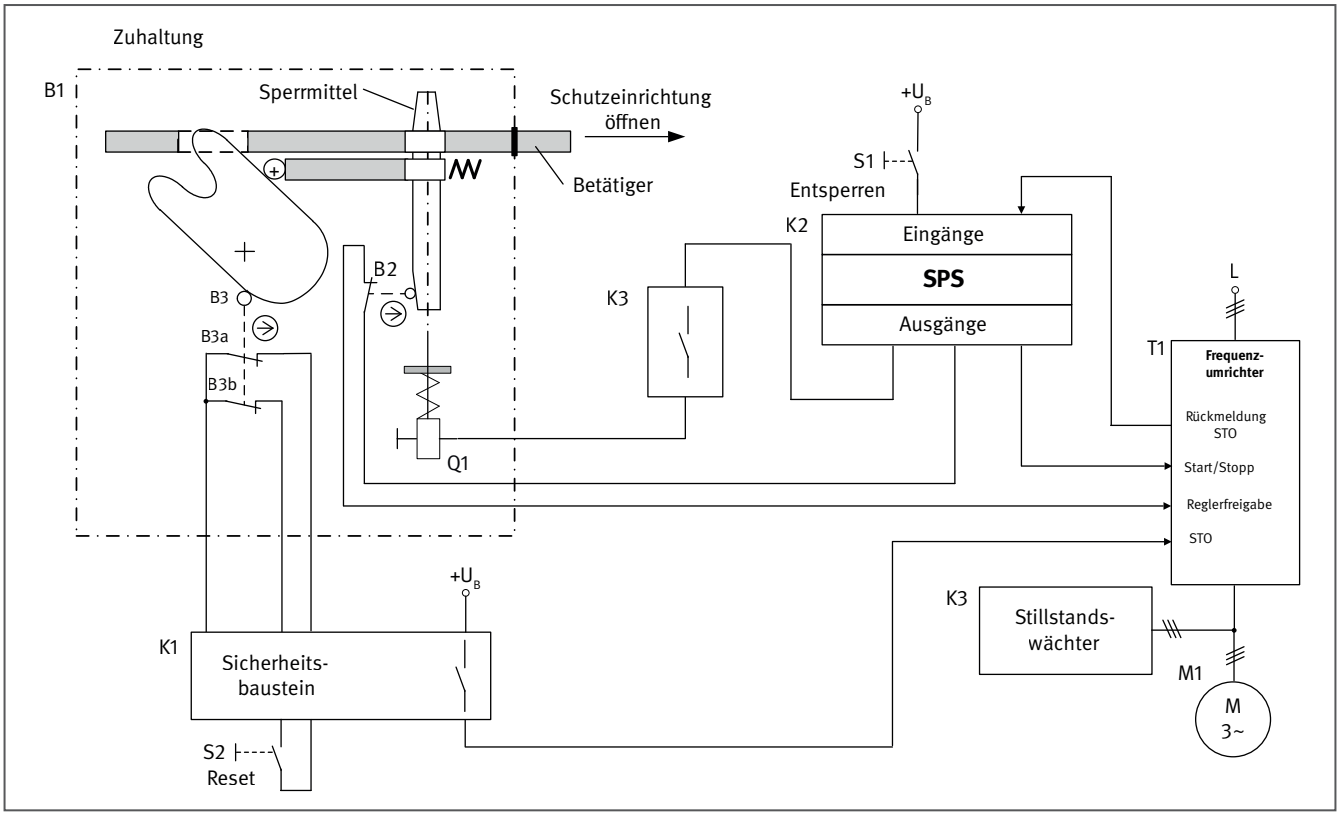
Berechnung der Ausfallwahrscheinlichkeit

- Für den Positionsschalter B1 mit zwangsöffnendem Kontakt wird ein B_{10d} von 20 000 000 Schaltspielen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} = 3 840 Zyklen/Jahr und eine $MTTF_D$ von 52 083 Jahren. Für den Positionsschalter B2 wird ein B_{10d} von 1 000 000 Schaltspielen [H] angegeben. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} = 3 840 Zyklen/Jahr und eine $MTTF_D$ von 2 604 Jahren.
- Der Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 4, PL e und SIL3. Die PFH_D beträgt $2{,}3 \cdot 10^{-9}$/Stunde [H].
- Der Frequenzumrichter T1 mit der integrierten Sicherheits-Teilfunktion STO erfüllt die Anforderungen der Kategorie 3, PL d und SIL 2. Die PFH_D beträgt $2{,}0 \cdot 10^{-7}$/Stunde [H].
- Der DC-Wert für die Positionsschalter B1 und B2 beträgt 99 % aufgrund der Plausibilitätsprüfung durch den Sicherheitsbaustein K1.
- Für das Subsystem Positionsschalter B1/B2 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (70 Punkte): Trennung (15), Verwendung bewährter Bauteile (5), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10).
- Das Subsystem B1/B2 entspricht Kategorie 3 mit hoher $MTTF_D$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}5 \cdot 10^{-8}$/Stunde.

- Für die Sicherheitsfunktion ergibt sich folgende Bewertung: Die Kombination der Subsysteme Positionsschalter B1/B2, Sicherheitsbaustein K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}3 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 7: Sicherung einer Gefahrenstelle durch eine beweglich trennende Schutzeinrichtung mit Zuhaltung – PL d

Abbildung A.13:
Sicherung einer Gefahrenstelle durch beweglich trennende Schutzeinrichtung mit Zuhaltung



Sicherheitsfunktionen

- SF 1: Entsperrung der Zuhaltung nur bei Stillstand des Antriebs
- SF 2: STO des Antriebs beim Öffnen der beweglich trennenden Schutzeinrichtung mit Zuhaltung

Funktionsbeschreibung

- Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung B1 so lange verhindert, bis die Bewegung zum Stillstand gekommen ist. Die Tür wird durch einen federkraftbetätigten Bolzen (Sperrmittel) eines Hubmagneten zugehalten, der ein Herausziehen des Betätigers aus dem Schalterkopf verhindert.
- Der Zugang zum Gefahrenbereich wird durch Betätigung des Tasters S1 angefordert. Die Standard-SPS K2 leitet daraufhin zunächst das Stillsetzen des Antriebs durch den Frequenzumrichter T1 ein. Nach Erreichen des Stillstands ermöglicht der Stillstandswächter K3 die Ansteuerung des Zuhaltemagneten durch die SPS K2 und somit das Entsperren der Zuhaltung.
- Die Stellung des Sperrmittels wird überwacht. Der Bolzen des Hubmagneten wirkt auf den Positionsschalter B2, der bei Betätigung die Reglerfreigabe des Frequenzumrichters T1 unterbricht.
- Das Öffnen der Schutzeinrichtung wird über die zwei Öffnerkontakte B3a/B3b des Positionsschalters B3 erfasst und in einem Sicherheitsbaustein K1 ausgewertet. Über den Freigabepfad von K1 wird im Frequenzumrichter T1 der STO-Eingang abgeschaltet, wodurch die Generierung eines Drehfeldes verhindert wird. Mit dieser Sicherheitsfunktion wird der Schutz vor unerwartetem Anlauf des Motors realisiert.

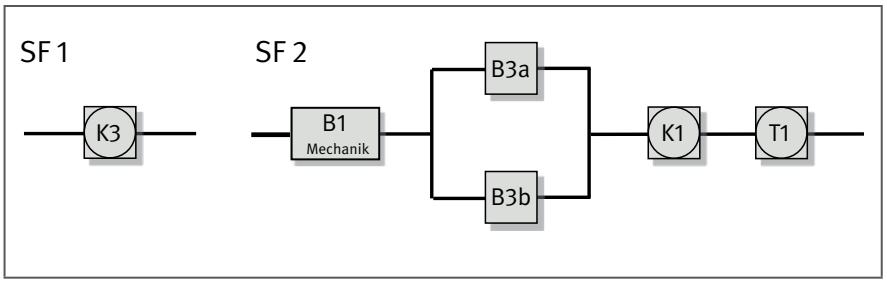


Abbildung A.14:
Sicherheitsbezogene Blockdiagramme zu Beispiel 7

- Die gefahrbringende Bewegung kann nur bei geschlossener und zugehaltener Schutzeinrichtung wieder in Gang gesetzt werden.
- Fehler im Positionsschalter B3 werden durch den Plausibilitätsvergleich im Sicherheitsbaustein K1 aufgedeckt.
- Die im Frequenzumrichter T1 integrierte Sicherheits-Teilfunktion STO ist einfehlersicher ausgeführt und bedarf keiner externen Überwachung. Die Rückmeldung des STO-Status an die SPS K2 dient alleine funktionalen Zwecken.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Steuerstromkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.
- Bei B1 handelt es sich um eine Zuhaltung mit Stellungsüberwachung der Schutzeinrichtung. Die Öffnerkontakte B3a, B3b und der Überwachungskontakt B2 für das Sperrmittel sind zwangsöffnende Kontakte, die die Anforderungen gemäß DIN EN 60947-5-1, Anhang K erfüllen. Das Sperrmittel wird durch Federkraft in der Sperrstellung gehalten (Ruhestromprinzip).
- Die Zuhaltung B1 erfüllt die Anforderungen der DIN EN ISO 14119 für Verriegelungseinrichtungen und des Prüfgrundsatzes GS-ET-19.
- Der Sicherheitsbaustein K1 erfüllt die Anforderungen der Kategorie 4 und PL e.
- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO. Die Anforderungen der Kategorie 3 und PL d werden erfüllt. Eine einkanalige Ansteuerung für STO ist bei diesem Produkt ausreichend.
- Der Stillstandswächter K3 erfüllt die Anforderungen der Kategorie 3 und PL d.
- K2 ist eine handelsübliche Standard-SPS, die an den Sicherheitsfunktionen nicht beteiligt ist.

Berechnung der Ausfallwahrscheinlichkeit

- Für die Mechanik der Zuhaltung einschließlich Bruch des Sperrmittels kann ein Fehlerausschluss angenommen werden, wenn die folgenden Bedingungen erfüllt sind:

  – Anwendung entsprechend der Betriebsanleitung, insbesondere Montageanleitung und technische Daten (z. B. Betätigungsradius, Betätigungsgeschwindigkeit)
  – Verhinderung des Selbstlockerns
  – die statischen Kräfte auf die Zuhaltung sind geringer als die im Datenblatt angegebene Zuhaltekraft
  – es treten keine dynamischen Kräfte auf, da die Bestromung des Entriegelungsmagneten erst bei geschlossener Schutztür erfolgt; siehe hierzu auch DGUV Information 203-079 „Auswahl und Anbringung von Verriegelungseinrichtungen“
  – keine Verwendung als mechanischer Endanschlag
  – unlösbare Befestigung des Betätigers
  – regelmäßige Wartung
  – Formschluss nach Montage
  – ausreichende mechanische Festigkeit aller Träger- und Funktionselemente
  – ein Absenken der Tür führt nicht dazu, dass der Betätiger außerhalb des vom Hersteller spezifizierten Bereichs eingesetzt wird
  – Schäden, die durch vorhersehbare äußere Einflüsse (z. B. Eindringen von Schmutz, Staub und mechanische Erschütterung) entstehen könnten, werden durch die Art der Montage ferngehalten oder sind aufgrund der Einsatzbedingungen nicht zu erwarten.

  Der Fehlerausschluss ist vom Hersteller zu bestätigen.

- Für die zwangsöffnenden elektrischen Kontakte B3a und B3b kann eine B_{10D} von 2 000 000 Schaltspielen [N] angenommen werden. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} zu 3 840 Zyklen/Jahr und eine $MTTF_D$ zu 5 208 Jahren.

- Der Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 4, PL e und SIL 3. Die PFH beträgt $3{,}0 \cdot 10^{-8}$/Stunde [H].

- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO. Er erfüllt die Anforderungen für Kategorie 3, PL d und SIL 2. Die PFH_D beträgt $2{,}0 \cdot 10^{-7}$/Stunde [H].

- Der Stillstandswächter K3 erfüllt die Anforderungen für Kategorie 3, PL d und SIL 2. Die PFH_D beträgt $2{,}3 \cdot 10^{-7}$/Stunde [H].

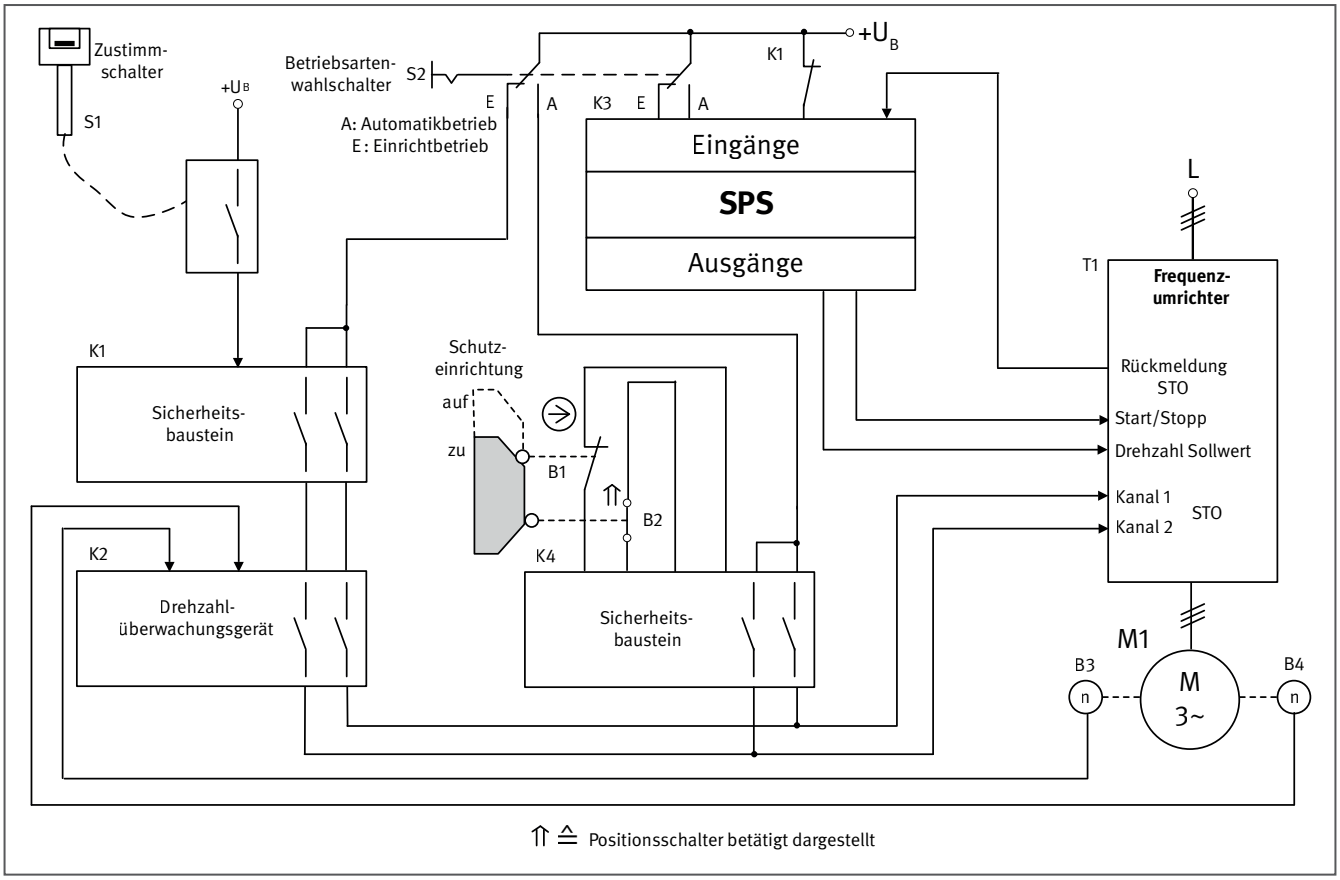
- Aufgrund der Plausibilitätsprüfung durch den Sicherheitsbaustein K1 kann ein DC-Wert von 99 % für die elektrischen Kontakte von B3 angenommen werden.

- Für die Sicherheitsfunktion SF 1 „Entsperren der Zuhaltung nur bei Stillstand des Antriebs“ ergibt sich folgende Bewertung: Für das Subsystem Drehzahlerfassung (K3) ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}3 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 2 „STO des Antriebs nach Öffnung der beweglich trennenden Schutzeinrichtung mit Zuhaltung“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme B1 Mechanik, Positionsschalter B3a/B3b, Sicherheitsbaustein K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}5 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 8: Antriebssteuerung für Automatik- und Einrichtbetrieb mit begrenzter Geschwindigkeit PL d und Zustimmungsschalter PL c

Abbildung A.15:
Sicherung einer Gefahrenstelle durch beweglich trennende Schutzeinrichtung mit Zuhaltung



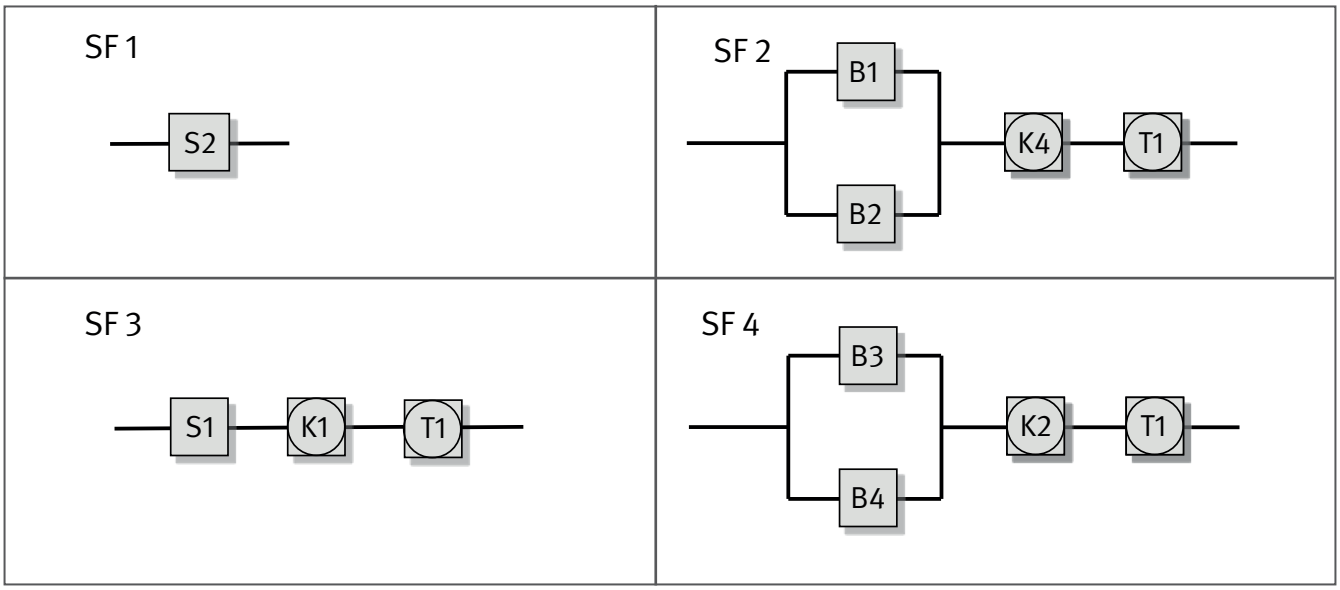
Sicherheitsfunktionen

- SF 1: Betriebsartenwahl
- SF 2: Automatikbetrieb; Öffnen der beweglich trennenden Schutzeinrichtung setzt den Antrieb still (STO)
- SF 3: Einrichtbetrieb; Loslassen des Zustimmungsschalters am Handbediengerät setzt den Antrieb still (STO)
- SF 4: Einrichtbetrieb; Überschreiten der maximal zulässigen Drehzahl führt zum Stillsetzen des Antriebs (SLS)

Funktionsbeschreibung

- Der Betriebsartenwahlschalter S2 lässt die Wahl zwischen Automatikbetrieb und Einrichtbetrieb zu. Im Automatikbetrieb sind die Kontakte der Positionsschalter B1/B2 an der Schutzeinrichtung geschlossen und der Antrieb lässt sich mit beliebiger Geschwindigkeit betreiben. Das Öffnen der Schutzeinrichtung wird über B1/B2 und den Sicherheitsbaustein K4 erfasst und führt zur Aktivierung der Sicherheits-Teilfunktion STO im Frequenzumrichter T1.
- Im Einrichtbetrieb ist die Automatiksteuerung gesperrt. Ein Betrieb ist bei offener Schutzeinrichtung nur mit begrenzter Geschwindigkeit und durch die Betätigung des Zustimmungsschalters S1 möglich. Die Einleitung der Bewegung erfolgt durch eine separate Befehlseinrichtung auf einem Handbediengerät (nicht dargestellt).
- Beim Loslassen des Zustimmungsschalters S1 wird über den Sicherheitsbaustein K1 die gefahrbringende Bewegung durch Abschalten der STO-Eingänge des Frequenzumrichters T1 stillgesetzt.

Abbildung A.16:
Sicherheitsbezogene Blockdiagramme zu Beispiel 8



- Die Drehzahlüberwachung im Einrichtbetrieb erfolgt durch ein Überwachungsgerät K2 (Kategorie 3, PL d). Zur Erfassung der Drehzahl werden zwei Geber oder alternativ ein Geber und das Drehzahlsignal aus dem Frequenzumrichter verwendet. Bei Überschreitung der im Überwachungsgerät eingestellten maximalen Geschwindigkeit fallen die Ausgangsrelais ab und die STO-Funktion des Frequenzumrichters wird aktiviert.
- Fehler in den Positionsschaltern B1 und B2 werden durch den Plausibilitätsvergleich im Sicherheitsbaustein K4 aufgedeckt. Der Frequenzumrichter T1 ist intern mit einer Überwachungsfunktion des STO ausgerüstet. Diese verhindert im Fehlerfall einen erneuten Start des Antriebs. Eine entsprechende Fehlermeldung wird an die SPS K3 gegeben.
- Die Drehzahlerfassung erfolgt zweikanalig. Fehler in den Gebersignalen werden durch den Plausibilitätsvergleich im Drehzahlüberwachungsgerät K2 aufgedeckt.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Stromkreises, Vorladung des Frequenzumrichter-Zwischenkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.
- Bei dem Betriebsartenwahlschalter S2 handelt es sich um einen nockenbetätigten Wahlschalter mit zwangläufigem Betätigungsmodus. Aufgrund der Konstruktion des Betriebsartenwahlschalters sind die Fehlerausschlüsse gemäß DIN EN ISO 13849-2, Tabelle D.8 möglich.
- Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden. Der Positionsschalter B1 ist ein bewährtes Bauteil nach DIN EN ISO 13849-2 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K.

- Bei dem zweistufigen Zustimmungsschalter S1 handelt es sich um ein einkanaliges Gerät mit Schließerkontakt. Der Zustimmungsschalter S1 entspricht den Anforderungen in DIN EN 60204-1, Abschnitt 10.9.
- Die Sicherheitsbausteine K1 und K4 erfüllen die Anforderungen der Kategorie 4 und PL e.
- Das Drehzahlüberwachungsgerät K2 erfüllt die Anforderungen der Kategorie 3 und PL d.
- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO. Es werden die Anforderungen der Kategorie 3 und PL d erfüllt.
- K3 ist eine handelsübliche speicherprogrammierbare Steuerung, die nicht an den Sicherheitsfunktionen beteiligt ist.

Bemerkungen:

- Die Stillsetzzeit (Nachlaufzeit) der Sicherheits-Teilfunktion STO, ausgelöst durch eine Geschwindigkeitsüberschreitung mit maximal möglicher Beschleunigung, darf nicht zu Gefährdungen führen. Dasselbe gilt für den Nachlauf nach Öffnen der Schutztür.
- Im Fehlerfall des Zustimmungsschalters S1 kann das federkraftbetätigte Öffnen des Schließerkontakts beim Loslassen versagen. Das Bedienhandgerät muss daher über ein Befehlsgerät zum Stillsetzen im Notfall verfügen.
- Die Anbringung der zwei Drehgeber B3, B4 muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z. B. Geberwellenbruch) ausgeschlossen ist.

