IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

7/2013

IFA Report

Sichere Antriebssteuerungen mit Frequenzumrichtern

Verfasser: Ralf Apfeld, Helmut Zilligen, Burkhard Köhler
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstr. 111
53757 Sankt Augustin
Telefon: 02241 23102
Telefax: 02241 2312234
Internet: www.dguv.de/ifa
E-Mail: ifa@dguv.de

Publikationsdatenbank: www.dguv.de/publikationen

Herausgeber: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Mittelstr. 51
10117 Berlin
Telefon: 030 288763800
Telefax: 030 288763808
Internet: www.dguv.de
E-Mail: info@dguv.de

– Juli 2013 –

Satz und Layout: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)

ISBN: 978-3-86423-071-4

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 notwendig sind. In diesen Fällen ist der Maschinenbetrieb bei aufgehobener Schutzwirkung von Schutzeinrichtungen erforderlich. Um trotzdem die Sicherheit der Beschäftigten zu gewährleisten, werden die gefahrbringenden Bewegungen dann bei sicher begrenzten Geschwindigkeiten, Drehzahlen, Drehmomenten und häufig im Tippbetrieb und/oder nur während ein Zustimmungsschalter betätigt wird, ausgeführt. Zur Realisierung der hierfür notwendigen Maschinenfunktionen wurden Sicherheitsfunktionen für Antriebssteuerungen definiert, wie z. B. STO (Sicher abgeschaltetes Moment), SLS (Sicher begrenzte Geschwindigkeit) und SS1 (Sicherer Stopp 1).

Es wird der Einsatz von Antriebssteuergeräten behandelt, die abhängig von Applikation und Risiken, Sicherheitsfunktionen in einem bestimmten Performance Level nach DIN EN ISO 13849-1 umsetzen. Die grundlegenden Sicherheitsfunktionen von Antriebssteuerungen und die Anforderungen bei deren Anwendung werden vorgestellt. Die prinzipielle Funktionsweise von Frequenzumrichtern und Gleichstromstellern wird beschrieben und das Konzept der Integration von Sicherheitsfunktionen 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 BGIA-Report 2/2008 „Funktionale Sicherheit von Maschinensteuerungen“ und setzt Grundkenntnisse über Kategorien und Performance Level voraus.

Abstract

Safe drive controls with frequency converters

Machine drives with speed control are state of the art. As on drives without speed control, variable speed of movement of a machine part frequently gives rise to a hazard against which the users of the machine must be protected. The simplest means of preventing movements during manual intervention in danger zones is the (safe) 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. Such cases require the machine to be operated with protective equipment disabled. In order to assure the user‘s safety despite this, the hazardous movements are performed in such cases at safely limited speeds and/or torques, and frequently in inching mode and/or only when an enabling switch is actuated. Safety 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 is intended for parties using drive control equipment who wish to use safety functions at a certain Performance Level to EN ISO 13849-1 in consideration of the application and risks. The basic safety functions of drive controls and the requirements relating to their use are presented. The principles of operation of frequency converters and DC-DC converters are described, and the concept of integrated safety functions explained. Examples of applied circuits are shown 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 converters and frequency converters with integral safety functions.

This report supplements BGIA Report 2/2008, „Functional safety of machine controls“, and requires a basic understanding of Categories and Performance Levels.

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. Cependant, ceci n'est fréquemment pas possible, par exemple lorsqu'il est nécessaire d'effectuer des interventions sur une machine en fonctionnement pour éliminer des défauts, procéder à des réglages ou des marches d'essai, etc. Dans ces cas, la machine doit fonctionner bien que des dispositifs de protection soient désactivés. Pour que la sécurité de l'opérateur soit malgré tout assurée, les déplacements pouvant présenter un danger pour celui-ci sont exécutés fréquemment en mode manuel à vue et / ou uniquement pendant qu'un bouton d'assentiment est actionné, à des vitesses et avec des couples limités de façon sûre. Pour la réalisation des fonctions machine nécessaires à cet effet, des fonctions de sécurité pour commandes d'entraînement, telles que STO (Suppression sûre du couple), SLS (Vitesse limitée de façon sûre), SS1 (Arrêt sûr 1) par exemple, ont été définies. Ce compte rendu s'adresse aux utilisateurs de variateurs de vitesse qui, en fonction de l'application et des risques, désirent mettre en œuvre des fonctions de sécurité ayant un Performance Level déterminé (EN ISO13849-1). Les fonctions de sécurité de base de commandes d'entraînement et les exigences qui doivent être satisfaites lors de leur utilisation sont présentées. Les principes de fonctionnement des convertisseurs de fréquence et des hacheurs sont décrits, et le concept d'intégration de fonctions de sécurité est expliqué à l'aide d'exemples de montages permettant de réaliser diverses fonctions de sécurité à des machines. Les fichiers SISTEMA correspondants pour la quantification de ces fonctions de sécurité peuvent être téléchargés gratuitement. Les exemples comportent aussi bien des convertisseurs de fréquence standards que des convertisseurs de fréquence avec fonctions de sécurité intégrées.

Ce compte rendu complète le compte rendu BGIA 2/2008 « Sécurité fonctionnelle de commandes de machines » et requiert des connaissances de base sur les catégories et les Performance Level.

Resumen

Controles de los accionamientos seguros con los convertidores de frecuencia

Los accionamientos con regulación de revoluciones en máquinas forman parte de la tecnología más avanzada. Exactamente del mismo modo que en los accionamientos sin regulación, el movimiento variable de revoluciones de un componente de la máquina a menudo conlleva un riesgo del que los operarios de máquinas deben protegerse. La solución más sencilla para evitar los movimientos durante las intervenciones manuales en los puntos peligrosos es la desconexión (segura) de la energía de los accionamientos de los motores respectivos. No obstante, esto a menudo no es posible, p. ej. cuando se requiere que la máquina esté en marcha para subsanar a averías, hacer ajustes, realizar una prueba de funcionamiento u otras intervenciones. En dichos casos, se requiere anular el efecto protector de los dispositivos de protección durante el funcionamiento de la máquina. A pesar de ello, para garantizar la seguridad del usuario, los movimientos que implican un riesgo se ejecutan a velocidades, revoluciones, pares de torsión limitados de forma segura y a menudo durante el modo por impulsos o solamente mientras esté pulsado un conmutador de autorización. Para ejecutar las funciones de la máquina necesarias, se han definido funciones de seguridad para los controles de los accionamientos, como p. ej. STO (momento de desconexión segura), SLS (velocidad limitada segura), SS1 (parada segura 1). Este informe va dirigido a los usuarios de los aparatos de control de los accionamientos que quieren emplear las funciones de seguridad que dependen de la aplicación y los riesgos en un nivel de prestaciones determinado conforme a DIN EN ISO13849-1. Se presentan las funciones de seguridad básicas de los controles de accionamiento y los requisitos para su empleo. Se describe el funcionamiento principal de los convertidores de frecuencia y los interruptores periódicos y se explica el concepto de la integración de las funciones de seguridad. En los ejemplos se muestran conmutaciones de aplicación con las que se pueden llevar a cabo diferentes funciones de seguridad en máquinas. Los archivos de SISTEMA respectivos para cuantificar estas funciones de seguridad están disponibles para descargar gratuitamente. En los ejemplos se emplean tanto convertidores de frecuencia estándares, como también convertidores de frecuencia con funciones de seguridad integradas.

Este informe es una ampliación del informe 2/2008 de BGIA „Seguridad funcional de los controles de máquinas“ y presupone unos conocimientos básicos de categorías y niveles de prestaciones.

Inhaltsverzeichnis

1 Einleitung

Mit dem BIA-Report 5/2003*) wurde die Anwendung von Frequenzumrichtern in sicherheitsgerichteten Stromkreisen beschrieben. Ausgehend von den Sicherheitsfunktionen wurde anhand von Beispielen der Einsatz von Frequenzumrichtern ohne (PDS, Power Drive Systems) und mit integrierten Sicherheitsfunktionen (PDS(SR), Power Drive Systems Safety Related), erläutert. Basis 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 IEC 61800-5-2 [3] für die Anforderungen an die Funktionale Sicherheit von elektrischen Leistungsantriebssystemen mit einstellbarer Drehzahl erforderte eine Überarbeitung und Anpassung dieses Reports. Zusätzlich wird 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 Report versteht sich insofern als Ergänzung zum BGIA-Report 2/2008 „Funktionale Sicherheit von Maschinensteuerungen“ [4].

Die hier aufgeführten Beispiele setzen voraus, dass der energielose Zustand einer Antriebssteuerung ein sicherer Zustand für die Maschine ist. Der Abschnitt 6.4 „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 Produktnorm DIN EN IEC 61800-5-2 [3] festlegt, die auf DIN EN IEC 61508 [5] basiert. Wo notwendig, wird in diesem Report daher auf die speziellen Zusammenhänge mit der DIN EN IEC 61508 [5] eingegangen. Die Gesamtbetrachtung der Sicherheitsfunktionen erfolgt jedoch immer aus Sicht des Maschinenherstellers; daher wird stets die 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.

*) Sichere Antriebssteuerungen mit Frequenzumrichtern (BIA-Report 5/2003). Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003.

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 „3-Stufen-Verfahren“ bezeichnete Reihenfolge (Abschnitt 6.1 der DIN EN ISO 12100):

- 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 erforderlichen 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] angewendet, deren Anwendungsbereich beim Sensor, also an der Schnittstelle zum technischen Prozess, beginnt, die Logik umfasst und mit dem Leistungssteuerelement – z. B. Motorschütz oder Ventil – endet. Der eigentliche Aktor, z. B. der Motor oder der Hydraulikzylinder, liegt außerhalb des Anwendungsbereichs der Norm. Diese Abgrenzung ist nachvollziehbar, sofern der Ausfall eines Aktors nicht zu einem gefährlichen Zustand führen kann. Wirken an einer Maschine jedoch äußere Kräfte, wie z. B. bei Vertikalachsen, kann der Ausfall eines Aktors (Bremse, Motor) zum Absturz der Last führen. Daher stellt sich die Frage, ob es sinnvoll ist, an die Ansteuerung eines Aktors Anforderungen in Form eines PL_r zu stellen, den Aktor selbst aber nicht zu betrachten. Die Methodik der DIN EN ISO 13849-1 lässt sich auch hier anwenden, allerdings müssen ggf. zusätzliche sicherheitsrelevante Eigenschaften (z. B. Festigkeiten) berücksichtigt werden. Diese Situation ist bisher nicht abschließend geklärt. Zusammen mit dem Fachbereich Holz und Metall der Deutschen Gesetzlichen Unfallversicherung (DGUV) hat das Institut für Arbeitsschutz der DGUV (IFA) beschlossen, in solchen Fällen den Aktor in der Sicherheitsfunktion ebenfalls zu berücksichtigen. Im Fachausschuss-Informationsblatt Nr. 050 (siehe Anhang C, Seite 105) wurde diese Vorgehensweise veröffentlicht und damit zur Diskussion gestellt.

2.2 Überlagerte Gefährdungen

Der Ersatz der DIN EN 954-1 [1] durch DIN EN ISO 13849-1 [2] erfordert aufgrund der zusätzlichen probabilistischen Betrachtung auch, überlagerte Gefährdungen durch Bewegungen zu berücksichtigen. 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. Die Methode wurde im Fachbereichs-Informationsblatt Nr. 047 beschrieben (siehe Anhang C, Seite 105). Weitere Informationen bietet auch ein Vortragsmanuskript [9].

3 Antriebssteuergeräte als sicherheitsbezogene Teile von Steuerungen

Antriebssteuergeräte, wie z. B. Frequenzumrichter 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 durch ein Netzschütz in der Energieversorgung des Antriebs oder ein Motorschütz zwischen Antriebssteuergerät und Motor realisierbar sind. Antriebssteuergeräte mit integrierten Sicherheitsfunktionen 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 also andere Maßnahmen notwendig, die für den Maschinenbediener eine vergleichbare Sicherheit gewährleisten. Dies wird z. B. durch die Anwendung der in DIN EN 61800-5-2 [3] definierten Sicherheitsfunktionen (Tabelle 1) erreicht.

Tabelle 1:
Sicherheitsfunktionen aus DIN EN 61800-5-2

Abkürzung	siehe Abschnitt	Bezeichnung englisch	Bezeichnung deutsch	Funktion
STO	3.1.1.1	Safe torque off	Sicher abgeschaltetes Moment	Motor erhält keine Energie, die eine Drehbewegung erzeugen kann; Stopp-Kategorie 0 nach DIN EN 60204-1
SS1	3.1.1.2	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	3.1.1.3	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	3.1.2.1	Safe operating stop	Sicherer Betriebshalt	Motor steht still und widersteht externen Kräften.
SLA	3.1.2.6	Safely-limited acceleration	Sicher begrenzte Beschleunigung	Das Überschreiten eines Beschleunigungsgrenzwerts wird verhindert.
SAR	---	Safe acceleration range	Sicherer Beschleunigungsbereich	Die Beschleunigung des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
SLS	3.1.2.2	Safely-limited speed	Sicher begrenzte Geschwindigkeit	Das Überschreiten eines Geschwindigkeitsgrenzwerts wird verhindert.
SSR	---	Safe speed range	Sicherer Geschwindigkeitsbereich	Die Geschwindigkeit des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
SLT	3.1.2.3	Safely-limited torque	Sicher begrenztes Moment	Das Überschreiten eines Drehmoment-/Kraftgrenzwerts wird verhindert.
STR	---	Safe torque range	Sicherer Momentenbereich	Das Drehmoment des Motors wird innerhalb spezifizierter Grenzwerte gehalten.
SLP	3.1.2.5	Safely-limited position	Sicher begrenzte Position	Das Überschreiten eines Positionsgrenzwerts wird verhindert.
SLI	3.1.2.4	Safely-limited increment	Sicher begrenztes Schrittmaß	Der Motor wird um ein spezifiziertes Schrittmaß verfahren und stoppt anschließend.
SDI	3.1.2.7	Safe direction	Sichere Bewegungsrichtung	Die nicht beabsichtigte Bewegungsrichtung des Motors wird verhindert.
SMT	3.1.2.8	Safe motor temperature	Sichere Motorentemperatur	Das Überschreiten eines Motortemperaturgrenzwerts wird verhindert.

Tabelle 1: Fortsetzung

Abkürzung	siehe Abschntt	Bezeichnung englisch	Bezeichnung deutsch	Funktion
SBC	3.1.2.9	Safe brake control	Sichere Bremsen-ansteuerung	Sichere Ansteuerung einer externen Bremse
SCA	3.1.2.10	Safe CAM	Sichere Nocken	Während sich die Motorposition in einem spezifizierten Bereich befindet, wird ein sicheres Ausgangssignal erzeugt.
SSM	3.1.2.11	Safe speed monitor	Sichere Geschwindig-keitsüberwachung	Während die Motordrehzahl niedriger als ein spezifizierter Wert ist, wird ein sicheres Ausgangssignal erzeugt.

Diese in der Norm definierten Sicherheitsfunktionen stellen eine Art Basis dar. Die Hersteller von PDS(SR) bieten darüber hinaus eine Vielzahl weiterer Sicherheitsfunktionen an. Eine Beschreibung einiger der Basisfunktionen erfolgt in Abschnitt 3.1.

Die vorstehend genannten Sicherheitsfunktionen 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.

3.1 Beschreibung der Sicherheitsfunktionen

Unter einer Sicherheitsfunktion wird nach DIN EN ISO 12100-1 [7] eine Funktion einer Maschine verstanden, deren Ausfall zur unmittelbaren Erhöhung des Risikos führt. Eine Sicherheitsfunktion in diesem Sinne wird üblicherweise durch die Komponenten Sensor, Logik und Ausgang ausgeführt[1]. Die in diesem Report behandelten Antriebssteuergeräte decken dabei den Teil Ausgang ab, je nach Implementierung einschließlich der Logik. Eigentlich sind es also nur Teil-Sicherheitsfunktionen. Eine solche Bezeichnung ist in der Sicherheitstechnik jedoch nicht gebräuchlich.

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.

Die Benutzerinformation eines PDS(SR) sollten diese Informationen enthalten.

Die Sicherheitsfunktionen lassen eine Einteilung in Stoppfunktionen und „andere Sicherheitsfunktionen“ zweckmäßig erscheinen.

Die folgenden Beschreibungen der Sicherheitsfunktionen 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 [10] 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.

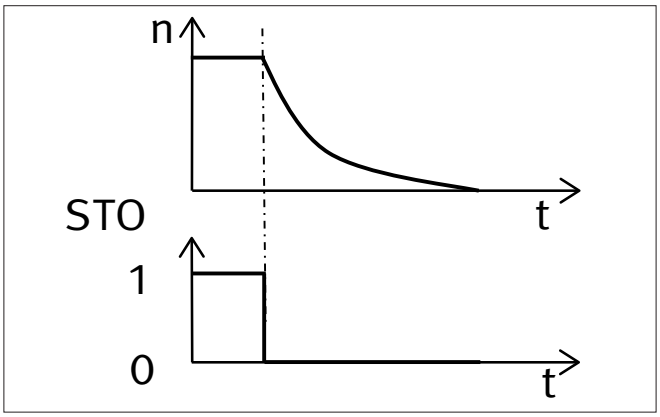
3.1.1.1 Sicher abgeschaltetes Moment (Safe torque off, STO)

„Dem Motor wird keine Energie zugeführt, die eine Drehung (oder bei einem Linearmotor eine Bewegung) verursachen kann. Das PDS(SR) liefert keine Energie an den Motor, die ein Drehmoment (oder bei einem Linearmotor eine Kraft) erzeugen kann.“ [3].

[1] 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“

In Abbildung 1 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von STO und der Motordrehzahl gezeigt. Die Sicherheitsfunktion STO entspricht einem ungesteuerten Stillsetzen nach DIN EN 60204-1, Stopp-Kategorie 0. Sie kann angewendet werden, wenn die Abschaltung der Energie zur Verhinderung eines unerwarteten Anlaufs erforderlich ist. Eine Überwachung der Stillstandsposition erfolgt nicht. Sollte die Sicherheitsfunktion STO während des Betriebs aktiviert werden, dann trudelt der Motor ungebremst aus.

Abbildung 1:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion STO
(Safe torque off, sicher abgeschaltetes Moment)



Bei vorhandenen äußeren Kräften (z. B. durch die Schwerkraft bei Vertikalachsen) können zur Risikominderung zusätzliche Maßnahmen wie z. B. mechanische Bremsen erforderlich sein (siehe auch Abschnitt 6.4).

Elektronische Einrichtungen und Schütze (unzureichender Kontaktabstand), mit denen Sicherheitsfunktionen umgesetzt werden, bilden keinen ausreichenden Schutz gegen elektrischen Schlag und es können zusätzliche Maßnahmen zur galvanischen Trennung erforderlich sein.

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

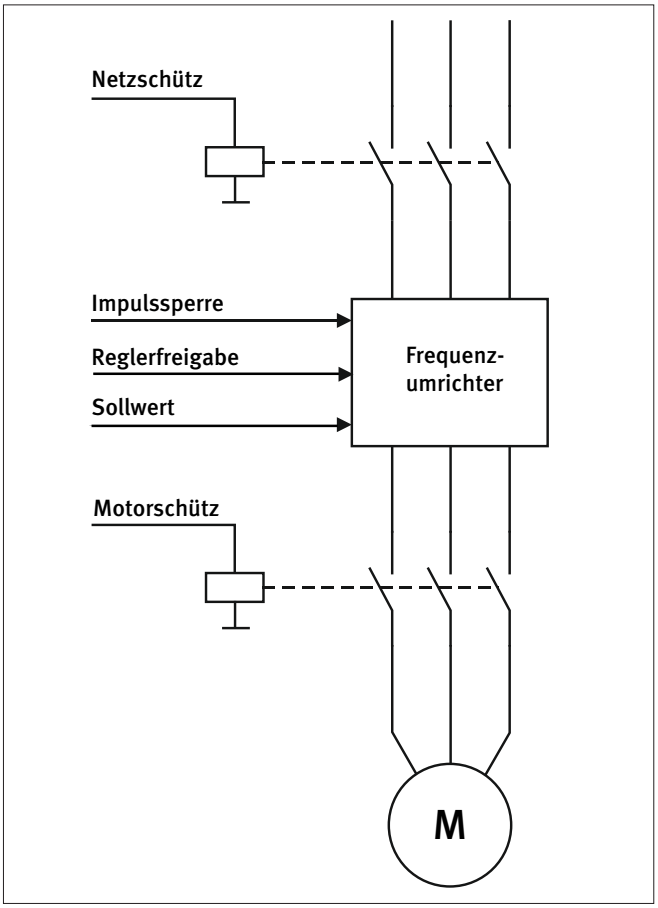
- Schütz zwischen Netz und Antriebssystem (Netzschütz)
- Schütz zwischen Leistungsteil und Antriebsmotor (Motorschütz)
- Impulssperre (Sperren der Ansteuerung der Leistungshalbleiter innerhalb des Frequenzumrichters)
- Reglerfreigabe
- Sollwert

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)

„Das PDS(SR) führt eine dieser Funktionen aus:

a) entweder Auslösen und Steuern der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der STO-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt[2], oder

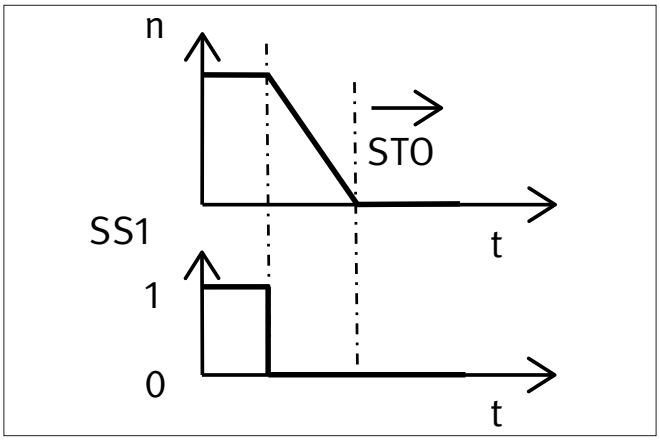
b) Auslösen und Überwachen der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der STO-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt, oder

c) Auslösen der Motorverzögerung und nach einer anwendungsspezifischen Zeitverzögerung Auslösen der STO-Funktion.“ [3].

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

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

Abbildung 3:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SS1 (Safe stop 1, sicherer Stopp 1)



Bei der Umsetzung der Sicherheitsfunktion SS1 gemäß c), 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 SS1-Funktion in dieser Art nicht geeignet.

Wird dagegen die Sicherheitsfunktion SS1 mit Überwachung der Bremsrampe (Größe der Motorverzögerung) (b) realisiert, 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. Deshalb ist Lösung b) zwingend erforderlich, durch einen fehlerhaften Antriebsregler kann eine Beschleunigung anstelle der Verzögerung nicht ausgeschlossen werden. Dies wird durch die Überwachung der Bremsrampe schnell erkannt und als Fehlerreaktion wird STO eingelegt.

3.1.1.3 Sicherer Stopp 2 (Safe stop 2, SS2)

„*Das PDS(SR) führt eine dieser Funktionen aus:*

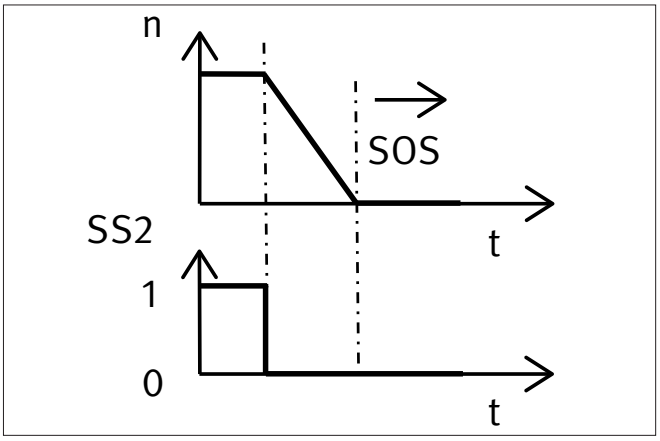
a) entweder Auslösen und Steuern der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der SOS-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt[3], oder

b) Auslösen und Überwachen der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der SOS-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt, oder

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

In Abbildung 4 ist das zeitliche Verhalten des Eingangssignals zur Aktivierung von SS2 und der Motordrehzahl gezeigt. Die Sicherheitsfunktion SS2 entspricht einem gesteuerten Stillsetzen nach DIN EN 60204-1 [10], Stopp-Kategorie 2.

Abbildung 4:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SS2 (Safe stop 2, sicherer Stopp 2)



Bei der Umsetzung der Sicherheitsfunktion SS2 gemäß c), 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 SS2-Funktion in dieser Art nicht geeignet.

Wird dagegen die Sicherheitsfunktion SS2 mit Überwachung der Bremsrampe (Größe der Motorverzögerung) realisiert, 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

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

wird SS2 ausgelöst. Die gefahrbringende Bewegung wird stillgesetzt und anschließend der unerwartete Anlauf durch SOS verhindert.

- Die Last an einer Vertikalachse wird beim Öffnen einer Schutztür stillgesetzt und durch anschließenden SOS in Position gehalten. Je nachdem, wie Bedienpersonen sich im Gefahrenbereich aufhalten können, sind weitere Maßnahmen erforderlich (siehe Informationsblatt 005 des Fachbereichs Holz und Metall, Anhang C, Seite 105).

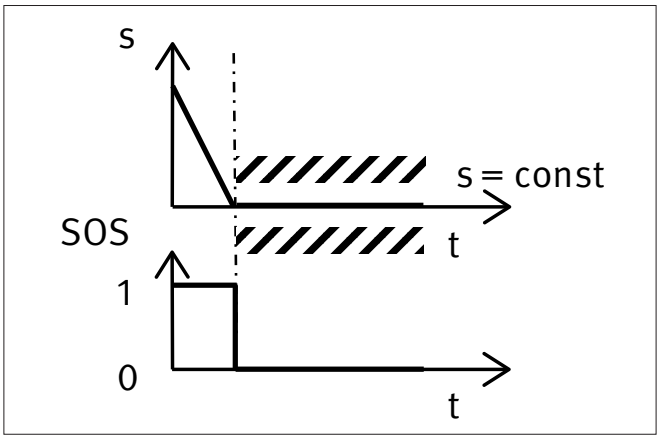
3.1.2 Andere Sicherheitsfunktionen

3.1.2.1 Sicherer Betriebshalt (Safe operating stop, SOS)

„Die Sicherheitsfunktion SOS 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.“

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 Sicherheitsfunktion 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. Es wird STO eingelegt, sodass eine Gefährdung von Personen vermieden wird. Nach Aufheben von SOS kann die Antriebsbewegung unmittelbar von der Stopp-Position aus fortgesetzt werden.

Anwendungsbeispiele:

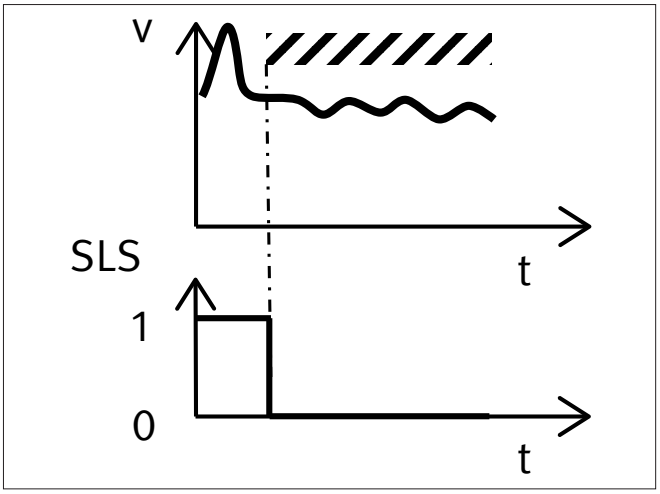
- Einrichtbetrieb an Drehautomaten/Bearbeitungszentren,
- manuelles Messen während der Bearbeitung.

3.1.2.2 Sicher begrenzte Geschwindigkeit (Safely-limited speed, SLS)

„Die SLS-Funktion verhindert, dass der Motor die festgelegte Begrenzung der Geschwindigkeit überschreitet.“

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

Abbildung 6:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SLS
(Safely-limited speed, sicher begrenzte Geschwindigkeit)



Bei dieser Sicherheitsfunktion verhindert eine sichere Überwachung, dass der Antrieb einen vorgegebenen Geschwindigkeitsgrenzwert überschreitet. Ein Überschreiten des Grenzwerts wird erkannt und der Antrieb wird sicher stillgesetzt.

Anwendungsbeispiele:

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

Hinweis:

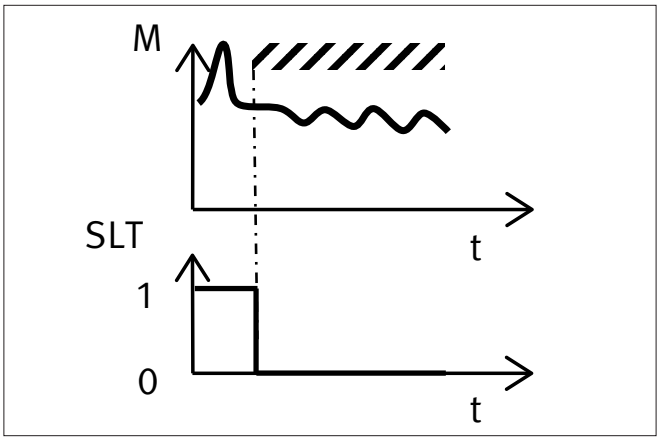
Es existiert keine allgemeine Festlegung für Drehzahl- oder Geschwindigkeitsgrenzwerte, die als so sicher angesehen werden, dass Bedienpersonen dadurch nicht gefährdet sind. Je nach Maschine werden unterschiedliche Geschwindigkeiten als sicher angesehen. Das IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz, Kennzahl 330216 [11], enthält eine Übersicht über entsprechende Festlegungen in maschinenspezifischen Normen (C-Normen).

3.1.2.3 Sicher begrenztes Moment (Safely-limited torque, SLT)

„Die SLT-Funktion verhindert, dass der Motor das festgelegte Drehmoment oder bei Anwendung eines Linearmotors die festgelegte Kraft überschreitet.“

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

Abbildung 7:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SLT (Safely-limited torque, sicher begrenztes Moment)



Das Schadensausmaß durch eine gefahrbringende Bewegung wird durch SLT verringert. Orientierende Werte hinsichtlich der Einwirkung von Kräften enthält Kapitel 6 der Grenzwerteliste 2013 [12].