Berechnung der Ausfallwahrscheinlichkeit

- Bei dem Betriebsartenwahlschalter S2 handelt es sich um einen nockenbetätigten Wahlschalter mit zwangläufigem Betätigungsmodus (direkt öffnend) gemäß DIN EN 60947-5-1, Anhang K. Es erfolgt ein Fehlerausschluss für die zwangsöffnenden Kontakte.
  Weiterhin erfolgt ein Fehlerausschluss für Kurzschlüsse von Kontakten, die voneinander isoliert sind.
  Darüber hinaus erfolgt ein Fehlerausschluss für unterschiedliche Stellungen der zwei Wechslerebenen.
  Aufgrund der vorhandenen Steuerungsstruktur und eines Einbaus im Schaltschrank mit der Mindestschutzart IP 54 können Fehler u. a. zwischen benachbarten Leiterbahnen und Kontaktstellen sowie Leitungen ausgeschlossen werden. Die Bedingungen für Fehlerausschlüsse gemäß DIN EN ISO 13849-2, Abschnitt D.5 werden eingehalten.
  Fehler in der Betriebsartenwahl können nicht zu einem gefährlichen Ausfall einer Sicherheitsfunktion führen. Jede Unterbrechung im Pfad der aktiven Betriebsart führt durch die konsequente Verwendung des Ruhestromprinzips zur Einleitung des sicheren Zustands (STO).
- Bei dem Positionsschalter B1 mit zwangsöffnenden Kontakten wird ein B_{10d}-Wert von 20 000 000 Schaltspielen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} = 3 840 Zyklen/Jahr und eine $MTTF_D$ von 52 083 Jahren.
- Für den Positionsschalter B2 mit Schließerkontakt wird ein B_{10d}-Wert von 1 000 000 Schaltspielen [H] angegeben. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} = 3 840 Zyklen/Jahr und eine $MTTF_D$ von 2 604 Jahren.
- Die Sicherheitsbausteine K1 und K4 erfüllen die Anforderungen für Kategorie 4, PL e und SIL 3. Die PFH_D beträgt $2{,}3 \cdot 10^{-9}$/Stunde [H].
- Der Frequenzumrichter T1 mit der integrierten Sicherheits-Teilfunktion STO erfüllt die Anforderungen der Kategorie 3, PL d und SIL 2. Die PFH_D beträgt $2{,}0 \cdot 10^{-7}$/Stunde [H].
- Der zweistufige Zustimmungsschalter S1 verfügt über einen Schließerkontakt. Der Hersteller gibt einen B_{10d}-Wert von 100 000 Schaltspielen [H] an. Mit n_{op} = 480 Zyklen/Jahr ergibt sich $MTTF_D$ zu 2 083 Jahren.

- Bei dem Drehzahlüberwachungsgerät K2 handelt es sich um einen Sicherheitsbaustein, der die Anforderungen von Kategorie 3, PL d und SIL 2 erfüllt. Die PFH_D beträgt $2 \cdot 10^{-7}$/Stunde [H].

- Die Drehgeber B3 und B4 sind rechts und links am Motor angeflanscht. Der Geberhersteller gibt eine $MTTF_D$ von jeweils 40 Jahren unter Annahme eines Fehlerausschlusses für den Wellenbruch an. Die Bedingungen für einen solchen Fehlerausschluss sind im Prüfgrundsatz GS-IFA-M21 Tabelle A.1 angegeben.

- Der DC-Wert für die Positionsschalter B1 und B2 beträgt 99 % aufgrund der Plausibilitätsprüfung durch den Sicherheitsbaustein K4.

- Der DC-Wert für die Drehgeber B3 und B4 wird aufgrund des Kreuzvergleichs der Signale durch das Drehzahlüberwachungsgerät K3 mit 99 % abgeschätzt.

- Für das Subsystem Positionsschalter B1/B2 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (70 Punkte): Trennung (15), Verwendung bewährter Bauteile (5), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10).

- Für das Subsystem Drehgeber B3/B4 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10).

- Für die Sicherheitsfunktion SF 1 „Betriebsartenwahl“ ergibt sich folgende Bewertung: Die Formulierung der Fehlerausschlüsse aufgrund der konstruktiven Eigenschaften lässt eine Einstufung für die Abgrenzung Automatik, Einrichten und Funktionssteuerung zueinander in PL d zu. Es erfolgt eine Einschränkung auf PL d, weil PL e sich nicht allein auf Fehlerausschlüsse beziehen darf (siehe DIN EN ISO 13849-2, Tabelle D.8).

- Für die Sicherheitsfunktion SF 2 „Automatikbetrieb; Öffnen der beweglich trennenden Schutzeinrichtung setzt den Antrieb still (STO)“ ergibt sich folgende Bewertung: Das Subsystem B1/B2 entspricht Kategorie 3 mit hoher $MTTF_D$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}5 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Positionsschalter B1/B2, Sicherheitsbaustein K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}3 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

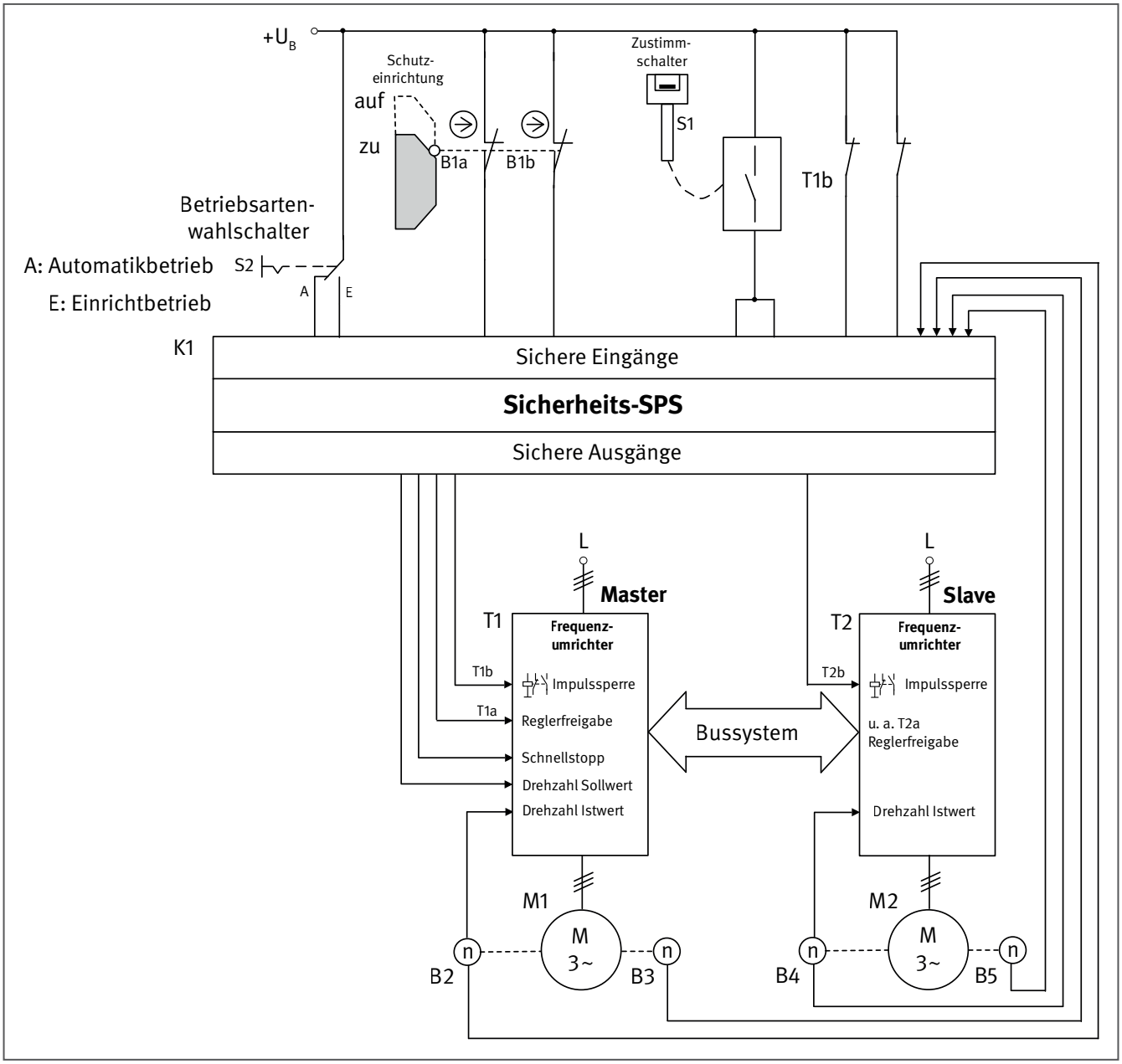
- Für die Sicherheitsfunktion SF 3 „Einrichtbetrieb; Loslassen des Zustimmungsschalters S1 am Handbediengerät setzt den Antrieb still (STO)“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme Zustimmungsschalter S1, Sicherheitsbaustein K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}3 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

- Für die Sicherheitsfunktion SF 4 „Einrichtbetrieb; Überschreiten der maximal zulässigen Drehzahl führt zum Stillsetzen des Antriebs (SLS)“ ergibt sich folgende Bewertung: Das Subsystem B3/B4 entspricht Kategorie 3 mit hoher $MTTF_D$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 6{,}9 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Drehgeber B3/B4, Drehzahlüberwachung K2 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 4{,}7 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 9: Antriebssteuerung für Automatik- und Einrichtbetrieb mit begrenzter Geschwindigkeit PL d und Zustimmungsschalter PL c

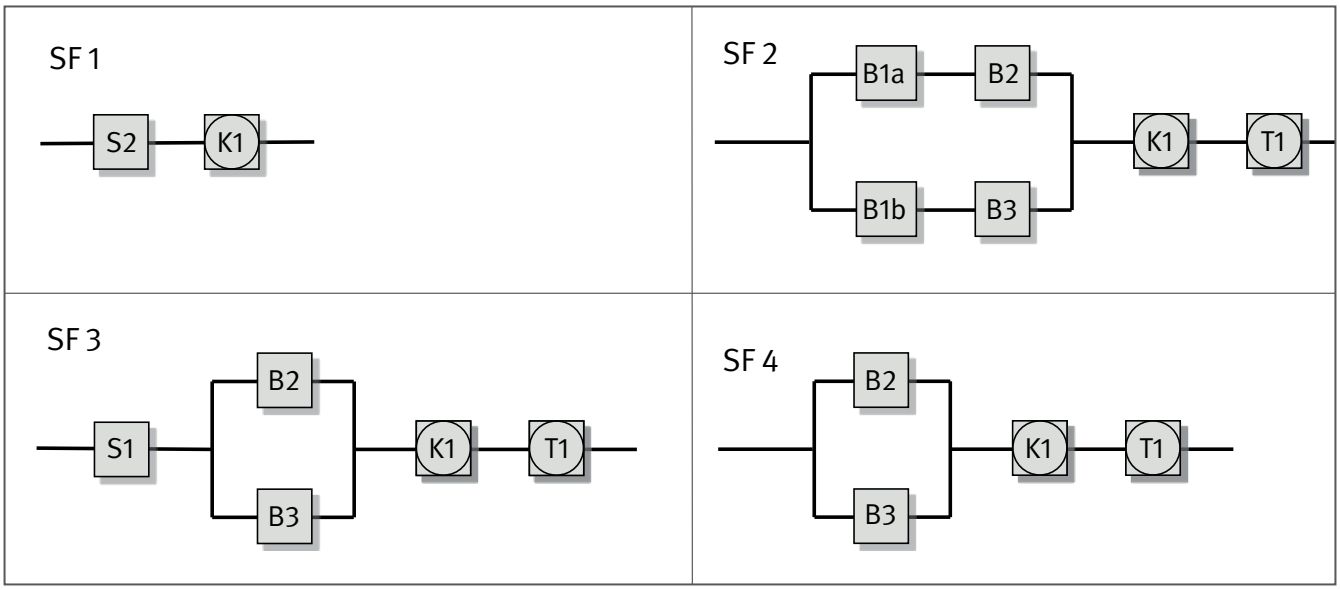
Abbildung A.17:
Prinzipschaltbild der Antriebssteuerung



Sicherheitsfunktionen

- SF 1: Betriebsartenwahl
- SF 2: Automatikbetrieb; SS1 nach Öffnen einer Schutzeinrichtung
- SF 3: Einrichtbetrieb; Loslassen oder vollständiges Durchdrücken des dreistufigen Zustimmungsschalters S1 setzt den Antrieb still (SS1)
- SF 4: Einrichtbetrieb; Sicher begrenzte Geschwindigkeit – Überschreiten der maximal zulässigen Drehzahl führt zum Stillsetzen des Antriebs (STO)

Abbildung A.18:
Sicherheitsbezogene Blockdiagramme zu Beispiel 9



Hinweis:
Bei der Ermittlung des Performance Levels für SF 2 und der folgenden Sicherheitsfunktionen werden Gefährdungen durch einzelne Maschinenteile betrachtet. Dabei erfolgt die Bewegung eines Maschinenteils durch einen einzigen Antrieb. Das heißt in diesem Fall, jeder Antrieb, der eine gefahrbringende Bewegung verursacht, wird separat betrachtet. In die Berechnung des jeweiligen PL müssen daher nicht beide Frequenzumrichter und nicht alle Drehgeber einbezogen werden. In diesem Beispiel werden die Sicherheitsfunktionen betrachtet, an denen der Frequenzumrichter T1 beteiligt ist. Bei der Berechnung für T2 ist zusätzlich die Signalverarbeitung für die Reglerfreigabe über T1 zu berücksichtigen. Weitere Informationen zur Betrachtung einzelner Maschinenteile sind dem Abschnitt 2.2 dieses Reports („Überlagerte Gefährdungen“) zu entnehmen.

Funktionsbeschreibung

- Die Antriebssteuerung realisiert synchronisierte Bewegungen mit sicher begrenzter Geschwindigkeit im Einrichtbetrieb. Die Frequenzumrichter T1/T2 werden als Master/Slave betrieben. Der erste Frequenzumrichter T1 (Master) erhält einen Sollwert und steuert über einen Datenbus den nachfolgenden Frequenzumrichter T2 (Slave) an.

- Der Betriebsartenwahlschalter S2 lässt die Wahl zwischen Automatikbetrieb und Einrichtbetrieb zu (SF 1). Im Automatikbetrieb sind die Kontakte des Positionsschalters B1 an der Schutzeinrichtung geschlossen und der Antrieb lässt sich mit beliebiger Geschwindigkeit betreiben. Ein Öffnen der Schutzeinrichtung im Automatikbetrieb (Auslösung SF 2) wird von der Sicherheits-SPS K1 erfasst, die daraufhin einen Schnellstopp des Antriebs über den entsprechenden Eingang des Master-Frequenzumrichters einleitet. Der Slave-Frequenzumrichter T2 erhält diesen Befehl über den Bus und folgt dem Master. Die Sicherheits-SPS K1 überwacht die Bremsrampe, deaktiviert nach erreichtem Stillstand die Reglerfreigabe der Frequenzumrichter T1a/T2a und schaltet die Impulssperre T1b/T2b weg. Durch die Ergänzung der Rampenüberwachung in der Sicherheits-SPS K1 zu den Frequenzumrichtern mit STO wird die Sicherheits-Teilfunktion SS1 (entspricht Stopp-Kategorie 1 nach DIN EN 60204-1) umgesetzt.

- Bei offener Schutzeinrichtung ist nur ein Einrichtbetrieb mit begrenzter Geschwindigkeit möglich (SF 4). Dabei muss der Zustimmungsschalter S1 betätigt sein (SF 3). Die Einleitung der Bewegung erfolgt durch eine separate Befehlseinrichtung auf einem Handbediengerät (nicht dargestellt).

- Nach Loslassen bzw. Durchdrücken des Zustimmungsschalters S1 in die dritte Stufe wird über die Sicherheits-SPS K1 die gefahrbringende Bewegung stillgesetzt. Dies erfolgt zunächst über den Schnellstopp in den Frequenzumrichtern T1 und T2. Das Stillsetzen wird durch die Sicherheits-SPS K1 überwacht und nach Stillstand wird STO in den Frequenzumrichtern aktiviert. Durch diesen Ablauf wird SS1 realisiert.

- Die Überwachung der Drehzahl im Einrichtbetrieb (SF 4) erfolgt durch die Sicherheits-SPS K1 für jede Achse. Zur Erfassung der Drehzahl werden jeweils zwei Geber (B2/B3 bzw. B4/B5) verwendet. Bei Überschreitung der maximal zulässigen Geschwindigkeit wird die gefahrbringende Bewegung durch Aktivierung der Sicherheits-Teilfunktion STO in den Frequenzumrichtern T1 bzw. T2 stillgesetzt.

- Fehler in dem Positionsschalter B1, den Impulssperre-Relais von T1b/T2b und den Drehgebern B2 bis B5 werden durch die Sicherheits-SPS K1 aufgedeckt. Die Überwachung der Schnellstopp-Rampe und die Erkennung des Stillstands erfolgt mithilfe der Drehgeber ebenfalls durch die Sicherheits-SPS K1.

- Beide Abschaltpfade von T1 und T2 werden überwacht. Die Relais der Impulssperre T1b bzw. T2b verfügen zur Fehleraufdeckung jeweils über einen zwangsgeführten Öffnerkontakt, der von der Sicherheits-SPS K1 eingelesen wird. Fehler der Reglerfreigabe machen sich durch Störungen im Maschinenablauf bemerkbar.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Stromkreises, Vorladung der Frequenzumrichter-Zwischenkreise), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.

- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.

- Bei dem Betriebsartenwahlschalter S2 handelt es sich um einen nockenbetätigten Wahlschalter mit zwangläufigem Betätigungsmodus. Aufgrund der Konstruktion des Betriebsartenwahlschalters sind die Fehlerausschlüsse gemäß DIN EN ISO 13849-2, Tabelle D.8 möglich.

- Bei B1 handelt es sich um einen Positionsschalter mit getrenntem Betätiger. Der Schalter ist mit zwei zwangsöffnenden Kontakten B1a/B1b bestückt, die die Anforderungen gemäß DIN EN 60947-5-1, Anhang K erfüllen. Die Anfahrmechanik muss bestimmungsgemäß konstruiert und angebracht sein.

- Bei dem dreistufigen Zustimmungsschalter S1 handelt es sich um ein einkanaliges Gerät. Der Zustimmungsschalter S1 entspricht den Anforderungen in DIN EN 60204-1, Abschnitt 10.9.

- T1 und T2 sind Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO gemäß Kategorie 3 und PL d. Die Aktivierung von STO erfolgt durch Abschalten von Impulssperre und Reglerfreigabe.

- Die Sicherheits-SPS K1 erfüllt die Anforderungen der Kategorie 4 und PL e.

- Die Programmierung der Software (SRASW) für die Sicherheits-SPS K1 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 4.6.3 und ggf. 4.6.4 der DIN EN ISO13849-1.

Bemerkung:

- Die Anbringung der zwei Drehgeber B2/B3 bzw. B4/B5 am jeweiligen Motor muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z. B. Geberwellenbruch) ausgeschlossen ist.

Berechnung der Ausfallwahrscheinlichkeit

- Für den Betriebsartenwahlschalter S2 mit zwangläufigem Betätigungsmodus und für die Trennung der Betriebsarten in diesem Schalter erfolgt ein Fehlerausschluss. Aufgrund der vorhandenen Steuerungsstruktur und des Einbaus im Schaltschrank mit der Mindestschutzart IP 54 können Fehler, u. a. Kurzschlüsse, zwischen benachbarten Leiterbahnen und Kontaktstellen sowie Leitungen ausgeschlossen werden. Die Bedingungen für Fehlerausschlüsse bis maximal PL d gemäß DIN EN ISO 13849-2, Tabelle D.8 werden eingehalten. Aufgrund einer Analyse können Fehler in der Betriebsartenwahl, die verhindern könnten, dass erforderliche Sicherheitsfunktionen wirksam werden, ausgeschlossen werden.

- Für den Positionsschalter B1 mit zwangsöffnenden Kontakten B1a/B1b wird jeweils ein B_{10D} von 20 000 000 Schaltspielen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 30 Minuten ergibt sich n_{op} zu 7 680 Zyklen pro Jahr und eine $MTTF_D$ von 26 042 Jahren.
  Unter anderem erfolgt ein verdeckter Einbau des Positionsschalters, sodass Einwirkungen durch Umgebungseinflüsse minimiert sind; damit ist gleichzeitig auch einer Manipulation vorgebeugt.

- Für den Zustimmungsschalter S1 wird in diesem Beispiel nur das Loslassen (Stufe 2 nach Stufe 1) betrachtet. Hierfür wird ein B_{10D} von 100 000 Schaltspielen [N] angenommen. Bei täglichem Einrichten und 10 Betätigungen des Zustimmungsschalters S1 ergibt sich n_{op} zu 2 400 Zyklen pro Jahr. Hieraus ergibt sich $MTTF_D$ zu 416,7 Jahren und in Kategorie 1 eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}1 \cdot 10^{-6}$/Stunde.

- Die Sicherheits-SPS K1 erfüllt die Anforderungen der Kategorie 4, PL e und SIL 3. Die $PFH_D = 3{,}2 \cdot 10^{-8}$/Stunde [H].

- Bei T1 und T2 handelt es sich um Frequenzumrichter mit der integrierten Sicherheits-Teilfunktion STO. Sie erfüllen die Anforderungen für Kategorie 3, SIL 2 und PL d. Die PFH beträgt $3{,}2 \cdot 10^{-7}$/Stunde [H]. Diese Angaben für T1 und T2 sind nur dann gültig, wenn die Vorgaben des Herstellers zur Fehleraufdeckung durch externe Komponenten umgesetzt werden.

- Die Drehgeber B2/B3 sowie B4/B5 sind jeweils rechts und links an den Motoren angeflanscht. Der Geberhersteller gibt eine $MTTF_D$ von jeweils 40 Jahren unter Annahme eines Fehlerausschlusses für den Wellenbruch an.

- Der DC-Wert für die Drehgeber B2/B3 bzw. B4/B5 ergibt sich mit 99 % aufgrund des Kreuzvergleichs der Signale durch die Sicherheits-SPS K1.

- Für das Subsystem mit dem Positionsschalter B1 und den Drehgebern B2/B3 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10).

- Für die Sicherheitsfunktion SF 1 „Betriebsartenwahl“ ergibt sich folgende Bewertung: Die Formulierung der Fehlerausschlüsse für S2 aufgrund der konstruktiven Eigenschaften lässt eine Einstufung für die Abgrenzung von Einricht- und Automatikbetrieb in PL d zu. Es erfolgt eine Einschränkung auf PL d, da die Bewertung des Betriebsartenwahlschalters ausschließlich auf Fehlerausschlüssen basiert (siehe DIN EN ISO 13849-2, Tabelle D.8). Der PFH_D-Wert wird alleine durch den Beitrag der Sicherheits-SPS K1 bestimmt und beträgt $3{,}2 \cdot 10^{-8}$/Stunde.

- Für die Sicherheitsfunktion SF 2 „Automatikbetrieb; SS1 nach Öffnen einer Schutzeinrichtung“ ergibt sich folgende Bewertung: Das Subsystem B1/B2/B3 entspricht Kategorie 3 mit hoher $MTTF_D$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH_D $6{,}9 \cdot 10^{-8}$/Stunde. Die Kombination der Subsysteme Positionsschalter/Drehgeber B1/B2/B3, Sicherheits-SPS K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 4{,}2 \cdot$ 10-7/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 3 „Einrichtbetrieb; Loslassen oder vollständiges Durchdrücken des dreistufigen Zustimmungsschalters S1 setzt den Antrieb still (SS1)“ ergibt sich folgende Bewertung: Das Subsystem B2/B3 entspricht Kategorie 3 mit hoher $MTTF_D$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 6{,}9 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Zustimmungsschalter S1, Drehgeber B2/B3, Sicherheits-SPS K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}6 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

- Für die Sicherheitsfunktion SF 4 „Einrichtbetrieb; Sicher begrenzte Geschwindigkeit – Überschreiten der maximal zulässigen Drehzahl führt zum Stillsetzen des Antriebs (STO)“ ergibt sich folgende Bewertung: Das Subsystem B2/B3 entspricht Kategorie 3 mit hoher $MTTF_D$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 6{,}9 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Drehgeber B2/B3, Sicherheits-SPS K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 4{,}2 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 10: **Gesteuertes Stillsetzen eines Antriebs beim Öffnen der Schutzeinrichtung mit Quittierungsfunktion – PL d**

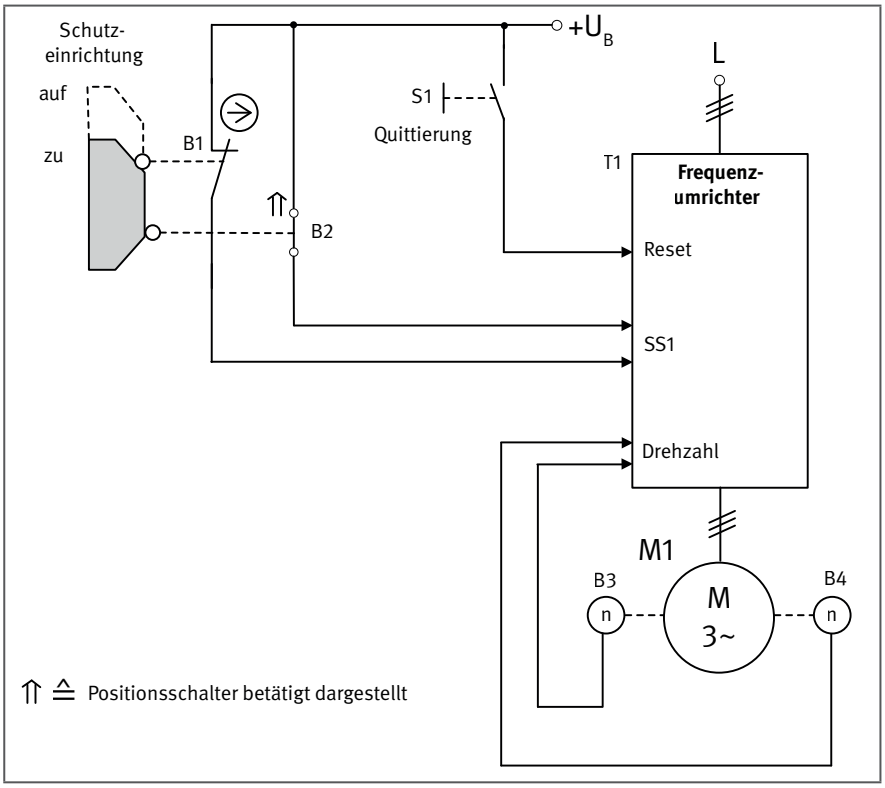


Abbildung A.19:
Prinzipschaltbild der Stellungs-
überwachung

Sicherheitsfunktionen

- SF 1: Sicheres Stillsetzen beim Öffnen der Schutztür
- SF 2: Manuelle Rückstellung durch Loslassen des betätigten Quittierungstasters B3 bei geschlossener Schutzeinrichtung

Funktionsbeschreibung

- Beim Öffnen der Schutzeinrichtung wird über die Positionsschalter B1 und B2 zweikanalig der Eingang „Sicheres Stillsetzen“ (SS1) des Frequenzumrichters T1 unterbrochen. Der Frequenzumrichter T1 leitet das Stillsetzen ein und überwacht die Verzögerungsrampe des Motors. Bei Stillstand wird der STO eingelegt.
- Die Drehgeber B3 und B4 liefern die entsprechenden Drehzahlinformationen, die zur Überwachung der Verzögerungsrampe benötigt werden. Fehler in den Drehgebern werden durch den Vergleich der beiden Signale im Frequenzumrichter T1 aufgedeckt.
- Der Frequenzumrichter überwacht die Funktion des Positionsschalters B1 im Vergleich mit B2. Im Fehlerfall wird der weitere Betrieb verhindert.
- Die Schutzeinrichtung ist hintertretbar, sodass zusätzlich eine Quittierung (manuelle Rückstellung) nach Verlassen des Gefahrenbereichs und Schließen der Schutztür vorgesehen ist. Vom Ort der Quittierung muss der Gefahrenbereich einsehbar sein.