Anwendungsbeispiele:

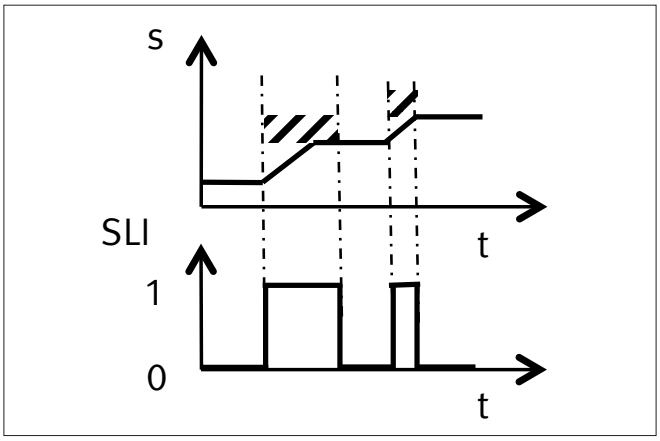
- Kraftbegrenzung an Schließkanten von kraftbetätigten Türen und Toren,
- Verhinderung des Einzugs von Bedienpersonal an Wickelmaschinen.

3.1.2.4 Sicher begrenztes Schrittmaß (Safely-limited increment, SLI)

„Die SLI-Funktion verhindert, dass die Motorwelle die festgelegte Begrenzung eines Lageschrittmaßes überschreitet."

Abbildung 8 zeigt das zeitliche Verhalten des Eingangssignals zur Aktivierung von SLI und einer Achsposition.

Abbildung 8:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SLI (Safely-limited increment, sicher begrenztes Schrittmaß)



Bei dieser Sicherheitsfunktion 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:

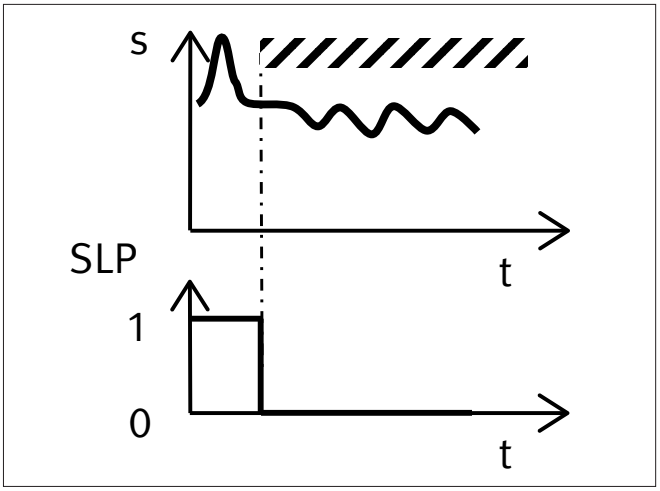
- Einrichtbetrieb an Drehautomaten/Bearbeitungszentren,
- wegbegrenztes Tippen an Druckmaschinen.

3.1.2.5 Sicher begrenzte Position (Safely-limited position, SLP)

„Die SLP-Funktion verhindert, dass die Motorwelle die festgelegte(n) Lagebegrenzung(en) überschreitet."

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

Abbildung 9:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SLP (Safely-limited position, sicher begrenzte Position)



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:

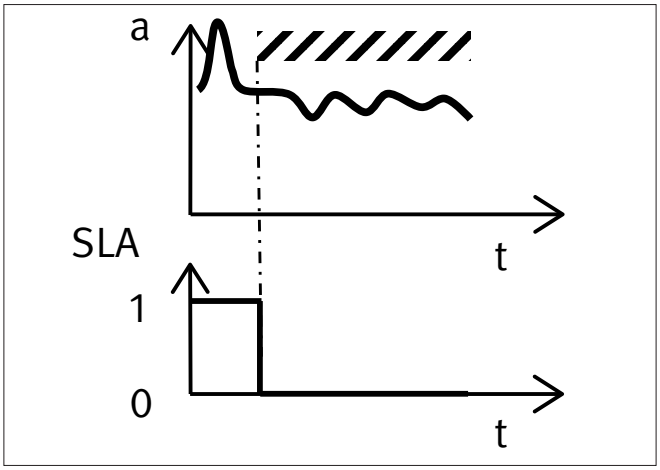
- Bereichsaufteilung an einer Maschine in Fertigungs- und Beschickungsbereich,
- Begrenzung eines Verfahrbereichs (Ersatz von elektromechanischen Endschaltern),
- Begrenzung der Reichweite von Roboterarmen.

3.1.2.6 Sicher begrenzte Beschleunigung (Safely-limited acceleration, SLA)

„Die SLA-Funktion verhindert, dass der Motor die festgelegte Begrenzung der Beschleunigung überschreitet.“

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

Abbildung 10:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SLA (Safely-limited acceleration, sicher begrenzte Beschleunigung)



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 Abbremsung begrenzt werden kann.

Die Sicherheitsfunktion hält die Motorbeschleunigung oder -abbremsung innerhalb festgelegter Grenzwerte. Das Überschreiten der Grenzwerte wird erkannt und das Antriebssystem wird sicher stillgesetzt.

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.

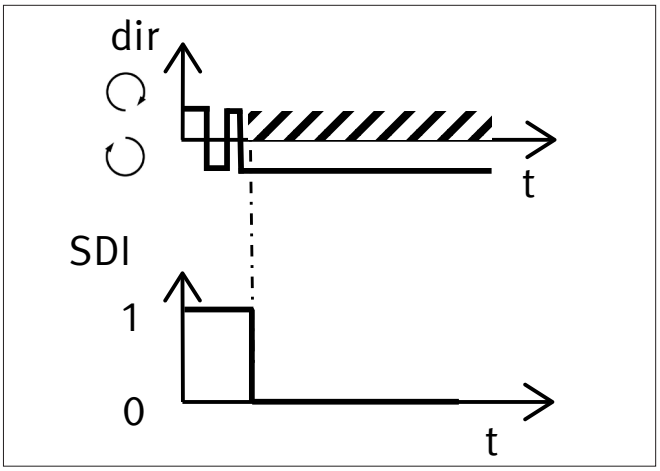
3.1.2.7 Sichere Bewegungsrichtung (Safe direction, SDI)

„Die SDI-Funktion verhindert, dass sich die Motorwelle in die unbeabsichtigte Richtung bewegt.“

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

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

Abbildung 11:
Beispiel für den zeitlichen Ablauf der Sicherheitsfunktion SDI (Safe direction, sichere Bewegungsrichtung)



Anwendungsbeispiele:

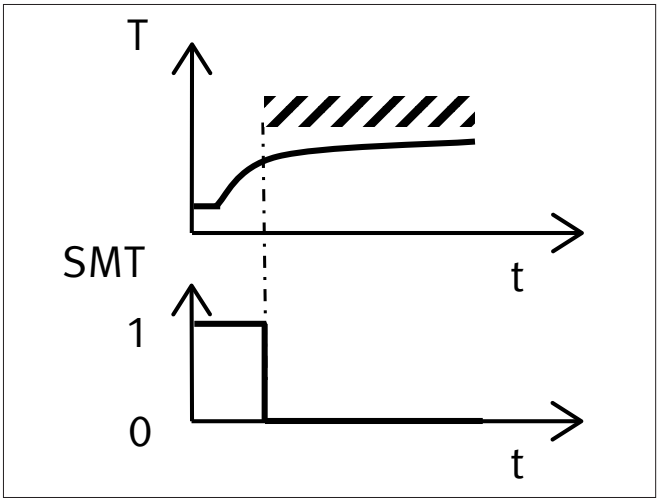
- Es wird verhindert, dass sich Maschinenteile auf die Bedienperson zubewegen.
- Eine Richtungsumkehr von Walzen wird verhindert, da ansonsten Einzugsstellen entstehen können.

3.1.2.8 Sichere Motortemperatur (Safe motor temperature, SMT)

„Die SMT-Funktion verhindert, dass die Motortemperatur einen festgelegten Grenzwert überschreitet.“

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 Sicherheitsfunktion SMT (Safe motor temperature, sicher 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 Sichere Bremsenansteuerung (Safe brake control, SBC)

„Die SBC-Funktion liefert (ein) sichere(s) Ausgangssignal(e) zur Ansteuerung (einer) (von) externen Bremse(n).“

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 Sicherheitsfunktion 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:

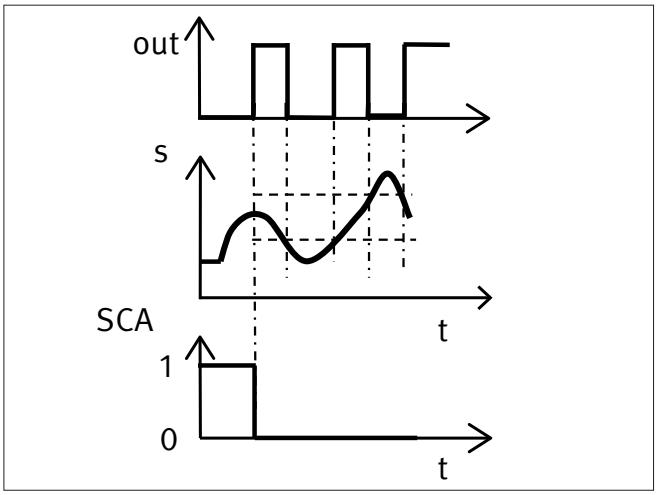
- Ansteuerung einer externen Bremse an einer Vertikalachse gleichzeitig mit Aktivierung von STO,
- Ansteuerung einer externen Bremse an einer Vertikalachse bei Spannungsausfall.

3.1.2.10 Sicherer Nocken (Safe cam, SCA)

„Die SCA-Funktion liefert ein sicheres Ausgangssignal, um anzuzeigen, ob die Lage der Motorwelle innerhalb eines festgelegten Bereiches ist.“

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 Sicherheitsfunktion SCA (Safe cam, sichere 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 innerhalb des PDS(SR), es wird lediglich das Ausgangssignal entsprechend gesetzt.

Anwendungsbeispiele:

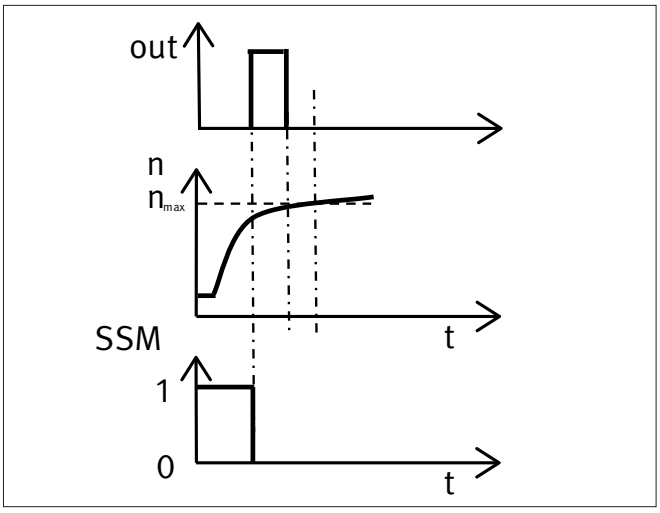
- Die Entsperrung einer Zuhaltung an einer Schutztür wird nur dann erlaubt, wenn sich das Maschinenteil in einem sicheren Bereich befindet. Ggf. ist zusätzlich der unerwartete Anlauf zu verhindern (STO),
- Ersatz von Positionssensoren,
- Lagebegrenzung von Roboterachsen.

3.1.2.11 Sichere Geschwindigkeitsüberwachung (Safe speed monitor, SSM)

„Die SSM-Funktion liefert ein sicheres Ausgangssignal, um anzuzeigen, ob die Motordrehzahl unterhalb eines festgelegten Grenzwerts liegt.“

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 Sicherheitsfunktion SSM (Safe speed monitor, sichere Geschwindigkeitsüberwachung)



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.

4 Sicherheitsfunktionen in der Anwendung

4.1 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 Wahlmittel 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 und 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, Zustimmungsschaltung).
- 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 Abschnitt 9.2.4 der DIN EN IEC 60204-1 [10] 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 Bildschirm-Darstellung. 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 Sicherheitsfunktionen aktiviert oder deaktiviert. Bauteilfehler in der Betriebsartenwahl könnten somit dazu führen, dass erforderliche Sicherheitsfunktionen 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 gehört 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 (probability of a dangerous failure per hour) erhöht.

4.1.1 Gleichzeitig ausgeführte Sicherheitsfunktionen

Bei einigen Betriebsarten an Maschinen wird die erforderliche Risikominderung durch ein Zusammenspiel mehrerer Maßnahmen, u. a. auch durch mehrere gleichzeitig ausgeführte Sicherheitsfunktionen, 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 Sicherheitsfunktionen zur Begrenzung der Geschwindigkeit (SLS) und für den Tipp-/Zustimmbetrieb gleichzeitig aktiv. Die erforderlichen PL für diese Sicherheitsfunktionen werden jeweils durch eine Risikoanalyse ermittelt. Hierbei kann u. U. eine gleichzeitig ausgeführte weitere Sicherheitsfunktion das Risiko durch die gefahrbringende Bewegung desselben Maschinenteils bereits mindern, sodass eine erneute Risikoanalyse über die verbliebene Gefährdung zu einer zusätzlichen Sicherheitsfunktion mit einem geringeren PL_r führt (siehe Anhang A, Beispiel 4 im BGIA-Report 2/2008 [4]). Eine wechselseitige Reduzierung des PL_r durch die Sicherheitsfunktionen 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 (begrenzte Drehzahlen) bestimmt. Beim Tippbetrieb in SF 3 kann dann unterstellt werden, dass durch die Drehzahlbegrenzung von SF 2 die Maschinenbewegungen für den Bediener überschaubar sind und er gefahrbringenden Bewegungen ausweichen kann (Risikoparameter P1 statt P2). Durch die gleichzeitige Ausführung von SF 2 ergibt sich also PL_r = c anstatt PL_r = d für SF 3[4].

4.1.2 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 sicherheitstechnisch, indem 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 (z. B. Standard-SPS).

Im Folgenden werden übliche Bedienelemente zur Betriebsartenwahl genannt.

a) Nockenbetätigte Wahlschalter

   Schalter mit zwangläufigem Betätigungsmodus (direktöffnend) gelten als bewährte Bauteile, wenn sie DIN EN 60947-5-1:2005 [13] (IEC 60947-5-1:1997), Anhang K entsprechen. Daher ist eine Einstufung in Kategorie 1 nach DIN EN ISO 13849 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 werden – Nachweis zum Beispiel durch Failure Mode and Effects Analysis (FMEA). Dadurch sind auch höhere Kategorien als Kategorie 1 möglich (siehe hierzu auch Beispiel 8 im Anhang B, Seite 70 ff.).

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.

4.1.3 Sicherheitsfunktion Tippschaltung

Als Befehlsgeräte für die Tippschaltung dienen üblicherweise handelsübliche federrückstellende Tipptaster. Durch die Einhaltung des Ruhestromprinzips wird erreicht, dass beim Loslassen des Stellteils des Befehlgerätes die Bewegung stillgesetzt wird. Besondere Anforderungen an die Konstruktion der Tippschalter bestehen nicht, obwohl im Fehlerfall (z. B. bei Federbruch) das Öffnen der Kontakte beim Loslassen des Tipptasters versagen kann. Für die Quantifizierung der Sicherheitsfunktion Tippschaltung ist die Kenntnis des B_{10d}-Werts der Taster notwendig. Üblicherweise gibt der Bauteilhersteller diesen Wert an. Alternativ enthält DIN EN 13849-1 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. Zustimmungsschalter oder Not-Halt über Not-Halt-Befehlsgerät, erforderlich sind.

4.1.4 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. Bis zu einer Betätigungszahl von 100 000 Schaltspielen sind für diese Produkte Fehlerausschlüsse zulässig (siehe auch BGIA-Report 2/2008 [4], Tabelle D.2).

Falls zweistufige Befehlsgeräte zum Einsatz gelangen, ist zusätzlich die Anordnung eines Not-Halt-Befehlsgerätes in der Nähe des Zustimmungsschalters erforderlich.

4 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.

4.1.5 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, sodass an der Maschine keine automatischen (Teil-)Abläufe ausgeführt werden.

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

4.1.6 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 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 den Maschinenbediener gefährden, was zu verhindern ist. Die Maschinenrichtlinie 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.

4.1.7 Verwendung einer tragbaren Bedienstation

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

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

4.2 Stillsetzen im Notfall

Den Anforderungen der Maschinenrichtlinie 2006/42/EG, 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. Dies 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 Sicherheitsfunktion 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 [10] 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.

Eine Maschine im Notfall möglichst schnell zum Stillstand zu bringen, kann man über das gesteuerte Stillsetzen durch die Antriebssteuerung erreichen. Dabei kommt die Sicherheitsfunktion 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 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 Drehbewegung eines Motors, 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. Für das Freischalten zum Arbeiten an der elektrischen Ausrüstung ist der Not-Halt also völlig 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 eingeführt, hat sich aber noch nicht vollständig durchgesetzt.

4.3 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, Abs. 5.4b „Mögliche Betriebszustände der Maschine: Störung der Energieversorgung“, DIN EN ISO 13849-1, Abs. 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, und solchen, bei denen die Speisung der Steuerelektronik aus dem Versorgungsnetz erfolgt.

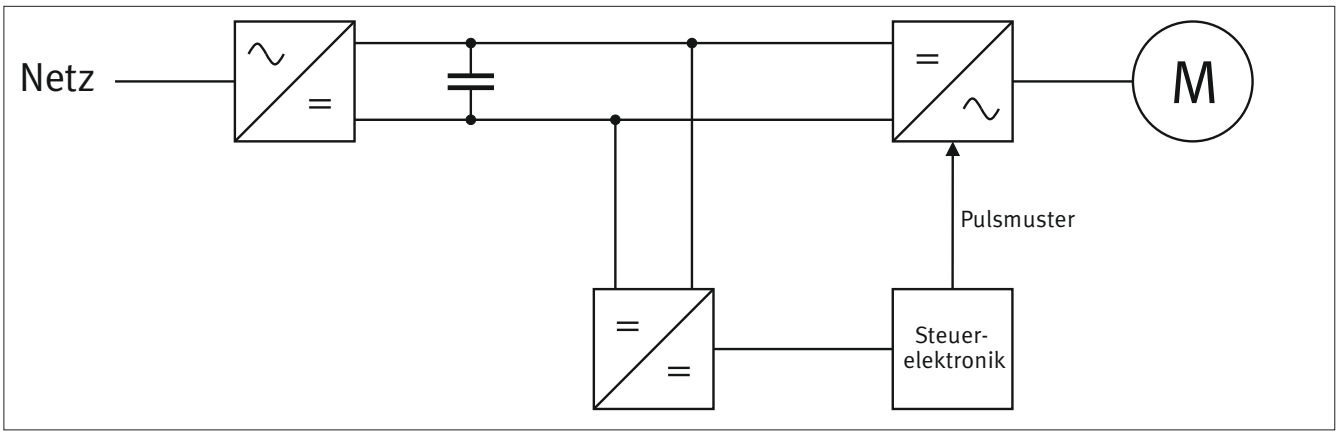
4.3.1 Versorgung der Steuerelektronik aus dem Gleichspannungszwischenkreis

Bei dieser Bauform erhält die Steuerelektronik über einen DC/DC-Wandler ihre Spannungsversorgung aus dem Gleichspannungszwischenkreis (Abbildung 15).

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 das 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 zurückzugewinnen 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 Sicherheitsfunktion 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.

Abbildung 15:
Spannungsversorgung der Steuerelektronik aus dem Gleichspannungszwischenkreis



4.3.2 Versorgung der Steuerelektronik aus dem Versorgungsnetz

Bei dieser Bauform erhält die Steuerelektronik über ein Netzteil ihre Betriebsspannung aus dem Versorgungsnetz (Abbildung 16). Üblich ist auch die Versorgung aus einem separaten 24-V-Netz, das jedoch bei Netzausfall ebenfalls versagt, sofern keine unterbrechungsfreie Spannungsversorgung (USV) eingesetzt wird.

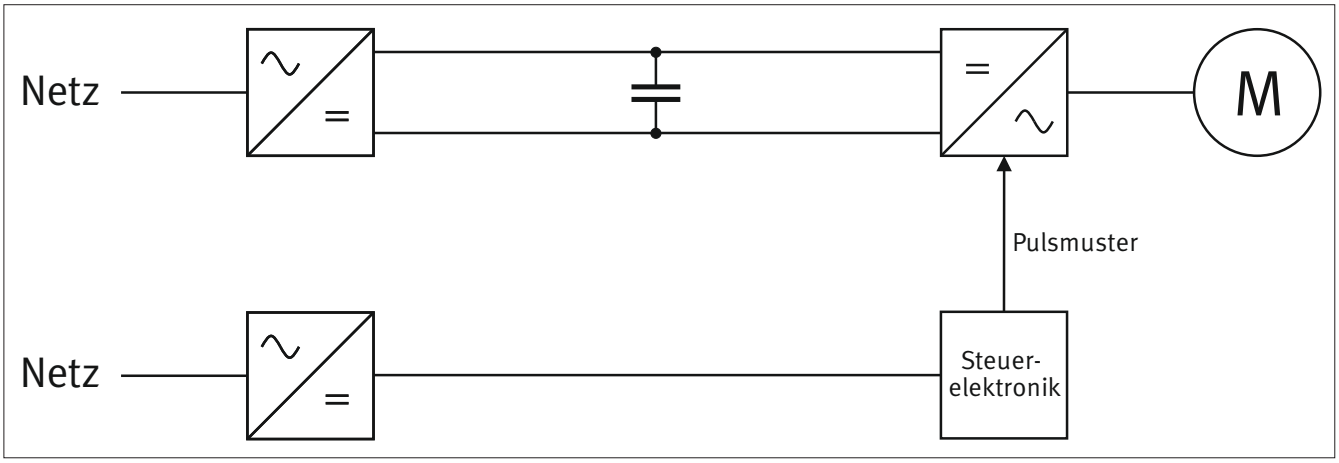
Fällt die Netzversorgung aus, steht auch an der Steuerelektronik keine Versorgungsspannung mehr zur Verfügung und es können keine Pulsmuster für den Leistungsteil des Frequenzumrichters erzeugt werden. Der Motor kann kein Drehmoment mehr aufbringen, weder ist ein gesteuertes Stillsetzen noch das Hochhalten einer Last möglich. Der Motor trudelt aus bzw. bei Vertikalachsen stürzt die Last ab. Dieses Verhalten weisen auch Frequenzumrichter mit den integrierten Sicherheitsfunktionen 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 Sicherheitsfunktion SBC erfolgen.

4.3.3 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-Werte ergeben. Das IFA schlägt für diesen Fall vor, jeweils unterschiedliche Sicherheitsfunktionen vorzusehen. Da man davon ausgehen kann, dass die Energieversorgung in der Regel vorhanden ist, kann sich durch diesen Ansatz ein geringerer PL_r für die nur bei Spannungsausfall erforderlichen Sicherheitsfunktionen ergeben. In der Anwendung des Risikographen der DIN EN ISO 13849-1 [2] würde sich bei ausgefallener Energieversorgung eine geringe Aufenthaltsdauer im Gefahrenbereich ergeben, sodass der F-Parameter „Expositionsdauer“ wohl immer mit F1 zu bewerten ist.

Das IFA hat im Jahr 2012 einen entsprechenden Vorschlag für die geplante Änderung zur DIN EN ISO 13849-1 eingebracht.

Abbildung 16:
Spannungsversorgung der Steuerelektronik aus dem Versorgungsnetz



5 Frequenzumrichter ohne integrierte Sicherheitsfunktionen (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 17 ist der prinzipielle Aufbau dargestellt.

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 in einem Mikroprozessor berechnet oder in einem separaten Baustein (z. B. Field Programmable Gate Array, FPGA) 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 Sicherheitsfunktion „Sicher abgeschaltetes Moment“ (Safe Torque Off, STO) kann dies verdeutlicht werden.

Die Aktivierung der Sicherheitsfunktion STO kann beispielsweise über die Reglersperre 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 einkanalig unter Beteiligung des Mikroprozessors, damit ist maximal PL b möglich. 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).

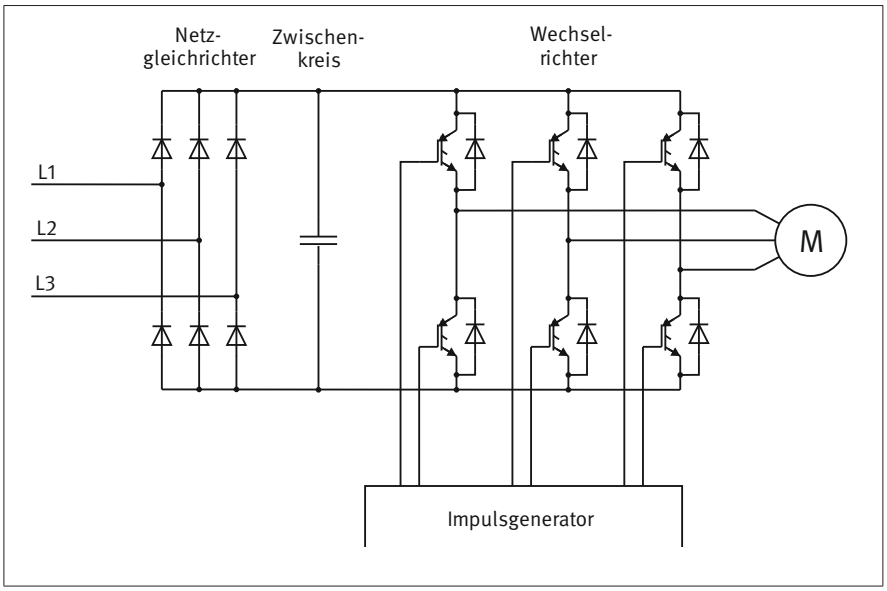


Abbildung 17:
Prinzipschaltbild eines konventionellen Frequenzumrichters

6 Frequenzumrichter mit integrierten Sicherheitsfunktionen (PDS(SR))

Konventionelle Frequenzumrichter, wie sie in Kapitel 5 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 Sicherheitsfunktionen wie STO oder eine sichere Bewegungssteuerung 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 Sicherheitsfunktionen im Frequenzumrichter zu realisieren, werden unterschiedliche Anforderungen an die Komplexität und die Ausführung der Hardware gestellt. Sicherheitsfunktionen wie beispielsweise STO können mit relativ geringem Aufwand in einen Frequenzumrichter integriert werden. Dagegen erfordert beispielsweise die Sicherheitsfunktion SLS eine deutlich komplexere Gestaltung. Im Folgenden soll für die Realisierung von Sicherheitsfunktionen zwischen „Impulssperre“ und „Sicherer Bewegungssteuerung“ unterschieden werden.

6.1 Impulssperre

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 Maßnahmen zur Realisierung einer Sicherheitsfunktion STO vorgestellt.

Die Fehlerbetrachtung entstammt einer Untersuchung im IFA (damals noch BIA). 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.

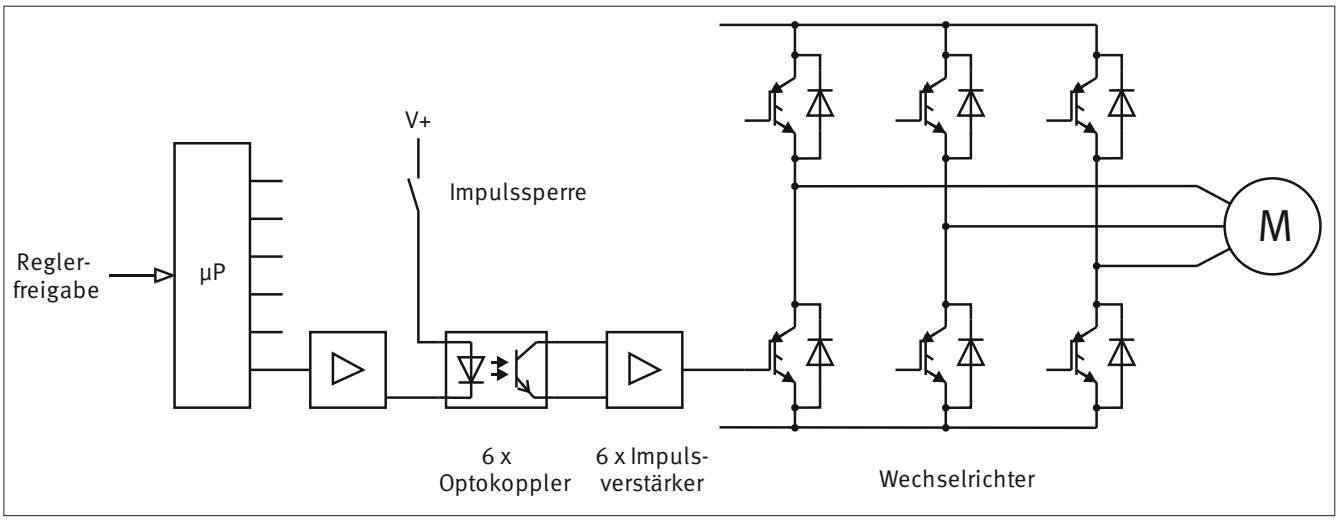
Mit Bauteilausfällen oder einer Beeinflussung der Frequenzumrichtereingänge, die jede denkbare, unbeabsichtigte oder fehlerhafte Ansteuerung der Impulsmustererzeugung zur Folge hat, muss jedoch gerechnet werden. Dies kann zu spontanen und unerwarteten Fehlfunktionen führen, wie beispielsweise unerwarteter 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.

Wird nun durch eine geeignete zusätzliche Schaltung sicher verhindert, dass die Leistungshalbleiter des Wechselrichters mit Impulsmustern angesteuert werden, so ist dies eine Möglichkeit, die Sicherheitsfunktion STO zu realisieren. Im Wechselrichter kann kein Drehfeld mehr erzeugt werden, folglich auch kein Moment im Motor. Mit der Sicherheitsfunktion STO kann der Schutz vor unerwartetem Anlauf 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 18). Sobald an den Anoden der Optokoppler keine Spannung anliegt, können keine Signale mehr übertragen werden, selbst wenn der Mikroprozessor Impulsmuster generiert.