Bemerkungen

- In diesem Beispiel wird die Sicherheits-Teilfunktion SS1 durch Überwachung der Bremsrampe realisiert (SS1-r).

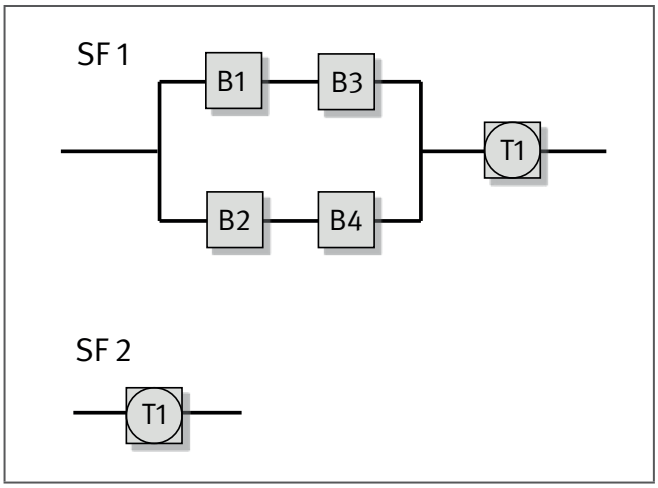


Abbildung A.20:
Sicherheitsbezogene Blockdiagramme zu Beispiel 10

- Die Steuerspannung U_B sowie die interne Steuerspannung des Frequenzumrichters T1 werden aus der Zwischenkreisspannung des Frequenzumrichters generiert. Ein gesteuertes Stillsetzen des Antriebs erfolgt auch bei Spannungsausfall.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Stromkreises, Vorladung des Frequenzumrichter-Zwischenkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.
- Der Frequenzumrichter T1 ist mit der integrierten Sicherheits-Teilfunktion SS1 mit Rampenüberwachung (SS1-r) gemäß Kategorie 3 und PL d ausgestattet.
- Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden.
- Der Positionsschalter B1 ist ein zwangsöffnender Positionsschalter, der die Anforderungen nach DIN EN 60947-5-1, Anhang K erfüllt.
- Störungen im Anfahr- und Betätigungsmechanismus der Schutzeinrichtung werden durch zwei gegensätzlich betätigte Positionsschalter B1, B2 (Öffner-Schließer-Kombination) erkannt.
- Der Frequenzumrichter T1 ist mit einer Quittierungsfunktion (manuelle Rückstellfunktion) ausgestattet.
- Die Anforderungen an die manuelle Rückstellfunktion gemäß DIN EN ISO 13849-1, Abschnitt 5.2.2 werden eingehalten. Dies bedeutet u. a., dass T1 die Rückstellfunktion erst beim Loslassen von S1 aktiviert und die Rückstellung selbst noch nicht zum Wiederanlauf von T1 führt.
- Die Anbringung der beiden Drehgeber muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z. B. Geberwellenbruch) ausgeschlossen ist.

Berechnung der Ausfallwahrscheinlichkeit

- Der Positionsschalter B1 weist eine B_{10D} von 20 000 000 Schaltspielen [N] auf. Mit n_{op} = 7 680 Zyklen ergibt sich eine $MTTF_D$ von 26 041 Jahren.

- Für den Positionsschalter B2 wird ein B_{10d}-Wert von 1 000 000 Schaltspielen [H] angegeben. Mit n_{op} = 7 680 Zyklen/Jahr ergibt sich eine $MTTF_D$ von 1 302 Jahren.
- Der Frequenzumrichter T1 mit der integrierten Sicherheits-Teilfunktion SS1 und der Quittierungsfunktion erfüllt die Anforderungen der Kategorie 3 und von PL d. Die PFH_D beträgt $2{,}0 \cdot 10^{-7}$/Stunde [H].
- Der Taster S1 für die manuelle Rückstellung ist ein handelsüblicher Tastschalter. Da für die Signalgebung eine abfallende Flanke durch das Loslassen des Tasters erforderlich ist (siehe DIN EN ISO 13849-1, Abschnitt 5.2.2), führt ein Ausfall des Tasters nicht zu einem gefährlichen Fehler. Aus diesem Grund wird B3 in der Quantifizierung nicht berücksichtigt.
- Der Geberhersteller gibt für die Drehgeber B3 und B4 eine $MTTF_D$ von jeweils 40 Jahren unter Annahme eines Fehlerausschlusses für den Geberwellenbruch an.
- Der DC-Wert für die Positionsschalter B1 und B2 beträgt 99 % aufgrund der Plausibilitätsprüfung durch den Frequenzumrichter T1.
- Der DC-Wert für die Drehgeber B3 und B4 wird aufgrund des Kreuzvergleichs der Signale im Frequenzumrichter T1 mit 99 % abgeschätzt.
- Für das Subsystem bestehend aus den Positionsschaltern B1/B2 und den Drehgebern B3/B4 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10).
- Für die Sicherheitsfunktion SF 1 „Sicheres Stillsetzen beim Öffnen der Schutztür“ ergibt sich folgende Bewertung: Das Subsystem B1/B2/B3/B4 entspricht Kategorie 3 mit hoher $MTTF_D$ (38 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}0 \cdot 10^{-8}$/Stunde. Die Kombination der Subsysteme Positionsschalter/Drehgeber (B1/B2/B3/B4) und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}7 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.
- Für die Sicherheitsfunktion SF 2 „Manuelle Rückstellung durch Loslassen des betätigten Quittierungstasters S1 bei geschlossener Schutzeinrichtung“ ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}0 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 11: Antriebssteuerung mit Frequenzumrichter mit integrierter sicherer Bewegungsüberwachung

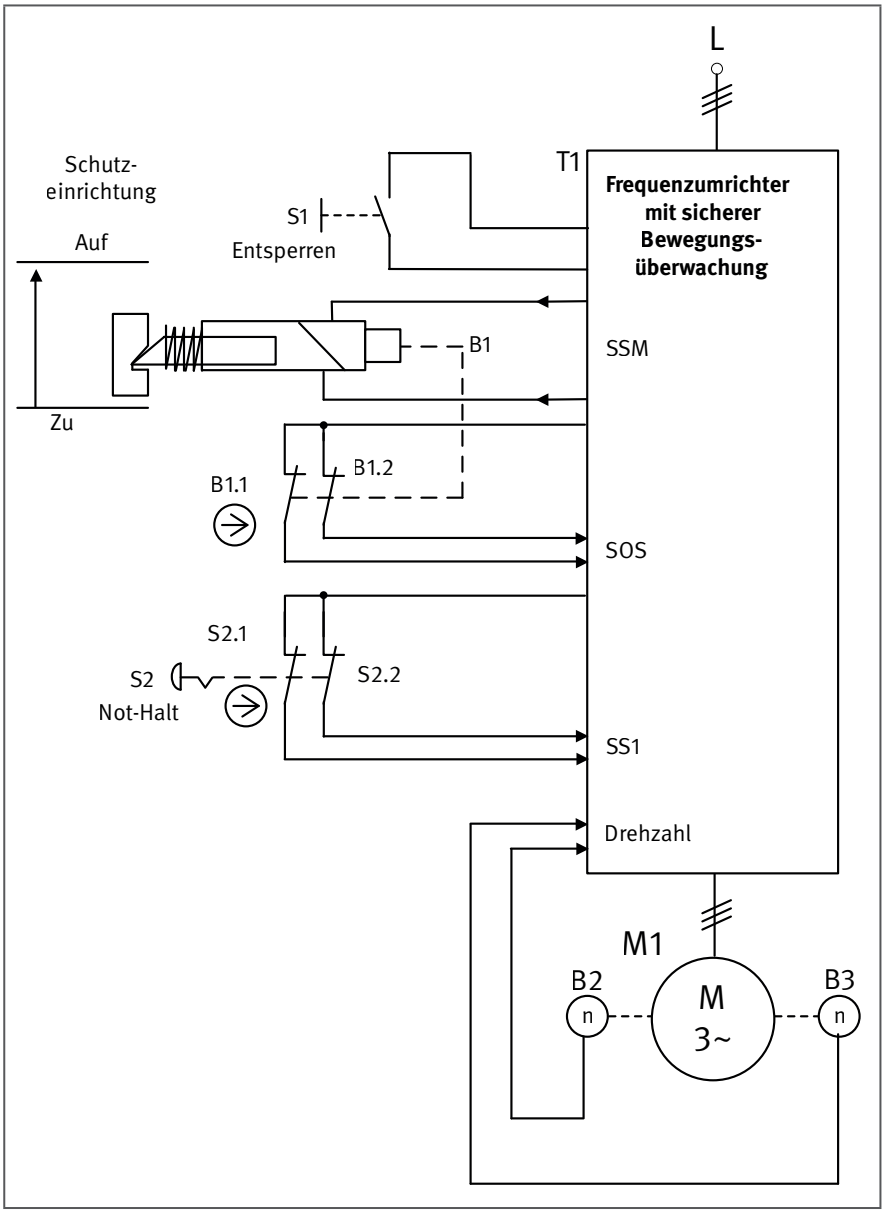


Abbildung A.21:
Stellungsüberwachung einer Schutzeinrichtung mit Zuhaltung sowie Not-Halt

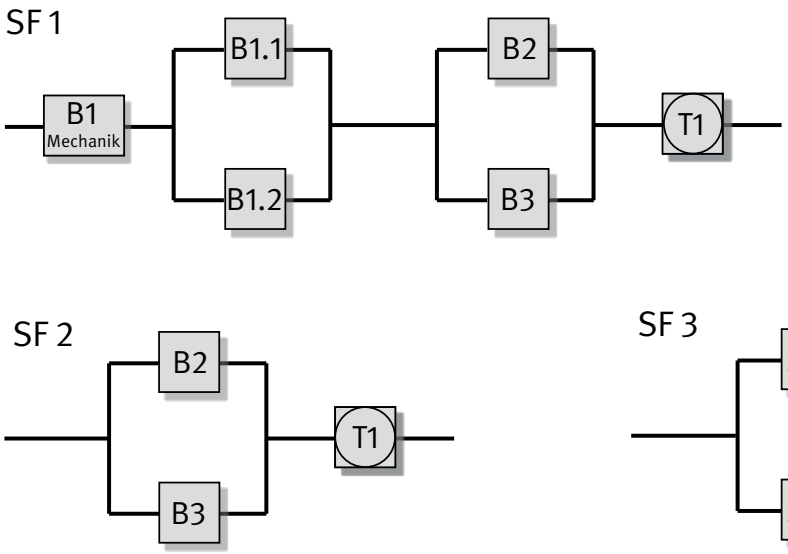
Sicherheitsfunktionen

- SF 1: Sicherer Betriebshalt (SOS) bei entsperrter Zuhaltung
- SF 2: Entsperrung der Zuhaltung im Stillstand
- SF 3: Betätigung des Not-Halt-Geräts führt zum gesteuerten Stillsetzen SS1-r

Funktionsbeschreibung

- Das Entsperren der Schutzeinrichtung wird durch Betätigung des Tipptasters S1 angefordert. Daraufhin steuert der Frequenzumrichter T1 den Antrieb auf die Drehzahl Null. Ein Öffnen der Schutzeinrichtung ist nur im Stillstand möglich. Mit der Sicherheits-Teilfunktion SSM (Sichere Geschwindigkeitsüberwachung) erzeugt der Frequenzumrichter bei einer Motordrehzahl von (fast) Null ein sicheres Ausgangssignal zur Entriegelung des Sperrmittels in der Zuhaltung B1.

Abbildung A.22:
Sicherheitsbezogene Blockdiagramme zu Beispiel 11



- Das Entsperren der Schutzeinrichtung wird durch die Positionsschalter B1.1 und B1.2 erkannt. Im Frequenzumrichter T1 wird daraufhin die Sicherheits-Teilfunktion SOS (Sicherer Betriebshalt) aktiviert.
- Bei Betätigung des Not-Halt-Geräts S2 während einer Motorbewegung erfolgt ein schnellstmögliches gesteuertes Stillsetzen des Antriebs durch SS1 (Sicherer Stopp 1 mit Überwachung der Verzögerungsrampe SS1-r).
- Bei hintertretbarer Schutzeinrichtung ist eine Quittierung (manuelle Rückstellung) nach Verlassen des Gefahrenbereichs und Schließen der Schutztür vorzusehen. Vom Ort der Quittierung muss der Gefahrenbereich einsehbar sein.

Konstruktive Merkmale

- Der Frequenzumrichter T1 verfügt über die integrierten Sicherheits-Teilfunktionen SOS, SS1-r, SSM und STO (in diesem Beispiel nicht verwendet).
- Bei der Funktion SS1-r ist zu beachten, dass im Fehlerfall des Frequenzumrichters ggf. nur ein reduziertes Bremsmoment zur Verfügung steht.
- Die Anbringung der zwei Drehgeber B2 und B3 muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z. B. Geberwellenbruch) ausgeschlossen ist.
- Die Erfassung der Drehzahl erfolgt in diesem Beispiel zweikanalig durch zwei Geber (B2 und B3). Je nach eingesetztem Frequenzumrichter und zu realisierender Sicherheitsfunktion kann auf den zweiten Geber verzichtet werden, in einigen Fällen ist auch ein sensorloser Betrieb möglich. Die Anforderungen des Frequenzumrichter-Herstellers zur Verwendung der Drehzahlgeber sind einzuhalten.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.
- Bei der Schutzeinrichtung handelt es sich um eine Schutztür mit Zuhaltung B1. Der Zugang zur gefahrbringenden Bewegung wird so lange verhindert, bis die Bewegung zum Stillstand gekommen ist (SF 2). Die Tür wird durch einen federkraftbetätigten Bolzen (Sperrmittel) eines Magneten zugehalten, der ein Herausziehen des Betätigers

aus dem Schalterkopf verhindert, bis die Ansteuerung des Entriegelungsmagneten erfolgt. Die Zuhaltung besitzt gemäß Herstellerangabe eine Fehlschließsicherung. Der unerwartete Anlauf des Motors bei geöffneter Schutztür wird verhindert, da durch die Fehlschließsicherung die Kontakte B1.1 und B1.2 nur dann schließen können, wenn die Schutztür geschlossen ist und das Sperrmittel der Zuhaltung sich in der Position „zugehalten“ befindet (SF 2).

Berechnung der Ausfallwahrscheinlichkeit

- B1.1 und B1.2 sind die zwangsöffnenden Kontakte zur Überwachung des Sperrmittels der Zuhaltung. In Verbindung mit der Fehlschließsicherung der Zuhaltung wird damit auch die geschlossene Stellung der Schutztür erfasst. Für B1.1 und B1.2 wird jeweils ein B_{10D} von 2 000 000 Schaltspielen [N] angenommen. Mit n_{op} von 46 080 Zyklen pro Jahr ergibt sich jeweils $MTTF_D$ zu 434 Jahren.

- Für die Mechanik der Zuhaltung einschließlich Bruch des Sperrmittels kann ein Fehlerausschluss angenommen werden, wenn die folgenden Bedingungen erfüllt sind:

  – Anwendung entsprechend der Betriebsanleitung, insbesondere Montageanleitung und technische Daten (z. B. Betätigungsradius, Betätigungsgeschwindigkeit)
  – Verhinderung des Selbstlockerns
  – die statischen Kräfte auf die Zuhaltung sind geringer als die im Datenblatt angegebene Zuhaltekraft
  – es treten keine dynamischen Kräfte auf, da die Bestromung des Entriegelungsmagneten erst bei geschlossener Schutztür erfolgt; siehe hierzu auch DGUV Information 203-079 „Auswahl und Anbringung von Verriegelungseinrichtungen“
  – keine Verwendung als mechanischer Endanschlag
  – unlösbare Befestigung des Betätigers
  – regelmäßige Wartung
  – Formschluss nach Montage
  – ausreichende mechanische Festigkeit aller Träger- und Funktionselemente
  – ein Absenken der Tür führt nicht dazu, dass der Betätiger außerhalb des vom Hersteller spezifizierten Bereichs eingesetzt wird
  – Schäden, die durch vorhersehbare äußere Einflüsse (z. B. Eindringen von Schmutz, Staub und mechanische Erschütterung) entstehen könnten, werden durch die Art der Montage ferngehalten oder sind aufgrund der Einsatzbedingungen nicht zu erwarten.

  Der Fehlerausschluss ist vom Hersteller zu bestätigen.

- Für das Not-Halt-Gerät S2, das nach der Produktnorm DIN EN 60947-5-5 gebaut ist, wird ein B_{10D} von 100 000 Schaltspielen [N] für jeden Kontakt angenommen. Bei 30 Betätigungen pro Jahr beträgt die $MTTF_D$ jeweils 33 333 Jahre. Aufgrund der Kürzung auf $MTTF_D$ von jeweils 100 Jahre ergibt sich für das Not-Halt-Gerät S2 eine PFH_D von $4{,}3 \cdot 10^{-8}$/Stunde.

- Die Drehgeber B2 und B3 sind auf einer Welle aufgebaut. Es handelt sich um herkömmliche Geber mit Impulsausgängen. Die Signalauswertung findet im Frequenzumrichter statt. Der Hersteller gibt eine $MTTF_D$ von 50 Jahren für die Geber an.

- Bei dem Frequenzumrichter T1 mit sicherer Bewegungsüberwachung handelt es sich um ein Gerät mit den integrierten Sicherheits-Teilfunktionen

  – Sicher abgeschaltetes Drehmoment (STO)
  – Sicherer Stopp1 mit Überwachung der Verzögerungsrampe (SS1-r)
  – Sicherer Betriebshalt (SOS)
  – Sichere Geschwindigkeitsüberwachung (SSM)

  Der Hersteller gibt für die Sicherheits-Teilfunktionen einzeln und in Kombination eine PFH von $5 \cdot 10^{-8}$/Stunde [H] an.

- Aufgrund des Kreuzvergleichs durch den Frequenzumrichter T1 wird für die Drehgeber B2 und B3 jeweils ein DC-Wert von 90 % angenommen. Die DC für die Stellungsüberwachung des Sperrmittels B1.1/B1.2 wird jeweils mit 99 % abgeschätzt.

- Für das Subsystem B2/B3 sind ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache vorhanden (65 Punkte): Physikalische Trennung (15), Schutz gegen Überspannung etc. (15), Schutz vor Verunreinigung und EMV sowie Schutz gegen Umgebungsbedingungen (25 + 10).

- Für das Subsystem B1.1/B1.2 sind ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache vorhanden (70 Punkte): Physikalische Trennung (15), Schutz gegen Überspannung etc. (15), Verwendung bewährter Bauteile (5), Schutz vor Verunreinigung und EMV sowie Schutz gegen Umgebungsbedingungen (25 + 10).

- Das Subsystem B1.1, B1.2 der Zuhaltung entspricht Kategorie 3, PL e mit hoher $MTTF_D$ (100 Jahre) und hohem DC_{avg} (99 %). Dies ergibt eine PFH_D von $2{,}5 \cdot 10^{-8}$ /Stunde.

- Das Subsystem B2/B3 entspricht Kategorie 3 mit hoher $MTTF_D$ (50 Jahre) und mittlerem DC-Wert (90 %). Dies ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}2 \cdot 10^{-7}$/Stunde im Bereich von PL d.

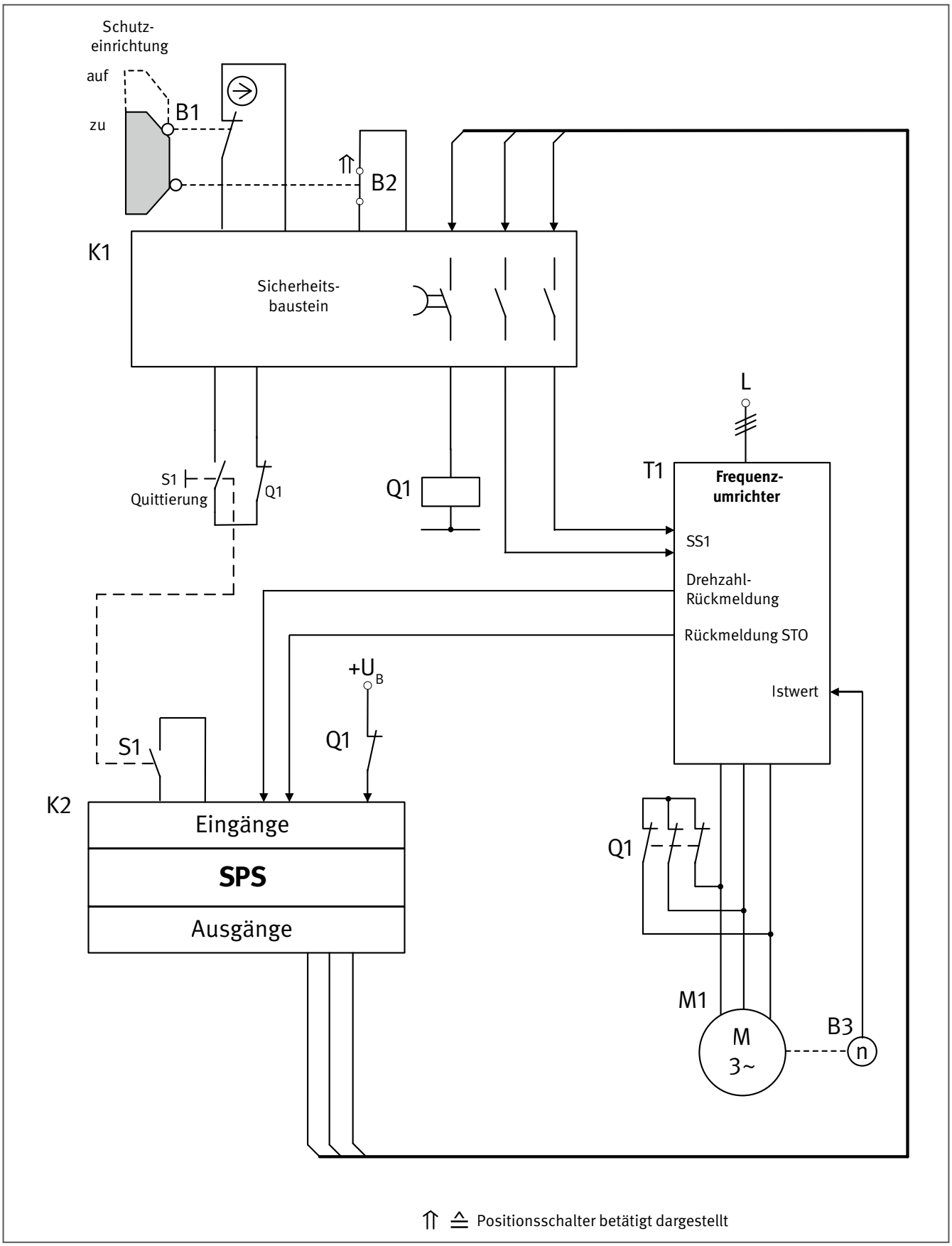
- Für die Sicherheitsfunktion SF 1 „Sicherer Betriebshalt (SOS) bei entsperrter Zuhaltung“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme Positionsschalter B1.1/B1.2, Drehgeber B2/B3 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}0 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 2 „Entsperrung der Zuhaltung im Stillstand durch SSM“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme Drehgeber B2/B3 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}7 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 3 „Betätigung des Not-Halt-Befehlsgeräts führt zum gesteuerten Stillsetzen SS1“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme Not-Halt Gerät S2 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 9{,}3 \cdot 10^{-8}$/Stunde. Dies entspricht rechnerisch PL e. Da jedoch der Frequenzumrichter nur bis PL d eingesetzt werden kann, ergibt sich für SF 3 ein PL d.