Abbildung 18:
Unterbrechung der Versorgungsspannung für die Optokoppler



Kombiniert man diese Impulssperre mit dem Wegschalten der Reglerfreigabe, so wird zweikanalig verhindert, dass der Wechselrichter mit geeigneten Impulsmustern angesteuert wird. Verbunden mit einer entsprechenden Fehlererkennung (siehe Abschnitt 6.1.1) lässt sich somit die Kategorie 3 oder 4 nach DIN EN ISO 13849-1 [2] realisieren.

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 Anruckbewegung 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.

6.1.1 Fehlererkennung

Die beiden Abschaltpfade Impulssperre und Reglerfreigabe 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 sicherheitsgerichtete Reaktion (in der Regel Verhinderung weiterer Bewegungen) erfolgen autark. 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 in der Regel auch die Sicherheitsfunktion im Frequenzumrichter aktiviert wird. Der Hersteller des Frequenzumrichters legt in der Benutzerinformation entsprechende Anforderungen für die Anwendung fest, deren Einhaltung für die Gewährleistung des angegebenen PL und der PFH erforderlich ist.

6.1.1.1 Fehlererkennung der Impulssperre

Am folgenden Beispiel soll das Funktionsprinzip der Fehlererkennung für die Impulssperre erläutert werden. Abbildung 19 zeigt eine Schaltung, bei der die Impulsmuster zur Ansteuerung der Leistungshalbleiter über Optokoppler übertragen werden. Der Impulsgenerator (z. B. Mikroprozessor) ist in dieser Abbildung nicht dargestellt.

Beim Öffnen der Schutztür wird der Positionsschalter B1 betätigt und dessen Öffnerkontakt unterbricht die Ansteuerung des Relais K1. Durch Abfall von K1 werden die Optokoppler von der Versorgungsspannung getrennt und können keine Impulsmuster mehr übertragen. Eine Ansteuerung des Motors ist dann nicht mehr möglich. Das Relais K1 verfügt über Kontakte mit Zwangsführung (gemäß DIN EN 60947-5-1, Anhang L), sodass Öffner und Schließer mechanisch verbunden sind und nicht gleichzeitig geschlossen sein können. Der Öffnerkontakt wird von der SPS gelesen und auf Plausibilität mit der Stellung der Schutztür geprüft. Dazu muss ein (Melde-)Kontakt des Positionsschalters B1 ebenfalls in der SPS erfasst werden. Ein Hängenbleiben von Relais K1 beim Öffnen der Schutztür kann dadurch aufgedeckt werden. Die Verwendung mechanisch verbundener Kontakte, z. B. für Überwachungsfunktionen, gehört zu den bewährten Sicherheitsprinzipien gemäß DIN EN ISO 13849-2 [8].

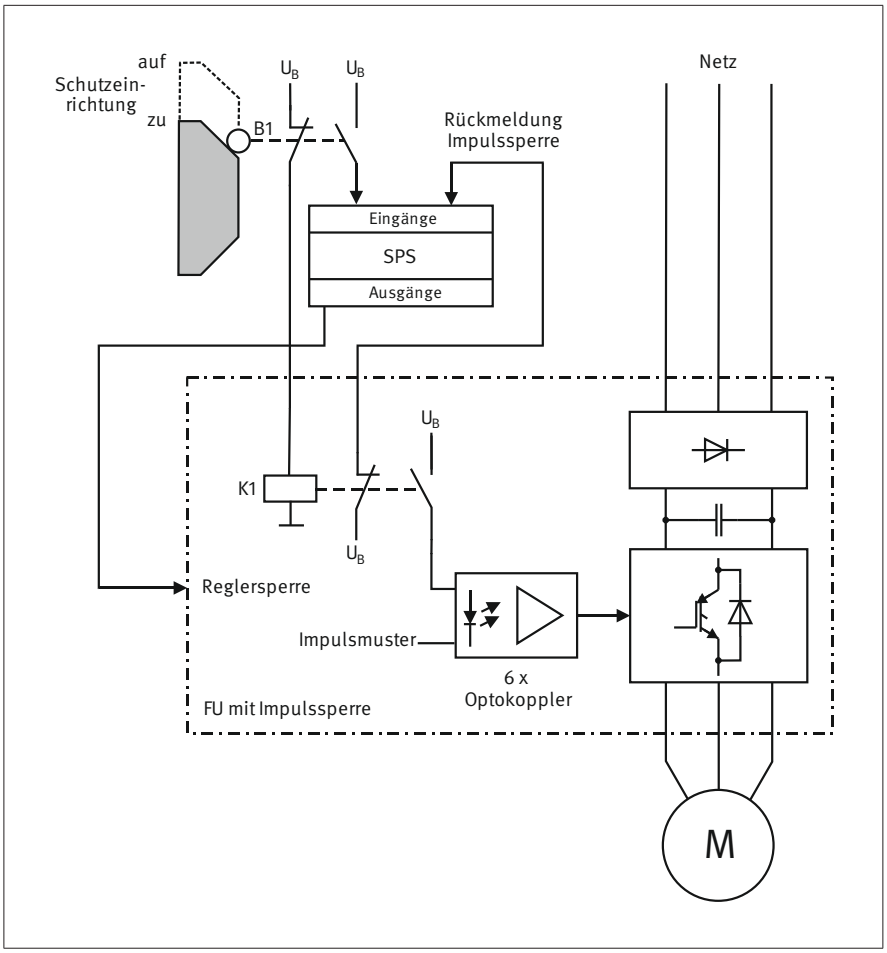


Abbildung 19:
Fehlererkennung der Impulssperre

Anstelle des Relais können auch elektronische Komponenten verwendet werden, soweit sie über eine Rückmeldung verfügen.

Für den Fehlerfall muss die SPS über einen geeigneten Abschaltpfad verfügen. Dies könnte beispielsweise die Rücknahme der Reglerfreigabe sein oder ein übergeordnetes Netzschütz, mit dem u. a. der weitere Betrieb dieses Motors verhindert wird.

Hinweis (an Hersteller von Frequenzumrichtern):

Durch das Rücklesen des zwangsgeführten Kontakts von K1 und die Plausibilitätsprüfung in der SPS können ausschließlich Fehler im Relais selbst und in der Schaltung außerhalb des Frequenzumrichters aufgedeckt werden. Es wird nicht festgestellt, ob an den Optokopplern tatsächlich keine Versorgungsspannung mehr anliegt. Bei der Integration einer solchen Impulssperre ist deshalb darauf zu achten, dass die Optokoppler nicht aufgrund eines Bauteilfehlers oder eines Kurzschlusses zwischen benachbarten Leiterbahnen/Kontaktstellen auf der Leiterkarte fehlerhaft mit Spannung versorgt werden. Hinweise für entsprechende Fehlerausschlüsse sind in den Tabellen von Anhang D der DIN EN ISO 13849-2 [8] zu finden.

6.1.1.2 Fehlererkennung der Reglerfreigabe[5]

Bei Verwendung der Reglerfreigabe als Abschaltpfad ist auch dessen Verhalten im Fehlerfall zu betrachten. So muss beispielsweise damit gerechnet werden, dass die Reglerfreigabe aufgrund eines zufälligen Hardwarefehlers im Umrichter ständig als „1“-Signal gelesen wird, obwohl sie tatsächlich abgeschaltet wurde. Ein solcher Fehler kann z. B. unbemerkt bleiben, wenn gleichzeitig mit der Sperrung der Reglerfreigabe der Sollwert auf Drehzahl Null gesetzt wird.

Durch einen Test kann dieser Fehler jedoch aufgedeckt werden. Die SPS gibt hierzu dem Frequenzumrichter einen entsprechenden Sollwert vor, sperrt aber gleichzeitig die Reglerfreigabe (siehe Abbildung 20). Sollte es bei diesem Test zu einer Motorbewegung kommen, die über den Drehgeber erfasst wird, ist der Abschaltpfad „Reglerfreigabe“ defekt. Für diesen Fall muss die SPS über einen separaten Abschaltpfad verfügen.

Zu beachten ist, dass der Test selbst nicht zu einer Gefährdungssituation führen darf. Abhängig von der Applikation muss also sehr genau überlegt werden, wann ein solcher Test möglich ist.

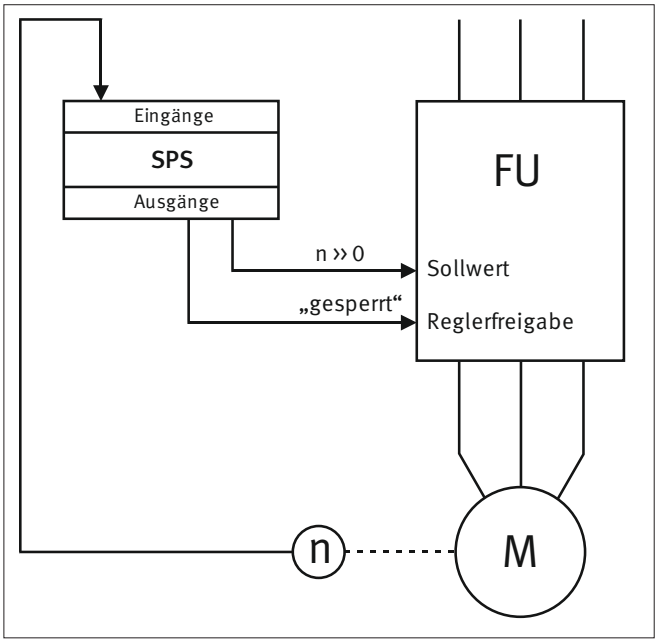
Um Fehler im Drehgeber aufzudecken, führt die SPS während des Motorbetriebs Plausibilitätsprüfungen durch. Dabei wird der

[5] Das hier beschriebene Verfahren der Fehlererkennung im Abschaltpfad Reglerfreigabe kann bei Frequenzumrichtern ohne integrierte Sicherheit ebenfalls eingesetzt werden.

vorgegebene Sollwert zyklisch mit dem Istwert des Drehgebers verglichen. Nur wenn der Drehgeber fehlerfrei funktioniert, hat der zuvor beschriebene Test der „Reglerfreigabe“ einen Sinn.

Unter bestimmten Umständen können Fehler im Abschaltpfad „Reglerfreigabe“ auch über den technischen Prozess erkannt werden. Dies ist beispielsweise dann möglich, wenn die Reglerfreigabe nicht ausschließlich der Aktivierung der Sicherheitsfunktion dient, sondern auch betriebsmäßig zum funktionalen Starten und Stoppen des Motors geschaltet wird. Eine defekte Reglersperre würde sich dann im fehlerhaften Betriebsverhalten der Maschine bemerkbar machen, vorausgesetzt, es wird bei diesem Test nicht gleichzeitig auch der Sollwert auf Drehzahl Null gesetzt.

Abbildung 20:
Fehlererkennung der Reglerfreigabe



6.2 Sichere Bewegungssteuerung

Mit Ausnahme der Sicherheitsfunktion STO erfordern alle anderen Sicherheitsfunktionen komplexe Berechnungen von Drehzahlen, Positionen 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 21 zeigt das Konzept einer derartigen zweikanaligen Steuerung.

Die Messung der Motordrehzahl oder der Achslagepositionen geschieht in Abbildung 21 über zwei unabhängige motorseitige Geber[6]. 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 21 führt den STO zweikanalig aus und ist entsprechend dem Prinzip in Abschnitt 6.1 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). 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 verbessert.

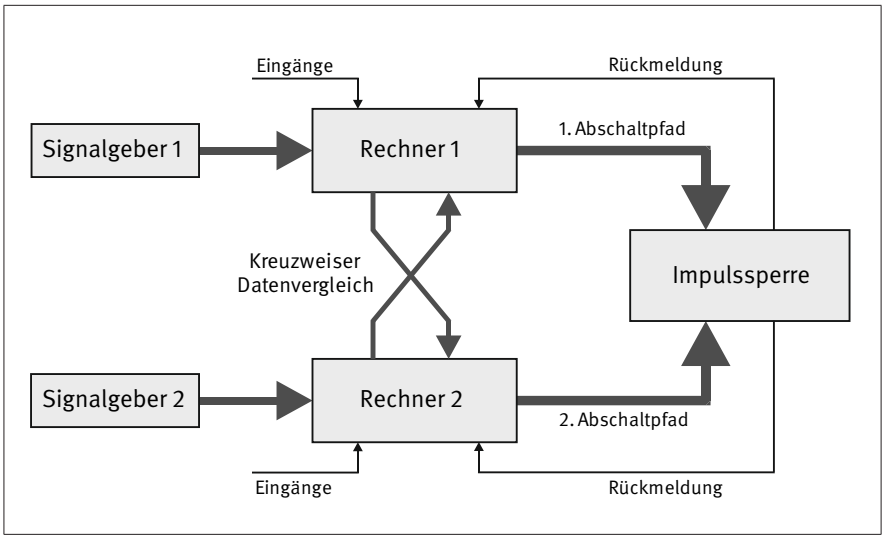


Abbildung 21:
Sichere Bewegungssteuerung

[6] 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 Ersatz eines Gebers in die Rechnersteuerungen implementiert (siehe Kapitel 9).

Fehlerreaktionen und Fehlerrekationszeiten geben die Hersteller in der Betriebsanleitung an; sie müssen für die jeweilige Applikation geeignet sein (siehe auch Abschnitt 6.5).

6.3 PL, PFH und SIL

Frequenzumrichter mit integrierten Sicherheitsfunktionen (PDS(SR)) sind Sicherheitsbauteile und Logikeinheiten für Sicherheitsfunktionen gemäß Anhang IV aus [6], für deren Einsatz Angaben zu den sicherheitsrelevanten Eigenschaften erforderlich sind. Das PDS(SR) wird zur Realisierung einer (oder mehrerer) Sicherheitsfunktion(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 IEC 62061 [15]) für die integrierten Sicherheitsfunktionen 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 Sicherheitsfunktionen des PDS(SR) die jeweiligen PFH-Werte kennen. Die PFH kann für unterschiedliche Sicherheitsfunktionen auch unterschiedliche Werte annehmen, da hier ggf. unterschiedliche Bauteile des PDS(SR) verwendet werden. Werden mehrere Sicherheitsfunktionen eines PDS(SR) gleichzeitig verwendet, so ist prinzipiell die Addition der einzelnen PFH-Werte möglich. Allerdings verwenden die Sicherheitsfunktionen 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 Sicherheitsfunktionen 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 DIN EN ISO 13849-1 im Abschnitt „Benutzerinformation“ diese Angabe und einige C-Normen enthalten Kategorieanforderungen.

6.4 Stillsetzen und Position halten

6.4.1 Stillsetzen von Lasten

Das Abbremsen einer Bewegung ist dann eine Sicherheitsfunktion und nach DIN EN ISO 13849-1 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 während des Stillsetzvorgangs 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 mit Antrieben durch Asynchronmotore sind im Allgemeinen gebräuchlich:

- Gegenstrombremsung,
- Gleichstrombremsung,
- Widerstandsbremsung.

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

Mit mechanischen Bremsen kann ein Stillsetzen von Bewegungen realisiert werden (Betriebsbremse), oder es wird eine bereits stillgesetzte Last in Position gehalten (Haltebremse). Die Bremskraft 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

Bei der Risikobeurteilung an der Maschine ergeben sich bestimmte Anforderungen an die Sicherheitsfunktion „Stillsetzen“. Insbesondere muss entsprechend des erforderlichen PL 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 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 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 Sicherheitsfunktionen SS1 bzw. SS2, bei denen nach Auftreten eines Fehlers das Abschalten des Antriebs (STO) erfolgt, ein gesteuertes Stillsetzen also nicht mehr möglich ist (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 für die Funktion des sicheren Stillsetzens erreicht werden muss, sind zusätzlich zur Abbremsung mit Frequenzumrichter weitere Maßnahmen erforderlich, z. B. der Einsatz einer mechanischen Betriebsbremse (linear oder rotatorisch) oder eine Bremsung durch Gleichstromaufschaltung.

Hinweis:

Einige Frequenzumrichter bzw. Servoregler sind in der Lage, trotz Energieausfalls mit einer Spannungsversorgung aus dem Zwischenkreis eine Bewegung gesteuert stillzusetzen (siehe Abschnitt 4.3.1).

6.4.2 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 12100:2011-03 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:

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

Im gestörten Betrieb muss Stillsetzen und Hochhalten durch eine mechanische Bremse erfolgen (z. B. Federdruckbremse mit Not-Stopp-Eigenschaft, siehe [16]).

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 [10], Abs. 9.2.5.4.2 ist die Ausführung des Not-Halts 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 und zu möglichen Schutzmaßnahmen finden sich im Fachbereichs-Informationsblatt 005 „Schwerkraftbelastete Achsen“ (siehe Anhang C, Seite 105) detaillierte Hinweise. Zusätzlich können die Anmerkungen im Abschnitt 4.3 „Ausfall der Energieversorgung“ berücksichtigt werden.

6.4.3 Mechanische Bremsen als Bauteile in Sicherheitsfunktionen

Haltebremsen, die der Hersteller zum sicheren Hochhalten von Lasten anbietet, sind Sicherheitsbauteile nach Maschinenrichtlinie, 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 [17].

Anforderungen an mechanische Bremsen in Sicherheitsfunktionen sind bislang nur für „Notfallbremsen mit Haltebremsfunktion für lineare Bewegungen“ verfügbar: Prüfgrundsatz DGUV Test GS-MF-28/02.2012 [16].

Neben konstruktiven Anforderungen sind Prüfungen zum Nachweis der mechanischen Lebensdauer festgelegt. Hierbei müssen $1 \cdot 10^6$ Schaltspiele mit statischer Last und 2 000 Schaltspiele mit dynamischer Last nachgewiesen werden.

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 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 1,5-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 in jährlichen Abständen erfolgen.

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:

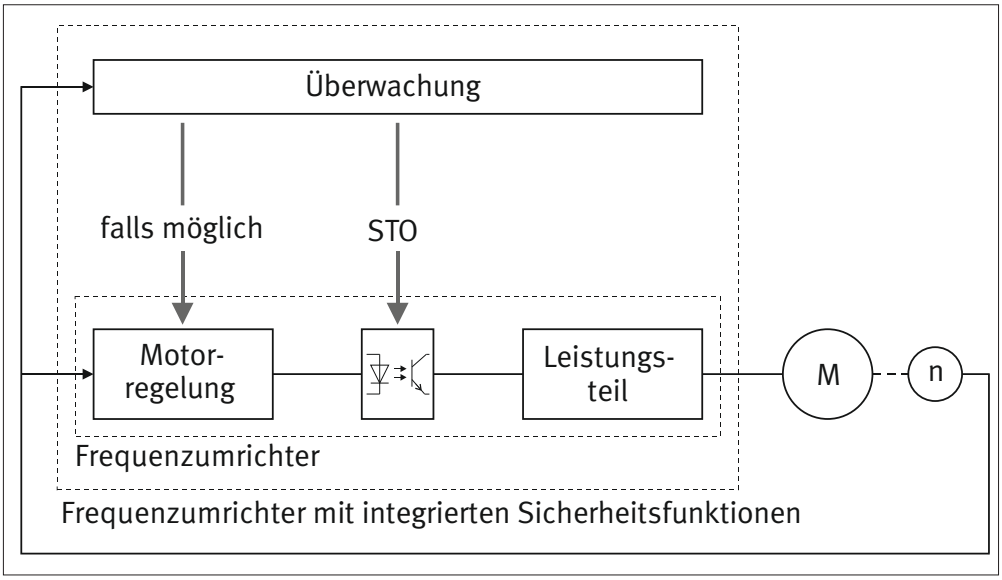
Der dynamische Test soll sicherstellen, dass sich der Nachlauf beim Bremsvorgang während der Betriebszeit nicht unzulässig verlängert (z. B. durch Verhärtung der Bremsbeläge). Trotz erfolgreich bestandenem statischen Bremsentest ist ein geringfügig vergrößerter Nachlauf möglich. Dies ergibt sich u. a. 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.

6.5 Anwendungsgrenzen von Sicherheitsfunktionen

Sicherheitsfunktionen, 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 Sicherheitsfunktion ausführende Teil der Steuerung selbst einen Fehler aufweist.

Man geht bei Maschinen grundsätzlich davon aus, dass der energielose Zustand ein sicherer Zustand ist. Daher wird kein Wert gelegt auf die Verfügbarkeit einer Motorsteuerung. Entsprechend sind im Fehlerfall die Reaktionen auf das Stillsetzen von Bewegungen ausgerichtet. Wird z. B. eine Überschreitung der maximal zulässigen Geschwindigkeit festgestellt (Sicherheitsfunktion 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 Sicherheitsfunktion 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 Sicherheitsfunktionen



Diese Problematik besteht bei allen bekannten Frequenzumrichtern mit integrierten Sicherheitsfunktionen. 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 Sicherheitsfunktionen ist eine Festlegung von Parametern erforderlich, die das Verhalten der Sicherheitsfunktion 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 Sicherheitsfunktion 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 $t_2 - t_0$ 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 Sicherheitsfunktion berücksichtigt und der Grenzwert entsprechend niedriger eingestellt werden, sodass der zulässige Bereich nicht verlassen wird.

Die Sicherheitsfunktion 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 von 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.

Alle Sicherheitsfunktionen 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 Sicherheitsfunktionen 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 Sicherheitsfunktion 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)?

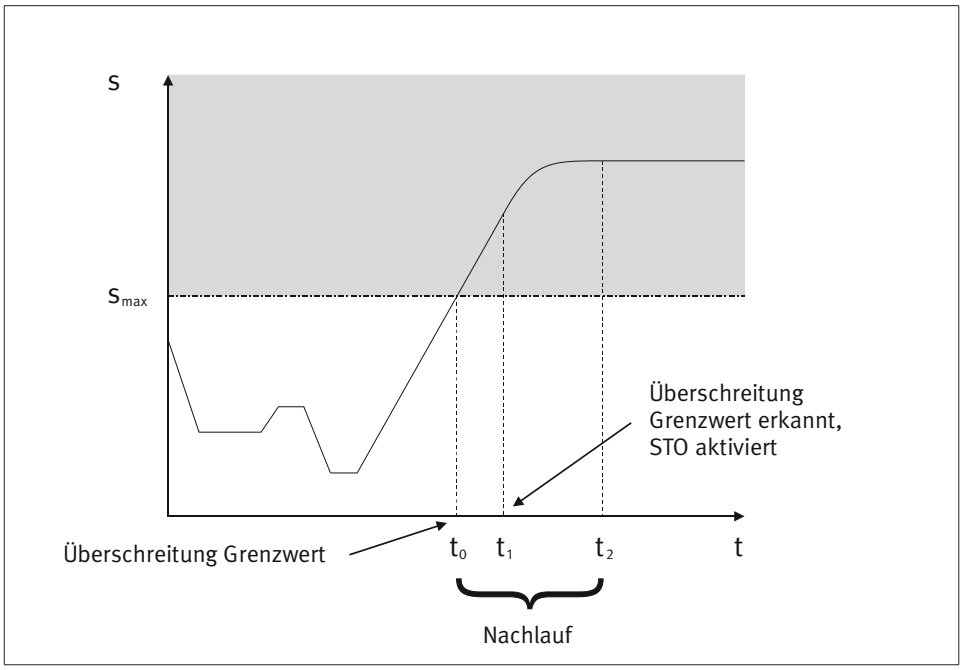


Abbildung 23:
Weg/Zeit-Diagramm der Sicherheitsfunktion SLP (Sicher begrenzte Position)

7 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 überwiegend Drehstromantriebe mit Frequenzumrichtern oder Servoreglern diese Funktion. Dieser Report beschäftigt sich aus diesem Grund 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 im Feldstromrichter erzeugt, der Anker bezieht seine Energie aus dem Ankerstromrichter (Abbildung 24).

Die Drehzahl des Motors kann bis zu seiner Grunddrehzahl über die Ankerspannung verstellt werden. Bei gleichbleibender Belastung bewirkt eine Erhöhung der Ankerspannung eine 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. Um die Drehzahl der Maschine über die Grunddrehzahl hinaus zu steigern, ist es erforderlich, den Feldstrom zu reduzieren und damit das Erregerfeld abzuschwächen. Die entsprechende Schaltung hierfür ist in dem separaten Feldstromrichter enthalten.

Die Integration von Sicherheitsfunktionen in Antriebssteuerungen für Gleichstrommotoren ist prinzipiell ähnlich wie für Drehstrommotoren. Ein großer Unterschied besteht jedoch für die Sicherheitsfunktion STO.

Um die Sicherheitsfunktion 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. Es bringt Vorteile, die Sicherheitsfunktion in die Antriebssteuerung zu integrieren. Als geeignete Maßnahme zur Realisierung der Sicherheitsfunktion STO in der 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 dargestellt. Die Verwendung von Schützen ist nicht immer sinnvoll (Kontaktabbrand, Kosten ...).

Abbildung 24:
Prinzipieller Aufbau einer Antriebssteuerung für fremderregte Gleichstrommotoren

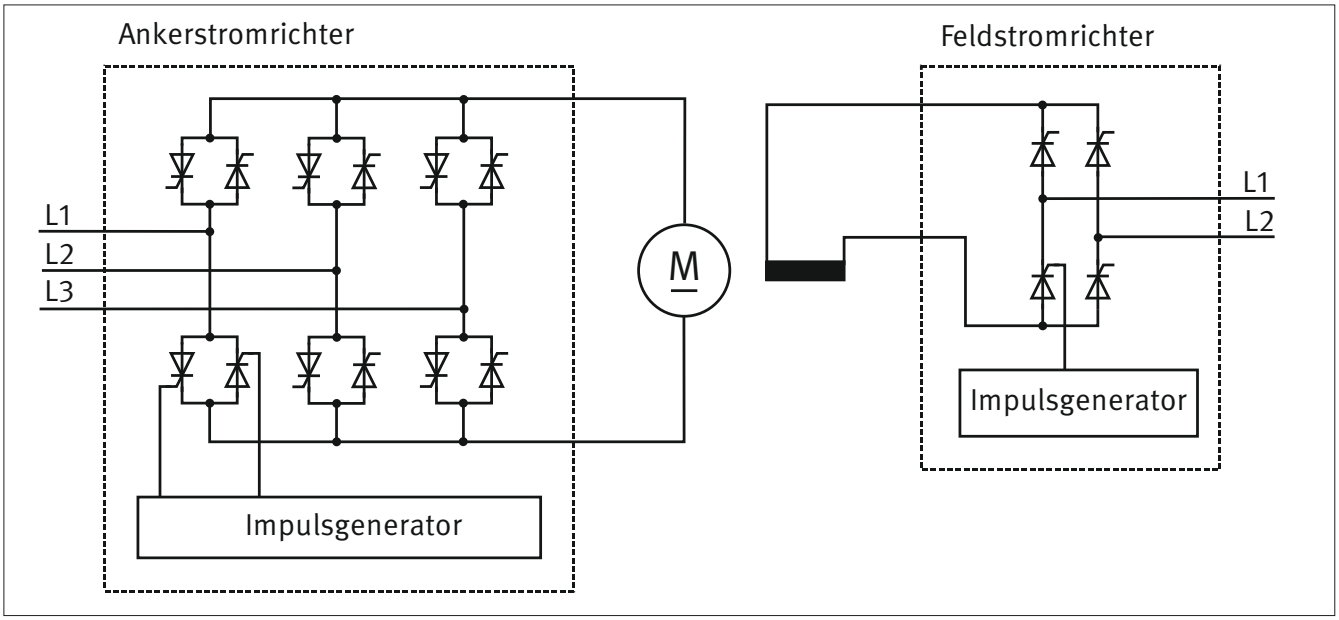
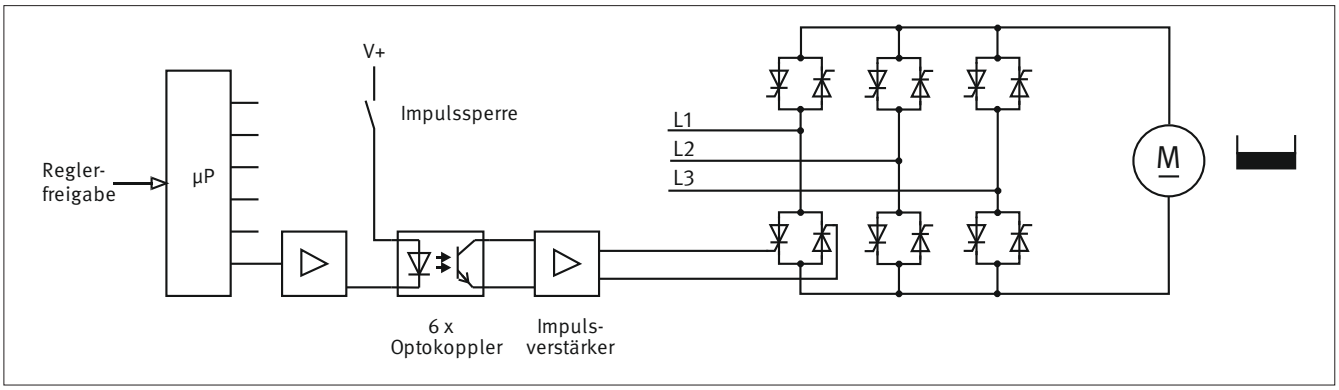


Abbildung 25:
Impulssperre im Ankerstromrichter



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 Sicherheitsfunktion 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 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 Kategorie 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 zusätzliches Netzschütz im Ankerstromkreis sein oder aber eine zusätzliche Impulssperre im Feldstromrichter.

8 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 (Anhang B, siehe Seite 51 ff.). Eine integrierte Lösung mit einem PDS(SR) bietet jedoch Vorteile und je nach Applikation kann die Leistungsfähigkeit einer externen Lösung auch unzureichend sein. Abbildung 26 zeigt beispielhaft die beiden Lösungskonzepte für die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit“ (SLS). Die Motordrehzahl wird auf einen bestimmten Grenzwert hin überwacht. Bei Überschreitung dieser Drehzahl, also im Fehlerfall, wird die Sicherheitsfunktion „Sicher abgeschaltetes Moment“ (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.

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.