Beispiel 12: Vermeidung des unerwarteten Anlaufs mit Frequenzumrichter und Kurzschlussschütz – PL e

Abbildung A.23:
Prinzipschaltbild der Antriebssteuerung



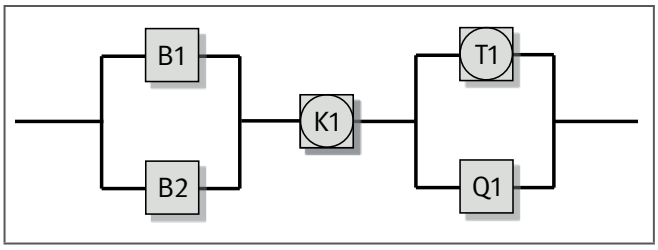


Abbildung A.24:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 12

Sicherheitsfunktion

- SF 1: STO des Motors nach Öffnen der Schutzeinrichtung und erfolgter Stillsetzung

  Bemerkung:

  Für das „Stillsetzen“ und die „Vermeidung des unerwarteten Anlaufs“ werden unterschiedliche Komponenten eingesetzt, da das zusätzliche Kurzschlussschütz Q1 nur für die Vermeidung des unerwarteten Anlaufs benötigt wird. Das Kurzschlussschütz Q1 stellt einen dritten Abschaltpfad dar, durch den ein höherer PL erreicht wird. Zur Berechnung der PFH erfolgt die genannte Aufteilung in zwei getrennte Sicherheitsfunktionen. An dieser Stelle wird jedoch nur die Vermeidung des unerwarteten Anlaufs betrachtet.

Funktionsbeschreibung

- Das Öffnen der Schutzeinrichtung wird vom Sicherheitsbaustein K1 über die Positionsschalter B1 und B2 erkannt. Die unverzögerten Freigabepfade vom Sicherheitsbaustein K1 fallen ab. Der SS1 des Frequenzumrichters T1 wird eingeleitet, der Antrieb wird gesteuert stillgesetzt. Anschließend erfolgt ein zeitverzögertes Abfallen vom Kurzschlussschütz Q1. Das Schließen der Öffnerkontakte vom Kurzschlussschütz Q1 führt zum Kurzschluss der Anschlussleitungen zum Motor. Der Antrieb befindet sich im STO.

- Ein Verschweißen des Kurzschlussschützes Q1 würde sich beim Aufschalten der Versorgungsspannung des Motors über den Frequenzumrichter T1 durch Ansprechen der Ausgangsabsicherung stets bemerkbar machen. Das Kurzschlussschütz Q1 wird über den Rückführkreis des Sicherheitsbausteins K1 überwacht. Darüber hinaus erfolgt eine zusätzliche Fehlererkennung in der SPS K2 auf „Hängenbleiben“.

- Ein Ausfall der Versorgungsspannung führt zum gesteuerten Stillsetzen des Motors und zum verzögerten Kurzschluss der Anschlussleitungen vom Frequenzumrichter T1 zum Motor. Dazu ist es erforderlich, dass

  – die Steuerelektronik vom Frequenzumrichter T1 aus dem Gleichspannungszwischenkreis versorgt wird,
  – der Sicherheitsbaustein K1 über eine unterbrechungsfreie Spannungsversorgung verfügt.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen. Im vorliegenden Beispiel werden als grundlegende Sicherheitsprinzipien u. a. das Ruhestromprinzip und die Erdung des Steuerstromkreises verwendet. Als bewährtes Sicherheitsprinzip wird u. a. die Überdimensionierung der Kontaktbelastung von B1, B2 und Q1 angewendet.

- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.

- Der Frequenzumrichter T1 verfügt über die integrierten Sicherheits-Teilfunktionen STO und SS1.

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

- Störungen im Anfahr- und Betätigungsmechanismus der Schutzeinrichtung werden durch zwei gegensätzlich betätigte Positionsschalter B1, B2 (Öffner-Schließer-Kombination) erkannt.

- Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden.

Bei hintertretbarer Schutzeinrichtung ist eine Quittierung (manuelle Rückstellung) nach Verlassen des Gefahrenbereichs und Schließen der Schutztür vorzusehen. Vom Ort der Quittierung muss der Gefahrenbereich einsehbar sein.

Bemerkungen

- Die Verwendung von sogenannten Kurzschlussschützen ist umstritten. Dennoch wird die Methode z. B. bei Pressen für die Sicherstellung des PL e zur Vermeidung des unerwarteten Anlaufs angewendet. Dies erfolgt insbesondere bei prozessbedingt komplexen Funktionssteuerungen, um den PFH-Wert zu verbessern. Die Verwendung von Kurzschlussschützen setzt jedoch eine versuchstechnische Erprobung zum Verhalten bei Kurzschluss des Schützes voraus. Bei einem Versagen der Sicherheits-Teilfunktion SS1 bewirkt das Schütz Q1 einen Kurzschluss der Betriebsspannung des Motors und wird voraussichtlich beschädigt. Daher ist das Kurzschlussschütz Q1 anschließend zu tauschen und es sind eventuelle weitere Fehler durch Reparatur zu beseitigen.

- Die dargestellte Funktion der Steuerung ist nur ein Teil der Steuerung. Auf die Darstellung z. B. der Betriebsartenwahl wurde verzichtet.

Berechnung der Ausfallwahrscheinlichkeit

- Für den Positionsschalter B1 beträgt B_{10D} 20 000 000 Schaltspielen [N]. Bei 200 Arbeitstagen, 8 Arbeitsstunden pro Tag und einer Zykluszeit von einer Minute ergibt sich n_{op} zu 96 000 Zyklen/Jahr und eine $MTTF_D$ von 2 083 Jahren.

- Für den Positionsschalter B2 wird ein B_{10d} von 1 000 000 Schaltspielen [H] angegeben. Bei 200 Arbeitstagen, 8 Arbeitsstunden pro Tag und einer Zykluszeit von einer Minute ergibt sich n_{op} = 96 000 Zyklen/Jahr und eine $MTTF_D$ von 104 Jahre. Der Positionsschalter weist eine begrenzte Betriebszeit $T10_D$ von 10 Jahren auf. Nach dieser Zeit ist der Positionsschalter zu ersetzen. In SISTEMA liegt hierzu eine Warnmeldung mit gelbem Status vor.

- Bei dem Sicherheitsbaustein K1 handelt es sich um ein handelsübliches Gerät für den Einsatz in PL e und Kategorie 4. Der PFH_D-Wert beträgt $1{,}8 \cdot 10^{-8}$/Stunde [H].

- Das Kurzschlussschütz Q1 hat eine mechanische Lebensdauer von 2 000 000 Schaltspielen. In dieser Anwendung wird es elektrisch praktisch nicht belastet, daher wird die mechanische Lebensdauer als B_{10d}-Wert angesetzt. Der $MTTF_D$-Wert ergibt sich mit n_{op} = 96 000 Zyklen/Jahr zu $MTTF_D$ = 208 Jahre.

- Der Frequenzumrichter T1 verfügt über die Sicherheits-Teilfunktion STO mit einem Rückmeldeausgang. Er ist geeignet für den Einsatz in PL d und Kategorie 3, der PFH_D-Wert des STO beträgt $2 \cdot 10^{-7}$/Stunde.

  Wie im sicherheitsbezogenem Blockdiagramm (Abbildung B.24) dargestellt, ist der Frequenzumrichter T1 ein gekapseltes Subsystem, dem ein zusätzlicher Kanal bestehend aus Q1 zugeordnet ist. Diese Struktur entspricht keiner der vorgesehenen Architekturen der DIN EN ISO 13849-1. Die Berechnung der PFH für dieses Subsystem erfolgt daher nach der im SISTEMA-Kochbuch 4, Kapitel 2 dargelegten Methodik:

  Mit der Beziehung $MTTF_D = 1/PFH_D$ ergibt sich für den Frequenzumrichter T1 eine $MTTF_D$ = 570 Jahre. Die interne DC vom Frequenzumrichter T1 kann nicht erneut verwendet werden, da dies bereits zu einer Reduzierung der PFH von T1 geführt hat. Es kann jedoch eine zusätzliche DC durch andere Bauteile berücksichtigt werden.

- Die zusätzliche Fehlererkennung bzgl. der Sicherheits-Teilfunktion STO des Frequenzumrichters T1 erfolgt extern, im vorliegenden Fall in der SPS K2 durch Vergleich vom Schütz Q1 und Rückmeldung STO. Für diese Fehlererkennung wird ein DC-Wert von 99 % angenommen.

- Der DC-Wert für die Positionsschalter B1 und B2 wird mit 99 % aufgrund der Überwachung durch den Sicherheitsbaustein K1 angegeben.

- Der DC-Wert von Schütz Q1 wird mit 99 % angenommen. Das Kurzschlussschütz Q1 wird über den Rückführkreis des Sicherheitsbausteins K1 überwacht. Darüber hinaus erfolgt eine zusätzliche Fehlererkennung in der SPS K2 auf „Hängenbleiben“.

  Hinweis:

  Ein Verschweißen der Kontakte führt zu einem Kurzschluss beim Aufschalten der Versorgungsspannung des Motors. Die Ausgangsabsicherung des Frequenzumrichters T1 spricht an. Es erfolgt ein Ausfall in die sichere Richtung.

  Für die Ausführung der Sicherheitsfunktion ist ein Schließen der Öffnerkontakte vom Kurzschlussschütz Q1 erforderlich, sodass im Fehlerfall vom Frequenzumrichter T1 ein Stromfluss möglich ist (Abweichung vom Ruhestromprinzip).

  Der Hersteller vom Kurzschlussschütz Q1 gibt an, dass die Wahrscheinlichkeit für einen Ausfall dieser Fähigkeit (Fehlschaltsicherheit) $1 \cdot 10^{-8}$ beträgt. Das entspricht einem Fehler auf 100 Millionen Schaltspiele. Da dieser Wert wesentlich kleiner ist als die mechanische Lebensdauer des Schützes, erfolgt für diesen Fall keine mathematische Berücksichtigung.

- Für das Subsystem aus B1 und B2 sind ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache vorhanden (75 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15), bewährte Bauteile (5), Ausfallanalyse (5) und Schutz gegen Umgebungsbedingungen (25 + 10). Für das Subsystem aus Frequenzumrichter T1 und Kurzschlussschütz Q1 sind ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache vorhanden (90 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15), Ausfallanalyse (5) und Schutz gegen Umgebungsbedingungen (25 + 10).

- Das Subsystem B1/B2 entspricht Kategorie 4 mit hoher $MTTF_D$ pro Kanal (1 392 Jahre) und hohem DC-Wert (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}6 \cdot 10^{-9}$/Stunde.

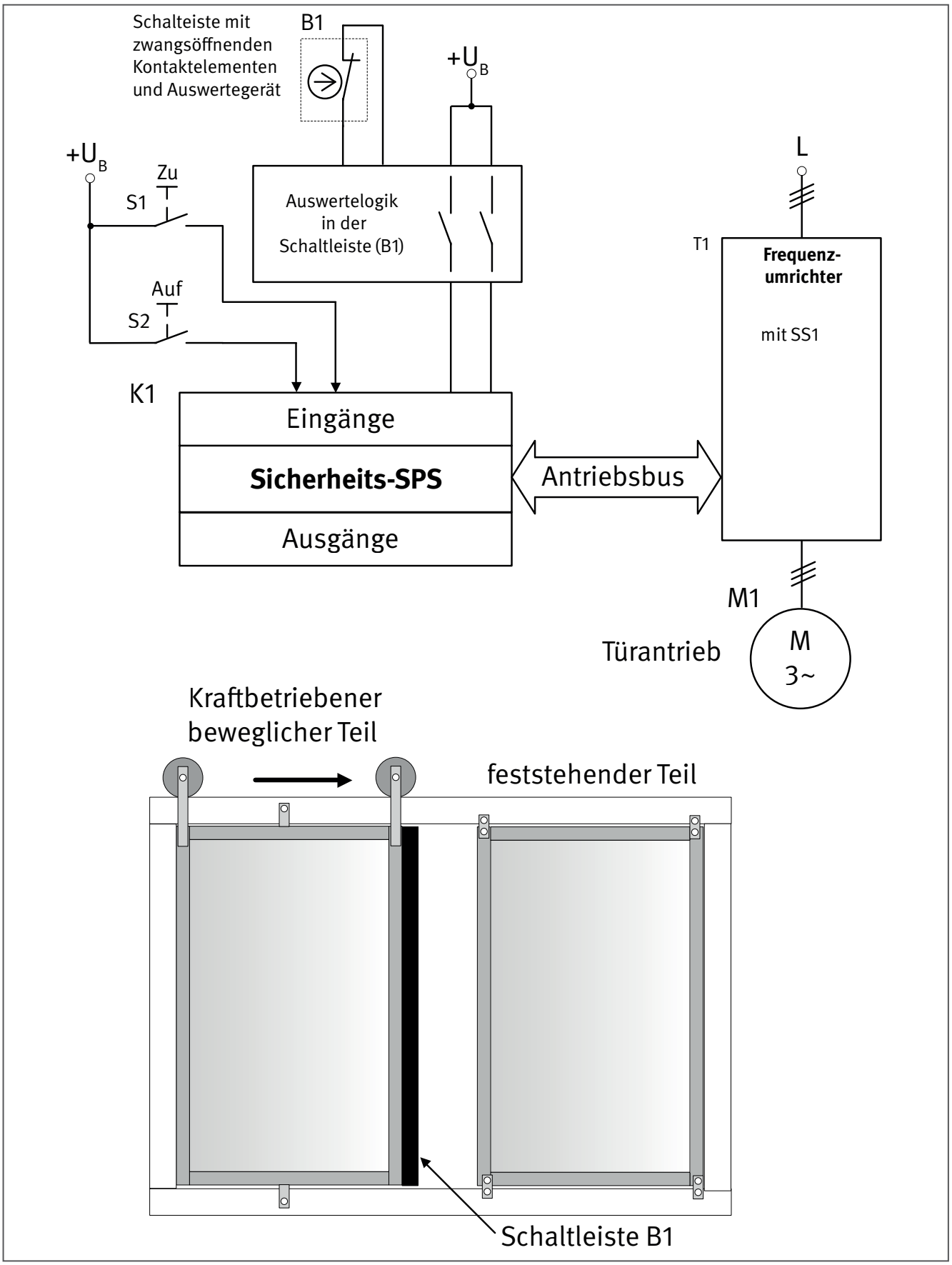
- Wegen der in dieser Anwendung begrenzten Gebrauchsdauer vom Positionsschalter B2 ist ein rechtzeitiger Austausch nach zehn Jahren erforderlich.

- Das Subsystem T1/Q1 entspricht Kategorie 4 mit hoher $MTTF_D$ pro Kanal (100 Jahre) und hohem DC-Wert (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 5{,}5 \cdot 10^{-9}$/Stunde.

- Für die Sicherheitsfunktion SF 1 „STO des Motors nach Öffnen der Schutzeinrichtung und erfolgter Stillsetzung“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme B1/B2, K1 und T1/Q1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Beispiel 13: Kraftbetriebene beweglich trennende Schutzeinrichtung (Schutztür) – PL d

Abbildung A.25:
Prinzipschaltbild der Antriebssteuerung



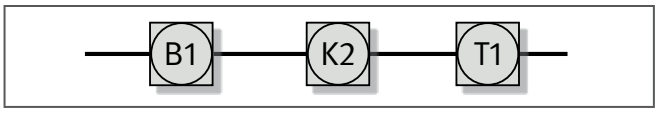


Abbildung A.26:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 13

Sicherheitsfunktion

- SF 1: Begrenzung der Schließkräfte einer kraftbetriebenen Tür durch Betätigung einer Schaltleiste

Funktionsbeschreibung

- Für das Be- und Entladen mit Werkstücken sowie das Wechseln der Werkzeuge ist das Öffnen der Schutztür (beweglich trennende Schutzeinrichtung) erforderlich. Das kraftbetriebene Öffnen der Schutztür kann manuell durch den Bediener, aber auch automatisch z. B. bei Be- und Entnahme durch Roboter, eingeleitet werden. Das Öffnen und Schließen der Schutztür darf nicht zu Gefährdungen, wie z. B. Quetschen des Bedieners bei einer Schließbewegung, führen. Werden die Grenzwerte für kraftbetriebene trennende Schutzeinrichtungen eingehalten, wird davon ausgegangen, dass keine Gefährdung vorliegt (siehe Bemerkungen).

  Können die Grenzwerte nicht eingehalten werden, ist der Gefahrenbereich durch zusätzliche Schutzeinrichtungen zu sichern.

  Im vorliegenden Beispiel ist die Schutztür mit einer Schaltleiste B1 an der Schließkante ausgerüstet. Die Betätigung der Schaltleiste B1, die nur dann erfolgt, wenn der Bediener sich beim Schließen im Gefahrenbereich der Schutztür befindet, setzt über die in der Schaltleiste integrierte Auswertelogik, die Sicherheits-SPS K1 und den Frequenzumrichter T1 den Antrieb so schnell still, dass die zulässigen Schließkräfte nicht überschritten werden.

Bemerkungen: Grenzwerte für kraftbetriebene trennende Schutzeinrichtungen

- Die Kraft an der Schließkante darf statisch 75 N nicht überschreiten und die kinetische Energie der trennenden Schutzeinrichtung darf nicht größer als 4 Joule sein. Ist die trennende Schutzeinrichtung mit einer zusätzlichen Schutzeinrichtung versehen, die bei Berührung mit einem Hindernis ein automatisches Öffnen (Reversieren) einleitet, darf die statische Kraft 150 N und die kinetische Energie 10 Joule nicht überschreiten (siehe DIN EN 953, Abschnitt 5.2.5.2). Diese Anforderungen gelten nur unter der Voraussetzung, dass die Schließkanten eine Breite von mindestens 8 mm aufweisen und dass keine Schergefährdung vorliegt.

- *„Scherstellen können durch Begrenzung der Kräfte, gemessen an der Schließkante, auf ‹ 75 N bzw. ‹ 150 N statisch und ‹ 400 N dynamisch gesichert werden, in Verbindung mit:*

  – *entweder einem Sicherheitsabstand von mindestens 25 mm zwischen dem feststehenden und beweglichen Teil der Schutzeinrichtung, oder*

  – *durch runde Kanten mit einem Radius von mindestens 2 mm für jede Kante und einem Summenradius (Summe der zwei Radien) von mindestens 6 mm (z. B. mindestens 2 mm plus 4 mm oder 3 mm plus 3 mm)“.*

  Quelle: Abschnitt 5.1.1.5.3 aus DIN EN 12453

- Für die Messung der Kräfte gilt DIN EN 12445 und der Zeitverlauf nach Anhang A, Bild A.1 und Tabelle A.1 der DIN EN 12453 (Abbildung A.27 und Tabelle A.2 in diesem Report).

  Hierbei ist

  F_d: maximale Kraft, gemessen mit einem Messgerät nach DIN EN 12453 Abschnitt 5.1.1.5, während der dynamischen Zeitdauer T_d

  F_s: maximale Kraft, gemessen mit einem Messgerät nach DIN EN 12453 Abschnitt 5.1.1.5, nach der dynamischen Zeitdauer T_d

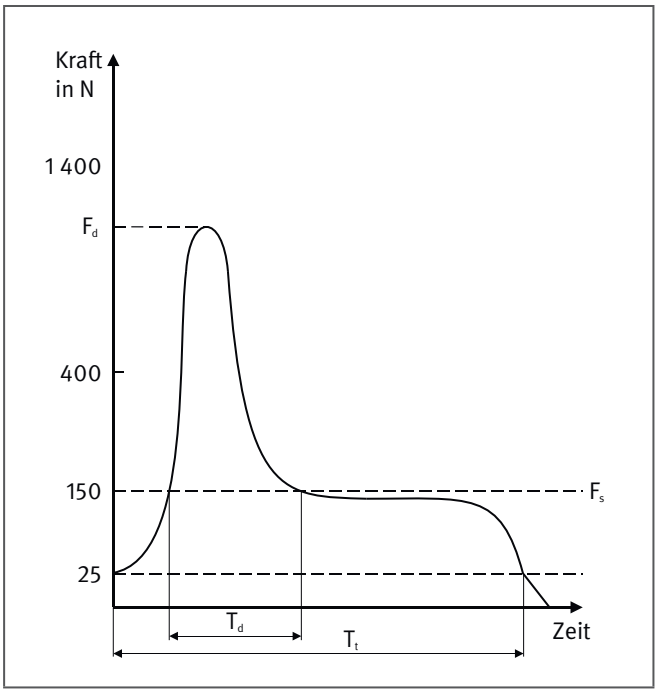


Abbildung A.27:
Schließkräfte in Abhängigkeit von der Zeit aus DIN EN 12453

Tabelle A.2:
Zulässige dynamische Kräfte

Zulässige dynamische Kräfte in N	Zwischen Schließkanten und Gegenschließkanten		Zwischen ebenen Fächen außer zwischen Schließ- und Gegenschließkanten › 0,1 m² mit keiner Seitenlänge ‹ 100 mm
	In Öffnungsweiten von 50 bis 500 mm	In Öffnungsweiten › 500 mm	
horizontal bewegtes Tor	400	1 400	1 400
Tor, das sich um eine Achse senkrecht zum Fußboden dreht	400	1 400	1 400
vertikal bewegtes Tor	400	400	1 400
Tor, das sich um eine Achse parallel zum Fußboden dreht – Schranken	400	400	1 400

T_d: Zeitdauer, in der die gemessene Kraft 150 N übersteigt

T_t: Zeitdauer, in der die gemessene Kraft 25 N übersteigt

- Die in Tabelle A.2 festgelegten Werte sind Maximalwerte, die in einer Zeit von maximal 0,75 s ($T_d \leq 0{,}75$ s) erlaubt sind. Die Gesamtzeit T_t darf 5 s nicht überschreiten. An der Nebenschließkante zwischen beweglich trennender Schutzeinrichtung und Gehäuse darf eine Spaltweite von 4 mm nicht überschritten werden.
- Falls die Anforderungen für die obigen Grenzwerte nicht eingehalten werden können, muss stattdessen zum Beispiel eine ortsbindende Schutzeinrichtung für den Bediener vorhanden sein.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Stromkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.

- Fehler in den elektrischen Anschlussleitungen dürfen sich nicht gefährlich auswirken. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Querschlüsse und Kurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4 sind zu betrachten. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.

- Die Schaltleiste mit integrierter Auswertelogik B1 erfüllt die Anforderungen nach DIN EN ISO 13856-2 und dient der Absicherung von Quetsch- und Scherstellen. Die Schaltleiste B1 ist über die integrierte Auswertelogik mit der Sicherheits-SPS K1 verbunden. Die Schaltleiste mit integrierter Auswertelogik B1 erfüllt die Anforderungen nach DIN EN ISO 13849-1 für Kategorie 3, PL d.

- Der Maschinenhersteller muss die Eignung der Schaltleiste für die jeweilige Applikation überprüfen (z. B. auf ausreichenden Verformungsweg, Berücksichtigung der Umgebungseinflüsse und Wirkbereich).

- Die Antriebssteuerung T1 verfügt über die Sicherheits-Teilfunktion SS1.

- Bei der Sicherheits-SPS K1 und der Antriebssteuerung T1 handelt es sich um Sicherheitsbauteile für den Einsatz bis Kategorie 4 und PL e (K1) bzw. Kategorie 3 und PL d (T1). Auftretende Fehler werden erkannt und der sichere Zustand wird eingeleitet. Die Verbindungen zwischen der Sicherheits-SPS K1 und der Antriebssteuerung T1 erfolgen über ein Sicherheitsbussystem für den Einsatz in PL d entsprechend dem IFA Report 2/2017, Abschnitt 6.2.18.

- Die Programmierung der Anwendungssoftware (SRASW) in der Sicherheits-SPS K1 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 4.6.3 und 4.6.4 der DIN EN ISO 13849-1.

Berechnung der Ausfallwahrscheinlichkeit

- Für die Schaltleiste mit integrierter Auswertelogik B1 wird vom Hersteller eine Kategorie 3, PL d und eine PFH_D von $3{,}2 \cdot 10^{-7}$/Stunde angegeben [H].