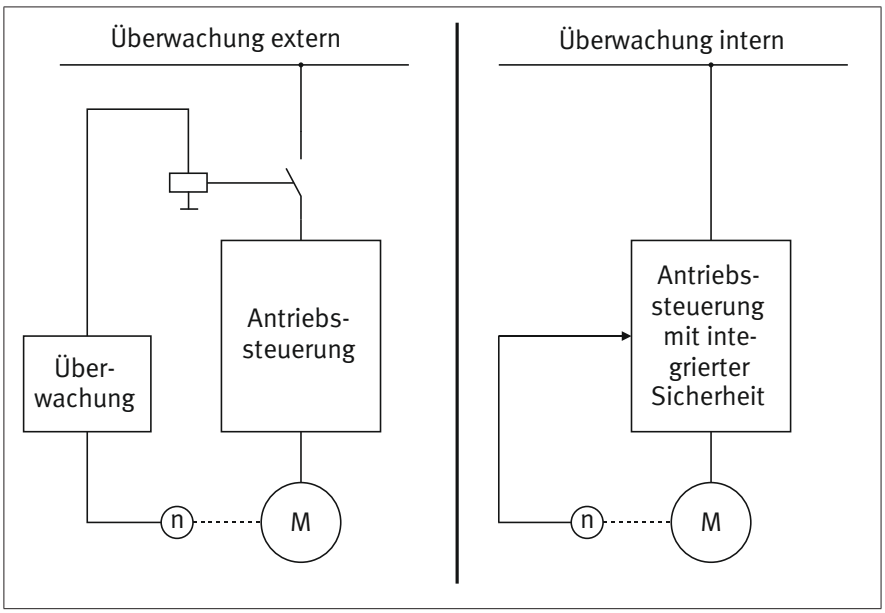
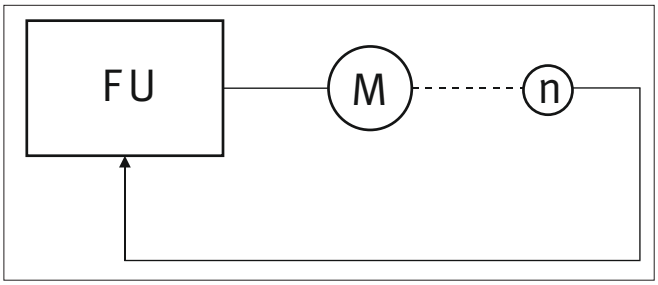


Abbildung 26:
SLS mit externer Überwachung und als integrierte Lösung

9 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 27).

Abbildung 27:
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 Sicherheitsfunktion 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 Sicherheitsfunktion SLP (Sicher begrenzte Position) erfolgen und hierfür ist die Kenntnis der absoluten Lage erforderlich. Inkrementalgeber müssen nach dem Einschalten des Netzes 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 sin/cos-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 sin/cos-Gebern ist häufig die Überprüfung auf $\sin^2 + \cos^2 = 1$ notwendig. Viele Fehler, jedoch nicht alle, werden dadurch erkannt. Der Diagnosedeckungsgrad DC beträgt in der Regel 90 bis 99 %.

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.16).

Hinweis:
Die Realisierung von PL e/SIL 3 unter Anwendung von Fehlerausschlüssen wird generell kritisch gesehen (siehe 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

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 Sicherheitsfunktionen realisieren.

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 [17]. Mittels einer FMEA müssen dazu für alle an der Signalerzeugung und -verarbeitung beteiligten Bauteile die möglichen Ausfallarten und deren Auswirkung auf die Sicherheitsfunktion untersucht werden. 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 eine weitere Möglichkeit zur Erkennung von Geberfehlern, 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 (DC mindestens 60 %).

Signalauswertung von sicheren sin-/cos-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.

Sin/cos-Geber werden zur Erhöhung der Auflösung eingesetzt, indem Positionswerte zwischen den sin/cos-Nulldurchgängen (Groblage) mittels einer arctan-Berechnung bestimmt werden (Feinlage). In der Regel ist diese erhöhte Auflösung für die Realisierung von Sicherheitsfunktionen jedoch nicht erforderlich. Darf z. B. ein Maschinenteil eine bestimmte Position nicht überfahren, um an einer potenziellen Quetschstelle den Fingerschutz zu realisieren, so ist für die Positionsüberwachung der entsprechenden Achse eine Auflösung im Bereich eines Millimeters vermutlich ausreichend. Diese Auflösung kann in der Regel durch die alleinige Auswertung des sin- oder cos-Kanals erreicht werden. Aus dieser Sichtweise wird ein sicherer Geber mit einem sin- und einem cos-Ausgangssignal als zweikanaliges System betrachtet. Sollte in einer speziellen Anwendung eine höhere Auflösung notwendig sein (z. B. an einem Drehtisch mit 4 m Durchmesser oder bei Verwendung eines Getriebes), sodass für eine Sicherheitsfunktion die Feinlage benötigt wird, müsste das Paar sin/cos als einzelner Kanal betrachtet werden. Je nach erforderlichem PL ist dann ggf. ein zweiter Kanal, z. B. durch Einsatz eines weiteren Gebers, hinzuzuziehen.

Soll eine Signalauswertung in Kategorie 3 oder Kategorie 4 realisiert werden, wobei die Auflösung der Groblage ausreichend ist, sind sin- und cos-Kanal getrennt voneinander zu verarbeiten. Dies muss durchgängig berücksichtigt werden. Eine Zusammenfassung von sin- und cos-Kanal würde zu einer Einkanaligkeit führen. Dies wäre z. B. dann der Fall, wenn zur Drehzahlermittlung anstelle einer getrennten Verarbeitung von sin und cos nur die Summe der Nulldurchgänge der sin- und cos-Signale ausgewertet wird, auch wenn dies zweikanalig erfolgt.

10 Abnahmetest

Das Systemverhalten jeder Antriebssteuerung wird über einstellbare Parameter an die jeweilige Applikation angepasst. Dabei werden z. B. maximal zulässige Geschwindigkeitswerte oder das Zeitverhalten beim Stillsetzen eines Antriebs festgelegt. Unabhängig davon, ob Sicherheitsfunktionen unter Verwendung von Steuerungen mit integrierter Sicherheit oder unter Verwendung von externen Überwachungseinrichtungen realisiert werden, muss eine Überprüfung der Einstellungen erfolgen. Ziel ist es, ein korrektes Systemverhalten (Zeit, Weg, Ablauf 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 des Abnahmetests nicht unterstellt. Für den Ablauf zur Einstellung von Parametern gelten spezifische Anforderungen in DIN EN ISO 13849-1, Abschnitt 4.6.4. Im Abnahmetest geht es also 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
- Parameter sind prinzipiell korrekt gewählt, aber für bestimmte Maschinenzustände ungeeignet
- Eingabefehler bei der Parametrierung
- Prioritätskonflikte mit anderen Sicherheitsfunktionen
- je nach Betriebsart unterschiedliche Anforderungen an die Parametrierung

Anhang A (siehe Seite 49) enthält einen von den Autoren leicht ergänzten Auszug aus [19], in dem weitere Hinweise zum Verfahren bei Erstinbetriebnahme, Parameteränderung und bei Serienmaschinen gegeben werden.

Für den Einsatz von Frequenzumrichtern mit integrierten Sicherheitsfunktionen stellen die Hersteller in der Betriebsanleitung Formulare zur Verfügung.

Die Durchführung des Abnahmetests ist eine gute Gelegenheit, um zusätzlich das Verhalten bei Energieausfall und beim Auftreten eines Fehlers innerhalb der Sicherheitsfunktion zu überprüfen. Beides ist in der Regel mit einem Verlust des Drehmoments am Motor verbunden, darf aber nicht zu einem gefährlichen Zustand führen.

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 (07.07). Beuth, Berlin 2007

[3] DIN EN IEC 61800-5-2 (VDE 0160-150-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (4/2008). Beuth, Berlin 2008

[4] *Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.:* Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849. BGIA-Report 2/2008. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Sankt Augustin 2008

[5] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme – Teil 0 bis Teil 7 (11/2002 bis 10/2005). Beuth, Berlin 2002 bis 2005

[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/LexUriServ/site/de/oj/2006/l_157/l_15720060609de00240086.pdf und http://eur-lex.europa.eu/LexUriServ/site/de/oj/2007/l_076/l_07620070316de00350035.pdf

[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] *Apfeld, R.; Schaefer, M.:* Sicherheitsfunktionen nach DIN EN 13849 bei überlagerten Gefährdungen. Fachmesse und Kongress SPS/IPC DRIVES, 23. bis 25. November 2010, Nürnberg – Vortrag. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2011. http://publikationen.dguv.de/dguv/pdf/10002/sicherheitsfunktionen.pdf

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

[11] *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

[12] Grenzwerteliste 2013 – Sicherheit und Gesundheitsschutz am Arbeitsplatz. IFA Report 1/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2013. www.dguv.de, Webcode: d164422

[13] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (2/2005). Beuth, Berlin 2005

[14] Grundsätze für die Prüfung und Zertifizierung von Elektromechanischen Zustimmungsschaltern und Zustimmungseinrichtungen (GS-ET-22). Ausg. 11/2009. Hrsg.: Fachausschuss Elektrotechnik, Prüf- und Zertifizierungsstelle im DGUV Test, Köln. www.bgetem.de/arbeitssicherheit-gesundheitsschutz/pruefen-zertifizieren/pruef-und-zertifizierungsstelle-elektrotechnik/pruefgrundsaetze

[15] DIN EN 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (10/2005). Beuth, Berlin 2005

[16] Prüfgrundsatz für Notfallbremsen mit Haltefunktion für lineare Bewegungen (GS-MF-28). Ausg. 23/2013. Hrsg.: Prüf- und Zertifizierungsstelle Maschinen und Fertigungsautomation im DGUV Test, Mainz 2012. www.dguv.de/dguv-test/de/produktsicherheit/pruefgrundlagen/pruefgrundsaetze/10mf/index.jsp

[17] *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

[18] ISO/TR 23849: Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen (5/2010). Beuth, Berlin 2010

[19] Sicherheitsgerichtete Funktionen elektrischer Antriebssysteme in Maschinen (6.98), Positionspapier DKE AK 226.03. Hrsg.: Deutsche Elektrotechnische Kommission im DIN und VDE

Anhang

Anhang A: Abnahmetest*

1 Vorbemerkung

Die folgenden Ausführungen stammen aus einem Positionspapier der DKE aus dem Jahr 1998. Inzwischen sind die meisten Inhalte hieraus in die internationale Normung eingeflossen. Die Anforderungen zum Abnahmetest sind jedoch nicht in dieser Ausführlichkeit übernommen worden (siehe [3], Abs. 7.1 f.) und werden daher hier wiedergegeben. Das Positionspapier richtet sich an die Hersteller von Antriebssteuerungen mit integrierten Sicherheitsfunktionen. Es gilt aber natürlich auch dann, wenn Sicherheitsfunktionen durch eine geeignete Applikation von konventionellen Komponenten realisiert werden. In diesem Fall sind die Anforderungen zum Abnahmetest sinngemäß vom Hersteller der Maschinensteuerung umzusetzen.

2 Anforderungen zum vollständigen Abnahmetest

Der vollständige Abnahmetest muss bei der Erstinbetriebnahme und bei Veränderung eines vollständigen gesicherten Datensatzes der sicherheitsrelevanten Parameter durchgeführt werden.

Zum vollständigen Abnahmetest muss die Steuerung mit einem geeigneten Warnhinweis auffordern. Der Warnhinweis sollte nach erfolgreichem Abnahmetest durch eine für die betriebsmäßige Quittierung nicht übliche Handlung (z. B. Betätigung einer speziellen Taste) quittiert werden. Der Antriebshersteller muss z. B. in Form einer Checkliste eine Anleitung zur Durchführung eines vollständigen Abnahmetests bereitstellen. In der Dokumentation ist darauf hinzuweisen, dass bei Inbetriebnahme der Maschine, bei Software- oder Hardwareänderungen (z. B. auch Änderungen durch Datenfernübertragung) ein vollständiger Abnahmetest durch autorisiertes Personal vorgenommen werden muss. In der Dokumentation ist ebenfalls zu vermerken, dass die Änderungen und die Ausführung des erfolgreichen vollständigen Abnahmetests geeignet protokolliert werden müssen. Der Abnahmetest muss durch vom Maschinenhersteller autorisiertes Personal durchgeführt werden.

3 Anforderungen zum partiellen Abnahmetest

Der partielle Abnahmetest muss durchgeführt werden, wenn nur einige, nicht alle gesicherten Daten der sicherheitsrelevanten Parameter verändert wurden. Zum partiellen Abnahmetest muss die Steuerung mit einem geeigneten Warnhinweis auffordern. Der Warnhinweis sollte nach erfolgreichem Abnahmetest durch eine für die betriebsmäßige Quittierung nicht übliche Handlung (z. B. Betätigung einer gesonderten Taste) quittiert werden. Der Antriebshersteller muss z. B. in Form einer Checkliste eine Anleitung zur Durchführung eines partiellen Abnahmetests bereitstellen. In der Dokumentation ist darauf hinzuweisen, dass bei teilweiser Änderung von sicherheitsrelevanten Daten diese mindestens durch einen partiellen Abnahmetest überprüft werden müssen. In der Dokumentation ist ebenfalls zu vermerken, dass die Änderungen und die Ausführung des erfolgreichen partiellen Abnahmetests geeignet protokolliert werden müssen. Der Abnahmetest muss durch vom Maschinenhersteller autorisiertes Personal durchgeführt werden.

4 Abnahmetest bei Serienmaschinen

Bei Serienmaschinen kann auf die Wiederholung des Abnahmetestes verzichtet werden, wenn ein vollständiger Abnahmetest an einer Mustermaschine durchgeführt wurde und dann die Daten der sicherheitsrelevanten Parameter gegen Veränderung gesichert in die Serienmaschinen übertragen werden.

---

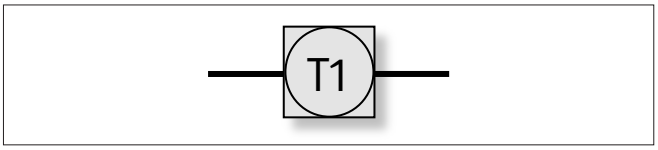
* Quelle: [19]

Anhang B:
Zusammenstellung von Schaltungsbeispielen 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 **H**ersteller, typische Werte aus Datenbanken (Kennzeichnung „[D]“ für **D**atenbank) oder als Werte aus der Norm DIN EN ISO 13849-1 (Kennzeichnung „[N]“ für **N**orm) und für angenommene Werte mit [G] markiert.

Zusätzlich zu den im BGIA-Report 2/2008 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 B.1 kann gezielt ein Schaltungsbeispiel ausgesucht werden, in dem eine bestimmte Sicherheitsfunktion in einem bestimmten PL realisiert wurde.

Tabelle B.1:
Übersicht über die Schaltungsbeispiele

Stichwort	Schaltungsbeispiel mit		
	PL c	PL d	PL e
Schutztürüberwachung, STO	1, 2	3, 6, 7, 8, 9, 10	12
Überwachung Parkposition	1, 2		
SLS		4, 8, 9	
Freigabesteuerung	8	4, 9	
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	

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

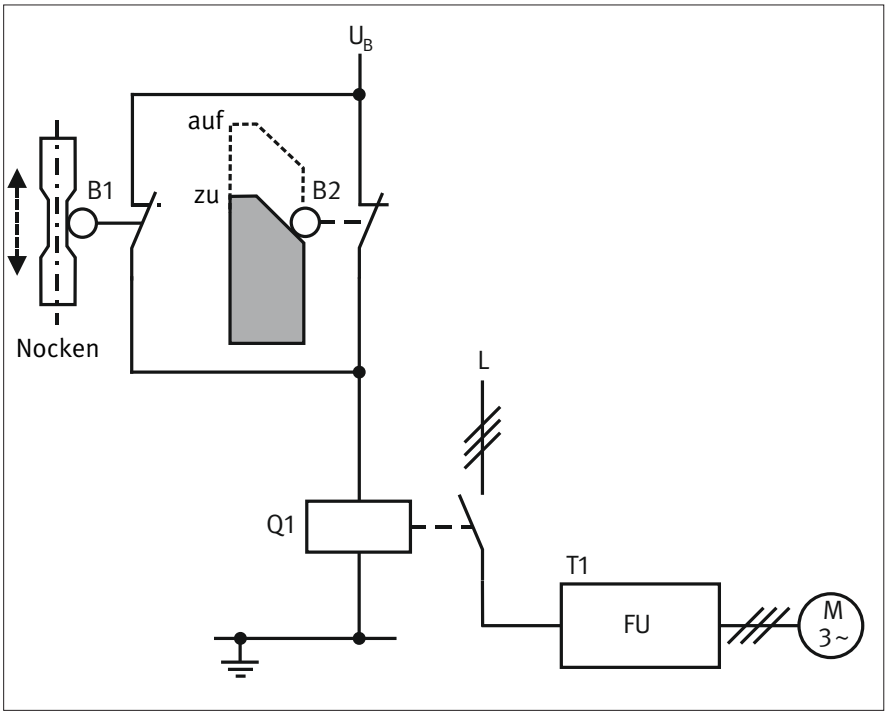


Abbildung B.1:
Kombinierte Stellungsüberwachung einer Schutztür und Positionsüberwachung einer Achse mithilfe eines Nockenschalters

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 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 BGIA-Reports 2/2008 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.
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen.
- 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

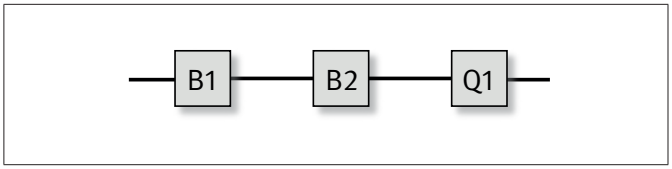


Abbildung B.2:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 1

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 Sicherheitsfunktionen. 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 kann ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt erfolgen. Für den mechanischen Teil von B1 bzw. B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 35 040 Zyklen/Jahr und $MTTF_d$ = 285 Jahre.
- Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert 1 300 000 Schaltspiele [H]. 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 = 1,14 · 10^{-6}/Stunde. Dies entspricht PL c.

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

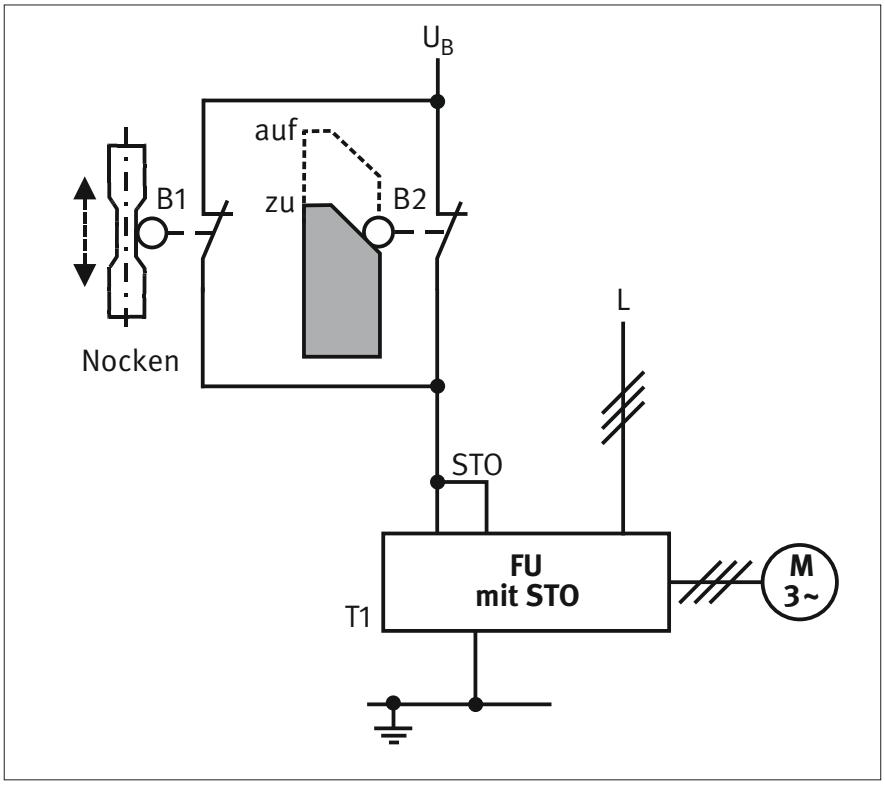


Abbildung B.3:
Kombinierte Stellungsüberwachung einer Schutztür und Positionsüberwachung einer Achse mithilfe eines Nockenschalters

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 BGIA-Reports 2/2008 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.

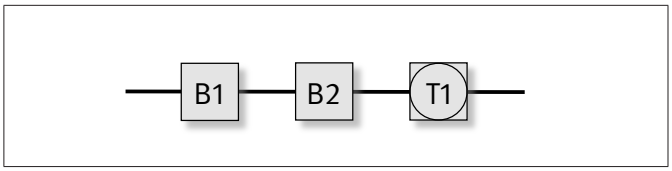


Abbildung B.4:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 2

- 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 Sicherheitsfunktion 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 im Frequenzumrichter T1 die Sicherheitsfunktion STO aktiviert.
- Das Zeitverhalten der Stillsetzung beim STO (Austrudeln) darf nicht zu Gefährdungen führen.

Berechnung der Ausfallwahrscheinlichkeit

- Für B1 und B2 kann ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt erfolgen. Für den mechanischen Teil von B1 bzw. B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 35 040 Zyklen/Jahr und $MTTF_d$ = 285 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 und PFH = 3,16 · 10^{-7}/Stunde an.
- Für SF 1 ergibt sich folgende Bewertung: Die Kombination der Subsysteme ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = 1,14 · 10^{-6}/Stunde + 3,16 · 10^{-7}/Stunde = 1,46 · 10^{-6}/Stunde. Dies entspricht PL c.

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

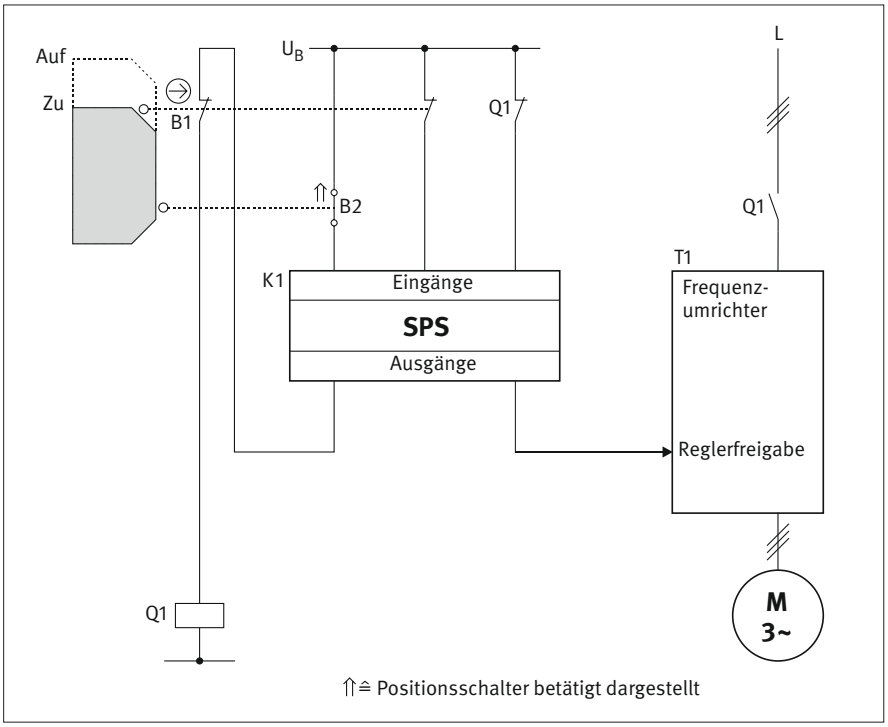


Abbildung B.5:
Prinzipschaltbild der Stellungsüberwachung

Sicherheitsfunktion

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

Funktionsbeschreibung

- Beim Öffnen der Schutzeinrichtung unterbricht B1 die Ansteuerung des Netzschützes Q1, sodass 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 6.1.1.2 „Fehlererkennung der Reglerfreigabe“).
- 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 BGIA-Reports 2/2008 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.

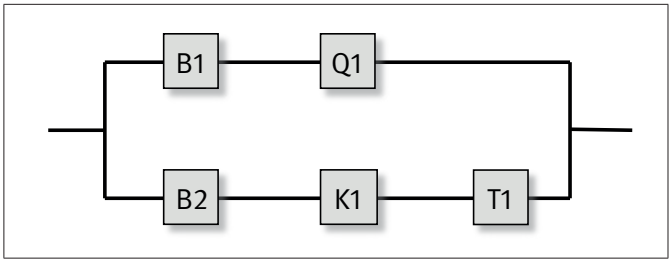


Abbildung B.6:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 3

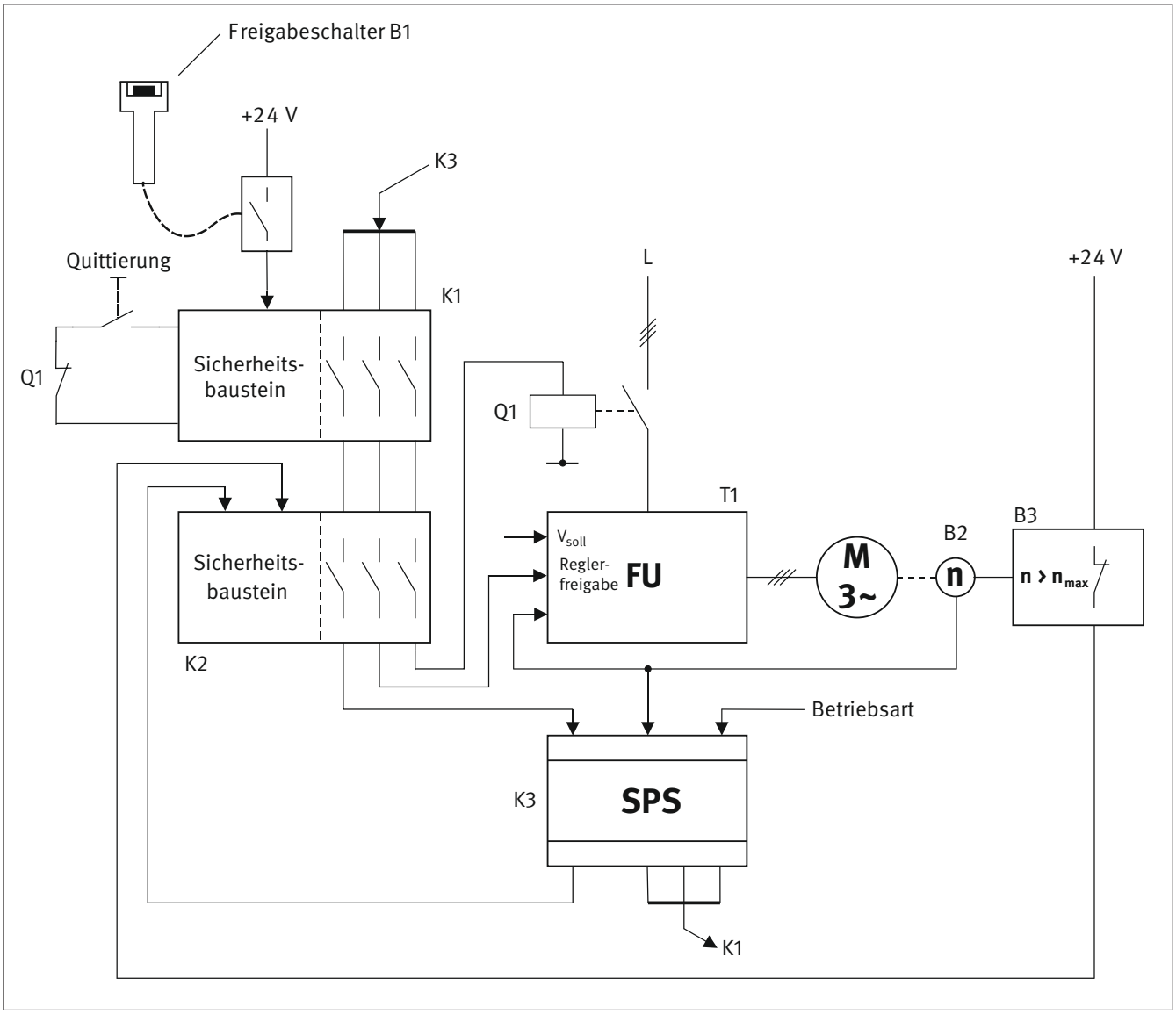
- Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden. Der Positionsschalter 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 Sicherheitsfunktionen.
- Die Standardkomponenten K1 (SPS) und T1 (Frequenzumrichter) werden entsprechend den Hinweisen in Abschnitt 6.3.10 (Anforderungen an SRESW) des BGIA-Reports 2/2008 eingesetzt.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3 des BGIA-Reports 2/2008.

Berechnung der Ausfallwahrscheinlichkeit

- Für B1 kann ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt erfolgen.
- Für den elektrischen Schließerkontakt von 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 den mechanischen Teil der Positionsschalter B1 und B2 wird ein B_{10d} von 1 000 000 Schaltspielen [H] angegeben. Mit n_{op} = 7 680 Zyklen/Jahr ergibt sich 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 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 = 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 erfolgt.
- Der DC 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 eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}78 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

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

Abbildung B.7:
Einrichtbetrieb mit begrenzter Geschwindigkeit und Freigabesteuerung – Kaskadierung von Sicherheitsbausteinen



Sicherheitsfunktionen

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

Funktionsbeschreibung

- Mit diesem Teil der Steuerung wird in der Betriebsart „Einrichten“ die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit“ (SLS) realisiert. Überdrehzahl führt zum ungesteuerten Stillsetzen mittels STO.
- Bewegungen des Antriebs werden in dieser Betriebsart durch Betätigen des Freigabeschalters B1 ermöglicht. Sie werden verhindert, wenn B1 nicht betätigt oder in Schaltstellung 3 durchgedrückt wird. Die Signale des Freigabeschalters B1 wirken auf den Sicherheitsbaustein K1.

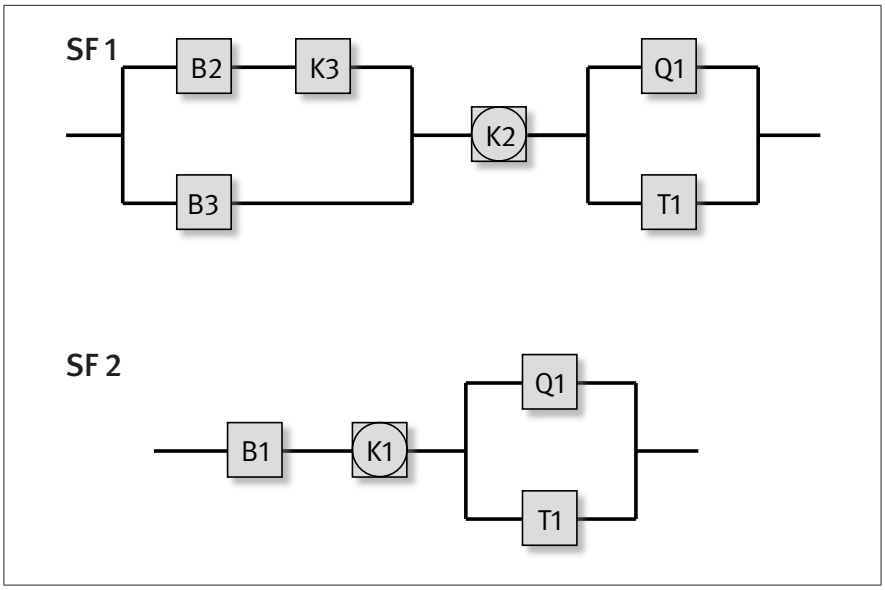


Abbildung B.8:
Sicherheitsbezogene Blockdiagramme zu Beispiel 4

- Auf die Darstellung der Betriebsartenwahl wurde aus Gründen der Übersichtlichkeit verzichtet.
- Die Drehzahlüberwachung erfolgt zweikanalig. Bei einem Kanal erfolgt die Signalverarbeitung über den Drehgeber B2 und die SPS K3. Der zweite Kanal wird mittels Drehzahlwächter B3 realisiert. Die Ausgänge der beiden Kanäle wirken auf den Sicherheitsbaustein K2.
- Die sicherheitsgerichteten Signale der Freigabesteuerung und der Drehzahlüberwachung werden über die Sicherheitsbausteine K1 und K2 kaskadiert. Das Öffnen der Freigabepfade eines Sicherheitsbausteins 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 Sicherheitsfunktion STO auszulösen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung), wie in den ersten Abschnitten von Kapitel 8 des BGIA-Reports 2/2008 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 Sicherheitsfunktionen. Sie werden entsprechend den Hinweisen in Abschnitt 6.3.10 (Anforderungen an SRESW) des BGIA-Reports 2/2008 eingesetzt.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3 des BGIA-Reports 2/2008.
- Die Drehzahlerfassung ist diversitär ausgeführt. Bei B2 handelt es sich um einen sin/cos-Geber, der an die SPS K3 angeschlossen ist. B3 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 Stillsetzzeit (Nachlaufzeit) bei STO nach einer Geschwindigkeitsüberschreitung mit maximal möglicher Beschleunigung darf nicht zu Gefährdungen führen.
- Die Freigabeeinrichtung B1 ist dreistufig ausgeführt. Sie verfügt über einen Schließerkontakt und einen zwangsöffnenden Kontakt (Öffnung in Schaltstellung 3).

Bemerkung:

Die Freigabesteuerung (früher Zustimmschaltung genannt) 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 SIL 2. Die PFH beträgt jeweils $2{,}31 \cdot 10^{-9}$/Stunde [H].
- Für den Drehgeber B2 wird die $MTTF_d$ zu 132 Jahren [H] angegeben.
- Für den Drehzahlwächter B3 gibt der Hersteller $MTTF_d$ = 60 Jahre [H] an.
- Das Schütz Q1 hat einen B_{10d}-Wert von $1 \cdot 10^6$ 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 Sicherheitsfunktionen. Da keine Herstellerangaben zur $MTTF_d$ vorliegen, werden in einer konservativen Abschätzung zehn Jahre für die Berechnung [N] (siehe DIN EN ISO 13849-1, Abschnitt 4.5.2) eingesetzt.
- Der dreistufige Freigabeschalter B1 ist nach der Produktnorm IEC 60947-5-8 hergestellt und die Anzahl der Betätigungszyklen ist kleiner als 100 000. Nach BGIA-Report 2/2008, Tabelle D.2 ist für Betätigungszyklen kleiner 100 000 ein Fehlerausschluss für das Nichtöffnen des Öffnerkontakts (Durchdrücken in die 3. Stufe) und des Schließerkontakts (Übergang 2. Stufe in 1. Stufe durch Loslassen) zulässig.
- Der DC für den Drehgeber B2 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 = 99 % angegeben werden, da eine Rücklesung des Spiegelkontakts durch den Sicherheitsbaustein K1 erfolgt (direkte Überwachung).
- Der Drehzahlwächter B3 wird einmal jährlich auf ordnungsgemäße Funktion bei der Wiederholungsprüfung der Maschine geprüft. Hierfür wird ebenfalls ein DC 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 für die SPS K3 wird aufgrund der Fehlererkennung durch den technischen Prozess auf 60 % angesetzt. Für den Frequenzumrichter T1 wird der DC 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 den Freigabeschalter kommt kein DC zum Ansatz, da aufgrund des Fehlerausschlusses keine Fehler angenommen werden müssen.
- Für das Subsystem B2/B3/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 (B2, B3, 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 $5{,}51 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 2 „Beim Loslassen des Freigabeschalters wird STO ausgelöst“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme Freigabeschalter (B1), Sicherheitsbaustein (K1) und Abschaltpfade (Q1, T1) ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}89 \cdot 10^{-7}$/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/enterprise/sectors/mechanical/files/machinery/vertical-rfu_en.pdf

Beispiel 5: Stillsetzen im Notfall – PL d

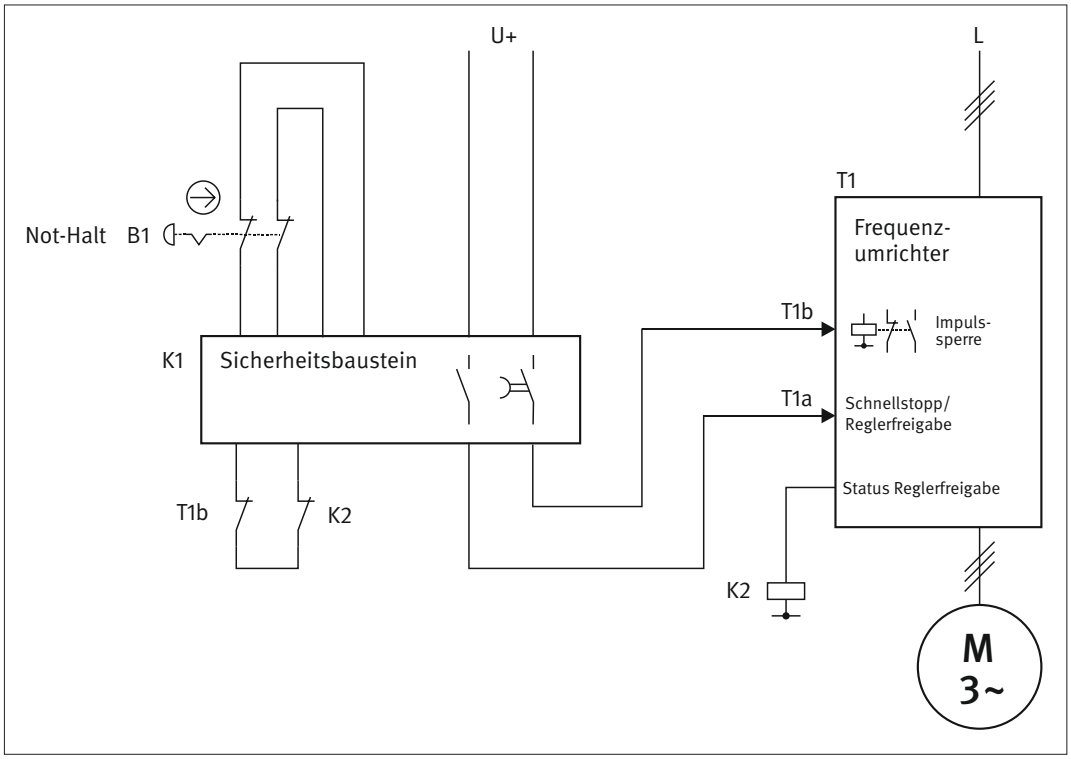


Abbildung B.9:
Prinzipschaltbild der
Antriebssteuerung

Sicherheitsfunktion

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

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch Betätigen des Not-Halt-Befehlsgeräts B1 schnellstmöglich stillgesetzt. Die Auswertung der redundanten Kontakte von B1 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 gerade ausreichend Zeit hat, den Antrieb gesteuert stillzusetzen.
- Die Kontakte des Not-Halt-Befehlsgeräts B1 sind redundant ausgeführt und werden zusammen mit der Verdrahtung durch 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.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung), wie in den ersten Abschnitten von Kapitel 8 des BGIA-Reports 2/2008 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.

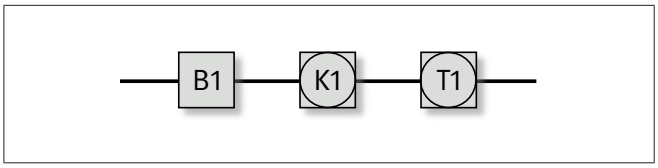


Abbildung B.8:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 5

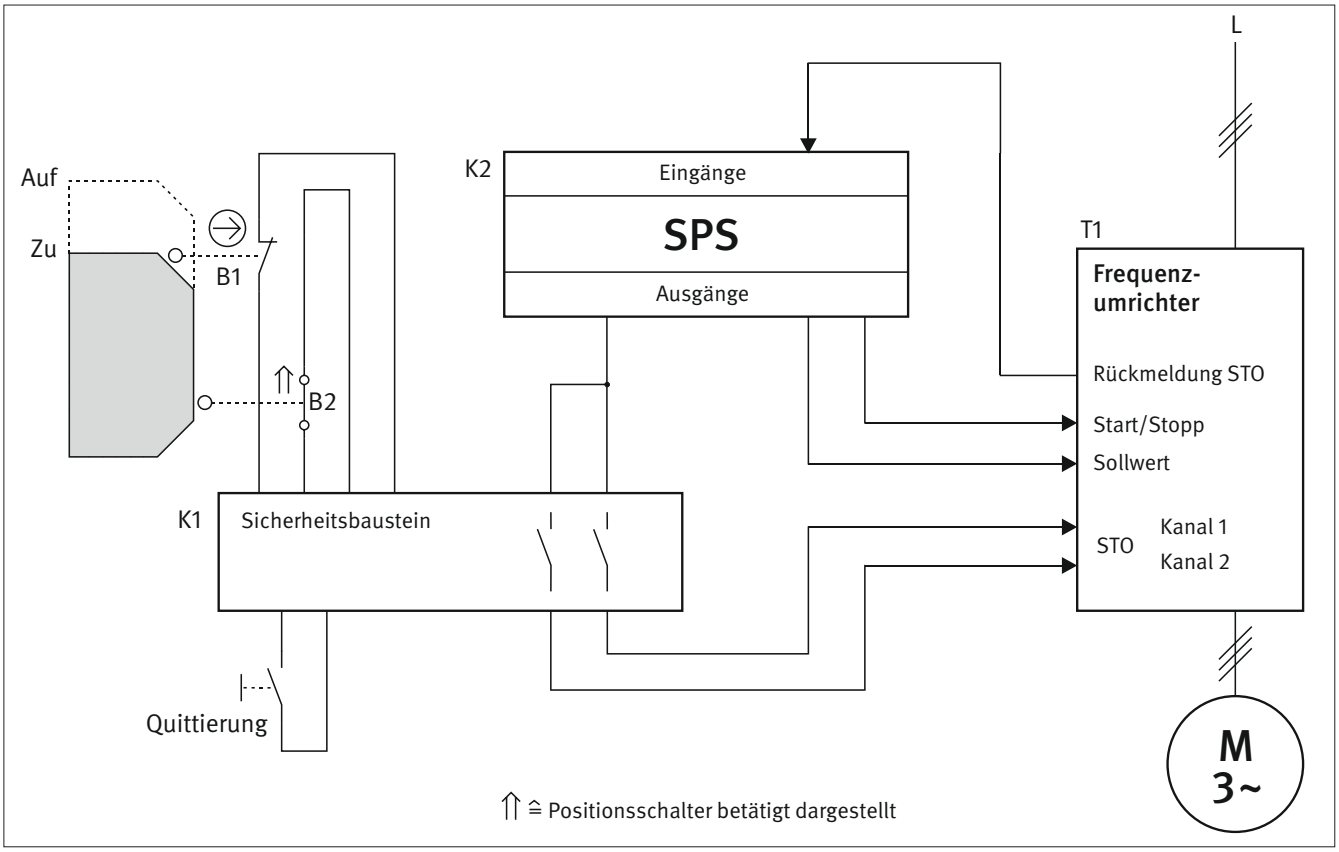
- Das Not-Halt-Befehlsgerät B1 erfüllt die Anforderungen der DIN EN ISO 13850 und ist mit zwangsöffnenden Kontakten entsprechend DIN EN 60947-5-1, Anhang K ausgestattet.
- Der Sicherheitsbaustein K1 verfügt über unverzögerte und verzögerte Freigabepfade und erfüllt die Anforderungen für Kategorie 3 und PL d.
- T1 ist ein Frequenzumrichter mit der integrierten Sicherheitsfunktion STO. Die Sicherheitsfunktion wird zweikanalig über die Eingänge Schnellstopp/Reglerfreigabe (T1a) und Impulssperre (T1b) realisiert. Durch die Kombination mit einem geeigneten Sicherheitsbaustein wird die Sicherheitsfunktion SS1 realisiert. Die Schnellstopp-Funktion wird in diesem Beispiel bei Wegnahme der Reglerfreigabe aktiviert.
- Beide Abschaltpfade von T1 werden von 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-Befehlsgeräts 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-Befehlsgerät B1 ist gemäß DIN EN ISO 13849-2, Tabelle D.8, und BGIA-Report 2/2008, Tabelle D.2, bis zu einer Betätigungszahl von 6 050 Zyklen ein Fehlerausschluss für zwangsöffnende Kontakte und die Mechanik möglich.
- Der Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 3, PL d und SIL 2. Die PFH beträgt $3{,}16 \cdot 10^{-7}$/Stunde [H].
- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheitsfunktion STO. Er erfüllt die Anforderungen für Kategorie 3, PL d und SIL 2. Die PFH beträgt $3{,}16 \cdot 10^{-7}$/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)“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme B1, K1 und T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}32 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

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

Abbildung B.11:
STO eines Frequenzumrichterantriebs



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 T1 den Sollwert vor, schaltet die beiden STO-Eingänge und kann den Antrieb starten und stoppen. Die SPS 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 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.

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 BGIA-Reports 2/2008 beschrieben, sind vorgesehen.

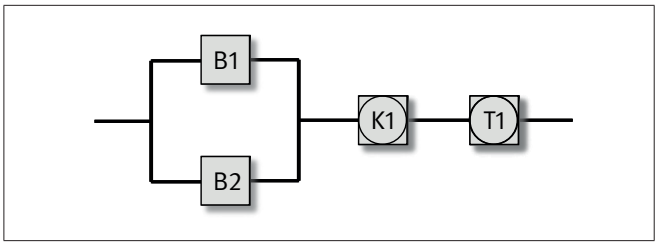


Abbildung B.12:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 6

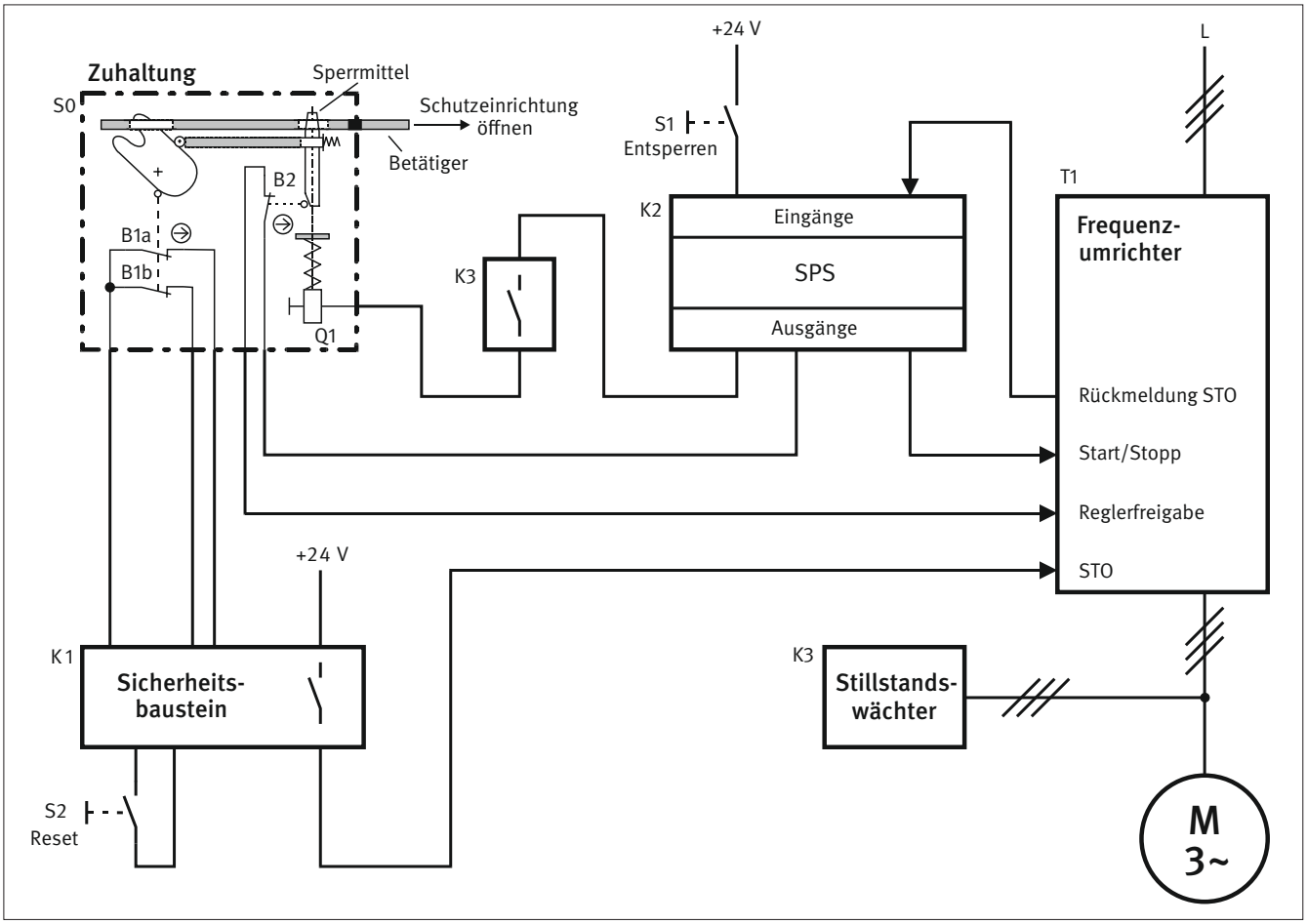
- Querschlüsse und Kurzschlüsse in elektrischen Anschlussleitungen sind entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler werden erkannt und ein sicherer Zustand wird eingeleitet. Alternativ müssen die Leitungen so verlegt sein, dass ein Fehlerausschluss für Querschluss 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 Sicherheitsfunktion STO. Es werden die Anforderungen der Kategorie 3 und PL d erfüllt.

Berechnung der Ausfallwahrscheinlichkeit

- Für den zwangsöffnenden Kontakt von B1 erfolgt ein Fehlerausschluss.
- Für den elektrischen Schließerkontakt von 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.
- Das Gleiche gilt für den mechanischen Teil der Positionsschalter B1 und B2. Mit einem B_{10d}-Wert von 1 000 000 Schaltspielen [H] und n_{op} = 3 840 Zyklen/Jahr ergibt sich jeweils eine $MTTF_d$ von 2 604 Jahren.
- Der Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 4 und PL e. Die PFH beträgt $2{,}31 \cdot 10^{-9}$/Stunde [H].
- Der Frequenzumrichter mit der integrierten Sicherheitsfunktion STO erfüllt die Anforderungen der Kategorie 3 und von PL d. Die PFH beträgt $2{,}0 \cdot 10^{-7}$/Stunde [H].
- Der DC 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).
- Für die Sicherheitsfunktion 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 $2{,}47 \cdot 10^{-8}$/Stunde.
- Die Kombination der Subsysteme Positionsschalter B1/B2, Sicherheitsbaustein K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $2{,}27 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

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

Abbildung B.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 S0 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 T1 ein. Nach Erreichen des Stillstands ermöglicht der Stillstandswächter K3 die Ansteuerung des Zuhaltemagneten durch 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 unterbricht.
- Das Öffnen der Schutzeinrichtung wird über die zwei Öffnerkontakte des Positionsschalters B1 erfasst und in einem Sicherheits-baustein K1 ausgewertet. Über den Freigabepfad von K1 wird im Frequenzumrichter T1 der STO-Eingang abgeschaltet, wodurch

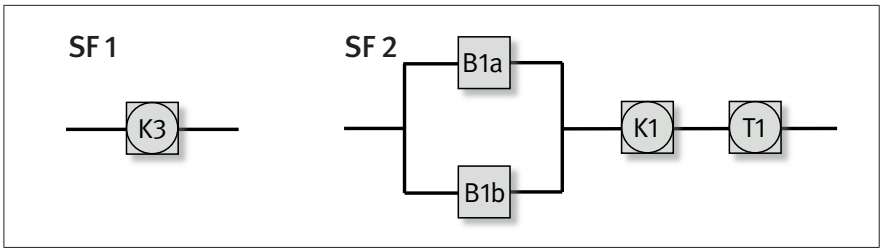


Abbildung B.14:
Sicherheitsbezogene Blockdiagramme zu Beispiel 7

die Generierung eines Drehfeldes verhindert wird. Mit dieser Sicherheitsfunktion wird der Schutz vor unerwartetem Anlauf des Motors realisiert.

- Die gefahrbringende Bewegung kann nur bei geschlossener und zugehaltener Schutzeinrichtung wieder in Gang gesetzt werden.
- Fehler im Positionsschalter B1 werden durch den Plausibilitätsvergleich im Sicherheitsbaustein K1 aufgedeckt.
- Die im Frequenzumrichter T1 integrierte Sicherheitsfunktion 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 BGIA-Reports 2/2008 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 S0 handelt es sich um einen Positionsschalter mit getrenntem Betätiger (Bauart 2) und integrierter Zuhaltung. Die Öffnerkontakte B1a, B1b und der Überwachungskontakt B2 für das Sperrmittel sind zwangsöffnende Kontakte, die die Anforderungen gemäß DIN EN 60947-5-1, Anhang K erfüllen.
- Die Zuhaltung wird als bewährtes Bauteil angesehen und erfüllt die Anforderungen der DIN EN 1088 für Verriegelungseinrichtungen. Die Feder der Zuhaltung ist eine bewährte Feder nach DIN EN ISO 13849-2, Anhang A3. Außerdem muss die Feder dauersicher nach DIN EN 13906-1 sein. Die Kriterien für die Zuhaltung mit Federkraft sind im Prüfgrundsatz GS-ET-19, Abschnitt 5.5.1 enthalten. Die Fehlschließsicherung der Zuhaltung stellt konstruktiv sicher, dass der Sperrbolzen bei geöffneter Schutztür nicht die Sperrstellung (Zuhaltestellung) einnehmen kann. Der Sperrbolzen wird durch einen zwangsöffnenden Kontakt B2 überwacht. Die Feder der Zuhaltung hält das Sperrmittel bei Energieausfall in der geschlossenen Position (Ruhestromprinzip). Ein einzelner Fehler in der Mechanik der Zuhaltung kann nicht gleichzeitig zum Ausfall von B1 und B2 führen.
- Der Sicherheitsbaustein K1 erfüllt die Anforderungen der Kategorie 4 und PL e.
- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheitsfunktion 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 zwangsöffnenden elektrischen Kontakte B1a und B1b kann ein Fehlerausschluss angenommen werden.

- 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 Neufassung der BGI 575/670 „Auswahl und Anbringung von Verriegelungseinrichtungen“ (in Vorbereitung)
  – keine Verwendung als mechanischer Endanschlag
  – unlösbare Befestigung des Betätigers
  – regelmäßige Wartung
  – Formschluss nach Montage
  – ausreichende mechanische Festigkeit aller Träger- und Funktionselemente
  – 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 Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 4, PL e und SIL 3. Die PFH beträgt $2{,}98 \cdot 10^{-8}$/Stunde [H].

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

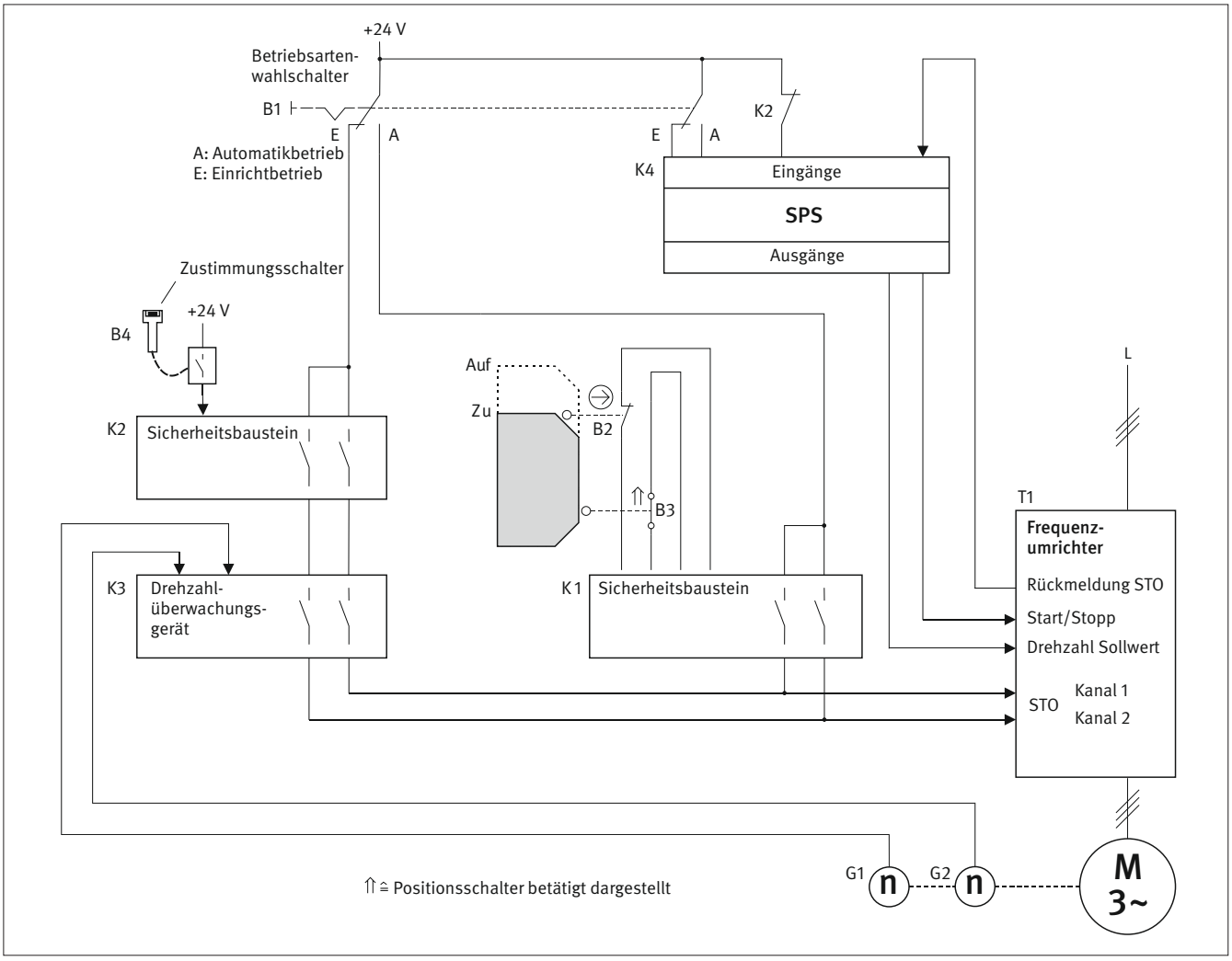
- Der Stillstandswächter K3 erfüllt die Anforderungen für Kategorie 3, PL d und SIL 2. Die PFH beträgt $2{,}31 \cdot 10^{-7}$/Stunde [H].

- 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 $2{,}31 \cdot 10^{-7}$/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 Positionsschalter B1a/B1b, Sicherheitsbaustein K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $2{,}3 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

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

Abbildung B.15:
Automatik- und Einrichtbetrieb einer Antriebssteuerung



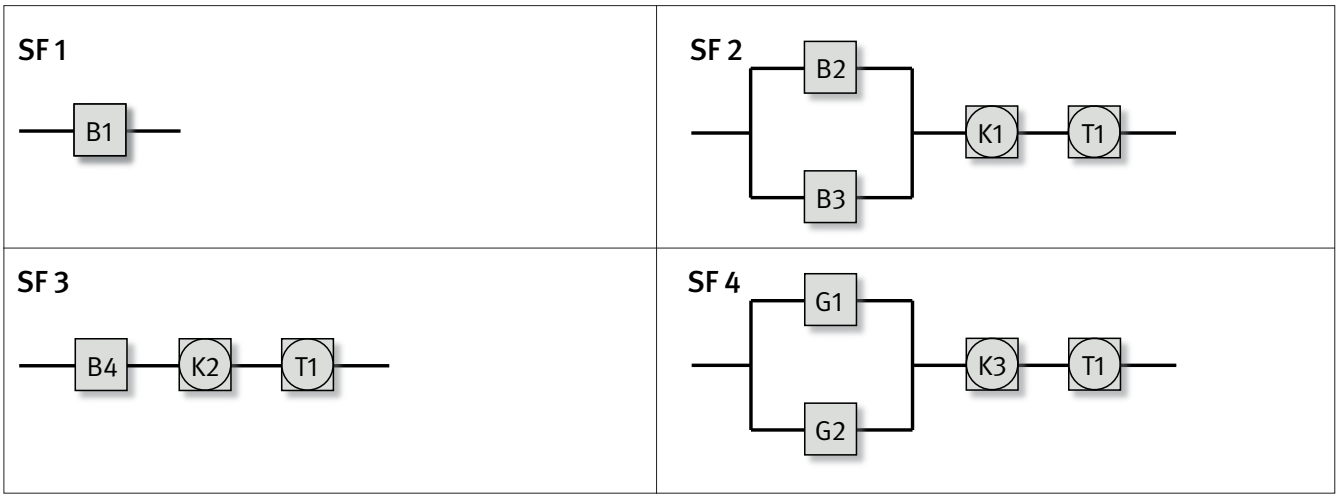
Sicherheitsfunktionen

- 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 B1 lässt die Wahl zwischen Automatikbetrieb und Einrichtbetrieb zu. Im Automatikbetrieb sind die Kontakte der Positionsschalter B2/B3 an der Schutzeinrichtung geschlossen und der Antrieb lässt sich mit beliebiger Geschwindigkeit betreiben. Das Öffnen der Schutzeinrichtung wird über B2/B3 und den Sicherheitsbaustein K1 erfasst und führt zur Aktivierung der Sicherheitsfunktion STO im Frequenzumrichter T1.