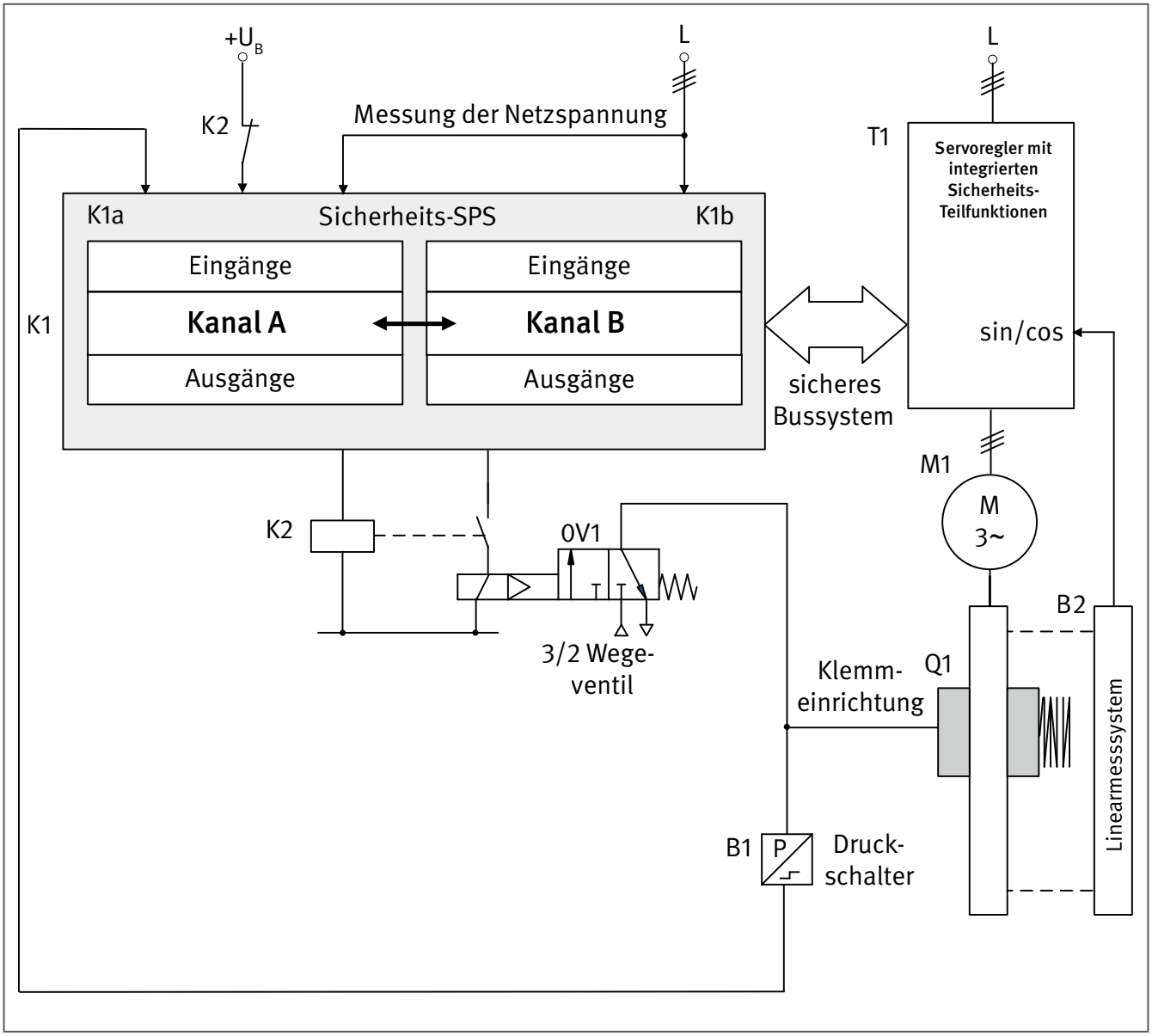
- Die Sicherheits-SPS K1 weist eine PFH_D von $1{,}0 \cdot 10^{-8}$/Stunde [H] auf.

- Die Antriebssteuerung T1 geht mit einer PFH_D von $1{,}5 \cdot 10^{-8}$/Stunde [H] und PL d in die Berechnung ein.

- Für die Sicherheitsfunktion SF 1 „Begrenzung der Schließkräfte einer kraftbetriebenen Tür durch Betätigung einer Schaltleiste“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme B1/K1/T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 3{,}4 \cdot 10^{-7}$/Stunde im Bereich von PL d.

Beispiel 14: Absicherung (Hochhaltung) einer gewichtsbelasteten Vertikalachse – PL c/PL d

Abbildung A.28:
Prinzipschaltbild der Antriebssteuerung



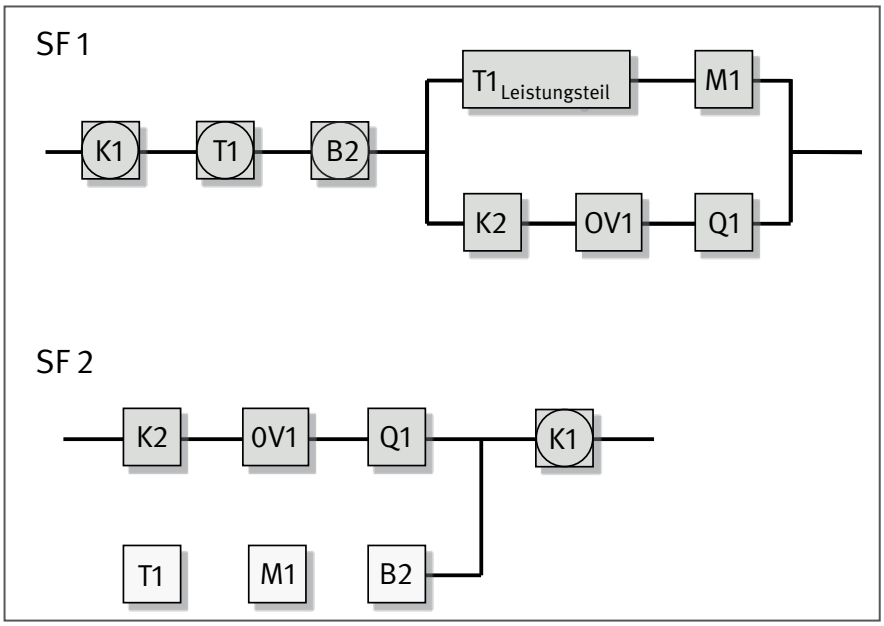
Sicherheitsfunktionen

- SF 1: Sicheres Hochhalten im Einricht- und Automatikbetrieb (SOS)
- SF 2: Sicheres Hochhalten bei Spannungsausfall

Funktionsbeschreibung

- Die Steuerung der gewichtsbelasteten Vertikalachse erfolgt durch die Sicherheits-SPS K1 in Verbindung mit dem Servoregler T1. Bei der Sicherheits-SPS K1 handelt es sich um eine SPS K1a in Verbindung mit einer NC-Achssteuerung K1b. Die Sicherheits-SPS K1 übernimmt Plausibilitätsprüfungen z. B. hinsichtlich des Steuerdrucks der Klemmeinrichtung Q1 und deren Ansteuerung.

Abbildung A.29:
Sicherheitsbezogene Blockdiagramme zu Beispiel 14



- Bei SF 1 „Sicheres Hochhalten im Einricht- und Automatikbetrieb (SOS)“ erfolgt das Abbremsen der Achse im Einricht- und Automatikbetrieb durch SS2. Beim anschließenden sicheren Hochhalten wird die Last der Vertikalachse durch die integrierte Sicherheits-Teilfunktion SOS (Safe Operating Stop, Motor steht still und widersteht externen Kräften) des Servoreglers T1 in der Lage gehalten. Die Position der Last wird vom Linearmesssystem F1 und dem Servoregler T1 zweikanalig erfasst, über den Sicherheitsbus an die Sicherheits-SPS K1 übertragen und überwacht. Die Sicherheits-SPS K1 setzt sich aus einer SPS (Kanal A, K1a) und der NC-Achssteuerung (Kanal B, K1b) zusammen, die in sicherer Weise miteinander kommunizieren. Jegliche fehlerhafte Abweichung der Lasthaltung von der Soll-Position führt zu einem STO durch den Servoregler T1 und dem Einfallen der pneumatisch gelüfteten Klemmeinrichtung Q1 durch die Sicherheits-SPS K1 und dem Hilfsschütz K2. Nach einer Verzögerungszeit, die sich aufgrund der Steuerungskette (K1-K2-0V1-Q1) ergibt, wird die Achse stillgesetzt. Die Verzögerung beim Einfallen der Klemmeinrichtung führt in diesem Fall nicht zu einer Gefährdung (geringer Nachlaufweg).

- Bei SF 2 „Sicheres Hochhalten bei Spannungsausfall“ handelt es sich um das Verhalten der Steuerung unter Berücksichtigung der Unterbrechung der Energieversorgung gemäß DIN EN ISO 12100 [7], Abschnitt 6.2.11.5. Die Unterbrechung der Spannungsversorgung wird in der Sicherheits-SPS K1 erkannt (Überwachung der Netzspannung). Da die Steuerspannung für die Sicherheits-SPS K1 über eine ausreichende Pufferzeit verfügt, erfolgt das Einfallen der Klemmeinrichtung Q1 nicht durch das „langsame“ Absinken der Ausgangsspannung der Sicherheits-SPS K1, sondern schnellstmöglich durch Wegschalten des Ausgangssignals. Nach der Stillsetzung vom Motor M1 verhindert die Klemmeinrichtung Q1 ein gefahrbringendes Abstürzen der hängenden Last an der Vertikalachse.

  Hinweis:

  Auf die Pufferung der Versorgungsspannung für die Sicherheits-SPS K1 kann verzichtet werden, wenn der Ausfall der Netzspannung vom Servoregler T1 erkannt und die Klemmeinrichtung Q1 direkt angesteuert wird (z. B. durch SSM). Hierzu muss jedoch die Steuerspannung für den Servoregler T1 aus dem Gleichspannungszwischenkreis gewonnen werden.

- Hinsichtlich der sicheren Hochhaltung sind für das System zwei Fälle zu unterscheiden:

  1. Einricht- und Automatikbetrieb:

  Im Einricht- und Automatikbetrieb wird die Funktion der sicheren Hochhaltung über den Frequenzumrichter T1 in der Sicherheitsfunktion SF 1 „Sicheres Hochhalten im Einricht- und Automatikbetrieb (SOS)“ gewährleistet.

2. Spannungsausfall:

Bei Erkennung des Spannungsausfalls durch die Sicherheits-SPS K1 wird SF 2 aktiviert. Der Servoregler T1 ist bei Spannungsausfall nicht mehr in der Lage, die Vertikalachse geregelt in Position zu halten. Die Sicherheits-SPS wird aus einem gepufferten Netzteil versorgt und lässt die federkraftbetätigte Klemmeinrichtung Q1 einfallen.

Für den Fall des Spannungsausfalls stellen die Klemmeinrichtung Q1, die Ansteuerung durch das Hilfsschütz K2 und das 3/2 Wegeventil 0V1 den Funktionskanal eines Kategorie-2-Systems nach DIN EN ISO 13849-1 dar. Die erforderliche Testung der Klemmeinrichtung Q1 erfolgt alle acht Stunden in statischer und halbjährlich in dynamischer Weise durch die Sicherheits-SPS K1, den Servoregler T1, den Motor M1 und das Linearmesssystem B2. Die Testung in den vorgegebenen Zeitabständen ist im vorliegenden Anwendungsfall ausreichend, da die Klemmeinrichtung nur bei Spannungsausfall einfällt.

- Test der Klemmeinrichtung Q1 inklusive Ansteuerung durch das Hilfsschütz K2 und dem 3/2 Wegeventil 0V1:

  1. statischer Test

  Die Klemmeinrichtung Q1 inklusive Ansteuerung wird durch einen täglichen Test (bzw. alle acht Stunden) auf Funktion überprüft. Beim Test wird die Klemmeinrichtung Q1 über den Linearmotor M1 mit dem 1,3-fachen Lastmoment belastet. Falls die Position der Last im vorgegebenen Bereich gehalten wird, ist die ordnungsgemäße Funktion der Klemmeinrichtung Q1 gegeben. Falls die vorgegebene Position verlassen wird, muss die Klemmeinrichtung Q1 entsprechend der Betriebsanleitung überprüft oder gegebenenfalls getauscht werden. Die Position wird über das Linearmesssystem B2 erfasst.

  2. dynamischer Test

  Der dynamische Test erfolgt in regelmäßigen Abständen unter definierten Bedingungen von Geschwindigkeit und Masse (der zeitliche Testabstand ist abhängig von den betrieblichen Umgebungsbedingungen, beträgt jedoch maximal ein halbes Jahr). Kurz vor Einleitung des Bremsvorgangs durch die Klemmeinrichtung Q1 wird der Antriebsmotor M1 momentenfrei geschaltet und das 3/2 Wegeventil 0V1 abgeschaltet.

  Bei dem dynamischen Test der Klemmeinrichtung Q1 wird der Nachlaufweg ermittelt. Der ermittelte Wert wird mit den zulässigen Werten verglichen. Überschreitet ein ermittelter Wert den zulässigen Wert, darf ein Weiterbetrieb der Maschine nicht mehr möglich sein. Die Klemmeinrichtung Q1 ist ggf. auszutauschen.

  Hinweis:

  Der Test soll sicherstellen, dass sich der Nachlauf während der Betriebszeit nicht unzulässig verlängert (z. B. durch Verhärtung der Beläge, Schmutzfilm).

- Auf die Darstellung der Betriebsartenwahl wurde aus Gründen der Übersichtlichkeit verzichtet.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B nach DIN EN ISO 13849-1 sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Überdimensionierung) sind vorgesehen.

- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.

- Bei der Sicherheits-SPS K1 und dem Servoregler T1 mit integrierten Sicherheits-Teilfunktionen handelt es sich um Sicherheitsbauteile für den Einsatz in PL d, die der Kategorie 3 und den jeweiligen Produktnormen entsprechen. Der Servoregler T1 beinhaltet hier die Sicherheits-Teilfunktionen SOS, SS2 und STO.

- Das Hilfsschütz K2 besitzt zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Die Kontaktstellung wird in die Sicherheits-SPS K1 zurückgelesen und auf Plausibilität geprüft.

- Das 3/2-Wege-Ventil 0V1 hat eine Federrückstellung. Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals über das Hilfsschütz K2 erreicht. Grundlegende und bewährte Sicherheitsprinzipien in Konstruktion, Installation und Betrieb (DIN EN ISO 13849-2) werden vorausgesetzt.

- Das Linearmesssystem B2 liefert redundante Positionsinformationen (sin/cos) und ist in den Regelkreis der Lageregelung eingebunden. Das Messsystem wird am Servoregler T1 angeschlossen. Für den Bruch der mechanischen Befestigung des Lesekopfes des Linearmesssystems und für das Lösen der Maßverkörperung (Glasmaßstab) wird ein Fehlerausschluss angenommen. Der Hersteller muss für die Fehlerausschlüsse den Nachweis der Dauerfestigkeit erbringen (siehe auch DIN EN 61800-5-2, Tabelle D. 16). Des Weiteren müssen die besonderen Instandhaltungsinformationen des Herstellers eingehalten werden.

- Die Programmierung der Software (SRASW) für die Sicherheits-SPS K1 und den Servorregler T1 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 4.6.3 und gegebenenfalls Abschnitt 4.6.4 der DIN EN ISO 13849-1.

- Bei dem Datenbus zwischen dem Servoregler T1 und der Sicherheits-SPS K1 handelt es sich um ein Sicherheits-Bussystem für den Einsatz in PL d.

- Die Versorgungsspannung (Netzspannung) wird in der Sicherheits-SPS K1 zweikanalig überwacht.

Bemerkungen

- Dieses Beispiel bezieht sich auf eine Vertikalachse ohne Gewichtsausgleich, die mit einer Klemmeinrichtung ausgestattet ist. Es wird vorausgesetzt, dass der Motor M1 alleine die notwendigen Momente zum Verfahren der Achse aufbringen kann. Ein pneumatisch verfahrbares Ausgleichsgewicht kann zum Beispiel dann notwendig sein, wenn die Klemmung nicht alleine in der Lage ist, das Gewicht der hängenden Achse zu halten. Das Ausgleichsgewicht müsste in einem solchen Fall mitberücksichtigt werden.

- Darüber hinaus können in produktspezifischen Normen (C-Normen) spezielle Anforderungen zur Ausführung der Stillsetzung und Hochhaltung beschrieben sein. Diese haben dann Vorrang vor Typ-A- oder Typ-B-Normen wie z. B. DIN EN ISO 13849-1 (siehe Abschnitt Einleitung in DIN EN ISO 13849-1).

- Bemerkung zur Klemmeinrichtung Q1 bei Versagen vom Motor M1:
  Ein Motorversagen wird erkannt, bevor eine Gefährdung durch ein Herabsinken der hängenden Last entstehen kann. Die Klemmeinrichtung muss so ausgelegt sein, dass die Motorkraft zuzüglich Last stets kleiner ist als die von der Klemmeinrichtung aufgebrachte Klemmkraft.

Berechnung der Ausfallwahrscheinlichkeit

- Bei K1 handelt es sich um eine Sicherheits-SPS. Der PFH_D-Wert beträgt $9{,}0 \cdot 10^{-8}$/Stunde [H]. Die Kategorie 3 und der PL d werden vom Hersteller bestätigt.

- Der Servoregler T1 verfügt über die integrierten Sicherheits-Teilfunktionen SOS, SS2 und STO. Der PFH_D-Wert für die Sicherheits-Teilfunktionen des Servoreglers beträgt $2{,}3 \cdot 10^{-8}$/Stunde [H]. Für SF 1 muss jedoch der Leistungsteil des Servoreglers T1 noch hinzugerechnet werden, weil die Vertikalachse aktiv hochgehalten werden muss, um ein Abstürzen zu verhindern. Der Leistungsteil vom Servoregler T1 geht mit einer geschätzten $MTTF_D$ von 40 Jahren in die Berechnung der SF 1 ein [G].

- Für das Hilfsschütz K2 wird ein B_{10d}-Wert von 2 000 000 Schaltspielen [N] angegeben. Hieraus ergibt sich bei einer täglichen Betätigung sowie dem statischen Test an sechs Tagen und 50 Wochen im Jahr n_{op} = 600 Schaltspiele/Jahr. Nimmt man 20 Betätigungen durch Spannungsausfall an, ergibt sich n_{op} = 620 Schaltspiele/Jahr und $MTTF_D$ = 32 258 Jahre.

- Bei M1 handelt es sich um einen Linearmotor der Isolierstoffklasse F [3]. Die Isolierstoff-Klassentemperatur wird um 20 K unterschritten. Hierdurch wird eine Lebensdauer der Wicklung von 80 000 Stunden angenommen [1]. Die tägliche Einschaltdauer beträgt acht Stunden. Hieraus ergibt sich $MTTF_D$ = 80 000 h/(8 h · 365 Tage) = 27,3 Jahre. Es wird angenommen, dass Wicklungsfehler zum gefahrbringenden Ausfall des Motors M1 führen, sodass in diesem Fall $MTTF_D$ = MTTF gilt.

- Für das Pneumatikventil 0V1 ist gemäß Tabelle C1 der DIN EN ISO 13849-1 ein B_{10d} von 20 000 000 Schaltspielen angegeben [N]. Hieraus ergibt sich bei einer jährlichen Betätigung von 620 Schaltspielen eine $MTTF_D$ von 322 580 Jahren.

- Bei der Klemmeinrichtung Q1 handelt es sich um eine spezielle Linearbremse (Notfallbremse mit Haltebremsfunktion für lineare Bewegungen) mit einem B_{10d}-Wert von 200 000 Schaltspielen [H] für statische Belastungen. Gemäß Herstellerangabe ist die Linearbremse mindestens alle sechs Monate zu überprüfen und bei Bedarf zu reinigen. Bremskraftkontrollen (statische Tests) sind alle acht Stunden mit der 1,5-fachen zu erwartenden Belastung durchzuführen. Hinsichtlich des Einsatzes für Not-Halt-Bremsungen erfolgte die Rücksprache mit dem Hersteller. Die Schaltspielzahl für NOT-HALT (dynamisches Bremsen) beträgt 2 000 Schaltspiele [H] und dient als Schätzwert für B_{10d}. Mit einer zur sicheren Seite hin abgeschätzten Betätigungshäufigkeit von 20 pro Jahr ergibt sich $MTTF_D$ = 1 000 Jahre. Für SF 2 ist die Klemmeinrichtung in einer Kategorie-2-Struktur angeordnet. Die Tests erfolgen wie bereits beschrieben.

  Hinweis:

  Gemäß DIN EN ISO 13849-1, Abschnitt 4.5.4 ist für Kategorie 2 eine Anforderungsrate ≤ 1/100 der Testrate Bedingung und $MTTF_{DTE}$ muss größer sein als 0,5 · $MTTF_D$ des Funktionskanals. Die Testrate (100-mal häufiger als die Anforderung der Sicherheitsfunktion) wird in SF 2 nicht eingehalten. Daher wurde für das Kategorie-2-Subsystem ein Aufschlag von 10 % addiert. Dies entspricht einer Worst-case-Abschätzung, die im IFA Report beschrieben wird (siehe IFA Report 2/2017, Abschnitt 6.2.14, S. 54, und Abschnitt 4 des SISTEMA-Kochbuchs 4).

- Für das Linearmesssystem B2 gibt der Hersteller eine Ausfallrate von 1,5 · 10^{-6}/Stunde [H] an. Eine Verteilung der Fehler in ungefährliche und gefährliche Ausfälle ist nicht bekannt. In diesem Fall erfolgt eine Abschätzung zur sicheren Seite, sodass alle möglichen Fehler als gefährlich angesehen werden. Der DC-Wert wird aufgrund der ständigen Überwachung durch den Frequenzumrichter T1 auf 99 % angesetzt. Unter Berücksichtigung des DC-Werts von 99 % ergibt sich eine gefahrbringende Ausfallwahrscheinlichkeit von 1,5 · 10^{-8}/Stunde. Es werden die Anforderungen der Kategorie 3 erfüllt.

- Für die Quantifizierung des Kategorie-2-Subsystems von SF 2 sind $MTTF_D$ -Werte für die einzelnen Blöcke erforderlich. Da für den Servoregler T1 und das Linearmesssystem B2 nur jeweils ein PFH-Wert vorhanden ist, gilt näherungsweise der Ansatz $MTTF_D = 1/PFH_D$ (siehe hierzu SISTEMA-Kochbuch 4, Abschnitt 2). Für das Linearmesssystem B2 ergibt sich $MTTF_D$ = 7 610 Jahre. Für den Servoregler T1 (Leistungsteil + Regler) ergibt sich die Ausfallwahrscheinlichkeit zu $MTTF_D = (1/40 + 1/4\,942)^{-1}$ Jahre = 39,6 Jahre.

- Für den DC-Wert des Hilfsschützes K2 kann ein Wert von 99 % angegeben werden, da stets eine Rücklesung in die Sicherheits-SPS K1 erfolgt.

- Für den DC-Wert des Linearmotors M1 wird ein Wert von 60 % angenommen, weil eine Fehlererkennung durch den Prozess vorliegt.

- Das Pneumatikventil 0V1 wird über den Druckschalter S1 auf seine Funktion getestet (DC-Wert = 99 %).

- Für die Klemmeinrichtung Q1 erfolgt für den DC-Wert ein Ansatz von 60 % aufgrund der statischen und dynamischen Testung.

- Für das Subsystem Lageregelung oder Klemmeinrichtung der Sicherheitsfunktion SF 1 mit $T1_{Leistungsteil}$, M1/K2, 0V1, Q1 sind ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache vorhanden (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10).

- Für die Sicherheitsfunktion SF 1 „Sicheres Hochhalten im Einricht- und Automatikbetrieb (SOS)“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme K1/T1/B2/Lageregelung oder Klemmeinrichtung ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle PFH_D von $3{,}1 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 2 „Sicheres Hochhalten bei Spannungsausfall“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}1 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Literatur

[1] *Farschtschi, A.*: Elektromaschinen in Theorie und Praxis. 2. Aufl. VDE, Berlin 2001

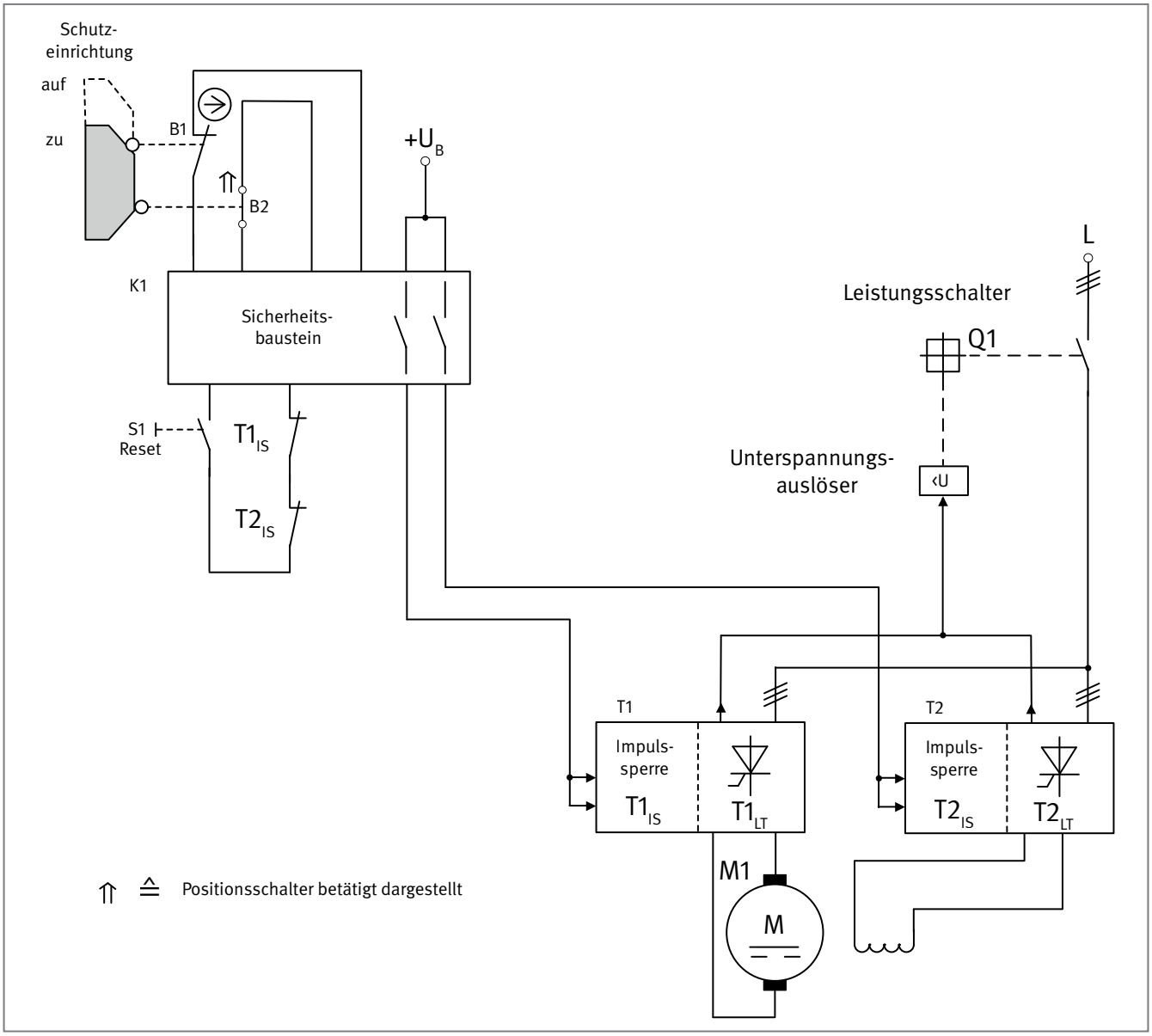
[2] Fachbereichs-Informationsblatt Nr. 005. Schwerkraftbelastete Achsen – Vertikalachsen. Ausg. 9/2012. Hrsg.: Fachbereich Holz und Metall der Deutschen Gesetzlichen Unfallversicherung, Mainz. https://www.bghm.de/fileadmin/user_upload/Arbeitsschuetzer/Praxishilfen/Fachbereichs-Informationsblaetter/005_FBHM-MAF_Vertikalachsen.pdf

[3] DIN EN 60085 (VDE 0301-1) 2008-08: Elektrische Isolierung, Thermische Bewertung und Bezeichnung (IEC 60085:2007) Deutsche Fassung EN 60085:2008

[4] *Hauke, M.; Apfeld, R.*: Das SISTEMA-Kochbuch 4. Wenn die vorgesehenen Architekturen nicht passen. Version 1.0 (DE). Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2012. www.dguv.de, Webcode: d109240

Beispiel 15: Sicherheitsbezogene Stoppfunktion STO in Gleichstromantrieben, eingeleitet durch eine bewegliche trennende Schutzeinrichtung – PL d

Abbildung A.30:
Prinzipschaltbild der Antriebssteuerung



Sicherheitsfunktion

- SF 1: Das Öffnen der beweglich trennenden Schutzeinrichtung führt zum STO des Gleichstromantriebs.