Abbildung B.16:
Sicherheitsbezogene Blockdiagramme zu Beispiel 8



- Im Einrichtbetrieb ist die Automatiksteuerung gesperrt. Ein Betrieb ist bei offener Schutzeinrichtung nur mit begrenzter Geschwindigkeit und durch die Betätigung des Zustimmungsschalters B4 möglich. Die Einleitung der Bewegung erfolgt durch eine separate Befehlseinrichtung auf einem Handbediengerät (nicht dargestellt).
- Beim Loslassen des Zustimmungsschalters B4 wird über den Sicherheitsbaustein K2 die gefahrbringende Bewegung durch Abschalten der STO-Eingänge des Frequenzumrichters T1 stillgesetzt.
- Die Drehzahlüberwachung im Einrichtbetrieb erfolgt durch ein Überwachungsgerät K3 (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 B2 und B3 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 K4 gegeben.
- Die Drehzahlerfassung erfolgt zweikanalig. Fehler in den Gebersignalen werden durch den Plausibilitätsvergleich im Drehzahlüberwachungsgerät K3 aufgedeckt.

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 BGIA-Reports 2/2008 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 B1 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 B2 und B3 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 B2 ist ein bewährtes Bauteil nach DIN EN ISO 13849-2 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K.

- Bei dem Gerät zur Freigabesteuerung B4 handelt es sich um einen zweistufigen Zustimmungsschalter mit einem Schließerkontakt. Der Zustimmungsschalter B4 entspricht den Anforderungen in DIN EN 60204-1, Abschnitt 10.9.
- Die Sicherheitsbausteine K1 und K2 erfüllen die Anforderungen der Kategorie 4 und PL e.
- Das Drehzahlüberwachungsgerät K3 erfüllt die Anforderungen der Kategorie 3 und PL d.
- Bei T1 handelt es sich um einen Frequenzumrichter mit der integrierten Sicherheitsfunktion STO. Es werden die Anforderungen der Kategorie 3 und PL d erfüllt.
- K4 ist eine handelsübliche speicherprogrammierbare Steuerung, die nicht an den Sicherheitsfunktionen beteiligt ist.

Bemerkungen:

- Die Stillsetzzeit (Nachlaufzeit) der Sicherheitsfunktion 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 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 muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z. B. Geberwellenbruch) ausgeschlossen ist.

Berechnung der Ausfallwahrscheinlichkeit

- Bei dem Betriebsartenwahlschalter B1 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 D5 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).
- Für den zwangsöffnenden Kontakt von B2 erfolgt ein Fehlerausschluss.
- Für den elektrischen Schließerkontakt von Positionsschalter B3 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.
- Das Gleiche gilt für den mechanischen Teil der Positionsschalter B2 und B3. Mit einem B_{10d}-Wert von 1 000 000 Schaltspielen [H] und n_{op} = 3 840 Zyklen/Jahr ergibt sich eine $MTTF_d$ von 2 604 Jahren.
- Die Sicherheitsbausteine K1 und K2 erfüllen die Anforderungen für Kategorie 4 und PL e. Die PFH beträgt $2{,}31 \cdot 10^{-9}$/Stunde [H].
- Der Frequenzumrichter mit der integrierten Sicherheitsfunktion STO erfüllt die Anforderungen der Kategorie 3 und von PL d. Die PFH beträgt 2,0 · 10/Stunde [H].
- Der zweistufige Zustimmungsschalter B4 verfügt über einen Schließerkontakt. Der Hersteller gibt sowohl für den mechanischen Teil als auch für den elektrischen Teil einen B_{10d}-Wert von $1 \cdot 10^5$ Schaltspielen an. Mit einem n_{op} = 3 840 Zyklen/Jahr ergibt sich $MTTF_d$ jeweils zu 260 Jahren.
- Bei dem Drehzahlüberwachungsgerät K3 handelt es sich um einen Sicherheitsbaustein, der die Anforderungen von Kategorie 3 und PL d erfüllt. Die PFH beträgt $2 \cdot 10^{-7}$/Stunde [H].

- Die Drehgeber G1, G2 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.

- Der DC für die Positionsschalter B2 und B3 beträgt 99 % aufgrund der Plausibilitätsprüfung durch den Sicherheitsbaustein K1.

- Der DC für die Drehgeber G1 und G2 wird aufgrund des Kreuzvergleichs der Signale durch das Drehzahlüberwachungsgerät K3 mit 99 % abgeschätzt.

- Für das Subsystem Positionsschalter B2/B3 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 G1/G2 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 B2/B3 entspricht Kategorie 3 mit hoher $MTTF_d$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Positionsschalter B1/B2, Sicherheitsbaustein K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $2{,}27 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

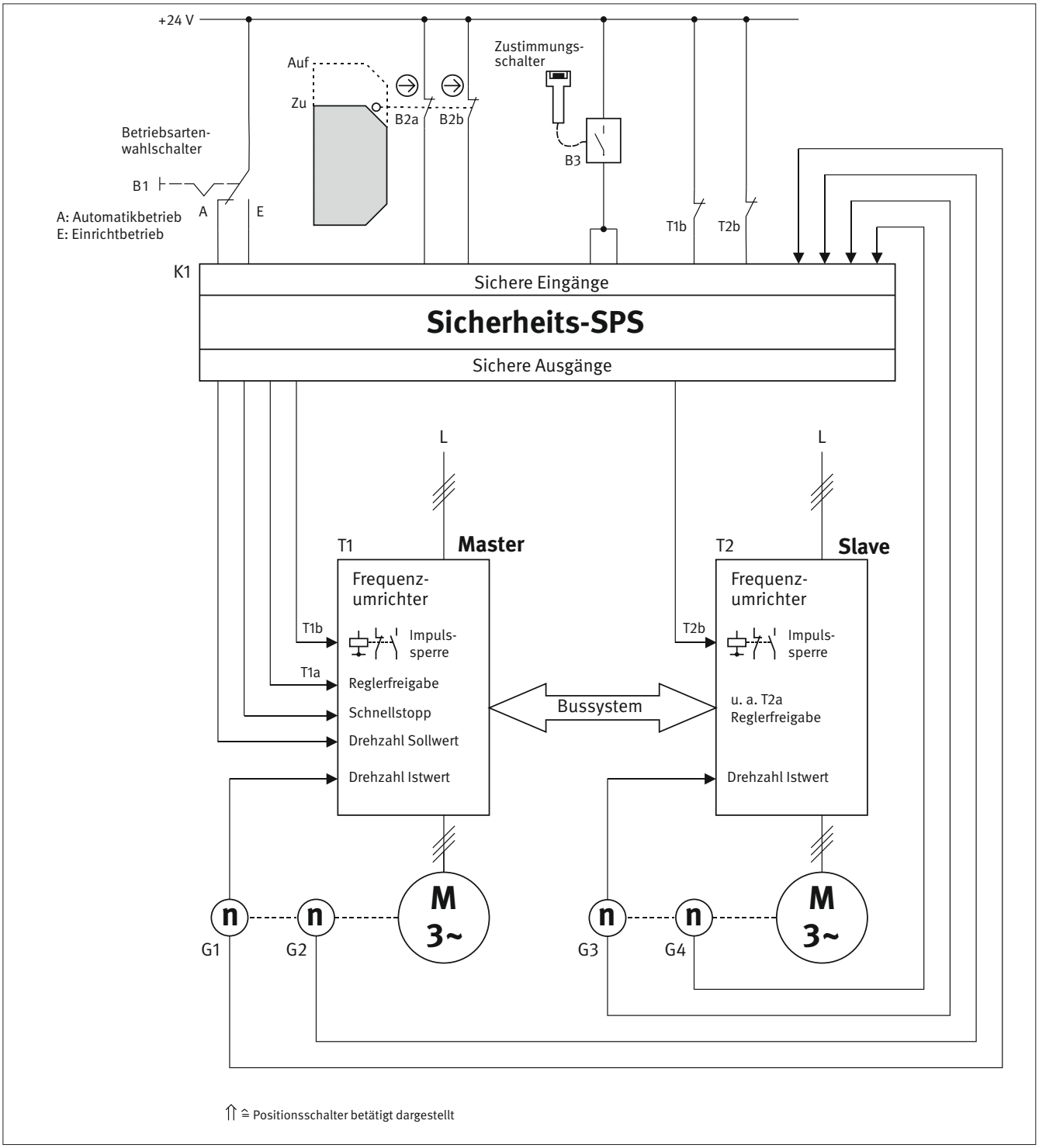
- Für die Sicherheitsfunktion SF 3 „Einrichtbetrieb; Loslassen des Zustimmungsschalters am Handbediengerät setzt den Antrieb still (STO)“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme Zustimmungsschalter B4, Sicherheitsbaustein K2 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $1{,}34 \cdot 10^{-6}$/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 G1/G2 entspricht Kategorie 3 mit hoher $MTTF_d$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}91 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Drehgeber G1/G2, Drehzahlüberwachung K3 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $4{,}69 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

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

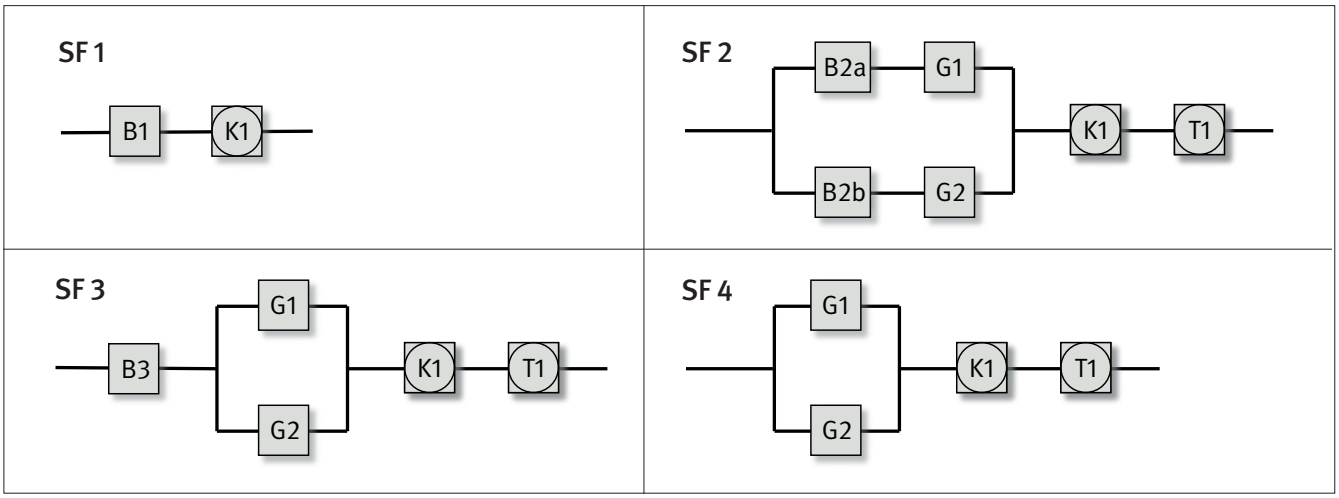
Abbildung B.17:
Prinzipschaltbild der Antriebssteuerung



Sicherheitsfunktionen

- SF 1: Betriebsartenwahl
- SF 2: Automatikbetrieb; SS1 nach Öffnen einer Schutzeinrichtung

Abbildung B.18:
Sicherheitsbezogene Blockdiagramme zu Beispiel 9



- SF 3: Einrichtbetrieb; Loslassen oder vollständiges Durchdrücken des dreistufigen Zustimmungsschalters setzt den Antrieb still (SS1)
- SF 4: Einrichtbetrieb; Sicher begrenzte Geschwindigkeit – Überschreiten der maximal zulässigen Drehzahl führt zum Stillsetzen des Antriebs (STO)

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 B1 lässt die Wahl zwischen Automatikbetrieb und Einrichtbetrieb zu (SF 1). Im Automatikbetrieb sind die Kontakte des Positionsschalters B2 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. 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 K1 zu den Frequenzumrichtern mit STO wird die Sicherheitsfunktion 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 B3 betätigt sein (SF 3). Die Einleitung der Bewegung erfolgt durch eine separate Befehlseinrichtung auf einem Handbediengerät (nicht dargestellt).
- Nach Loslassen bzw. Durchdrücken des Zustimmungsschalters B3 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 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 (G1/G2 bzw. G3/G4) verwendet. Bei Überschreitung der maximal zulässigen Geschwindigkeit wird die gefahrbringende Bewegung durch Aktivierung der Sicherheitsfunktion STO in den Frequenzumrichtern T1 bzw. T2 stillgesetzt.

- Fehler in dem Positionsschalter B2, den Impulssperre-Relais von T1b/T2b und den Drehgebern G1 bis G4 werden durch die Sicherheits-SPS K1 aufgedeckt. Die Überwachung der Schnellstopp-Rampe und die Erkennung des Stillstands erfolgt mithilfe der Drehgeber ebenfalls durch 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 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), wie in den ersten Abschnitten von Kapitel 8 des BGIA-Reports 2/2008 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 B1 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 B2 handelt es sich um einen Positionsschalter mit getrenntem Betätiger. Der Schalter ist mit zwei zwangsöffnenden Kontakten bestückt, die die Anforderungen gemäß DIN EN 60947-5-1, Anhang K erfüllen. Die Anfahrmechanik muss bestimmungsgemäß konstruiert und angebracht sein.

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

- Die Sicherheits-SPS 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 ISO 13849-1.

Bemerkung:

- Die Anbringung der zwei Drehgeber G1/G2 bzw. G3/G4 am jeweiligen Motor muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z. B. Geberwellenbruch) ausgeschlossen ist.

Berechnung der Ausfallwahrscheinlichkeit

- Für den zwangsöffnenden Kontakt von B1 und 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 die zwangsöffnenden Kontakte von B2 kann ein Fehlerausschluss für das Nichtöffnen gemacht werden. Für die Mechanik des Positionsschalters ist aufgrund der Umgebungs- und Einsatzbedingungen ein Fehlerausschluss begründet. Unter anderem

erfolgt ein verdeckter Einbau des Positionsschalters, sodass Einwirkungen durch Umgebungseinflüsse minimiert sind; damit ist gleichzeitig auch einer Manipulation vorgebeugt.

- Die Sicherheits-SPS K1 erfüllt die Anforderungen der Kategorie 4 und von PL e. Die PFH beträgt $3{,}16 \cdot 10^{-8}$/Stunde [H].
- Bei T1 und T2 handelt es sich um Frequenzumrichter mit der integrierten Sicherheitsfunktion STO. Sie erfüllen die Anforderungen für Kategorie 3, SIL 2 und PL d. Die PFH beträgt $3{,}16 \cdot 10^{-7}$/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 G1/G2 sowie G3/G4 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 für die Drehgeber G1/G2 bzw. G3/G4 ergibt sich mit 99 % aufgrund des Kreuzvergleichs der Signale durch die Sicherheits-SPS K1.
- Für das Subsystem mit dem Sicherheitsschalter B2 und den Drehgebern G1/G2 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 B1 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-Wert wird alleine durch den Beitrag von K1 bestimmt und beträgt $3{,}16 \cdot 10^{-8}$/Stunde.
- Für die Sicherheitsfunktion SF 2 „Automatikbetrieb; SS1 nach Öffnen einer Schutzeinrichtung“ ergibt sich folgende Bewertung: Das Subsystem B2/G1/G2 entspricht Kategorie 3 mit hoher $MTTF_d$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}91 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Positionsschalter/Drehgeber B2/G1/G2, Sicherheits-SPS K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $4{,}17 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.
- Für die Sicherheitsfunktion SF 3 „Einrichtbetrieb; Loslassen oder vollständiges Durchdrücken des dreistufigen Zustimmungsschalters setzt den Antrieb still (SS1)“ ergibt sich folgende Bewertung: Das Subsystem G1/G2 entspricht Kategorie 3 mit hoher $MTTF_d$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}91 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Zustimmungsschalter B3, Drehgeber G1/G2, Sicherheits-SPS K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $4{,}17 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.
- 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 G1/G2 entspricht Kategorie 3 mit hoher $MTTF_d$ (40 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}91 \cdot 10^{-8}$/Stunde.

  Die Kombination der Subsysteme Drehgeber G1/G2, Sicherheits-SPS K1 und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von PFH = $4{,}17 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 10: Gesteuertes Stillsetzen eines Antriebs beim Öffnen der Schutzeinrichtung mit Quittierungsfunktion

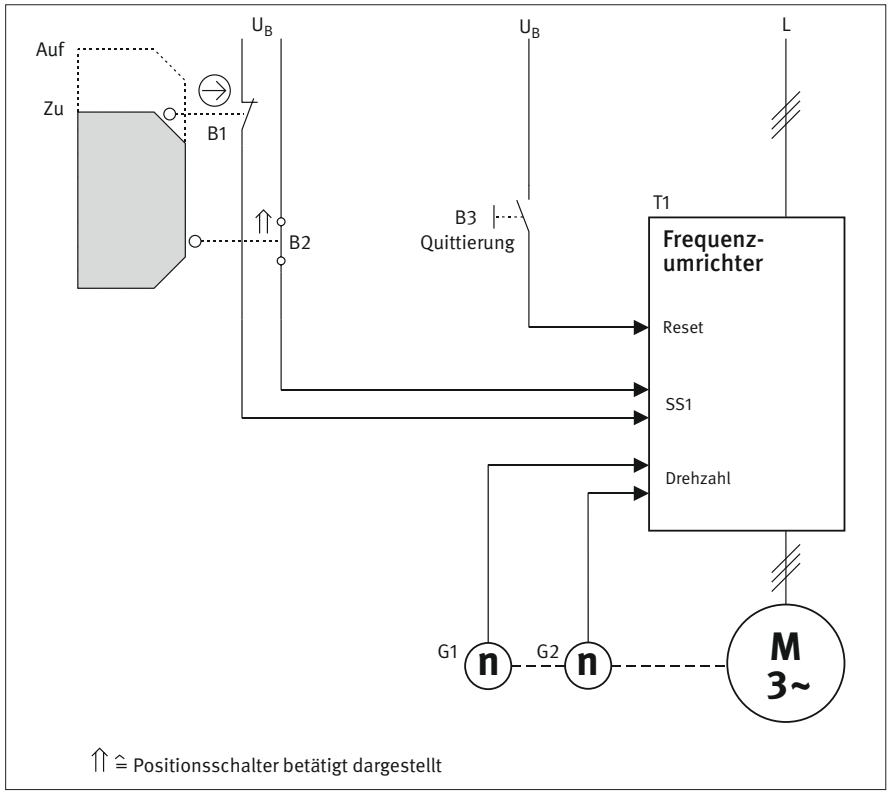


Abbildung B.19:
Prinzipschaltbild der Stellungsüberwachung

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 G1 und G2 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 von 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 Sicherheitsfunktion SS1 durch Überwachung der Bremsrampe realisiert.
- 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.

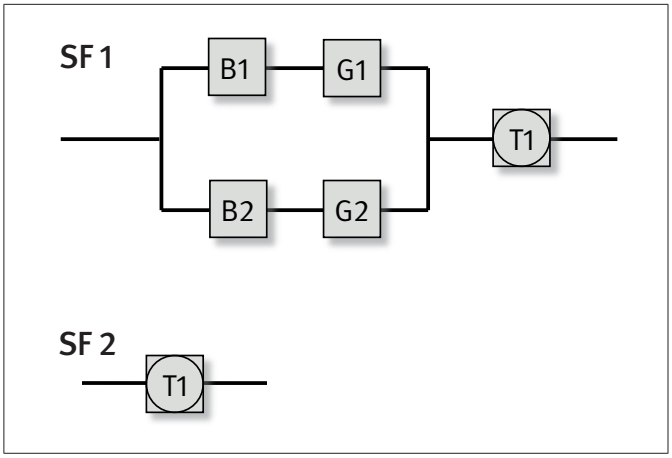


Abbildung B.20:
Sicherheitsbezogene Blockdiagramme zu Beispiel 10

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 BGIA-Reports 2/2008 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 Sicherheitsfunktion SS1 mit Rampenüberwachung 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 gemäß 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 B3 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

- Für den zwangsöffnenden Kontakt von B1 erfolgt ein Fehlerausschluss.
- Für den elektrischen Schließerkontakt von 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 Jahre.
- Das Gleiche gilt für den mechanischen Teil der Positionsschalter B1 und B2. Mit einem B_{10d}-Wert von 1 000 000 Schaltspielen [H] und n_{op} = 7 680 Zyklen/Jahr ergibt sich eine $MTTF_d$ von 1 302 Jahre.

- Der Frequenzumrichter mit der integrierten Sicherheitsfunktion SS1 und der Quittierungsfunktion erfüllt die Anforderungen der Kategorie 3 und von PL d. Die PFH beträgt $2{,}0 \cdot 10^{-7}$/Stunde [H].

- Taster B3 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.

  Hinweis: Derzeit ist zum Thema „Manuelle Rückstellung“ ein Informationsblatt des Fachbereichs Holz und Metall der DGUV, Sachgebiet Maschinen, Anlagen, Fertigungsautomation und -gestaltung in Vorbereitung (www.dguv.de/fb-holzundmetall/publikationen/infoblaetter/infoblatt_deutsch/067_rueckstellfunktion.pdf).

- Der Geberhersteller gibt für die Drehgeber G1 und G2 eine $MTTF_d$ von jeweils 40 Jahren unter Annahme eines Fehlerausschlusses für den Geberwellenbruch an.

- Der DC für die Positionsschalter B1 und B2 beträgt 99 % aufgrund der Plausibilitätsprüfung durch den Frequenzumrichter T1.

- Der DC für die Drehgeber G1 und G2 wird aufgrund des Kreuzvergleichs der Signale im Frequenzumrichter T1 mit 99 % abgeschätzt.

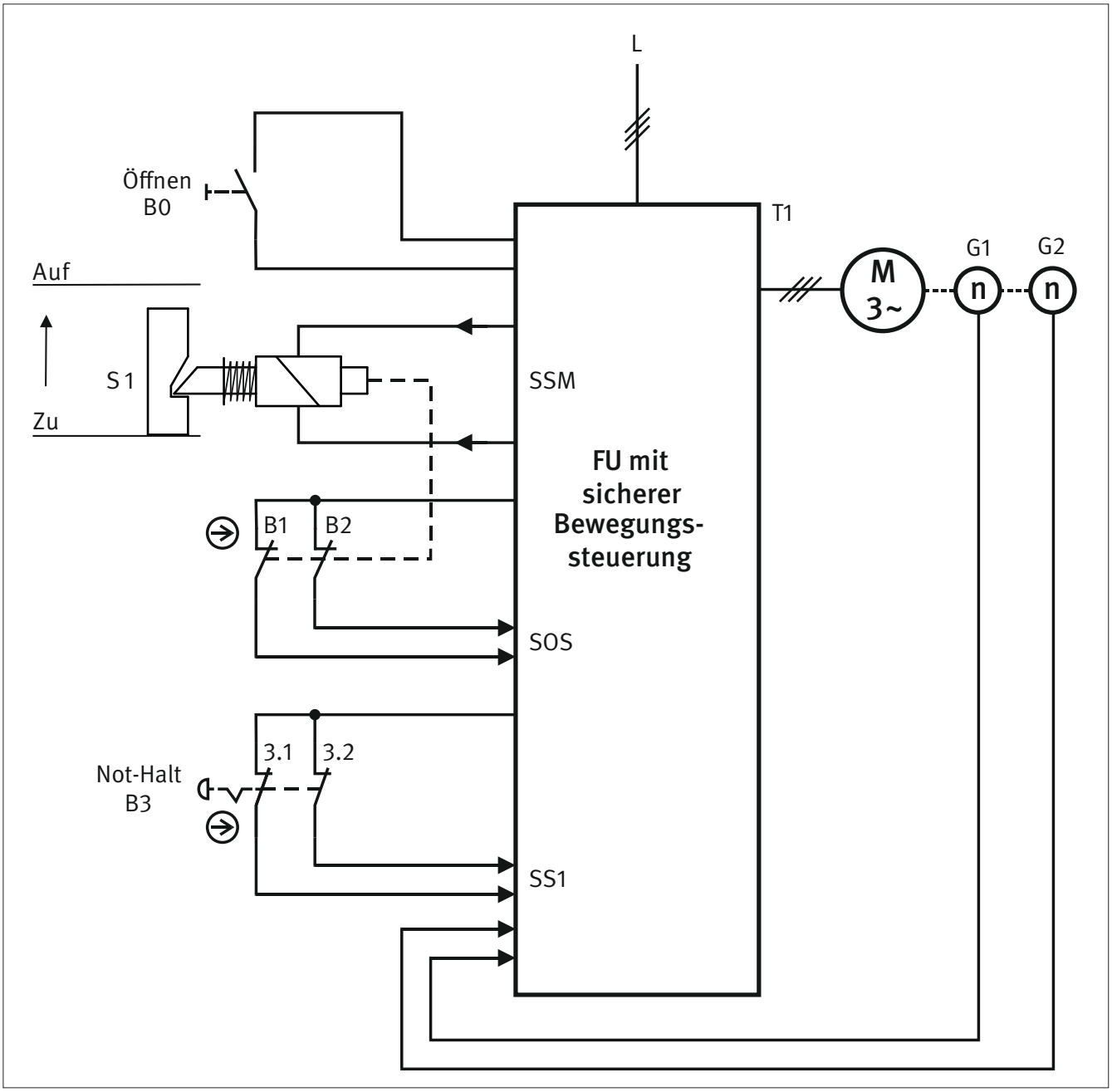
- Für das Subsystem bestehend aus den Positionsschaltern B1/B2 und den Drehgebern G1/G2 werden ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache getroffen (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Schutz gegen Umgebungsbedingungen (25 + 10).

- Für die Sicherheitsfunktion SF 1 „Sicheres Stillsetzen beim Öffnen der Schutztür“ ergibt sich folgende Bewertung: Das Subsystem B1/B2/G1/G2 entspricht Kategorie 3 mit hoher $MTTF_d$ (38 Jahre) und hoher DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}26 \cdot 10^{-8}$/Stunde. Die Kombination der Subsysteme Positionsschalter/Drehgeber (B1/B2/G1/G2) und Frequenzumrichter T1 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}73 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 2 „Manuelle Rückstellung durch Loslassen des betätigten Quittierungstasters B3 bei geschlossener Schutzeinrichtung“ ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}0 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Beispiel 11: Antriebssteuerung mit Frequenzumrichter mit integrierter sicherer Bewegungssteuerung – PL d

Abbildung B.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 durch SSM
- SF 3: Betätigung des Not-Halt-Befehlsgeräts führt zum gesteuerten Stillsetzen SS1

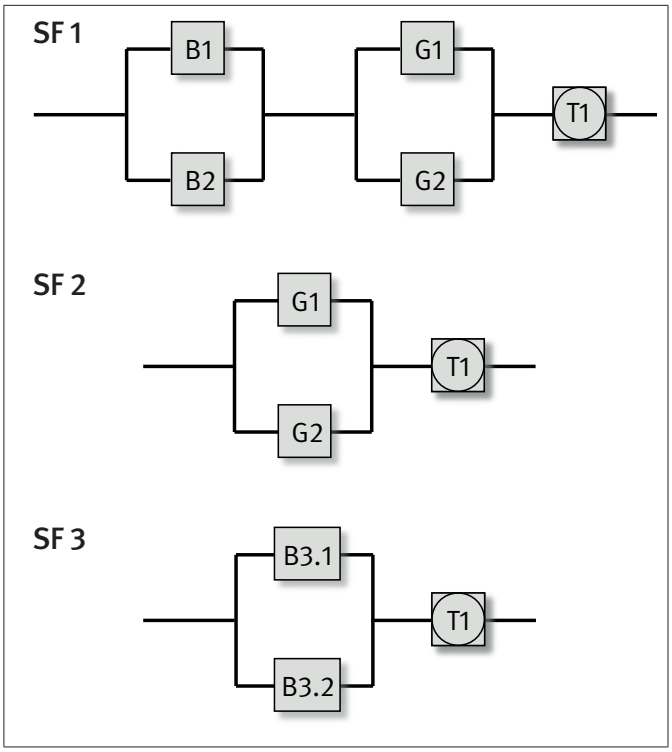


Abbildung B.22:
Sicherheitsbezogene Blockdiagramme zu Beispiel 11

Funktionsbeschreibung

- Das Entsperren der Schutzeinrichtung wird durch Betätigung des Tipptasters B0 angefordert. Daraufhin steuert der Frequenzumrichter T1 den Antrieb auf die Drehzahl Null. Ein Öffnen der Schutzeinrichtung ist nur im Stillstand möglich. Mit der Sicherheitsfunktion SSM (Sichere Geschwindigkeitsüberwachung) erzeugt der Frequenzumrichter bei einer Motordrehzahl von (fast) Null ein sicheres Ausgangssignal zur Entriegelung des Sperrmittels in der Zuhaltung S1.
- Das Entsperren der Schutzeinrichtung wird durch die zwei Positionsschalter B1 und B2 erkannt. Im Frequenzumrichter wird daraufhin die Sicherheitsfunktion SOS (Sicherer Betriebshalt) aktiviert.
- Bei Betätigung des Not-Halt-Befehlsgeräts B3 während einer Motorbewegung erfolgt ein schnellstmögliches gesteuertes Stillsetzen des Antriebs durch SS1 (Sicherer Stopp 1).
- Bei hintertretbaren Bereichen ist zusätzlich eine manuelle Rückstellung der Schutzeinrichtung (Reset) von einem Ort außerhalb des Gefahrenbereichs vorzusehen.

Konstruktive Merkmale

- Der Frequenzumrichter T1 verfügt über die integrierten Sicherheitsfunktionen SOS, SS1, SSM und STO (in diesem Beispiel nicht verwendet).
- Bei der Funktion SS1 ist zu beachten, dass im Fehlerfall des Frequenzumrichters ggf. nur ein reduziertes Bremsmoment zur Verfügung steht.
- Die Anbringung der zwei Drehgeber 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. Je nach eingesetztem Frequenzumrichter und zu realisierender Sicherheitsfunktion kann auf den zweiten Geber verzichtet werden, in einigen Fällen ist auch ein sensorloser Betrieb möglich. In jedem Fall sind die Anforderungen in der Anwenderdokumentation des Frequenzumrichter-Herstellers 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 der Zuhaltung S1. 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 und B2 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 und B2 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, da das Sperrmittel nur bei geschlossener Schutztür in die Stellung „zugehalten“ gelangen kann. Aufgrund der zwangläufigen Betätigung der Kontakte wird ein Fehlerausschluss für das Nichtöffnen des elektrischen Kontakts angenommen.

- Für die Mechanik der Zuhaltung 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 Neufassung der BGI 575/670 „Auswahl und Anbringung von Verriegelungseinrichtungen“ (in Vorbereitung).
  – keine Verwendung als mechanischer Endanschlag
  – unlösbare Befestigung des Betätigers
  – regelmäßige Wartung
  – Formschluss nach Montage
  – ausreichende mechanische Festigkeit aller Träger- und Funktionselemente
  – 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.

- Für das Not-Halt-Befehlsgerät B3 ist gemäß DIN EN ISO 13849-2:2013, Tabelle D.8, und BGIA-Report 2/2008, Tabelle D.2, bis zu einer Betätigungszahl von 6 050 Zyklen ein Fehlerausschluss für zwangsöffnende Kontakte und die Mechanik möglich.

- Die Drehgeber G1 und G2 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. Die Anbringung der Drehgeber muss so erfolgen, dass der gleichzeitige Ausfall durch einen einzigen Fehler (z. B. Geberwellenbruch) ausgeschlossen ist.

- Bei dem Frequenzumrichter T1 mit sicherer Bewegungssteuerung handelt es sich um ein Gerät mit den integrierten Sicherheitsfunktionen

  – Sicher abgeschaltetes Moment (STO)
  – Sicheres Stillsetzen (SS1)
  – Sicherer Betriebshalt (SOS)
  – Sichere Geschwindigkeitsüberwachung (SSM)

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

- Aufgrund der Plausibilitätsprüfung durch den Frequenzumrichter T1 wird für die Drehgeber G1 und G2 ein DC von 90 % angenommen.

- Für das Subsystem G1/G2 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).

- Das Subsystem G1/G2 entspricht Kategorie 3 mit hoher $MTTF_d$ (50 Jahre) und mittlerem DC (90 %). Dies ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}22 \cdot 10^{-7}$/Stunde im Bereich von PL d.

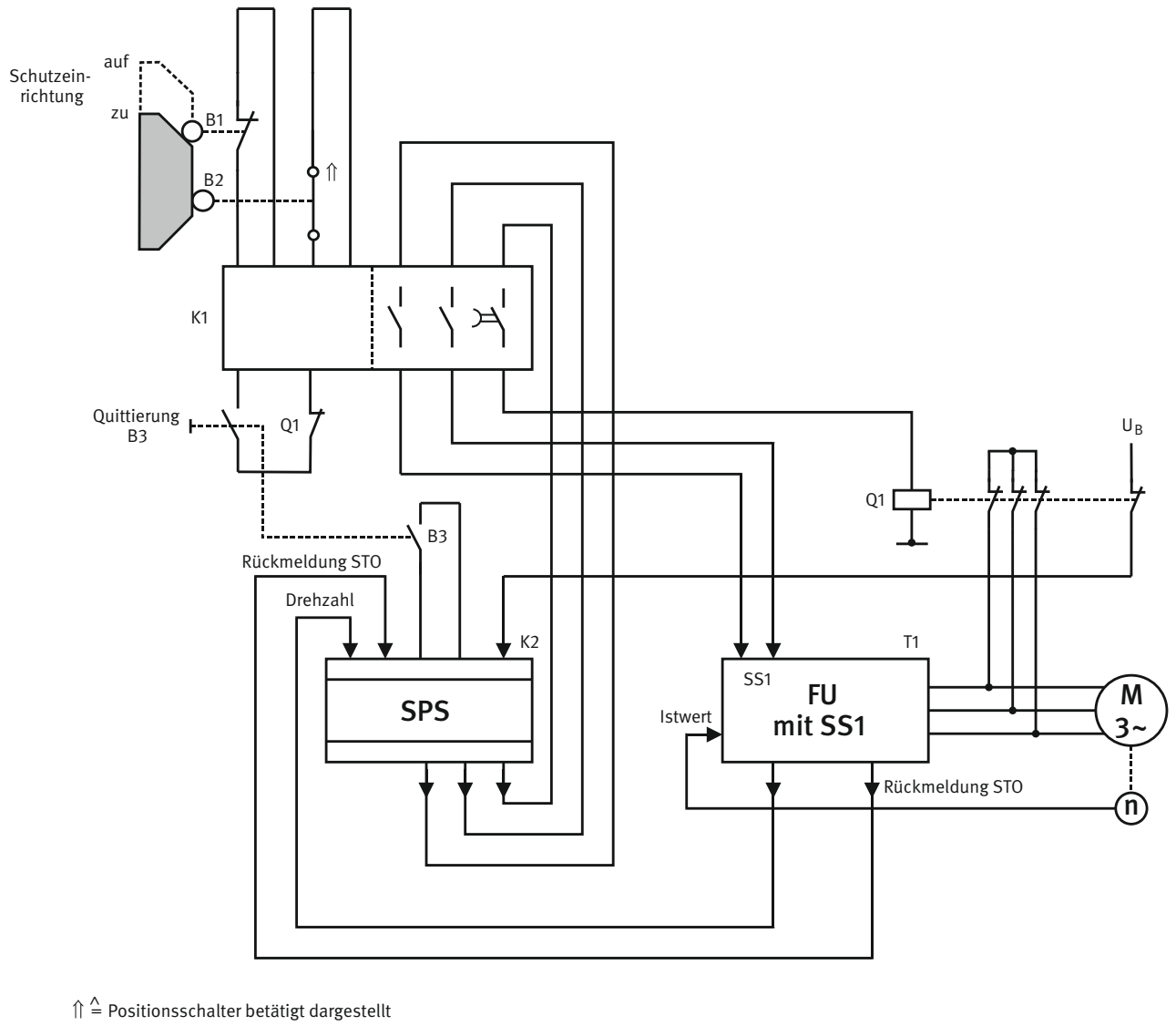
- Für die Sicherheitsfunktion SF 1 „Sicherer Betriebshalt (SOS) bei entsperrter Zuhaltung“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}72 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für die Sicherheitsfunktion SF 2 „Entsperrung der Zuhaltung im Stillstand durch SSM“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}72 \cdot 10^{-7}$/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 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5 \cdot 10^{-8}$/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 B.23:
Prinzipschaltbild der Antriebssteuerung



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. 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.

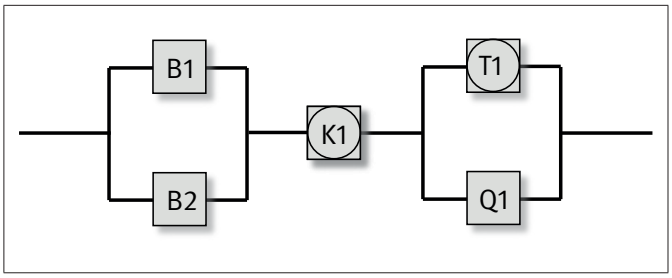


Abbildung B.24:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 12

Funktionsbeschreibung

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

- Ein Verschweißen des Schützes Q1 würde sich beim Aufschalten der Versorgungsspannung des Motors über T1 durch Ansprechen der Ausgangsabsicherung stets bemerkbar machen. Darüber hinaus wird das Schütz Q1 in der SPS K2 auf „Hängenbleiben“ überwacht.

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

  – die Steuerelektronik von T1 aus dem Gleichspannungszwischenkreis versorgt wird,
  – 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 BGIA-Reports 2/2008 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 Sicherheitsfunktionen 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 hintertretbaren Gefahrenbereichen ist eine Quittierung 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 des SS1 bewirkt das Schütz Q1 einen Kurzschluss der Betriebsspannung des Motors und wird voraussichtlich beschädigt. Daher ist 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 der Betriebsartenwahl wurde z. B. verzichtet.

Berechnung der Ausfallwahrscheinlichkeit

- Für den zwangsöffnenden Kontakt von B1 erfolgt ein Fehlerausschluss.
- Für den elektrischen Schließerkontakt von 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.
- Das Gleiche gilt für den mechanischen Teil der Positionsschalter B1 und B2. Mit einem B_{10d}-Wert von 1 000 000 Schaltspielen [H] und n_{op} = 96 000 Zyklen/Jahr ergibt sich eine $MTTF_d$ von 104 Jahre.
- Bei dem Sicherheitsbaustein K1 handelt es sich um ein handelsübliches Gerät für den Einsatz in PL e und Kategorie 4. Der PFH-Wert beträgt $1{,}8 \cdot 10^{-8}$/Stunde [H].
- Das Schütz Q1 hat eine mechanische Lebensdauer von $2 \cdot 10^6$ 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 $MTTF_d$ = 416 Jahre.
- Der Frequenzumrichter T1 verfügt über die Sicherheitsfunktion STO mit einem Rückmeldeausgang. Er ist geeignet für den Einsatz in PL d und Kategorie 3, der PFH-Wert des STO beträgt $2 \cdot 10^{-7}$/Stunde.

  Wie im sicherheitsbezogenem Blockdiagramm (Abbildung 24) dargestellt, ist 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 $MTTF_d = 1/PFH$ ergibt sich für T1 $MTTF_d$ = 570 Jahre. Die interne DC von 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 Sicherheitsfunktion STO des Frequenzumrichters T1 erfolgt extern, im vorliegenden Fall in der SPS K2 durch Vergleich von Q1 und Rückmeldung STO. Für diese Fehlererkennung wird eine DC von 99 % angenommen.
- Der DC für B1 und B2 wird mit 99 % aufgrund der Überwachung durch den Sicherheitsbaustein K1 angegeben.
- Der DC von Schütz Q1 wird mit 99 % angenommen. Das Schütz Q1 wird in der SPS K2 auf „Hängenbleiben“ überwacht.

  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.

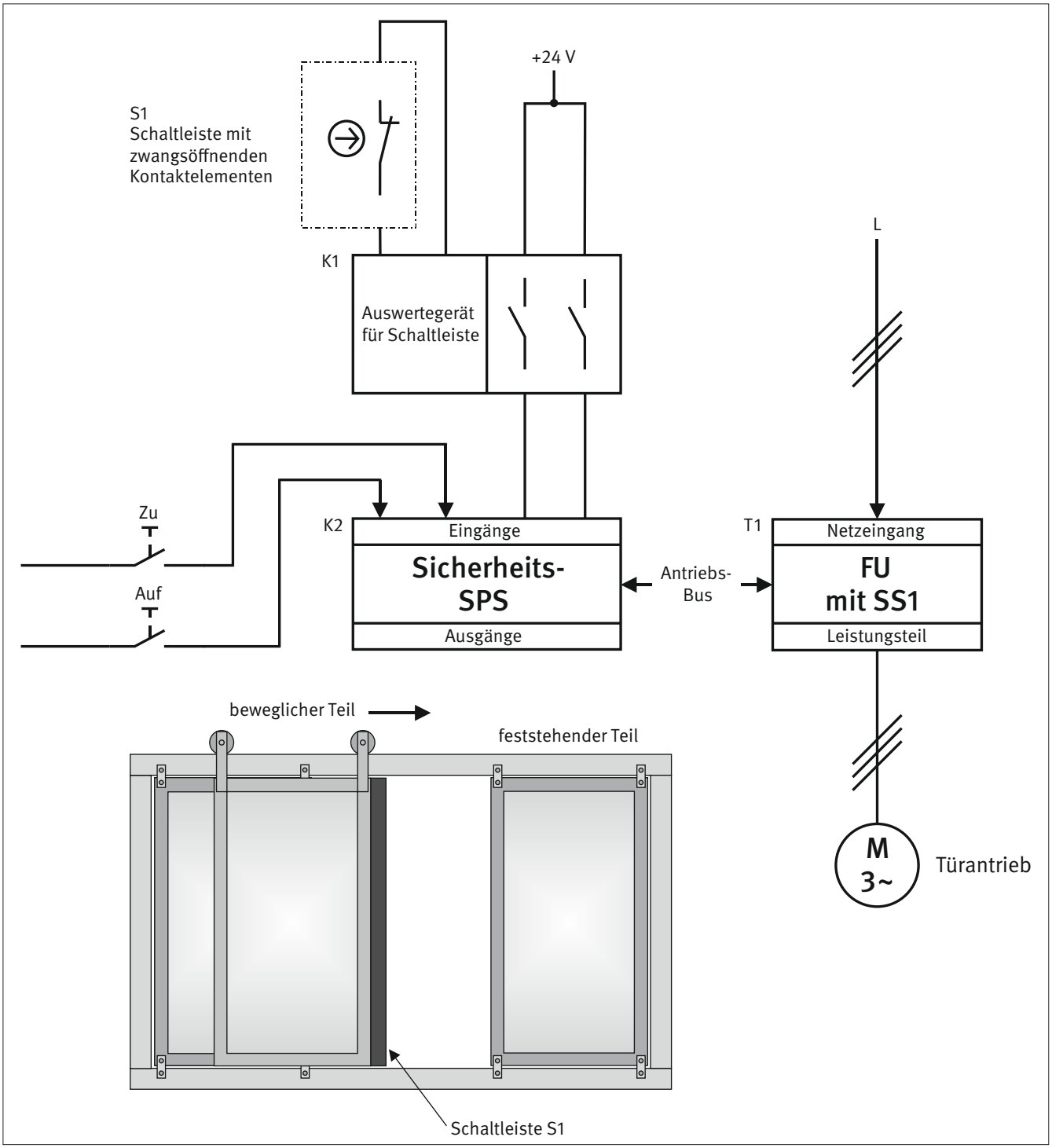
  Für die Ausführung der Sicherheitsfunktion ist ein Schließen der Öffnerkontakte von Q1 erforderlich, sodass im Fehlerfall von T1 ein Stromfluss möglich ist (Abweichung vom Ruhestromprinzip).

  Der Hersteller von 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 sowie für das Subsystem aus T1 und Q1 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).

- Das Subsystem B1/B2 entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (78,6 Jahre) und hohem DC (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $3{,}23 \cdot 10^{-8}$/Stunde.
- Wegen der in dieser Anwendung begrenzten Gebrauchsdauer von B1 und B2 wird ein rechtzeitiger Austausch nach zehn Jahren empfohlen.
- Das Subsystem T1/Q1 entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und hohem DC (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde.
- Für die Sicherheitsfunktion SF 1 „STO des Motors nach Öffnen der Schutzeinrichtung und erfolgter Stillsetzung“ ergibt sich folgende Bewertung: Die Kombination ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}5 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

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

Abbildung B.25:
Prinzipschaltbild der Antriebssteuerung



Sicherheitsfunktion

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

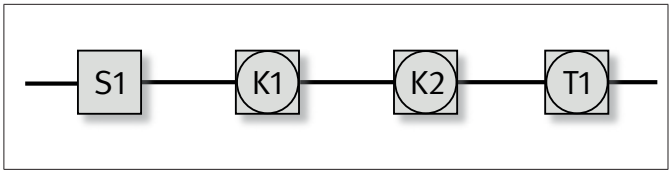


Abbildung B.26:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 13

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 S1 an der Schließkante ausgerüstet. Die Betätigung der Schaltleiste beim Schließen der Schutztür setzt über das Auswertegerät K1, die Sicherheits-SPS K2 und den Frequenzumrichter T1 den Antrieb so schnell still, dass die zulässigen Schließkräfte nicht überschritten werden.

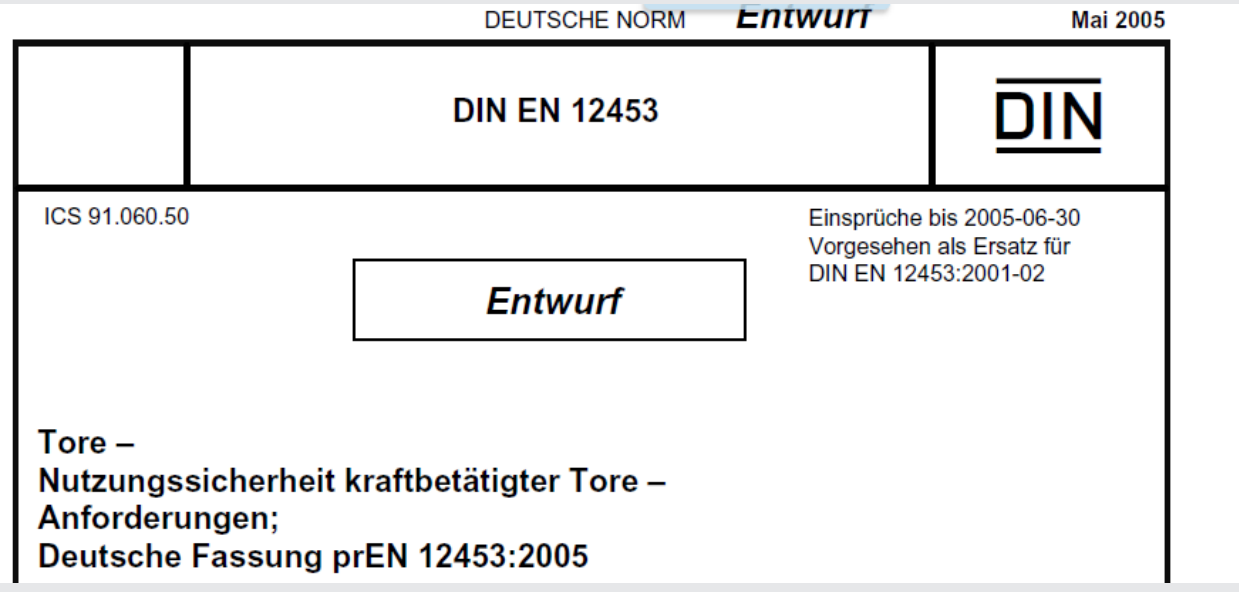
  Bemerkungen: Grenzwerte für kraftbetriebene trennende Schutzeinrichtungen.

- 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 hierzu 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


DEUTSCHE NORM Entwurf Mai 2005

DIN EN 12453

DIN

ICS 91.060.50

Einsprüche bis 2005-06-30
Vorgesehen als Ersatz für
DIN EN 12453:2001-02

Entwurf

Tore –
Nutzungssicherheit kraftbetätigter Tore –
Anforderungen;
Deutsche Fassung prEN 12453:2005

- 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 B.27 und Tabelle B.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

  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 B.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.

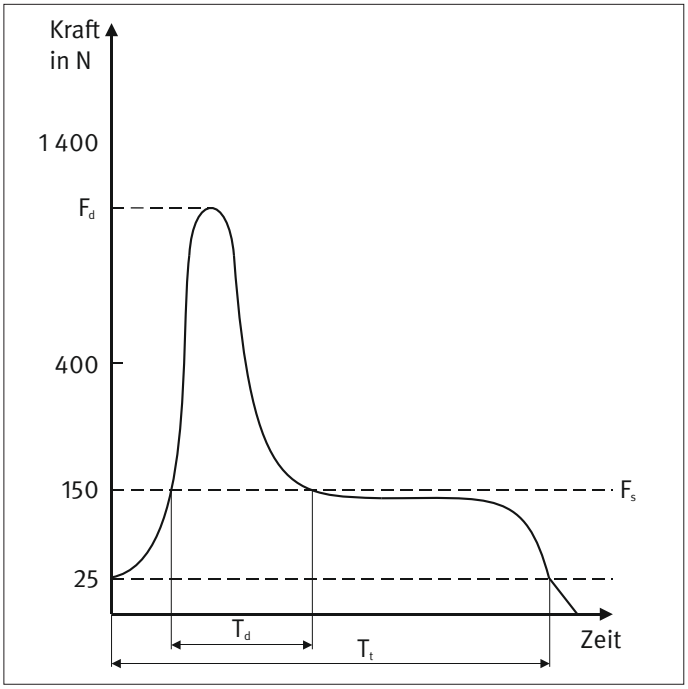


Abbildung B.27:
Schließkräfte in Abhängigkeit von der Zeit aus DIN EN 12453

Tabelle B.2:
Zulässige dynamische Kräfte

Zulässige dynamische Kräfte in N	Zwischen Schließkanten und Gegenschließkanten		Zwischen ebenen Flächen 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

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 BGIA-Reports 2/2008 beschrieben, sind vorgesehen.

- Fehler in den elektrischen Anschlussleitungen dürfen sich nicht gefährlich auswirken. Auftretende Fehler werden erkannt und ein sicherer Zustand 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 S1 erfüllt die Anforderungen nach DIN EN 1760-2 und dient der Absicherung von Quetsch- und Scherstellen. Die Schaltleiste ist über das Auswertegerät K1 mit der Steuerung verbunden. Das Auswertegerät K1 erfüllt die Anforderungen nach DIN EN ISO 13849-1 für Kategorie 4, PL e. Fehler in den Zuleitungen zur Schaltleiste werden über das Schaltgerät K1 erkannt und das Schaltgerät schaltet sicher ab.

- Der Maschinenhersteller muss die Eignung der Schaltleiste für die jeweilige Applikation überprüfen (z. B. auf ausreichenden Verformungsweg, Berücksichtigung der Umgebungseinflüsse und Wirkbereich). Der Hersteller der Schaltleiste bestätigt für die individuelle Applikation einen Fehlerausschluss für ein Nichtöffnen der Schaltleistenkontakte bei Betätigung.

- Die Antriebssteuerung T1 verfügt über die Sicherheitsfunktion SS1.

- Bei der Sicherheits-SPS K2 und der Antriebssteuerung T1 handelt es sich um Sicherheitsbauteile für den Einsatz bis Kategorie 4 und PL e (K2) bzw. Kategorie 3 und PL d (T1). Auftretende Fehler werden erkannt und der sichere Zustand wird eingeleitet. Die Verbindungen zwischen der Sicherheits-SPS K2 und der Antriebssteuerung T1 erfolgen über ein Sicherheitsbussystem für den Einsatz in PL d entsprechend dem BGIA-Report 2/2008, Abschnitt 6.2.17.

- Die Programmierung der Anwendungssoftware (SRASW) in K2 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 S1 wird vom Hersteller ein Fehlerausschluss für das Nichtschalten der Schaltleiste bei Betätigung bestätigt.

- Der Hersteller gibt für das Auswertegerät K1 eine PFH von $2 \cdot 10^{-8}$/Stunde [H] an.

- Die Sicherheits-SPS K2 weist eine PFH von $1{,}0 \cdot 10^{-8}$/Stunde [H] auf.

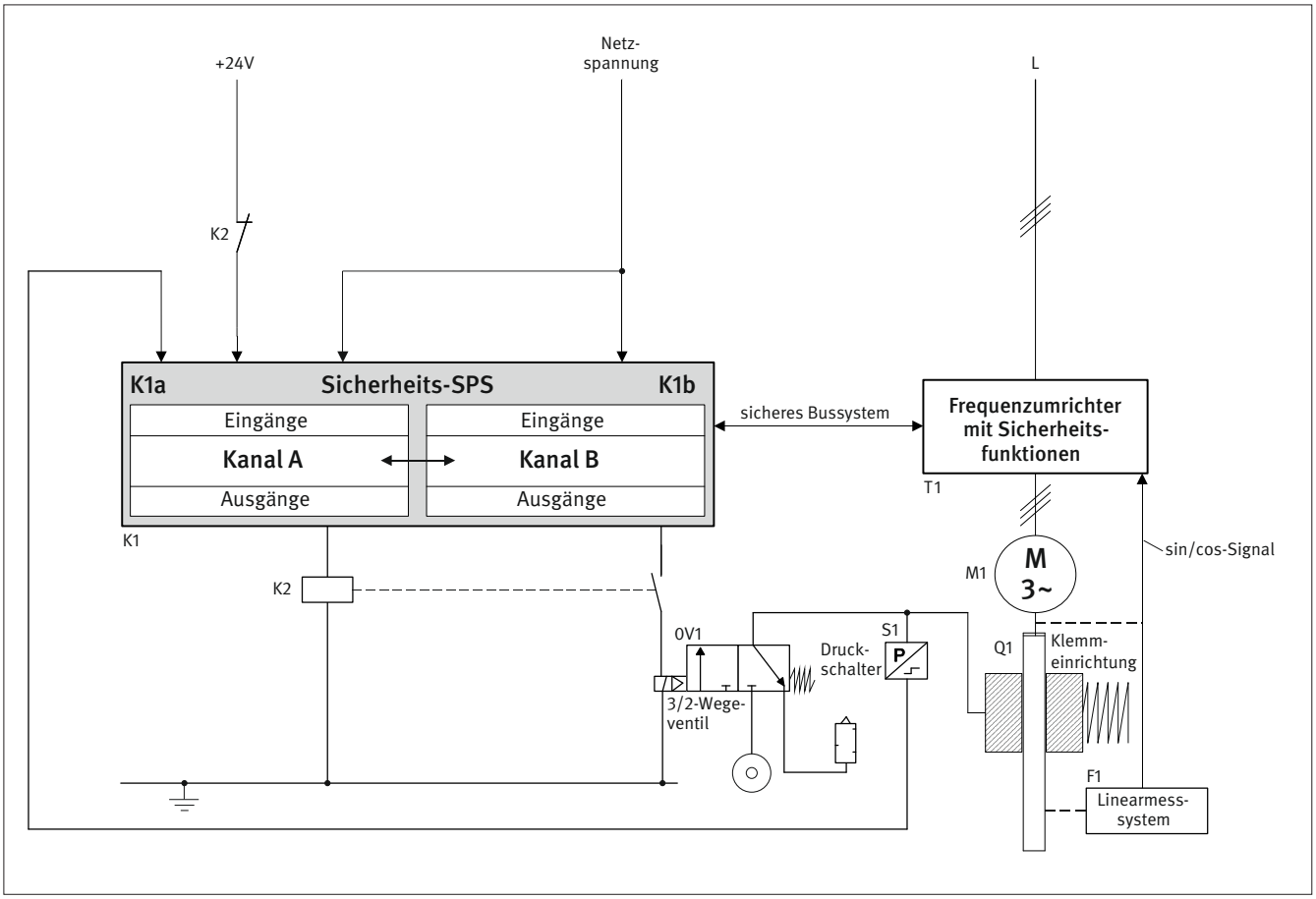
- Die Antriebssteuerung T1 geht mit einer PFH von $1{,}5 \cdot 10^{-8}$/Stunde [H] und PL d in die Berechnung ein.

- Da für S1 ein Fehlerausschluss zulässig ist und K1, K2 sowie T1 gekapselte Subsysteme sind, ist eine Betrachtung von CCF nicht erforderlich.

- Für die Sicherheitsfunktion SF 1 „Begrenzung der Schließkräfte einer kraftbetätigten Tür durch Betätigung einer Schaltleiste“ ergibt sich folgende Bewertung: Die Kombination der Subsysteme ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}5 \cdot 10^{-8}$/Stunde im Bereich von PL e. Aufgrund der Antriebssteuerung T1 in PL d ergibt sich für die gesamte Sicherheitsfunktion der PL zu d.

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

Abbildung B.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 Frequenzumrichter T1. Bei der Sicherheits-SPS handelt es sich um eine SPS K1a in Verbindung mit einer NC-Achssteuerung K1b. K1 übernimmt Plausibilitätsprüfungen z. B. hinsichtlich des Steuerdrucks der Klemmeinrichtung Q1 und deren Ansteuerung.

- Das Abbremsen der Achse im Einricht- und Automatikbetrieb erfolgt durch SS1. Beim anschließenden sicheren Hochhalten wird die Last der Vertikalachse durch die integrierte Sicherheitsfunktion SOS (Safe Operating Stop, Motor steht still und widersteht externen Kräften) des Frequenzumrichters T1 in der Lage gehalten. Die Position der Last wird vom Linearmesssystem F1 und dem Frequenzumrichter 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 T1 und dem Einfallen der pneumatisch gelüfteten Klemmeinrichtung Q1 durch K1 und 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).

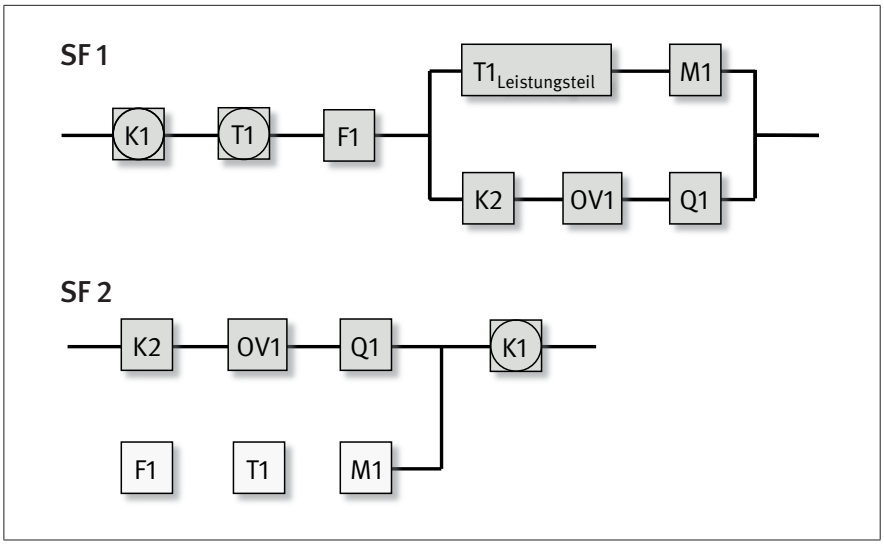


Abbildung B.29:
Sicherheitsbezogene Blockdiagramme zu Beispiel 14

- Bei SF 2 „Sicheres Hochhalten bei Spannungsausfall“ handelt es sich um das Verhalten der Steuerung unter Berücksichtigung der Unterbrechung der Energieversorgung gemäß DIN EN 12100, Abschnitt 6.2.11.5. Die Unterbrechung der Spannungsversorgung wird in K1 erkannt (Überwachung der Netzspannung). Da die Steuerspannung für K1 über eine ausreichende Pufferzeit verfügt, erfolgt das Einfallen der Klemmeinrichtung Q1 nicht durch das „langsame“ Absinken der Ausgangsspannung von K1, sondern schnellstmöglich durch Wegschalten des Ausgangssignals. Nach der Stillsetzung von M1 verhindert 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 Frequenzumrichter T1 erkannt und die Klemmeinrichtung direkt angesteuert wird (z. B. durch SSM). Hierzu muss jedoch die Steuerspannung für 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 SF1 „Sicheres Hochhalten im Einricht- und Automatikbetrieb (SOS)“ gewährleistet.