Funktionsbeschreibung

- Die Absicherung der Gefahrenstelle erfolgt durch eine beweglich trennende Schutzeinrichtung. Das Öffnen der Schutzeinrichtung wird durch die Positionsschalter B1 und B2 erfasst und in einem Sicherheitsbaustein K1 ausgewertet. Über die Freigabepfade des Sicherheitsbausteins K1 werden in den Gleichstromstellern T1 und T2 für den Ankerstrom (T1) und für das Erregerfeld (T2) jeweils die Eingänge der Impulssperre zweikanalig abgeschaltet. Im Gleichstrommotor M1 wird dadurch der Aufbau eines Drehmoments verhindert.

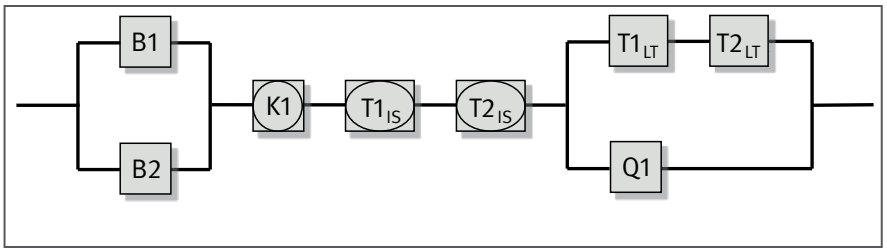


Abbildung A.31:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 15

- Der drehstromgespeiste Gleichstromantrieb wird funktional durch eine SPS gesteuert. Die SPS selbst ist nicht an der Sicherheitsfunktion beteiligt und ist nicht in Abbildung A.30 dargestellt. Das Prinzipschaltbild (Abbildung A.30) beschränkt sich auf die sicherheitsrelevante Steuerung, die der funktionalen Steuerung übergeordnet ist.

- Die Gleichstromsteller (DC-Stromrichter) T1 und T2 bestehen jeweils aus einem Steuerungsteil mit redundanter Impulssperre $T1_{IS}$ und $T2_{IS}$ und einem einkanaligen Leistungsteil $T1_{LT}$ und $T2_{LT}$.

- Fehler in den Positionsschaltern B1 und B2 werden durch den Sicherheitsbaustein K1 aufgedeckt.

- Die Gleichstromsteller T1 und T2 sind intern jeweils mit einer Überwachungsfunktion der Impulssperre (Rücklesekontakte $T1_{IS}$ und $T2_{IS}$) ausgerüstet. Diese verhindern im Fehlerfall ein erneutes Starten des Antriebs, da sie im Rückführkreis des Sicherheitsbausteins K1 eingebunden sind.

- Fehler im Leistungsteil der Gleichstromsteller T1 und T2 werden durch interne Diagnosefunktionen erkannt und im Fehlerfall wird jeweils ein Fehlersignal $T1_{LT}$ bzw. $T2_{LT}$ ausgegeben. Diese Fehlersignale schalten über einen Unterspannungsauslöser den drehstromseitigen Leistungsschalter Q1 ab und dieser trennt den Gleichstrommotor vom Versorgungsnetz. Der Leistungsschalter Q1 wird nicht bei jeder Anforderung der Sicherheitsfunktion abgeschaltet, sondern ausschließlich bei Fehlern im Leistungsteil der Gleichstromsteller T1 oder T2.

  Bemerkung:

  Anders als bei Drehstrommotoren ist für den STO bei Gleichstrommotoren die Impulssperre alleine nicht ausreichend, um den Aufbau eines Drehmoments sicher zu verhindern. Aufgrund von Fehlern in den Leistungsthyristoren kann es trotz Impulssperre zu einem Stromfluss kommen, der ausreicht, um ein Drehmoment zu erzeugen. Das ist beispielsweise der Fall, wenn zwei entsprechende Thyristoren ein Diodenverhalten aufweisen. Sollte es also aufgrund eines Fehlers im Leistungsteil des Anker-Stromrichters dazu kommen, dass beim Öffnen der Schutzeinrichtung lediglich der Feldstromrichter sicher abschaltet, kann es durch die extreme Feldschwächung (Abklingen des Erregerfeldes) bei fehlerhaft fließendem Ankerstrom zu einem Durchgehen des Gleichstrommotors kommen. Um dies zu verhindern, wird bei Fehlern im Leistungsteil eines Stromrichters zusätzlich der Leistungsschalter der Netzversorgung abgeschaltet. Der Leistungsteil der Gleichstromsteller ist folglich bei der sicherheitstechnischen Betrachtung des STO mit einzubeziehen.

- Fehler im Leistungsschalter Q1 (einschließlich Unterspannungsauslöser) werden durch manuelle Tests im Rahmen der Wiederholungsprüfung in regelmäßigen Abständen (mindestens jährlich) aufgedeckt.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Steuerstromkreises), wie in den ersten Abschnitten von Kapitel 8 des IFA Reports 2/2017 beschrieben, sind vorgesehen.

- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist. Im vorliegenden Beispiel befinden sich die Komponenten K1, T1, T2 und Q1 im selben elektrischen Einbauraum. Daher ist ein Fehlerausschluss für Kurzschlüsse von Leitungen untereinander zulässig.

- Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden. Der Positionsschalter B1 ist ein bewährtes Bauteil nach DIN EN ISO 13849-2, Tabelle D.3 mit zwangsöffnenden Kontakten gemäß DIN EN 60947-5-1, Anhang K.

- Der Sicherheitsbaustein K1 erfüllt die Anforderungen der Kategorie 4 und PL e.

- Bei den Gleichstromstellern T1 und T2 handelt es sich um Geräte mit einer integrierten Impulssperre. Für die Impulssperre werden die Anforderungen der Kategorie 3 und PL d erfüllt. Der Leistungsteil von den Gleichstromstellern T1 und T2 muss separat betrachtet werden.

- Der Leistungsschalter Q1 ist ein bewährtes Bauteil gemäß DIN EN ISO 13849-2, Tabelle D.3. Über eine manuell zu implementierende Testfunktion muss der Leistungsschalter Q1 (einschließlich Unterspannungsauslöser) regelmäßig überprüft werden. Ein solcher Test kann beispielsweise im Rahmen der Wiederholungsprüfungen durchgeführt werden.

Berechnung der Ausfallwahrscheinlichkeit

- Für den Positionsschalter B1 beträgt B_{10d} 20 000 000 Schaltspiele [N]. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} zu 3 840 Zyklen/Jahr und eine $MTTF_D$ von 52 083 Jahren.

- Für den Positionsschalter B2 wird ein B_{10d} von 1 000 000 Schaltspielen [H] angegeben. Bei 240 Arbeitstagen, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 60 Minuten ergibt sich n_{op} = 3 840 Zyklen/Jahr und eine $MTTF_D$ von 2 604 Jahren.

- Der Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 4 und PL e. Die PFH_D beträgt $2{,}3 \cdot 10^{-9}$/Stunde [H].

- Der Steuerungsteil der Gleichstromsteller mit Impulssperre $T1_{IS}$ und $T2_{IS}$ ist als gekapseltes Subsystem zu betrachten. Er erfüllt die Anforderungen für Kategorie 3 und PL d. Die PFH_D beträgt jeweils $3{,}2 \cdot 10^{-7}$/Stunde [H].

- Der Leistungsteil der Gleichstromsteller $T1_{LT}$ und $T2_{LT}$ ist einkanalig ausgeführt, die $MTTF_D$ beträgt jeweils 300 Jahre [H].

- Für den Leistungsschalter Q1 wird eine B_{10d} von 5 000 Schaltspielen [H] angegeben. Bei n_{op} = 100 Zyklen/Jahr ergibt sich eine $MTTF_D$ von 500 Jahren.

- Der DC-Wert für die Positionsschalter B1 und B2 beträgt 99 % aufgrund der Plausibilitätsprüfung durch den Sicherheitsbaustein K1.

- Die Diagnosefunktionen für den Leistungsteil in den Gleichstromstellern $T1_{LT}$ und $T2_{LT}$ finden innerhalb des Gerätes kontinuierlich mit einem DC-Wert von 99 % statt. Eine Abschaltung des Leistungsschalters Q1 erfolgt, sobald ein Fehler in $T1_{LT}$ oder $T2_{LT}$ aufgedeckt wird. Die Fehlerreaktionszeit ist so kurz, dass hierdurch keine Gefährdung entsteht. Ein Verlust der Sicherheitsfunktion zwischen den Tests kann nicht vorkommen. Die Einfehlersicherheit in diesem Subsystem ist somit gewährleistet und die Anforderung der Kategorie 3 in diesem Punkt erfüllt.

- Der DC-Wert für den Leistungsschalter Q1 beträgt 90 % aufgrund der manuellen Tests während der Wiederholungsprüfungen.

- Für das Subsystem Positionsschalter B1/B2 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (70 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15), Verwendung bewährter Bauteile (5) und Umgebungsbedingungen (25 + 10).

- Für das Subsystem Gleichstromsteller $T1_{LT}/T2_{LT}$ und Leistungsschalter Q1 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10)

- Für die SF 1 ergibt sich folgende Bewertung:

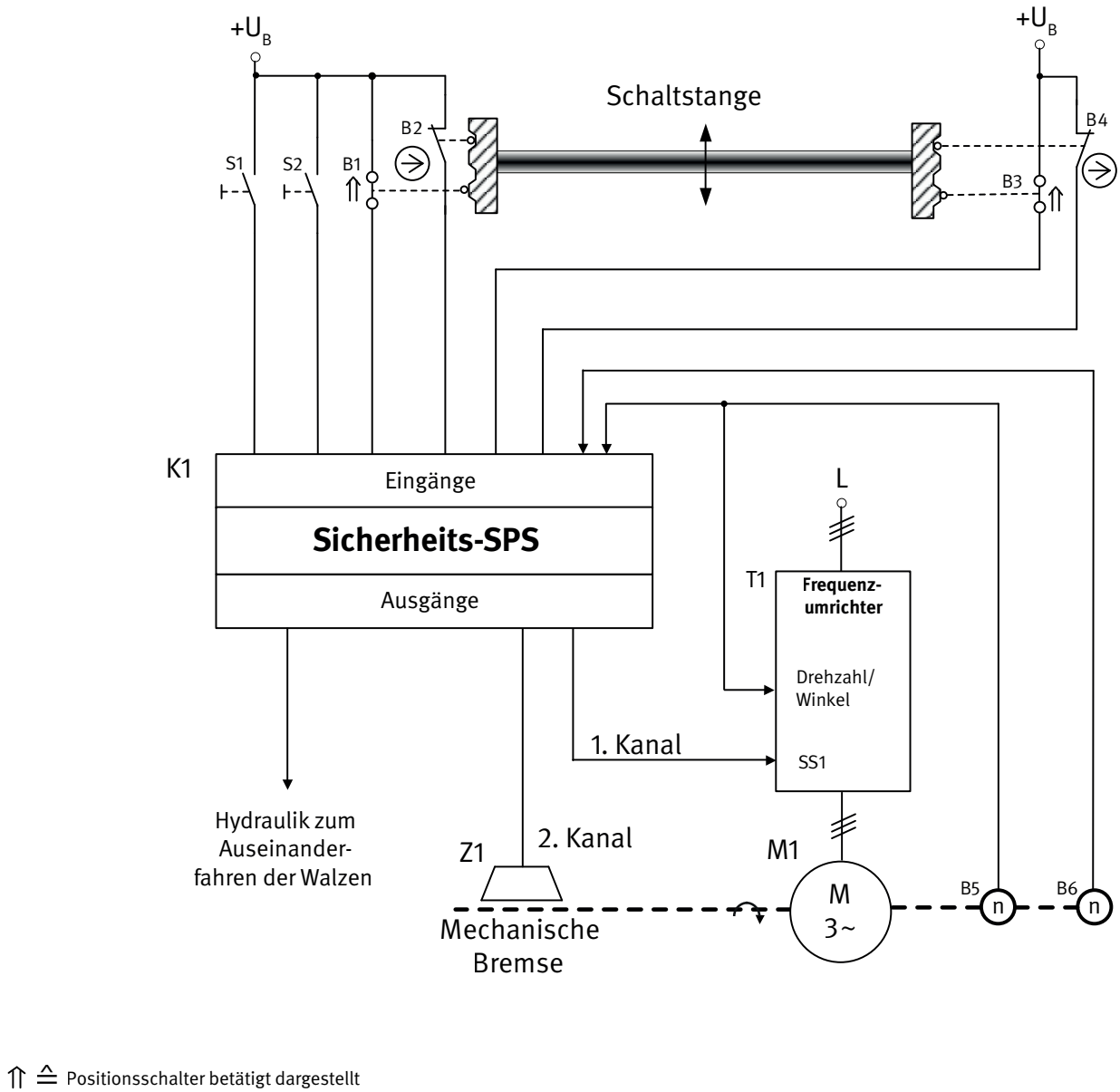
  Das Subsystem B1/B2 entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

  Das Subsystem $T1_{LT}/T2_{LT}$/Q1 entspricht Kategorie 3 mit hoher $MTTF_D$ pro Kanal (100 Jahre) und mittlerem DC_{avg} (97 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}9 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

  Für SF 1 (Das Öffnen der beweglich trennenden Schutzeinrichtung führt zum STO des Gleichstromantriebs) ergibt die Kombination der Subsysteme eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 6{,}9 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 16: Sicherheitsbezogene Stoppfunktion an Walzwerken zur Aufbereitung von Gummi und Kunststoffen – PL d

Abbildung A.32:
Sicherheitsbezogene Stoppfunktion des Walzenantriebs nach Betätigen der Schutzeinrichtung



Sicherheitsfunktionen

- SF 1: Sicherer Stopp bei Betätigung der Schutzeinrichtung (Schaltstange) mit einem Bremswinkel von maximal 60°

Funktionsbeschreibung

- Der Frequenzumrichterantrieb T1 der Walzen wird über die Sicherheits-SPS K1 gesteuert. Die Sicherheits-SPS K1 gibt den Drehzahl-Sollwert vor, steuert die Start-Stopp-Funktion des Frequenzumrichters T1 und übernimmt die Ansteuerung der mechanischen Bremse Z1.

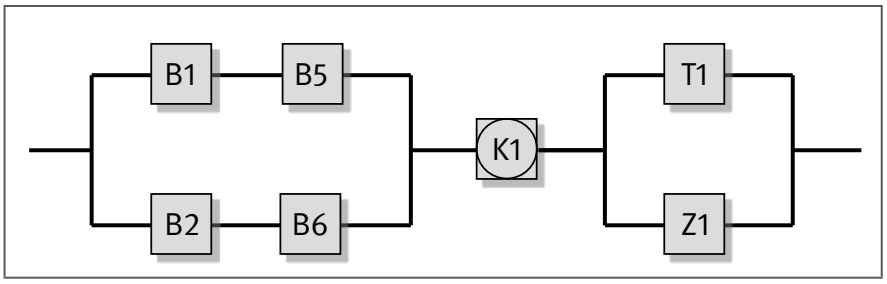


Abbildung A.33
Sicherheitsbezogenes Blockdiagramm zu Beispiel 16

- Bei Betätigen der Schaltstange aktiviert die Sicherheits-SPS K1 den Schnellstopp im Frequenzumrichter T1. Bei neuen Walzwerken nach DIN EN 1417:2015-03 muss die Befehlsgabe zum Reversieren und Auseinanderfahren der Walzen automatisch erfolgen. Das Auseinanderfahren erfolgt durch hydraulische Betriebsmittel über den Schalter S1.

  Hinweis:

  Für Altmaschinen ist die Implementierung des Schrittbetriebes zum Reversieren der Walzen oder der Betrieb der Walzen bei zeitbegrenzter Drehzahlreduzierung nachzurüsten.

- Die Absicherung der Gefahrenstellen am Walzeneinlauf erfolgt im vorliegenden Beispiel durch eine Schaltstange, die sich über die gesamte Länge der Walzen erstreckt. An den Enden der Schaltstange sind jeweils zwei Positionsschalter B1/B2 bzw. B3/B4 in Öffner-Schließer-Kombination angebracht, mit denen eine Betätigung der Schaltstange detektiert wird. Fehler in den Positionsschaltern werden durch Plausibilitätsvergleich in der Sicherheits-SPS K1 aufgedeckt.

- Nach dem Loslassen der Schaltstange geht diese wieder in die Ausgangsstellung zurück und die Kontaktelemente B1/B2 bzw. B3/B4 schließen wieder. Um einen automatischen Wiederanlauf der Maschine zu verhindern, ist eine Einrichtung zur manuellen Rückstellung S2 der Schutzeinrichtung vorzusehen.

- Die Bremsung des Walzenantriebs erfolgt über den Frequenzumrichter T1, üblicherweise im 4Q-Betrieb. Nach einem Drehwinkel von 30° oder Stillstand fällt die mechanische Bremse ein. Eine unzulässige Verlängerung des Nachlaufes wird mithilfe der Drehgeber B5 und B6 in der Sicherheits-SPS K1 aufgedeckt. Auch im Fehlerfall des Frequenzumrichters T1 darf der Nachlauf 60° nicht überschreiten.

  Hinweis:

  Bei dem Antriebs- und Bremssystem handelt es sich nicht um eine elektronische Bremse (EBS), die zur Verkürzung der Ansprechzeit einer mechanischen Bremse dient und nach dem Arbeitsstromprinzip funktioniert. Derartige elektronische Bremsen sind gemäß DIN EN 1417:2015-03 nicht zulässig.

- Um die sicherheitsbezogene Stoppfunktion des Walzenantriebs auch bei Ausfall der Netzspannung sicherzustellen, ist der Frequenzumrichter T1 in der Lage den Antrieb mithilfe der Energie aus dem Zwischenkreis gesteuert stillzusetzen. Im vorliegenden Beispiel wird auch die Sicherheits-SPS K1 mit einer Steuerspannung versorgt, die aus dem Zwischenkreis des Frequenzumrichters T1 generiert wird. Die Sicherheits-SPS K1 wird dadurch in die Lage versetzt, für eine bestimmte Zeit die erforderlichen sicherheitsrelevanten Steuerfunktionen ausüben zu können.

  Bei Ausfall der Netzspannung kann keine Rückspeisung der Bremsenergie aus dem Zwischenkreis erfolgen. In diesem Fall kann die Energie z. B. über einen Bremswiderstand in Wärme umgewandelt werden.

- Die Sicherheitsfunktion wird vor jeder Schicht (8 Stunden) automatisch durch die Steuerung überprüft. Hierzu wird auch vor jeder Schicht (8 Stunden) die mechanische Bremse Z1 mit 1,3-facher Last und eingefallener Bremse statisch auf Schlupf geprüft. Darüber hinaus findet z. B. einmal im Monat ein dynamischer Bremsentest bei verminderter Drehzahl der Walzen statt.

  Bezüglich des dynamischen Bremsentest sind die Angaben des Herstellers zu beachten.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B nach der Norm DIN EN ISO 13849-1 sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Überdimensionierung) sind vorgesehen.

- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss und Kurzschluss möglich ist.

- Bei der mechanischen Bremse Z1 handelt es sich um eine Federdruckbremse (Ruhestromprinzip). Folgende bewährte Sicherheitsprinzipien wurden angewendet:

  a) mechanische Bauteile
     – bewährte Federn
     – Sicherung von Schraubverbindungen nicht beweglicher Konstruktionsteile
     – formschlüssige oder gleichwertige Verbindungen für Konstruktionsteile im Kraftfluss
     – Nachweis der Eignung der Bremsbeläge, z. B. mehrjährige Betriebserfahrung

  b) elektrische Bauteile
     – Isolationskoordination nach Überspannungskategorie III
     – Gleichrichter, überdimensioniert (z. B. Betriebsstrom gleich 0,5-facher Nennstrom des Gleichrichters)

- Das Bremsmoment der mechanischen Bremse Z1 ist im gesamten Drehzahlbereich größer als das Antriebsmoment des Motors.

- Für die elektromechanischen Positionsschalter B1 bis B4 der Schaltstange muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageänderung zu sichern.

- Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden.

- Die Positionsschalter B2 und B4 sind bewährte Bauteile nach DIN EN ISO 13849-2, Tabelle D3 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K.

- Die Sicherheits-SPS K1 erfüllt die Anforderungen der Kategorie 4 und PL e und SIL 3 [H].

- Bei dem Frequenzumrichter T1 handelt es sich um einen Standard-Umrichter ohne integrierte Sicherheitsfunktion, der für den 4Q-Betrieb mit Netzrückspeisung geeignet ist. Die Steuerspannung wird aus dem eigenen Zwischenkreis generiert und kann auch zur Versorgung externer Stromkreise zur Verfügung gestellt werden.

- Als Geber zur Erfassung des Bremswinkels (B5, B6) kommen Standard-Inkrementalgeber zum Einsatz. Die Anbringung der Drehgeber muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z.B. Geberwellenbruch) ausgeschlossen ist.

Berechnung der Ausfallwahrscheinlichkeit

- Von den vier Positionsschaltern der Schutzeinrichtung (Schaltstange) werden nur zwei Positionsschalter (B1 und B2) als redundantes System betrachtet. Diese Betrachtung erfolgt aufgrund der Tatsache, dass eine einseitige Betätigung ausreicht, um die Sicherheitsfunktion auszulösen.

- Für den zwangsöffnenden Positionsschalter B2 beträgt der B_{10D}-Wert 20 000 000 Schaltspiele [N]. Bei 365 Arbeitstagen, 24 Arbeitsstunden pro Tag und mit 6 Betätigungszyklen am Tag (zwei pro Schicht) ergibt sich eine $MTTF_D$ von 91 324 Jahren.

- Für den Positionsschalter B1 (Schließerkontakt) beträgt der B_{10d}-Wert 100 000 Schaltspiele [H]. Bei 365 Arbeitstagen, 24 Arbeitsstunden pro Tag und mit 6 Betätigungszyklen am Tag (zwei pro Schicht) ergibt sich eine $MTTF_D$ von 456 Jahren.

- Die Drehgeber B5 und B6 haben jeweils eine $MTTF_D$ von 190 Jahren [H].

- Die Sicherheits-SPS K1 erfüllt die Anforderung für Kategorie 4, PL e und SIL 3. Die PFH_D beträgt $3{,}2 \cdot 10^{-8}$/Stunden [H].

- Der Frequenzumrichter T1 erfüllt die Anforderungen der Kategorie B. Die $MTTF_D$ beträgt 20 Jahre [H].