  2. Spannungsausfall:

  Bei Erkennung des Spannungsausfalls durch die SSPS K1 wird SF 2 aktiviert. Der Frequenzumrichter T1 ist bei Spannungsausfall nicht in der Lage, die Vertikalachse stillzusetzen, weil seine Steuerspannung nicht aus der Zwischenkreisspannung erzeugt wird (nicht gepuffert ist). Die Sicherheits-SPS wird aus einem gepufferten Netzteil versorgt und lässt die federkraftbetätigte Klemmeinrichtung Q1 einfallen.

  Für den Fall des Spannungsausfalls stellt die Klemmeinrichtung Q1 und die Ansteuerung durch K2 und 0V1 ein Kategorie-2-System nach DIN EN ISO 13849-1 dar. Die erforderliche Testung der Klemmeinrichtung erfolgt alle acht Stunden in statischer und halbjährlich in dynamischer Weise. 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 K2 und 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 über den Linearmotor M1 mit dem 1,5-fachen Lastmoment belastet. Falls die Position der Last im vorgegebenen Bereich gehalten wird, ist die ordnungsgemäße Funktion der Klemmeinrichtung gegeben. Falls

die vorgegebene Position verlassen wird, muss die Klemmeinrichtung entsprechend der Betriebsanleitung überprüft oder gegebenenfalls getauscht werden. Die Position wird über das Linearmesssystem F1 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 wird der Antriebsmotor momentenfrei geschaltet und das Wegeventil 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 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 Frequenzumrichter mit integrierten Sicherheitsfunktionen T1 handelt es sich um Sicherheitsbauteile für den Einsatz in PL d, die der Kategorie 3 und den jeweiligen Produktnormen entsprechen. Der Frequenzumrichter beinhaltet hier die Sicherheitsfunktionen SOS, SS1 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 F1 liefert redundante Positionsinformationen (sin/cos) und ist in den Regelkreis der Lageregelung eingebunden. Das Messsystem wird am Frequenzumrichter 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 Frequenzumrichter T1 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 4.6.3 und ggf. 4.6.4 der DIN EN ISO 13849-1.

- Bei dem Datenbus zwischen T1 und 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 mit berücksichtigt 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 DIN EN ISO 13849-1).

- Bemerkung zur Klemmeinrichtung Q1 bei Versagen von 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-Wert beträgt $8{,}97 \cdot 10^{-8}$/Stunde [H]. Die Kategorie 3 und der PL d wird vom Hersteller bestätigt.

- Der Frequenzumrichter T1 verfügt über die integrierten Sicherheitsfunktionen SOS, SS1 und STO. Der PFH-Wert für die Sicherheitsfunktionen des Frequenzumrichters beträgt $2{,}31 \cdot 10^{-8}$/Stunde [H]. Für SF 1 muss jedoch der Leistungsteil des Frequenzumrichters noch hinzugerechnet werden, weil die Vertikalachse aktiv hochgehalten werden muss, um ein Abstürzen zu verhindern. Der Leistungsteil von 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 $2 \cdot 10^6$ 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 angegeben [N]. Hieraus ergibt sich bei einer jährlichen Betätigung von 620 Schaltspielen eine $MTTF_d$ von 322 580 Jahre.

- Bei der Klemmeinrichtung Q1 handelt es sich um eine spezielle Linearbremse (Notfallbremse mit Haltebremsfunktion für lineare Bewegungen) mit einer Schaltspielzahl von 200 000 Zyklen [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 Zyklen [H] und dient als Schätzwert für B_{10d}. Mit einer zur sicheren Seite hin abgeschätzten Betätigungshäufigkeit von 20/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 $0{,}5 \cdot MTTF_d$ 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 BGIA-Report beschrieben wird (siehe BGIA-Report 2/2008, Abschnitt 6.2.14, S. 54, und Abschnitt 4 des SISTEMA-Kochbuchs 4).

- Für das Linearmesssystem F1 gibt der Hersteller eine Ausfallrate von $1{,}5 \cdot 10^{-6}$/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 wird aufgrund der ständigen Überwachung durch den Frequenzumrichter T1 auf 99 % angesetzt. Unter Berücksichtigung der DC von 99 % ergibt sich eine gefahrbringende Ausfallwahrscheinlichkeit von $1{,}5 \cdot 10^{-8}$/Stunde.

- Für die Quantifizierung des Kategorie-2-Subsystems von SF 2 sind $MTTF_d$-Werte für die einzelnen Blöcke erforderlich. Da für T1 und F1 nur jeweils ein PFH-Wert vorhanden ist, gilt näherungsweise der Ansatz $MTTF_d$ = 1/PFH (siehe hierzu SISTEMA-Kochbuch 4, Abschnitt 2). Für F1 ergibt sich $MTTF_d$ = 7 610 Jahre.

- Für T1 (Leistungsteil + Regler) ergibt sich die Ausfallwahrscheinlichkeit zu $MTTF_d = (1/40 + 1/4\,942)^{-1}$ Jahre = 39,6 Jahre.
- Für den DC des Hilfsschützes K2 kann ein Wert von 99 % angegeben werden, da stets eine Rücklesung in die Sicherheits-SPS K1 erfolgt.
- Für den DC des Linearmotors M1 wird ein Wert von 60 % angenommen, weil eine Testung durch den Prozess vorliegt.
- Das Pneumatikventil 0V1 wird über den Druckschalter S1 auf seine Funktion getestet (DC = 99 %).
- Für die Klemmeinrichtung Q1 erfolgt für den DC ein Ansatz von 60 %.
- Für das Subsystem Lageregelung oder Abschaltung der Sicherheitsfunktion SF1 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 ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $3{,}11 \cdot 10^{-7}$ 1/Stunde. Dies entspricht PL d.
- Für die Sicherheitsfunktion SF 2 „Sicheres Hochhalten bei Spannungsausfall“ ergibt sich folgende Bewertung: Die Kombination der Blöcke ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}14 \cdot 10^{-6}$ 1/Stunde. Dies entspricht PL c.

Literatur

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

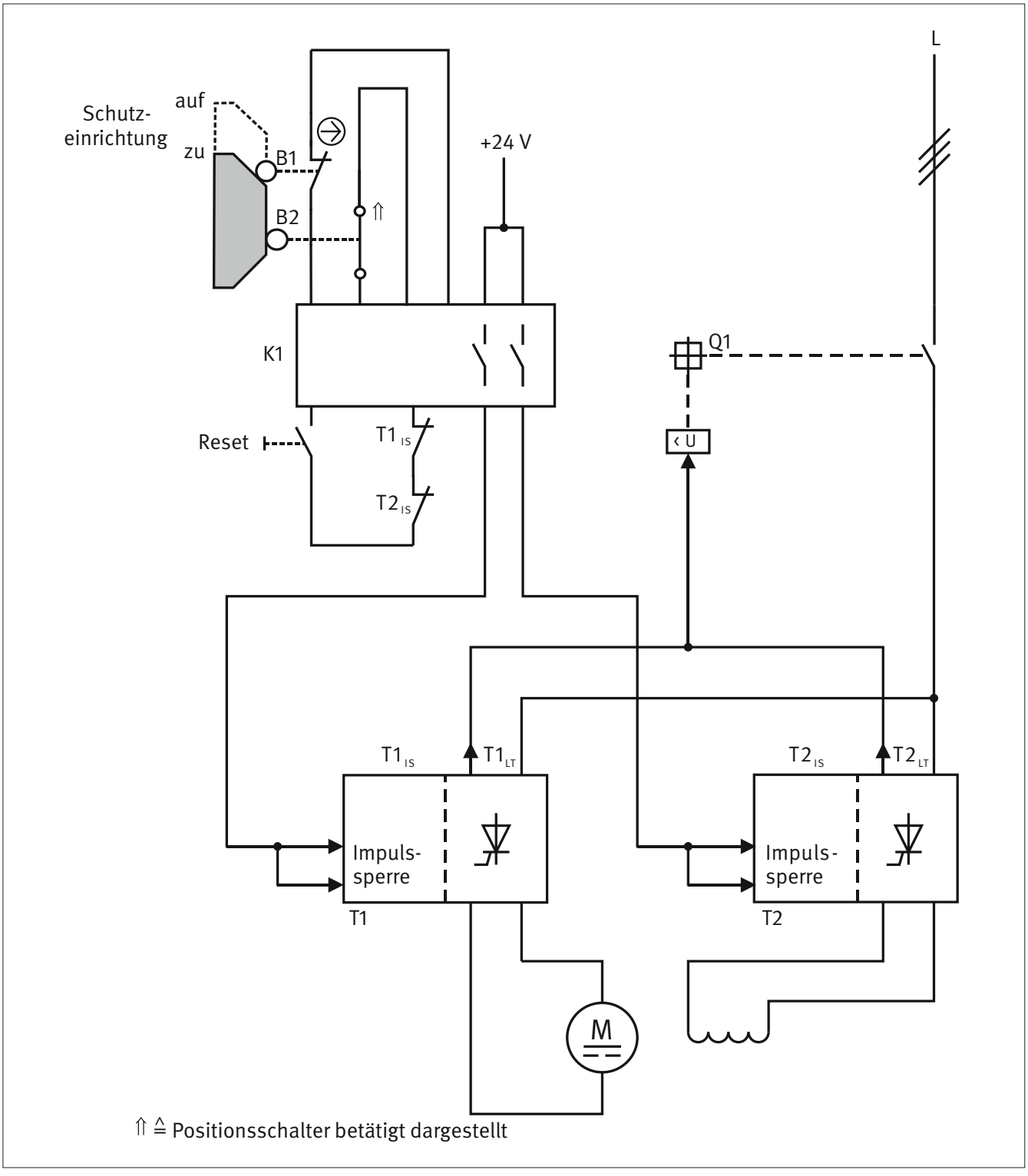
[2] Fachbereichs-Informationsblatt Nr. 005. Schwerkraftbelastete Achsen – Vertikalachsen. Ausg. 9/2012. Hrsg.: Fachbereich Holz und Metall der Deutschen Gesetzlichen Unfallversicherung, Mainz. www.dguv.de/fb-holzund metall/publikationen/infoblaetter/infobl_deutsch/005_vertikalachsen.pdf

[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 B.30:
Prinzipschaltbild der Antriebssteuerung



Sicherheitsfunktion

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

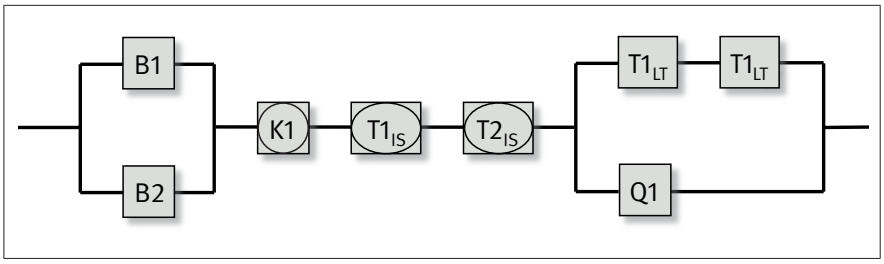


Abbildung B.31:
Sicherheitsbezogenes Blockdiagramm zu Beispiel 15

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 von K1 werden in den Gleichstromstellern für den Ankerstrom T1 und für das Erregerfeld T2 jeweils die Eingänge der Impulssperre zweikanalig abgeschaltet. Im Gleichstrommotor wird dadurch der Aufbau eines Drehmoments verhindert.

- Der drehstromgespeiste Gleichstromantrieb wird funktional durch eine SPS gesteuert. Die SPS selbst ist nicht an der Sicherheitsfunktion beteiligt und ist hier auch nicht dargestellt. Das Prinzipschaltbild (Abbildung B.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 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 von K1 eingebunden sind.

- Fehler im Leistungsteil von T1 und T2 werden 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. Q1 wird nicht bei jeder Anforderung der Sicherheitsfunktion abgeschaltet, sondern ausschließlich bei Fehlern im Leistungsteil der Gleichstromsteller.

  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 Motors 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 BGIA-Reports 2/2008 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 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 Q1 (einschließlich Unterspannungsauslöser) regelmäßig überprüft werden. Ein solcher Test kann beispielsweise im Rahmen der Wiederholungsprüfungen durchgeführt werden.

Berechnung der Ausfallwahrscheinlichkeit

- Für den zwangsöffnenden Kontakt von B1 erfolgt ein Fehlerausschluss.
- Für den elektrischen Schließerkontakt von 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.
- Das Gleiche gilt für den mechanischen Teil der Positionsschalter B1 und B2. Mit einem B_{10d}-Wert von 1 000 000 Schaltspielen [H] und n_{op} = 3 840 Zyklen/Jahr ergibt sich eine $MTTF_d$ von 2 604 Jahren.
- Der Sicherheitsbaustein K1 erfüllt die Anforderungen für Kategorie 4 und PL e. Die PFH beträgt $2{,}31 \cdot 10^{-9}$/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 beträgt jeweils $3{,}16 \cdot 10^{-7}$/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 ein B_{10d} von 5 000 Schaltspielen [H] angegeben. Bei n_{op} = 100 Zyklen/Jahr ergibt sich eine $MTTF_d$ von 500 Jahren.
- Der DC 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 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 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 Sicherheitsfunktion 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 = $2{,}47 \cdot 10^{-8}$/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 = $2{,}89 \cdot 10^{-8}$/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 = $6{,}88 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Anhang C:
Fachbereichs-Informationsblätter

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

Tabelle C.1:
Übersicht über die Fachbereichs-Informationsblätter in diesem Anhang

Nr. und Titel des Informationsblattes		Internetadresse
005	Schwerkraftbelastete Achsen – Vertikalachsen	www.dguv.de/fb-holzundmetall/publikationen/infoblaetter/infobl_deutsch/005_vertikalachsen.pdf
047	Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen	www.dguv.de/fb-holzundmetall/publikationen/infoblaetter/infobl_deutsch/047_ueberlagerte_gefaehrdung.pdf
050	Fluidtechnische Leistungselemente – Hydraulische und pneumatische Motoren und Zylinder	www.dguv.de/fb-holzundmetall/publikationen/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

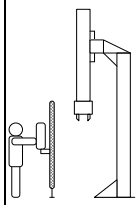
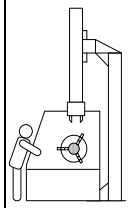
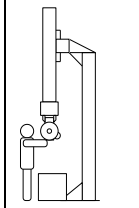
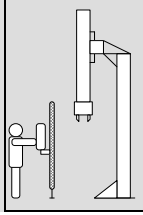
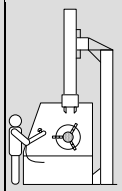
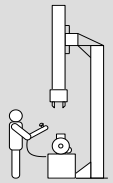
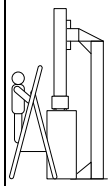
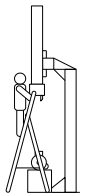
Betriebs-art	Gefährdungssituation/ Bestimmungsgemäße Verwendung		Schutzmaßnahmen	
			Technische	Organisatorische
Automatik-Manueller Eingriff A1		Die Vertikalachse befindet sich während des manuellen Eingriffs in einer für den Bediener gefahrlosen Position (Zugangsgesicherter Bereich).	- Für trennende 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.

Fachausschuss-Informationsblatt Nr. 047

Ausgabe 05/2010

Deutsche Gesetzliche Unfallversicherung
Fachausschuss
Maschinenbau, Fertigungssysteme, Stahlbau

Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen

In Arbeitsbereichen an komplexen Fertigungssystemen und Werkzeugmaschinen kann es zu Überlagerungen von Gefährdungen durch gefahrbringende Bewegungen kommen, hervorgerufen z. B. durch eine Vielzahl geregelter Achsantriebe. Dieses Fachausschuss-Informationsblatt beschreibt eine mit Arbeitsschutzexperten und dem Institut für Arbeitsschutz der DGUV abgestimmte Vorgehensweise, die es unter Anwendung der DIN EN ISO 13849-1 [1] oder DIN EN 62061 [2] erlaubt, Sicherheitsfunktionen bei überlagerten Gefährdungen abzubilden und zu berechnen.

Quelle: WFL Millturn Technologies GmbH & Co. KG

Bild 1: Achsschema einer Werkzeugmaschine

Überlagerte Gefährdungen sind charakterisiert durch das gleichzeitige Einwirken mehrerer Einzelgefährdungen auf eine oder mehrere zu schützende Personen, Körperteile oder Gliedmaßen, welche sich an einem Ort aufhalten oder gefahrbringende Bereiche erreichen können (siehe Bild 1).

Unter einer Einzelgefährdung wird sowohl die Bewegung einer einzelnen Achse, als z. B. auch eine Gefährdung durch die Bewegung eines gesamten Maschinenteils verstanden. Resultiert also die Bewegung eines Maschinenteils aus dem kinematischen Zusammenwirken einer oder mehrerer Achs- und Spindelantriebe (z. B. ein Fräswerkzeug am Support eines Bearbeitungszentrums), so kann dies als Einzelgefährdung betrachtet werden.

1 Ausgangslage

Die Betrachtung von Einzelgefährdungen ist in der Sicherheitstechnik gängige Praxis und hat sich bewährt. Aus der probabilistischen Betrachtung nach DIN EN ISO 13849-1 oder DIN EN 61508 [3, 4] und DIN EN 62061 und der Risikobeurteilung für eine Gefährdungssituation ergibt sich jedoch, dass auch die Überlagerung von Gefährdungen betrachtet werden muss. Eine Diskussionsvorlage zu den Auswirkungen des probabilistischen Ansatzes auf die Betrachtung überlagerter Gefährdungen findet sich in [5], welcher durch dieses Fachausschuss-Informationsblatt präzisiert und erweitert wird.

Auf Grund der weitgefächerten Bandbreite von Gefährdungssituationen an den oben genannten Mensch-Maschine-Schnittstellen kann dieses Fachausschuss-Informationsblatt hinsichtlich deren Betrachtungsweise keine universelle bzw. allgemeingültige Festlegung geben. Es ist sowohl die Freiheit als auch die Aufgabe der Normung diesbezüglich maschinenspezifische Festlegungen in den jeweiligen Produkt- oder C-Normen zu beschreiben.

Problematisch ist, dass für Mensch-Maschine-Schnittstellen, auf die eine hohe Anzahl überlagerter Gefährdungen wirken, eine ausreichend kleine Ausfallwahrscheinlichkeit aller beteiligten sicherheitsbezogenen Steuerungsteile (Sensoren, Logik, mehrere Aktoren) kaum oder nur mit sehr hohem rechnerischen Aufwand (z.B. Markov-Modellierung) nachweisbar ist.

Ferner erhöhen überlagerte Gefährdungen mit unterschiedlichem Risiko (mit unterschiedlichem PL_r oder SIL) die Komplexität der Bestimmung der Ausfallwahrscheinlichkeit von Sicherheitsfunktionen, welches wiederum den Aufwand der Berechnung drastisch erhöht.

2 Praktische Behandlung überlagerter Gefährdungen

Eine genaue Überprüfung, welche Gefährdungen sich in einem konkreten Gefährdungsbereich tatsächlich überlagern, ist unerlässlich. Dabei sind die Maße der gefährdeten Körperteile und die bestimmungsgemäßen Handlungen des Maschinenpersonals genauso zu berücksichtigen

Inhaltsverzeichnis

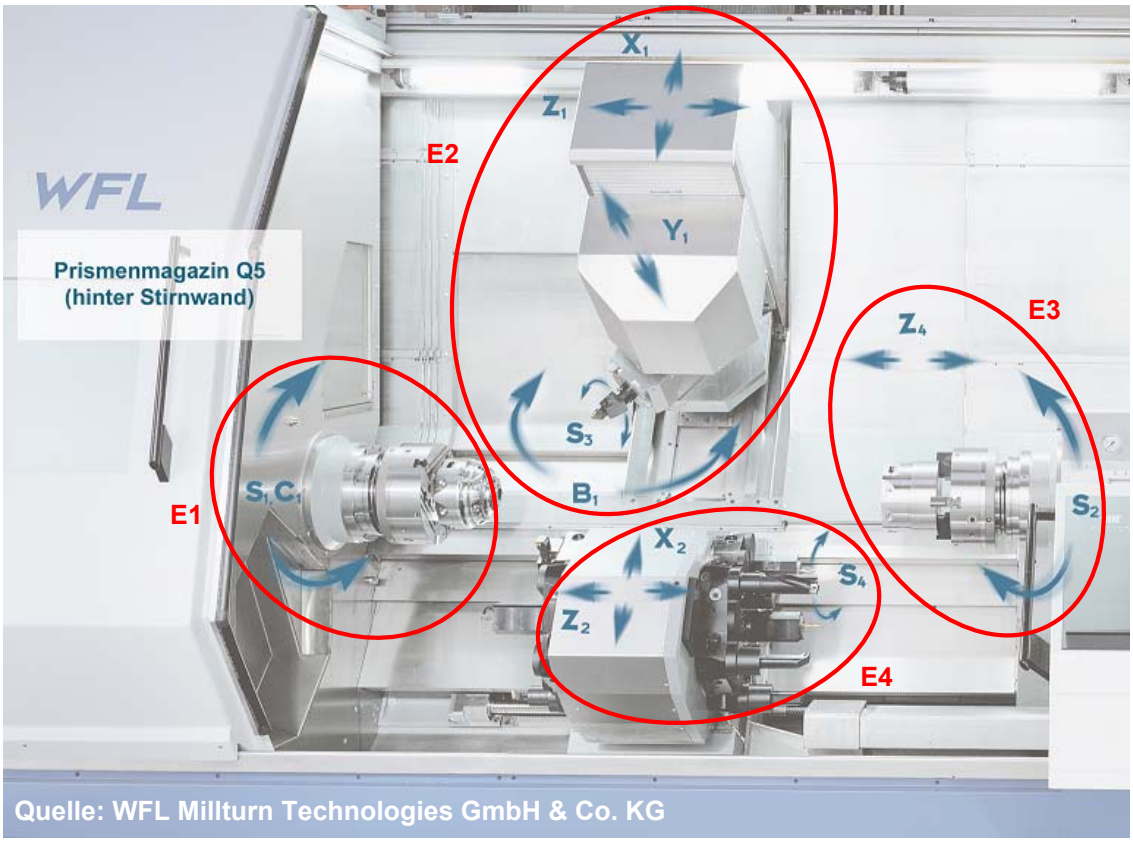


Bild 2: Unterschiedliche Einzelgefährdungen am Beispiel einer Werkzeugmaschine

wie die Bewegungsmöglichkeiten der gefährdenden Maschinenteile (z. B. durch Mehrachskinematik bewirkte vektorielle Bewegungen oder translatorische Einachsbewegungen).

Abhängig von der individuellen Risikobeurteilung ist es in der Praxis erlaubt, Sicherheitsfunktionen abzubilden, die, obwohl von überlagerten Gefährdungen gebildet, auf der Betrachtung deren Einzelgefährdungen basieren.

Leisten jedoch mehrere Aktoren (z. B. Schütze, Ventile, Antriebsregler) einen Beitrag zur Risikoreduzierung derselben Einzelgefährdung, müssen alle diese Aktoren in einer Sicherheitsfunktion zusammen betrachtet werden. Anders ausgedrückt: Alle Aktoren, die gefahrbringende Bewegungen ein und desselben Maschinenteils hervorrufen können, müssen in einer Sicherheitsfunktion zusammen betrachtet werden.

Wenn die individuelle Risikobeurteilung an der Maschine zur einer differenzierten Gefährdungsbeurteilung mit unterschiedlichen PL_r oder SIL führt, ist es in der Praxis erlaubt, Sicherheitsfunktionen abzubilden, die auf der Betrachtung von Einzelgefährdungen basieren.

Beispiele:

1. Resultiert die Bewegung eines Fräsers einer Werkzeugmaschine aus dem kinematischen Zusammenwirken von mehreren Einzelachsbewegungen, müssen alle diese Bewegung auslösenden Aktoren in einer Sicherheitsfunktion zusammengefasst werden. Die resultierende Bewegung setzt sich z.B. aus fünf Einzelbewegung zusammen, drei translatorischen Bewegungen in X_1, Y_1, Z_1-Richtung, einer Schwenkbewegung B_1 und einer rotatorischen Bewegung S_3 (siehe Bild 2, Einzelgefährdung E2).
2. Bewegungen eines einzigen Mehrachsroboters müssen in einer Sicherheitsfunktion zusammengefasst betrachtet werden (mehrere Roboter nebeneinander werden separat betrachtet).
3. Mehrere Spanneinrichtungen, die zusammen ein Teil festhalten (Ausfall einer der Spanneinrichtungen führt zum Lösen des Teils), müssen in einer Sicherheitsfunktion zusammengefasst werden.

Aus der Einzelbetrachtung kann nach Beispiel 1 die in Bild 2 gezeigte Berücksichtigung der von Antriebsachsen ausgehenden Gefährdungen beim Ableiten von Sicherheitsfunktionen ergeben. Das Bild zeigt beispielhaft vier rot umkreiste Einzelgefährdungen E1 bis E4 im Arbeitsraum einer Werkzeugmaschine:

E1: rotatorische (S_1) und translatorische (C_1, zur außermittigen Bearbeitung) Bewegung der linken Werkstückspindel

E2: rotatorische (S_3) und translatorische (X_1, Y_1, Z_1) Bewegung und Schwenkbewegung (B_1) der Frässpindel

E3: rotatorische (S_2) und translatorische (Z_4) Bewegung der rechten Werkstückspindel

E4: rotatorische (S_4) und translatorische Bewegung (X_2, Z_2) einer Werkzeugspindel (der Werkzeugrevolver ist indexiert, sodass dessen rotatorische Bewegung hier nicht betrachtet werden muss)

Aus diesen vier Einzelgefährdungen ergeben sich somit vier Sicherheitsfunktionen SF1 bis SF4. Die Sicherheitsfunktion SF1 zu E1 umfasst z. B. einen Achs- und einen Spindelantrieb (C_1, S_1). Die Sicherheitsfunktion SF2 zu E2 umfasst z. B. die Achsantriebe X_1, Y_1, Z_1, den Schwenkantrieb (B_1) und den Spindelantrieb (S_3).

Literatur:

[1] DIN EN ISO 13849-1 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze, 2008-12

[2] DIN EN IEC 62061 Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme, 2005-10

[3] IEC 61508-1 Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen, 2002-11 (vorgesehener Ersatz durch 65A/548/FDIS, 2009-12)

[4] IEC 61508-5 Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität, 1998-11 (vorgesehener Ersatz durch IEC 65A/552/FDIS, 2009-12)

[5] Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schäfer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) Nr. 6, S. 34-37

DGUV
Deutsche Gesetzliche Unfallversicherung
Fachausschuss Maschinenbau,
Fertigungssysteme, Stahlbau

Nr. **050**
Ausgabe 03/2011

Fachausschuss-Informationsblatt

Fluidtechnische Leistungselemente

Hydraulische u. pneumatische Motoren und Zylinder

Dieses FA-Infoblatt 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 13849-1 [2] 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

Dieses Informationsblatt beruht auf dem durch den Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau (FA MFS) zusammengeführten Erfahrungswissen auf dem Gebiet der Ausrüstungen von Maschinen und Anlagen mit hydraulischen und pneumatischen Steuerungen.

Das vorliegende Informationsblatt wurde unter Einbeziehung des Berufsgenossenschaftlichen Arbeitskreises Hydraulik und Pneumatik erarbeitet. Es soll der Information von Konstrukteuren und Betreibern von Maschinen, die zum Anwendungsbereich der europäischen Maschinenrichtlinie zählen, dienen und auf die Betrachtungsweise der fluidtechnischen Leistungselementen (z.B. Motoren, Zylinder) hinweisen.

Der Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau (FA MFS) setzt sich u.a. zusammen aus Vertretern von Unfallversicherungsträgern, staatlichen Stellen, Sozialpartnern, Herstellern von Maschinen und Betreibern.

Die Bestimmungen nach einzelnen Gesetzen und Verordnungen bleiben durch dieses Fachausschuss-Informationsblatt unberührt. Die Anforderungen der gesetzlichen Vorschriften gelten uneingeschränkt. Um vollständige Informationen zu erhalten, ist es erforderlich, die in Frage kommenden Vorschriftentexte einzusehen.

Weitere Informationsblätter des FA MFS stehen im Internet zum Herunterladen bereit [5].

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, 2008-09

[4] BIA-Report 6/1997, gebührenfreies Download unter: http://www.dguv.de/ifa/de/pub/rep/pdf/rep02/biar0697/rep697.pdf

[5] Internet: www.fa-mfs.bghm.de oder
www.bghm.de Webcode: <97>

Bildnachweis:

Bild 1: Das Bild dieses Fachausschuss-Informationsblattes wurde freundicherweise zur Verfügung gestellt von:
Institut für Arbeitsschutz (IFA)
der Deutschen Gesetzlichen Unfallversicherung DGUV,
53754 Sankt Augustin,
Deutschland

Herausgeber:

Fachausschuss
Maschinenbau, Fertigungssysteme, Stahlbau
Postfach 37 80
55027 Mainz

Anhang D: Abkürzungsverzeichnis

Tabelle D.1 enthält die in diesem Report verwendeten Abkürzungen; Tabelle 1 (siehe Seite 13) enthält die Abkürzungen und weitere Informationen zu den Sicherheitsfunktionen aus DIN EN 61800-5-2.

Tabelle D.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
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
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
FGPA	Field programmable gate array
FMEA	Failure mode and effect analysis; Ausfalleffektanalyse
FU	Frequenzumrichter
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	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