- Die mechanische Bremse Z1 weist einen B_{10D} von 2 000 000 Schaltspiele [H] für das statische Bremsen (Haltebremse) auf. Bei 365 Tagen, 24 Arbeitsstunden pro Tag und einer Zykluszeit von 10 Minuten ergibt sich n_{op} = 52 560 Zyklen/Jahr und eine $MTTF_D$ von 380 Jahren.
  Hinweis: Die eingesetzte Bremse Z1 ist für 2 000 dynamische Bremsungen ausgelegt.

- Der DC-Wert für die Positionsschalter B1 und B2 beträgt 99 % aufgrund der Plausibilitätsprüfung durch die Sicherheits-SPS K1.

- Der DC-Wert für die Drehgeber B5 und B6 beträgt 99 % aufgrund des Kreuzvergleichs durch die Sicherheits-SPS K1.

- Für den Frequenzumrichter T1 wird ein DC-Wert von 90 % angesetzt. Der Frequenzumrichter wird immer bei Betätigung der Schutzeinrichtung und zusätzlich alle acht Stunden hinsichtlich seiner Ausführung der Sicherheits-Teilfunktion getestet.

- Für die Federdruckbremse Z1 wird ein DC-Wert von 60 % aufgrund der statischen und dynamischen Testung in diesem Beispiel angenommen.
  Die Federdruckbremse wird automatisch durch die Steuerung alle acht Stunden der statischen Prüfung und monatlich einer dynamischen Prüfung unterzogen.

- Für das Subsystem der Positionsschalter und Drehgeber B1/B2/B5/B6 werden ausreichend Maßnahmen gegen Ausfälle gemeinsamer Ursache getroffen (70 Punkte): Trennung (15), Verwendung bewährter Bauteile (5), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingung (25+10).

- Für das Subsystem Frequenzumrichter T1 und mechanische Bremse Z1 werden ausreichende Maßnahmen gegen Ausfälle gemeinsamer Ursache getroffen (70 Punkte): Trennung (15), Diversität (20), Schutz gegen Umgebungsbedingungen (25+10).

- Für die Sicherheitsfunktion SF 1 ergibt sich folgende Bewertung: Das Subsystem B1/B2/B5/B6 entspricht Kategorie 3 mit hoher $MTTF_D$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 2{,}5 \cdot 10^{-8}$/Stunde.

  Das Subsystem T1/Z1 entspricht Kategorie 3 mit hoher $MTTF_D$ (68,9 Jahre) und niedrigem DC_{avg} (88 %). Das ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 8{,}1 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Positionsschalter B1/B2/G1/G2, Sicherheits-SPS K1 sowie Frequenzumrichter/mechanische Bremse T1/Z1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $PFH_D = 1{,}4 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur:

DIN EN 1417: Kunststoff- und Gummimaschinen – Walzwerke – Sicherheitsanforderungen (3/2015). Beuth, Berlin 2015

Anhang B:
Fachbereichs-Informationsblätter

Die folgenden Informationsblätter des Fachbereichs Holz und Metall können auf den Internetseiten der DGUV heruntergeladen den (siehe Tabelle B.1).

Nr. und Titel des Infoblattes		Internetadresse
005	Schwerkraftbelastete Achsen – Vertikalachsen	http://www.dguv.de/medien/fb-holzundmetall/publikationen-dokumente/infoblaetter/infobl_deutsch/005_vertikalachsen.pdf
050	Fluidtechnische Leistungssysteme – Hydraulische und pneumatische Motoren und Zylinder	http://www.dguv.de/medien/fb-holzundmetall/publikationen-dokumente/infoblaetter/infobl_deutsch/050_fluidleistungselemente.pdf

DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft
Holz und Metall

Nr. 005
Ausgabe 09/2012

Fachbereich-Informationsblatt

Schwerkraftbelastete Achsen

Vertikalachsen

Während bei horizontalen Bewegungen in der automatischen Fertigung, davon ausgegangen werden kann, dass im energielosen Zustand infolge Schwerkraft keine Gefährdungen für Personen entstehen, sind bei vertikalen Verfahrbewegungen, im Rahmen der Risikobeurteilung auch die Risiken des ungewollten Herabsinkens zu betrachten. Diese Gefährdungen treten besonders zutage bei Linearrobotern (Bild 1) zur Handhabung schwerer Teile, z.B. Motoren oder Getriebe, aber auch bei Gelenkarmrobotern oder innerhalb von Maschinen, z.B. bei vertikalen Achsen von Bearbeitungszentren oder Drehzentren. Wenn durch die prozessbedingt vorhandenen Haltebremsen kein ausreichender Schutz gegen ungewolltes Herabsinken erreicht wird, können steuerungstechnische Maßnahmen zur Minderung des Gefährdungsrisikos beitragen.

Bild 1: Vertikalachsen

Inhaltsverzeichnis

1 Motorbremsen

Während des fertigungstechnischen Ablaufs werden Vertikalachsen bei Stillstand üblicherweise allein durch die im Antriebsmotor eingebaute Haltebremse gehalten. Durch mechanischen Verschleiß oder Verölen kann es dazu kommen, dass das Nennhaltemoment der Bremsen unterschritten wird. Dies kann zum ungewollten Herabsinken bzw. zum Absturz der Achse führen.

Aus der Sicht des Arbeitsschutzes sind die Fälle zu betrachten, bei denen Personen Zutritt zu den Gefahrbereichen haben und bei denen ein vollständiger oder teilweiser Aufenthalt unter der Achse möglich ist, z.B. beim Teile Einlegen, beim Einrichten, bei der Instandhaltung etc. Wenn ein Versagen der Haltebremsen in diesen Situationen nicht ausgeschlossen werden kann, dann müssen Maßnahmen zur Risikominderung getroffen werden.

2 Risikobeurteilung und steuerungstechnische Maßnahmen

Entsprechend Maschinenrichtlinie [1] Anhang I ist jeder Maschinenhersteller verpflichtet, eine Risikobeurteilung zu erstellen. Eine spezielle Norm zur Beurteilung der Gefährdungen an Vertikalachsen existiert nicht. DIN EN ISO 12100 [2] gibt allgemeine Hinweise zur Durchführung der Risikobeurteilung an Maschinen einschließlich der Gefährdungsermittlung. Im Anhang B der DIN EN ISO 12100 befindet sich eine hilfreiche Tabelle mit möglichen Gefährdungen, die bei Maschinen in Betracht zu ziehen sind, u.a. infolge Schwerkraft. In Abhängigkeit vom praktischen Einsatzfall und des zu mindernden Risikos sind unter-

schiedliche sicherheitstechnische Einrichtungen zur Verhinderung des ungewollten Herabsinkens von Vertikalachsen geeignet (siehe Tabelle 3).

Die in Tabelle 1 aufgeführten Beispiele sollen eine Hilfestellung bei der Risikobeurteilung entsprechender Anlagen geben. Anhand typischer Gefährdungssituationen werden geeignete technische und organisatorische Maßnahmen zur Verhinderung des ungewollten Herabsinkens aufgezeigt. Neben den Maßnahmen in Tabelle 1 existieren in den zutreffenden EG-Richtlinien und Normen selbstverständlich weitere Anforderungen zur Arbeitssicherheit der betreffenden Maschinen, deren Gültigkeit unberührt bleibt.

3 Selbsttätig wirkende Tests zur Ertüchtigung vorhandener (Motor-)Bremsen

Die Übersicht in Tabelle 1 berücksichtigt entsprechend den Grundsätzen der Risikobetrachtung die Aufenthaltsdauer, die Schwere der möglichen Verletzung und die Wahrscheinlichkeit des Eintretens der gefährlichen Situation. Dementsprechend werden an besonders exponierten Arbeitsplätzen mit großer Aufenthaltsdauer oder häufigem Zugriff redundant wirkende Maßnahmen entsprechend DIN EN ISO 13849-1 Kategorie 3 vorgeschlagen [3]. Weitere Erläuterungen zur Umsetzung der Maßnahmen nach Kategorie 3 befinden sich in Tabelle 2.

Für andere Tätigkeiten, bei denen z.B. eine schützende Konstruktion den Zutritt unter die Vertikalachse verhindert oder die Wahrscheinlichkeit des Eintritts der Gefährdungssituation und die Aufenthaltsdauer geringer sind, kann ein zyklischer Test der nur einmal vorhandenen Motorbremse (Bremsentest) eine sehr wirkungsvolle Maßnahme sein. Dabei wird die Bremse, z.B. Motorbremse, mit einem Testmoment beaufschlagt. Dieser Test sollte entsprechend den Anforderungen von DIN EN ISO 13849-1, Kategorie 2 ausgeführt sein (siehe Tabelle 2). D.h. der Test muss selbsttätig während der normalen Produktion, z.B. während eines prozessbedingten Halts, bei Betriebsartenwechsel oder dgl. stattfinden. Wenn das nicht möglich ist, muss der Test spätestens vor Freigabe des Zugangs durch eine trennende zugehaltene Schutzeinrichtung erfolgen.

Anmerkung:

Nach DIN EN ISO 13849-1 ist für Steuerungssysteme der Kategorie 2 (Testung) die Testrate 100-mal häufiger als die Anforderung der Sicherheitsfunktion anzusetzen. Aufgrund der für Vertikalachsen gegeben Risiken, d.h. insbesondere aufgrund des Unfallgeschehens wird eine derart hohe Testrate als praktisch nicht erforderlich gesehen. Eine Berechnung des Performance-Levels ist deshalb mit den nach DIN EN ISO 13849-1 vorgesehenen vereinfachten Modellen nicht möglich und kann in diesem speziellen Fall entsprechend DIN EN ISO 13849-1, Abschnitt 6.2.2 entfallen.

4 Bremsen mit Not-Stopp-Eigenschaften

Falls die Bremsen neben sicherem Hochhalten auch Not-Stopp-Eigenschaften übernehmen sollen (z.B. bei Not-Halt Betätigung) sei darauf hingewiesen, dass die selbsttätig wirkendenden statischen Tests der Bremsen keinen vollständigen Aufschluss bringen in Bezug auf mangelnde oder zurückgehende Not-Stopp-Eigenschaften. D.h. trotz erfolgreich bestandenem statischen Bremsentest ist ein geringfügig vergrößerter Nachlaufweg bei Not-Stopp möglich, da die physikalischen Eigenschaften der Bremse dynamisch und statisch unterschiedlich wirken. Die Risikobeurteilung des Maschinenherstellers muss in diesen Fällen Aufschluss darüber geben, ob z.B. ein im Laufe der Lebensdauer geringfügig veränderter Nachlaufweg in Not-Stopp-Situationen ein nicht akzeptables Risiko darstellt.

Anmerkung: Um die Bremsen möglichst nicht mit Not-Stopp-Beanspruchungen zu beaufschlagen, sollte im Not-Halt-Fall ein Kategorie-1-Stopp (geführtes Stillsetzen) bevorzugt werden.

5 Bereits in Verkehr befindliche Anlagen

Die oben beschriebenen Maßnahmen zur Verbesserung der Arbeitssicherheit an Vertikalachsen sind vorzugsweise zur Anwendung an neu in Verkehr zu bringenden Anlagen geeignet.

Bereits in Verkehr befindliche Maschinen und Anlagen (Altanlagen) müssen den Anforderungen der Betriebssicherheitsverordnung [4] und den Unfallverhütungsvorschriften der Berufsgenossenschaften entsprechen. Die danach festzulegenden sicherheitstechnischen Maßnahmen müssen nicht zwingend dasselbe Niveau erreichen wie beim in Verkehr bringen nach Maschinenrichtlinie. Maßgebend ist der Stand der Technik beim erstmaligen in Verkehr bringen und ggf. die Fortschreibung des Standes der Technik durch die Unfallverhütungsvorschriften.

Insbesondere steuerungstechnische Maßnahmen zur Risikominderung haben sich vornehmlich erst aufgrund jüngster Erkenntnisse etabliert. Steuerungstechnische Maßnahmen lassen sich aufgrund der bereits vorhandenen Hard- und Software nicht ohne weiteres nachrüsten. Dementsprechend muss dann der Arbeitgeber nach § 4 der BetrSichV Maßnahmen treffen, um die Gefährdung so gering wie möglich zu halten. Können durch technische Schutzmassnahmen die Risiken nicht ausreichend gemindert werden, müssen organisatorische Maßnahmen den nötigen Beitrag zur Risikominderung leisten (Vermeiden des Aufenthalts unter der Achse, Unterbauen etc.). Die Beschäftigten müssen ferner durch Unterweisungen in die Lage versetzt werden, Gefährdungen hinreichend einschätzen zu können. Ein wesentliches Element in diesem Zusammenhang sollte auch das Vorsehen von wiederkehrenden Prüfungen zur Feststellung von gefährlichen Verschleißzuständen sein. Art, Umfang, Prüffristen und der Befähigungsgrad der mit der Prüfung beauftragten Personen sind vom Betreiber festzulegen. Die befähigte Person muss aufgrund ihrer fachlichen Ausbildung und Erfahrung ausreichende Kenntnisse auf dem Gebiet des zu prüfenden Arbeitsmittels haben und mit den einschlägigen staatlichen Arbeitsschutzvorschriften, berufsgenossenschaftlichen Vorschriften und allgemein anerkannten Regeln der Technik (z. B. vom Ausschuss für Betriebssicherheit ermittelte Regeln, BG-Regeln, DIN-Normen, VDE-Bestimmungen, technische Regeln anderer Mitgliedsstaaten der Europäischen Union oder anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum) soweit vertraut sein, dass sie den arbeitssicheren Zustand des Arbeitsmittels beurteilen kann.

6 Bremsen als Sicherheitsbauteil

Bremsen zum Hochhalten von Vertikalachsen können als Sicherheitsbauteil nach Maschinenrichtlinie 2006/42/EG Artikel 2 Nr. c) eingestuft werden. Voraussetzung ist, dass die Bremsen gesondert, d.h. unabhängig von der Maschine oder vom Antriebsmotor in Verkehr gebracht werden. In diesem Fall müssen die für Maschinen geltenden Konformitätsbewertungsverfahren angewendet werden, u.a. EG-Konformitätserklärung und CE-Zeichen.

Für Motorbremsen gelten diese Bestimmunen nicht, da sie durch den Einbau im Antriebsmotor nicht gesondert in Verkehr gebracht werden.

In diesem Zusammenhang sei darauf hingewiesen, dass durch Prüfungen und Zertifizierungen nach Prüfgrundsatz Nr. GS-MF-28 der Nachweis einer betriebsbewährten Bremse (Kategorie 1, PLc) zertifiziert werden kann [5].

7 Zusammenfassung und Anwendungsgrenzen

Die in diesem Fachbereich-Informationsblatt angegebenen Maßnahmen zur Arbeitssicherheit sind das Ergebnis von Beratungen im Fachbereich Holz und Metall hinsichtlich einer verbesserten Arbeitssicherheit bei Tätigkeiten an oder in der Nähe von Vertikalachsen durch praxisnahe steuerungstechnische Maßnahmen gegen ungewolltes Herabsinken durch die Schwerkraft. Das Informationsblatt beruht auf Erfahrungen der Hersteller von Industrierobotern einschließlich Linearrobotern und Handhabungssystemen, der Antriebs- und Steuerungshersteller sowie der Betreiber dieser Systeme insbesondere aus dem Automobilbau und des Fachbereiches Holz und Metall. Des Weiteren sind die Ergebnisse der Beratungen im Verein Deutscher Werkzeugmaschinenfabriken (VDW) eingeflossen.

Das Informationsblatt zeigt typische Gefahrensituationen in Verbindung mit Vertikalachsen und beschreibt geeignete Ansätze zur Risikominderung durch steuerungstechnische Maßnahmen. Andere, in diesem Merkblatt nicht beschriebene Maßnahmen gegen ungewolltes Herabsinken bleiben unberührt.

Betrachtet werden elektromotorisch angetriebene Vertikalachsen sowie geneigte Achsen mit in den Motor integrierter Bremse oder externer Bremse, die bei Versagen der Bremse schwerkraftbedingt herabsinken können. Relevante Anforderungen aus EG-Richtlinien und sonstigen Regeln der Technik bleiben unberührt. Die Entwicklung neuer Technologien sowie gleichwertige Lösungen werden durch dieses Informationsblatt nicht behindert. Die Übertragbarkeit der Erkenntnisse auf Maschinen und maschinelle Anlagen mit ähnlichen Gefährdungen wird nicht ausgeschlossen.

Die Maßnahmen können vorzugsweise Anwendung finden bei neu in Verkehr zu bringenden Anlagen. Auf Besonderheiten bei bereits in Verkehr befindlichen Anlagen wird gesondert eingegangen. Die Inhalte dieses Informationsblatt sind vorgesehen zur Einspeisung in das technische Regelwerk bzw. sind bereits eingeflossen.

Der Fachbereich Holz und Metall setzt sich u. a. zusammen aus Vertretern der Unfallversicherungsträger, Staatlichen Stellen, Sozialpartner, Herstellern von Maschinen sowie Betreibern. Dieses Informationsblatt beruht auf dem durch den Fachbereich zusammengeführten Erfahrungswissen auf dem Gebiet der Vertikalachsen und insbesondere den schwerkraftbelasteten Achsen.

Dieses Fachbereich-Informationsblatt wurde vom Fachbereich Holz und Metall, Sachgebiet Maschinen, Anlagen, Fertigungsautomation und -gestaltung erstellt. Dieses Fachbereich-Informationsblatt ersetzt das Fachausschuss-Informationsblatt Entwurf 07/2011. Weitere Informationsblätter vom Fachbereich Holz und Metall stehen im Internet zum Herunterladen bereit [6].

Zu den Zielen der Fachbereich-Informationsblätter siehe Fachbereich-Informationsblatt Nr. 001.

Literatur:

[1] Richtlinie 2006/42/EG (Maschinenrichtlinie). Amtsblatt der Europäischen Gemeinschaften Nr. L 157/24.

[2] DIN EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze –Risikobeurteilung und Risikominderung. März 2011

[3] DIN EN ISO 13849-1: Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze. Dezember 2008

[4] Verordnung über Sicherheit und Gesundheitsschutz bei der Bereitstellung von Arbeitsmitteln und deren Benutzung bei der Arbeit, über die Sicherheit beim Betrieb überwachungsbedürftiger Anlagen und über die Organisation des betrieblichen Arbeitschutzes (Betriebssicherheitsverordnung – BetrSichV). BGBl. I S. 3777 - 27. September 2002. Stand 2004

[5] Prüfgrundsatz Nr. GS-MF-28 Notfallbremsen mit Haltebremsfunktion für lineare Bewegungen. Prüf- und Zertifizierungsstelle Maschinen und Fertigungsautomation im DGUV Test, Wilhelm-Theodor-Römheld-Strasse 15, 55130 Mainz. (Inhaltlich gleichlautend vorhanden bei IFA).

[6] Internet: www.dguv.de/fb-holzundmetall Publikationen

Bildnachweis:

Die im Fachbereich-Informationsblatt gezeigten Bilder wurden freundlicherweise zur Verfügung gestellt von:

Bild 1: Fachbereich Holz und Metall

Herausgeber:

Fachbereich Holz und Metall der DGUV
Sachgebiet Maschinen, Anlagen, Fertigungsautomation und -gestaltung
Postfach 37 80
55027 Mainz

Tabelle 1: Typische Gefährdungssituationen und mögliche Schutzmaßnahmen

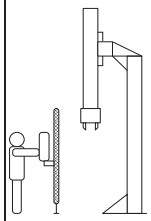
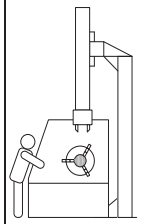
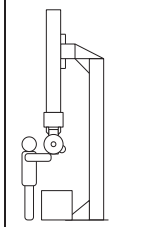
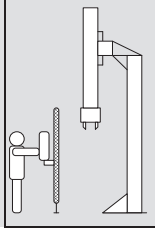
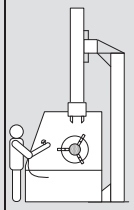
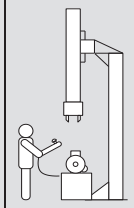
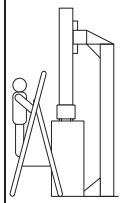
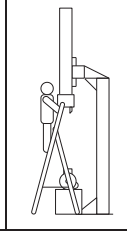
Betriebs-art	Gefährdungssituation/ Bestimmungsgemäße Verwendung		Schutzmaßnahmen	
			Technische	Organisatorische
Automatik-Manueller Eingriff A1		Die Vertikalachse befindet sich während des manuellen Eingriffs in einer für den Bediener gefahrlosen Position (Zugangsgesicherter Bereich).	- Für trennende Schutzeinrichtungen sind Zuhaltungen vorzusehen. - Bei Zugang muss das unerwartete Anlaufen der Vertikalachse sicher verhindert sein [1)]	- Warnschild an der Maschine/Anlage: „Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last hinweisen
A2		Die Vertikalachse befindet sich innerhalb des Gefährdungsbereiches Ein Aufenthalt unter der Vertikalachse mit dem ganzen Körper ist durch die Maschinen-/Anlagenkonstruktion verhindert und nicht vorgesehen. Eine Gefährdung besteht für die oberen Gliedmaßen mit geringer Aufenthaltsdauer.	- Zyklischer Test der Bremseinrichtung durch die Maschinensteuerung entspr. DIN EN ISO 13849-1, Kategorie 2 (siehe Tabelle 2). - Das unerwartete Anlaufen der Vertikalachse muss sicher verhindert sein [1)].	- Warnschild an der Maschine/Anlage: „ Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last sowie auf qualifiziertes Personal hinweisen. - Abnahmetest mittels Formblatt durch den Anlagenhersteller hinsichtlich der Wirksamkeit des Bremsentest.
A3		Die Vertikalachse befindet sich innerhalb des Gefährdungsbereiches Ein Aufenthalt unter der Vertikalachse kann nicht verhindert werden (z.B. bestimmungsgemäße Bestückungs- oder Montageaufgaben).	- Redundante Einrichtung zur Absturzsicherung entspr. DIN EN ISO 13849-1, Kategorie 3, PLc (siehe Tabelle 2) . - Das unerwartete Anlaufen der Vertikalachse muss sicher verhindert sein [1)].	- Warnschild an der Maschine/Anlage: „Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last sowie auf qualifiziertes Personal hinweisen. Den Aufenthalt unter der Vertikalachse soweit wie möglich einschränken.
Einrichten oder Programmieren E1		Die Vertikalachse befindet sich während des Einrichtens in einer für den Bediener gefahrlosen Position (Zugangsgesicherter Bereich).	- Für trennende Schutzeinrichtungen sind Zuhaltungen vorzusehen. - Bei Zugang muss das unerwartete Anlaufen der Vertikalachse sicher verhindert sein [1)].	- Warnschild an der Maschine/Anlage: „Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last hinweisen

Tabelle 1: (fortgesetzt)

Betriebs-art	Gefährdungssituation/ Bestimmungsgemäße Verwendung		Schutzmaßnahmen	
			Technische	**Organisatorische**
E2		Die Vertikalachse wird im Einrichtbetrieb verfahren und befindet sich innerhalb des Gefährdungsbereiches. Ein Aufenthalt unter der Vertikalachse mit dem ganzen Körper ist durch die Maschinen-/Anlagenkonstruktion verhindert und nicht vorgesehen. Eine Gefährdung besteht für die oberen Gliedmaßen mit geringer Aufenthaltsdauer.	- Maßnahmen für Einrichtbetrieb entspr. zutreffender Norm, z.B. DIN EN ISO 10218-1, DIN EN 12417 (Abschließbarer Betriebsartenwahlschalter, Reduzierte Geschwindigkeit + Zustimmungseinrichtung/ Sicher reduzierte Geschwindigkeit…) - Zyklischer Test der Bremseinrichtung durch die Maschinensteuerung entspr. DIN EN ISO 13849-1, Kategorie 2 (siehe Tabelle 2).	- Warnschild an der Maschine/Anlage: „Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last sowie auf qualifiziertes Personal hinweisen. - Abnahmetest mittels Formblatt durch den Anlagenhersteller hinsichtlich der Wirksamkeit des Bremsentest.
E3		Die Vertikalachse wird im Einrichtbetrieb verfahren und befindet sich innerhalb des Gefährdungsbereiches. Ein Aufenthalt unter der Vertikalachse mit dem ganzen Körper kann nicht verhindert werden, jedoch bei geringer Aufenthaltsdauer.	- Maßnahmen für Einrichtbetrieb entspr. zutreffender Norm, z.B. EN ISO 10218-1, DIN EN 12417 (Abschließbarer Betriebsartenwahlschalter, Reduzierte Geschwindigkeit + Zustimmungseinrichtung/ Sicher begrenzte Geschwindigkeit…) - Zyklischer Test der Bremseinrichtung durch die Maschinensteuerung entspr. DIN EN ISO 13849-1, Kategorie 2 (siehe Tabelle 2). - Wenn in Ausnahmefällen mit einer hohen Aufenthaltsdauer im Gefahrbereich zu rechnen ist und wenn sich der Aufenthalt unter der Vertikalachse nicht vermeiden lässt, sind Maßnahmen entspr. DIN EN ISO 13849-1, Kategorie 3, PLc vorzusehen (siehe Tabelle 2).	- Warnschild an der Maschine/Anlage: „Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last sowie auf qualifiziertes Personal hinweisen. - Abnahmetest mittels Formblatt durch den Anlagenhersteller hinsichtlich der Wirksamkeit des Bremsentest.
Wartung, Reparatur, Reinigung W1		An der Vertikalachse oder in unmittelbarer Nähe werden Wartungs-, Reinigungs- oder Reparaturarbeiten durchgeführt. Sicheres Unterbauen der Vertikalachse und/oder Anhängen ist mit vertretbarem Aufwand möglich.	- Die für Wartung/Reparatur/Reinigung geltenden Bestimmungen beachten, z.B. abschließbarer Hauptschalter. - Unterbauen oder, sofern noch möglich unterste Endlage anfahren	- Warnschild an der Maschine/Anlage: „ Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last hinweisen - Maßnahmen zum Sicheren Unterbauen beschreiben - Hauptschalter ausschalten und abschließen
W2		An der Vertikalachse oder in unmittelbarer Nähe werden Wartungs-, Reinigungs- oder Reparaturarbeiten durchgeführt. Sicheres Unterbauen der Vertikalachse und/oder Anhängen und/oder Anhängen ist nicht mit vertretbarem Aufwand möglich.	- Die für Wartung/Reparatur/Reinigung geltenden Bestimmungen beachten, z.B. abschließbarer Hauptschalter. - Automatische oder elektromechanisch bzw. manuell betätigbare Vorrichtung zum sicheren Festsetzen der Achse in definierten Positionen, z.B. Absteckeinrichtung - Eindeutige Kennzeichnung der Stellungen „Verriegelt/Entriegelt“. - Steuerungstechnische Abfrage der Stellungen „Verriegelt/Entriegelt“ und Verriegelung mit Antriebssteuerung	- Warnschild an der Maschine/Anlage: „Nicht unter der Vertikalachse aufhalten!“ - In der Betriebsanleitung auf Gefahren durch Vertikalachse und schwebende Last hinweisen - Maßnahmen zur Benutzung der Vorrichtungen zum sicheren Festsetzen (z.B. Absteckvorrichtung) beschreiben - Hauptschalter ausschalten und abschließen

[1)] Anmerkung: Steuerungskategorie und Performance Level (PL) bezüglich Schutz gegen unerwarteten Anlauf können üblicherweise den geltenden Produktnormen entnommen werden. In den meisten Fällen gilt Kategorie 3, PLd

Tabelle 2: Maßnahmenbeispiele gegen ungewolltes Herabsinken von schwerkraftbelasteten Achsen (Vertikalachsen) entsprechend DIN EN ISO 13849-1 Kategorie 2 und 3.

1 Allgemeine Anforderungen	
1.1	Die mechanischen Teile der Kraftübertragung und der Schutzeinrichtungen müssen mindestens für die auftretenden statischen und dynamischen Beanspruchungen bei 2-facher Gewichtslast ausgelegt sein.
1.2	Wird mit Hilfe steuerungstechnischer Maßnahmen entsprechend DIN EN ISO 13849-1, Kategorie 2 oder 3 ein Fehlzustand der Bremse detektiert, muss die Vertikalachse im Falle nichttrennender Schutzeinrichtungen oder nicht zugehaltener Schutztüren sofort eine gefahrlose Position anfahren, soweit dies noch möglich ist. Die Anzeigen der Maschinensteuerung müssen zur Reparatur der Bremse auffordern. Im Falle trennender Schutzeinrichtungen mit zugehaltenen Schutztüren muss eine gefahrlose Position erst nach Schutztüranforderung angefahren werden.
1.3	An der Maschine müssen gut sichtbar ein oder mehrere Warnschilder mit dem Hinweis auf Gefahren durch Vertikalachsen und schwebenden Lasten angebracht werden.
1.4	In der Betriebsanleitung müssen die Maßnahmen zur Absturzsicherung beschrieben werden. Auf die Gefahren durch Vertikalachsen und schwebenden Lasten muss hingewiesen werden.
1.5	Es müssen Maßnahmen gegen unbefugten Zugriff zu sicherheitsrelevanten Programmteilen der Steuerung vorgesehen werden z.B. durch eine der folgenden Maßnahmen: - Schreibschutz für die relevanten Programmteile - Passwortschutz - Änderungsschutz durch Schlüsselschalter
1.6	Um unnötigem Verschleiß der Haltebremsen vorzubeugen, ist soweit die Risikobetrachtung es zulässt zum betriebsmäßigen Stillsetzen sowie auch zum Stillsetzen im Notfall die Stop-Kategorie 1 (geführtes/gesteuertes Stillsetzen) entsprechend EN 60204-1 gegenüber einem Stillsetzen mit mechanischen Bremsen vorzuziehen.
2 Maßnahmen entsprechend DIN EN ISO 13849-1, Kategorie 2 (zyklischer Bremsentest)	
2.1	Der Bremsentest muss in einer für den Bediener gefahrlosen Position durchgeführt werden, z.B. sichere Parkposition, geschlossene Schutzeinrichtung.
2.2	Der Bremsentest muss selbsttätig während des normalen Betriebes der Vertikalachse wirksam werden, spätestens nach ca. 8 Stunden oder einer Schicht. Bei Anlagen, bei denen der Zugang sicher verhindert ist (z.B. durch Schutztüren mit Zuhaltungen), kann der Test unmittelbar vor dem Zutritt bei Anforderung der Schutztüre erfolgen. Anmerkung: Nach DIN EN ISO 13849-1 ist für Steuerungssysteme der Kategorie 2 (Testung) die Testrate 100-mal häufiger als die Anforderung der Sicherheitsfunktion anzusetzen. Aufgrund der für Vertikalachsen gegeben Risiken, d.h. insbesondre aufgrund des Unfallgeschehens wird eine derart hohe Testrate als praktisch nicht erforderlich gesehen. Eine Berechnung des Performance-Levels ist deshalb mit den nach DIN EN ISO 13849-1 vorgesehenen vereinfachten Modellen nicht möglich und kann entsprechend DIN EN ISO 13849-1 Abschnitt 6.2.2 entfallen.
2.3	Durch den Bremsentest muss detektiert werden, dass mindestens die im Einsatzfall maximal auftretende statische Gewichtskraft der Achse sicher gehalten wird. Die Höhe des Testmoments ist dementsprechend auszuwählen, d.h. 1,3-faches Lastmoment. Wenn mehrere Bremsen parallel eingesetzt werden (z.B. zwei Bremsen), gilt dies als erfüllt, wenn die Bremseinrichtungen nacheinander jeweils einzeln auf die einfache Gewichtskraft getestet werden.
2.4	Zur Sicherstellung einer vollständigen Entfaltung muss das Testmoment über eine ausreichende Zeitdauer anstehen.
2.5	Nach Instandsetzung einer defekten Bremse muss vor dem Weiterbetrieb ein Bremsentest steuerungstechnisch erzwungen und erfolgreich durchgeführt sein.
2.6	Hinsichtlich der Wirksamkeit des Bremsentests muss bei Inbetriebnahme der Maschine ein Abnahmetest durchgeführt und dokumentiert werden. Im Rahmen des Abnahmetests muss ein Fehlzustand der Bremseinrichtung simuliert werden und es muss die dementsprechende Fehlerreaktion kontrolliert werden. Für den Abnahmetest muss der Maschinenhersteller ein Formblatt bereitstellen und den Einsatz qualifizierten Personals vorschreiben. Der Abnahmetest muss mit vertretbarem Aufwand durchführbar sein.
3 Maßnahmen entsprechend DIN EN ISO 13849-1, Kategorie 3 (Redundante Maßnahmen zur Absturzsicherung):	
3.1	Die Einrichtungen zum Halten der Vertikalachse müssen redundant ausgeführt sein (siehe auch Tabelle 3: Zuordnung gebräuchlicher Bremseinrichtungen zu den einzelnen Betriebsarten). Kommen nicht in Tabelle 3 erfasste Einrichtungen zum Einsatz sind diese sinngemäß Tabelle 1 einzustufen.
3.2	Es müssen Maßnahmen zur partiellen Fehlererkennung entsprechend DIN EN ISO 13849-1 Kategorie 3, PLc vorgesehen werden. Diese Maßnahmen schließen ein:
3.2.1	Im Falle elektronischer Signalverarbeitungseinheiten: Zusammenstellung eines Maßnahmenkatalogs zur Erkennung und Beherrschung systematischer und zufälliger Fehler.
3.2.2	Auswertung der Signalzustände der Sensoren und Aktuatoren und Signalverarbeitungseinheiten. Fehlzustände müssen zu einer sicherheitsgerichteten Reaktion führen.
3.2.3	Wenn eine kontinuierliche Überwachung der Zustände von Teilen des Steuerungssystems technisch nicht möglich ist, müssen Zwangsdynamisierungen vorgesehen werden. Z.B.: Da Motorbremsen hinsichtlich des Zustandes der Bremse „geöffnet/geschlossen“ im allgemeinen über keine zuverlässigen Signalausgänge verfügen, kann, für den Fall, dass ein Kanal des 2-kanaligen Haltesystems mit Motorbremsen realisiert wird, eine Zwangsdynamisierung entsprechend Nr. 2) (zyklischer Bremsentest) als Maßnahme zur Fehlerkennung für die Motorbremse vorgesehen werden.

Tabelle 3: Zuordnung gebräuchlicher Bremseinrichtungen zu den einzelnen Betriebsarten

Ausführung der Bremseinrichtung(en)		**Geeignet für Betriebsart A1**	**Geeignet für Betriebsart A2**	**Geeignet für Betriebsart A3**	**Geeignet für Betriebsart E1**	**Geeignet für Betriebsart E2**	**Geeignet für Betriebsart E3**	**Geeignet für Betriebsart W1**	**Geeignet für Betriebsart W2**
		Die Vertikalachse befindet sich während des manuellen Eingriffs in einer für den Bediener gefahrlosen Position innerhalb des Gefährdungsbereichs (in Warteposition), oder in einem zugangsgesicherten Bereich.	Die Vertikalachse befindet sich innerhalb des Gefährdungsbereichs. Ein Aufenthalt unter der Vertikalachse ist durch die Maschinen-/Anlagenkonstruktion verhindert. Eine Gefährdung besteht für die oberen Gliedmaßen.	Die Vertikalachse befindet sich innerhalb des Gefährdungsbereichs Ein Aufenthalt unter der Vertikalachse kann nicht verhindert werden.	Die Vertikalachse wird im Einrichtbetrieb nicht verfahren und befindet sich während des manuellen Eingriffs in einer für den Bediener gefahrlosen Position innerhalb des Gefährdungsbereichs oder in einem zugangsgesicherten Bereich. Ein Aufenthalt unter der Vertikalachse ist aus technologischen Gründen nicht notwendig.	Die Vertikalachse wird im Einrichtbetrieb verfahren und befindet sich innerhalb des Gefährdungsbereichs Ein Aufenthalt unter der Vertikalachse ist durch die Maschinen-/Anlagenkonstruktion verhindert. Eine Gefährdung besteht für die oberen Gliedmaßen.	Die Vertikalachse wird im Einrichtbetrieb verfahren und befindet sich innerhalb des Gefährdungsbereichs Ein Aufenthalt unter der Vertikalachse kann nicht verhindert werden.	An der Vertikalachse werden Wartungs-, Reinigungs- oder Reparaturarbeiten durchgeführt. Sicheres unterbauen der Vertikalachse ist möglich.	An der Vertikalachse werden Wartungs-, Reinigungs- oder Reparaturarbeiten durchgeführt. Sicheres unterbauen der Vertikalachse ist nicht möglich.
V0	Haltebremse	✓	-	-	✓	-	-	-	-
V1	Haltebremse mit zyklischem Test	✓	✓	-	✓	✓	✓	-	-
V2	Haltebremse mit sicherheitsgerichteter Steuerung und Antriebe	✓	✓	✓*	✓	✓	✓	-	-
V3	Haltebremse + zweite Bremse	✓	✓	✓	✓	✓	✓	-	-
V4	Sichere Bremse	✓	✓	✓	✓	✓	✓	✓	✓
V5	Haltebremse + mechanischer Gewichtsausgleich	✓	✓	✓	✓	✓	✓	-	-
V6	Unterbau oder mechanischer Riegel	-	-	-	-	-	-	✓	✓
V7	Haltebremse + hydraulischer/pneumatischer Gewichtsausgleich	✓	✓	-	✓	✓	-	-	-
V8	Haltebremse + hydraulischer Gewichtsausgleich mit Bremsventil	✓	✓	✓	✓	✓	✓	✓	✓
V9	Haltebremse + sichere Klemmeinrichtung	✓	✓	✓	✓	✓	✓	✓	✓
V10	Hydraulische/pneumatische Achse + mechanischer Gewichtsausgleich	✓	✓	✓	✓	✓	✓	-	-
V11	Hydraulische/pneumatische Achse + Hydraulischer/pneumatischer Gewichtsausgleich	✓	✓	-	✓	✓	-	-	-

* V2 nur zulässig in der Betriebsart A3 mit zusätzlichem Schutz bei Energieausfall.

DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft
Holz und Metall

DGUV-Information

Fluidtechnische Leistungselemente

Hydraulische u. pneumatische Motoren und Zylinder

Ausgabe 03/2015 FB HM-050

Diese DGUV-Information gibt Hinweise für die Betrachtungsweisen von fluidtechnischen Leistungselementen (z.B. Motoren, Zylinder) in Maschinen und dient der Information von Konstrukteuren und Betreibern von Maschinen, die zum Anwendungsbereich der europäischen Maschinenrichtlinie [1] zählen.

Die DIN EN ISO 13849 Teile 1 und 2 [2, 3] stellt Anforderungen an die Gestaltung von sicherheitsbezogenen Teilen von Steuerungen für Maschinen. Entsprechend dem Anwendungsbereich der Norm beginnt eine Sicherheitsfunktion an dem Punkt, an dem sicherheitsbezogene Signale erzeugt werden und endet an den Ausgängen der Leistungssteuerungselemente (Ventile).

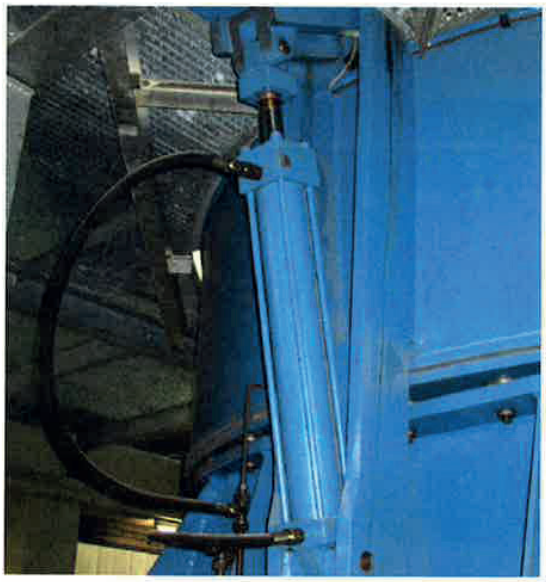


Bild 1: Leistungselement *Zylinder* an einer Prüfmaschine

1 Leistungselemente

Fluidtechnische Leistungselemente, z.B. Motoren und Zylinder, liegen außerhalb des Anwendungsbereiches der DIN EN ISO 13849-1 und zählen damit nicht zu den sicherheitsbezogenen Teilen der Steuerung (SRP/CS).

Treten im energielosen Zustand Gefährdungen auf, (z.B. eine gefahrbringende Bewegung des Leistungselementes aufgrund der Einwirkung äußerer Kräfte) so müssen die Leistungselemente zusätzlich sicherheitstechnisch ergänzt werden, z.B. durch Einsatz von entsperrbaren Rückschlagventilen, Bremsen oder Halteeinrichtungen.

Inhaltsverzeichnis

Dies wird unter Abschnitt 2 und 3 näher erläutert. Im Rahmen der Ermittlung des Performance-Levels (PL) für eine Sicherheitsfunktion werden die Leistungselemente (z.B. Motoren und Zylinder) nicht betrachtet.

Bei jeder Anwendung muss fallweise betrachtet werden, ob weitere Gefährdungen vorhanden sind oder ausgeschlossen werden können. Die arbeitsmittelspezifischen Anforderungen aus C-Normen sind ebenfalls zu berücksichtigen.

Merke:
Fluidtechnische Leistungselemente, z.B. Motoren und Zylinder, liegen außerhalb des Anwendungsbereiches der DIN EN ISO 13849-1 und zählen damit nicht zu den sicherheitsbezogenen Teilen der Steuerung (SRP/CS).

2 Äußere Kräfte

Wirken äußere Kräfte auf die Leistungselemente, wie z.B. an schwerkraftbelasteten Achsen (Drehachsen mit exzentrischen Lastmomenten, Vertikalachsen usw.), müssen die Leistungselemente ggf. mit zusätzlichen Bauteilen ausgerüstet werden, z.B. mittels zusätzlicher mechanischer Bremse.

Im Rahmen der Risikoermittlung müssen die Leistungselemente betrachtet werden. Sofern begründete Fehlerausschlüsse (z.B. ausreichende Dimensionierung) in Anspruch genommen werden können, müssen keine weiteren Maßnahmen getroffen werden.

Bei Hydromotoren ist die konstruktiv bedingte innere Leckage zu berücksichtigen.

Merke:
Die Eignung des Hydromotors bzgl. des Hochhaltens von Lasten ist zu überprüfen.

Zur Betrachtung möglicher Fehler können qualifizierte Konkretisierungen, wie z.B. die BIA-Fehlerliste 340225 für hydraulische und pneumatische Bauelemente, zu finden im BIA-Report 6/97 [4], herangezogen werden.

3 Sicherheitstechnische Ertüchtigung von Leistungselementen

Sofern der Einsatz eines Bauteils, wie z.B. Rückschlagventil, Senkbremsventil, Lasthalteventil, Leitungsbruchsicherung, lediglich zur Absicherung der schwerkraftbelasteten Achse bei Leitungsbruch dient und nicht direkt an der Ausführung einer Sicherheitsfunktion nach DIN EN ISO 13849-1 beteiligt ist, muss nicht dieses Bauteil sondern nur das Steuerventil (z.B. Richtungsventil mit Sperrmittelstellung) des Leistungselementes in die Betrachtung der Sicherheitsfunktion einbezogen werden. Gleiches gilt auch für den Einsatz einer Halteeinrichtung (Klemmkopf) für das statische Hochhalten einer Last bei Leitungsbruch.

Wird hingegen die gefahrbringende Bewegung eines Leistungselementes (z.B. Motor, Zylinder) durch eine Bremse an der Kolbenstange gesteuert abgebremst oder verhindert, so werden sowohl das Ansteuerventil der Bremse als auch die Bremse selbst in die Betrachtung der Steuerung nach DIN EN ISO 13849-1 einbezogen. Für eine Bremse sowie für deren Ansteuerung (z.B. Ventil) sind jedoch z.B. $B10_d$-Werte erforderlich.

4 Schwankungen, Verlust und Wiederkehr der Druckenergie

Die Schwankung, der Verlust und die Wiederkehr der Energie dürfen nicht zu einer gefahrbringenden Bewegung des Leistungselementes (z.B. Absenken einer Last) führen. Dies wird bereits in der Maschinenrichtlinie und in harmonisierten Normen gefordert.

Anmerkung:

Nach Abschnitt 5.2.8 der DIN EN ISO 13849-1 muss der sicherheitsbezogene Teil der Steuerung weiterhin Ausgangssignale bereitstellen oder einleiten, die anderen Teilen der Maschine ermöglichen, den sicheren Zustand aufrechtzuerhalten.

5 Zusammenfassung und Anwendungsgrenzen

Diese DGUV-Information beruht auf dem durch den Fachbereich Holz und Metall, Sachgebiet Maschinen, Anlagen, Fertigungsautomation der Deutschen Gesetzlichen Unfallversicherung DGUV zusammengeführten Erfahrungswissen auf dem Gebiet der hydraulischen Ausrüstungen von Maschinen und Anlagen.

Das vorliegende Informationsblatt wurde unter Einbeziehung des Instituts für Arbeitsschutz (IFA) der Deutschen Gesetzlichen Unfallversicherung (DGUV) erarbeitet. Es soll insbesondere der Information von Herstellern und Betreibern von Maschinen, die zum Anwendungsbereich der europäischen Maschinenrichtlinie zählen, dienen und auf die Betrachtungsweise der fluidtechnischen Leistungselementen (z.B. Motoren, Zylinder) hinweisen.

Die besonderen Bestimmungen für andere Anwendungsfälle (im Bergbau o. ä.) sind zu beachten.

Der Fachbereich Holz und Metall setzt sich u. a. zusammen aus Vertretern von Unfallversicherungsträgern, staatlichen Stellen, Sozialpartnern, Herstellern und Betreibern.

Die Bestimmungen nach einzelnen Gesetzen und Verordnungen bleiben durch dieses Informationsblatt unberührt. Die Anforderungen der gesetzlichen Vorschriften gelten uneingeschränkt.

Um vollständige Informationen zu erhalten, ist es erforderlich, die in Frage kommenden Vorschriftentexte und aktuellen Normen einzusehen.

Diese DGUV-Information ersetzt die gleichnamige Fassung, herausgegeben als Fachausschuss-Informationsblatt Ausgabe 03/2011 und enthält nur redaktionelle Änderungen. Weitere Informationsblätter vom Fachbereich Holz und Metall stehen im Internet zum Download bereit [5].

Zu den Zielen der DGUV-Information siehe DGUV-Information FB HM-001 „Ziele der DGUV-Information herausgegeben vom Fachbereich Holz und Metall".

Literatur:

[1] Richtlinie 2006/42/EG (Maschinenrichtlinie) Amtsblatt der Europäischen Gemeinschaften Nr. L 157/24 vom 09.06.2006 mit Berichtigung im Amtsblatt L76/35 vom 16.03.2007.

[2] DIN EN ISO 13849-1 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze, 2008-12

[3] DIN EN ISO 13849-2 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung, 2013-02

[4] BIA-Report 6/97: Kategorien für sicherheitsbezogene Steuerungen nach DIN EN 954-1, gebührenfreier Download unter: http://www.dguv.de/ifa/Publikationen/Reports-Download/BIA-Reports-1997-bis-1998/BIA-Report-6-97/index.jsp

[5] Internet: http://www.dguv.de/fb-holzundmetall/Publikationen oder www.bghm.de Webcode: <626>

Bildnachweis:

Die Bilder und Graphiken dieser DGUV-Information wurden freundlicherweise zur Verfügung gestellt von:

Bild 1 Institut für Arbeitsschutz (IFA)
der Deutschen Gesetzlichen Unfallversicherung DGUV,
53754 Sankt Augustin,
Deutschland

Herausgeber:

Fachbereich Holz und Metall der DGUV
Sachgebiet Maschinen, Anlagen, Fertigungsautomation
c/o Berufsgenossenschaft Holz und Metall
Postfach 3780
55027 Mainz

Anhang C:
Abkürzungsverzeichnis

Tabelle C.1 enthält die in diesem Report verwendeten Abkürzungen; Tabelle 1 (siehe Seite XX) enthält die Abkürzungen und weitere Informationen zu den Sicherheits-Teilfunktionen aus DIN EN 61800-5-2.

Tabelle C.1:
In diesem Report verwendete Abkürzungen

Abkürzung	Bezeichnung
[D]	B_{10D}- oder $MTTF_D$-Werte aus Datenbanken
[G]	Geschätzte B_{10D}- oder $MTTF_D$-Werte
[H]	B_{10D}- oder $MTTF_D$-Werte auf der Basis von Herstellerangaben
[N]	B_{10D}- oder $MTTF_D$-Werte auf der Basis von gelisteten Angaben in der Norm DIN EN ISO 13849-1
ASIC	Application-specific integrated circuit, anwendungsspezifische integrierte Schaltung
B_{10D}	Nominale Lebensdauer, die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der bis zu 10 % der betrachteten Einheiten gefährlich ausgefallen sind
BIA	Berufsgenossenschaftliches Institut für Arbeitssicherheit (heute: IFA)
CCF	Common cause failure; Ausfall infolge gemeinsamer Ursache
DC	Diagnostic coverage; Diagnosedeckungsgrad
DC_{avg}	Durchschnittlicher Diagnosedeckungsgrad (average)
DGUV	Deutsche Gesetzliche Unfallversicherung
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
EMV	Elektromagnetische Verträglichkeit
FPGA	Field programmable gate array
FMEA	Failure mode and effect analysis; Ausfalleffektanalyse
FU	Frequenzumrichter
IC	Integrated circuit, integrierte Schaltung
IFA	Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung
IGBT	Insulated-gate bipolar transistor; Bipolartransistor mit isolierter Gate-Elektrode
$MTTF_D$	Mean time to dangerous failure; mittlere Zeit bis zum gefahrbringenden Ausfall
NC	Numeric control
n_{op}	Mittlere Anzahl jährlicher Betätigungen; number of operations
PDS	Power Drive Systems
PDS(SR)	Power Drive Systems Safety Related
PFH_D	Probability of a dangerous failure per hour; Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde
PL	Performance Level
PL_r	Required Performance Level; erforderlicher Performance Level
PWM	Pulsweitenmodulation
SIL	Safety integrity level
SISTEMA	Sicherheit von Steuerungen an Maschinen
SPS	Speicherprogrammierbare Steuerung
SRASW	Safety-related application software; sicherheitsbezogene Anwender-Software
SRESW	Safety-related embedded software; sicherheitsbezogene eingebettete Software
SRP/CS	Safety related parts of control systems; sicherheitsbezogene Teile von Steuerungen
USV	Unterbrechungsfreie Spannungsversorgung