Serie I:

Sicherheitstechnik

im Maschinen und Anlagenbau | Teil II

Sichere Antriebstechnik

unter dem Gesichtspunkt der neuen Maschinenrichtlinie

Dr. Peter Wratil, Geschäftsführer der Firma innotec GmbH. www.innotec-safety.eu

Elektrische Antriebe führen heutzutage nahezu alle Bewegungsfunktionen von Maschinen aus. Sie sind hochdynamisch und vermögen bei allen noch so komplexen Arbeitsvorgängen extreme Kräfte zu entwickeln. Sie ersetzen träge und vibrationsbehaftete mechanische Getriebe durch synchronisierte Einzelachsen und tragen damit dazu bei, Maschinen kompakt zu bauen und mit hoher Drehzahl zu betreiben. Durch die flexible Programmierung oder Parametrierung gelingt die Anpassung an den Materialfluss vollkommen unproblematisch.

Autor: Dr. Peter Wratil / innotec

Allerdings stellen Antriebsfunktionen auch eine potenzielle Gefahr für den Menschen dar, der sich im Bereich der Maschinenbewegung zu schaffen macht. Fehler oder Defekte innerhalb der Ansteuerung führen zu schwerwiegenden Verletzungen oder gar zu Todesfällen. Die neue Maschinenrichtlinie mit den dort genannten Normen fordert daher, dass Antriebe ein Höchstmaß an Sicherheit mitbringen, damit jeder Umgang mit Maschinen oder Anlagen gefahrlos verläuft.

Anforderungen aufgrund der neuen Maschinerichtlinie

Mit der neuen Maschinenrichtlinie verliert die alte Norm EN 954 spätestens mit dem 30.12.2009 ihre Gültigkeit. Die neue Norm ISO 13849 [5] ersetzt die EN 954 und stellt gleichzeitig einen neuen Risikografen mit einer veränderten Bewertung der Maßnahmen für die Sicherheitstechnik vor. Innerhalb dieser Norm fordert jede PL-Einstufung (Performance Level) spezielle Maßnahmen, die zum Erreichen der Sicherheit notwendig sind. Dabei kommen insgesamt vier Kenngrößen in Betracht:

- Struktur des Sicherheitssystems,
- Ausfallsrate der Komponenten und Systeme [1],
- Möglichkeiten des Tests für die Funktion der Sicherheitseinheit,
- Vermeidung von Fehlern gemeinsamer Ursache.

Einen besonderen Wert legt die neue Norm ISO 13849 auf den Test der Sicherheitsfunktion. Während noch in der alten Norm (EN 954) oftmals eine Zweikanaligkeit zur Erfüllung gehobener Sicherheitsansprüche alleine ausreichend war, so geht es nun darum, auch durch Test nachzuweisen, dass die Sicherheitsfunktion noch verfügbar ist. Viele Maschinen werden aufgrund ihrer Risikobeurteilung in den Performance Level „d“ eingestuft. Zur Abdeckung der Anforderungen stellt die Norm insgesamt 4 Möglichkeiten vor:

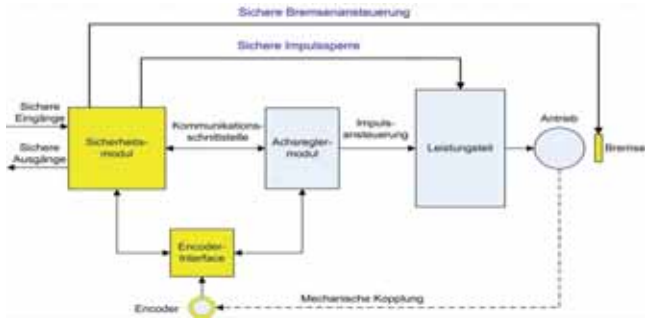
Struktur	Ausfallrate	Testmöglichkeit	Hinweise
1-kanalig	MTTFd > 60a	niedrig	DC zwischen 60 % und 90 %
1-kanalig	MTTFd > 30a	mittel	DC zwischen 90 % und 99 %
2-kanalig	MTTFd > 20a	niedrig	DC zwischen 60 % und 90 %
2-kanalig	MTTFd > 15a	mittel	DC zwischen 90 % und 99 %

Hinweis: MTTFd ist die mittlere Zeit, die vergeht, bis es zu einem gefährlichen Ausfall kommt. Dieser Wert hängt in erster Linie von der Qualität der verwendeten Komponenten ab. DC steht für „Diagnosedeckungsgrad“ (engl. Diagnostic Coverage) und gibt den Grad der Möglichkeit an, wie gut man das Sicherheitssystem testen kann.

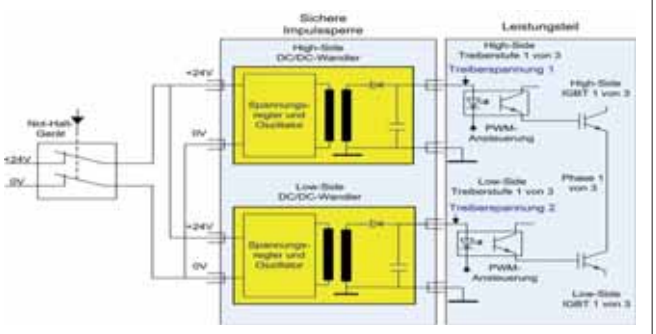
Sicherheitsprinzip für Antriebe

Eine typische Anordnung zur Realisierung eines sicheren Antriebskonzeptes ist im Bild 1 dargestellt. In der Abbildung erfolgen die Ausführung der spezifizierten Antriebsfunktionen und die Ansteuerung der Leistungsendstufe in gewohnter Weise durch die Standard-Steuerungselektronik des Achsreglermoduls.

Das dargestellte Sicherheitsmodul ist dem Achsregler übergeordnet und übernimmt die reine Überwachungsfunktion. Sicherheitsfunktionen werden immer über sichere Eingänge des Sicherheitsmoduls ausgelöst und zur Ausführung an den Achsregler über eine Kommunikationsschnittstelle weitergeleitet. Das Sicherheitsmodul überwacht im weiteren Verlauf die Einhaltung der Ausführung von Sicherheitsfunktionen und die Einhaltung definierter Parameter. Es handelt sich hier also um ein Zustimmprinzip. Damit das Sicherheitsmodul die Überwachungsfunktion wahrnehmen kann, wird der sicherheitsgerichtete Anteil der Encoder-Signale über ein Encoder-Interface rückwirkungsfrei ausgekoppelt und dem Sicherheitsmodul zugeführt. Stellt das Sicherheitsmodul eine Sollwertabweichung des Antriebes fest, löst es durch den direkten Zugriff auf die Kommutierung des Antriebs die Funktion Safe Torque Off (STO) aus [6], [7]. Die Funktion STO kann selbstverständlich auch direkt über ein angeschlossenes Not-Halt-Gerät, das über einen der sicheren Eingänge betrieben wird, ausgelöst werden. Durch sichere Ausgänge, die das Sicherheitsmodul bereitstellt, lassen sich z. B. Türzuhaltungen entriegeln oder, wie dargestellt, mechanische Bremsen sicherheitsgerichtet öffnen. →

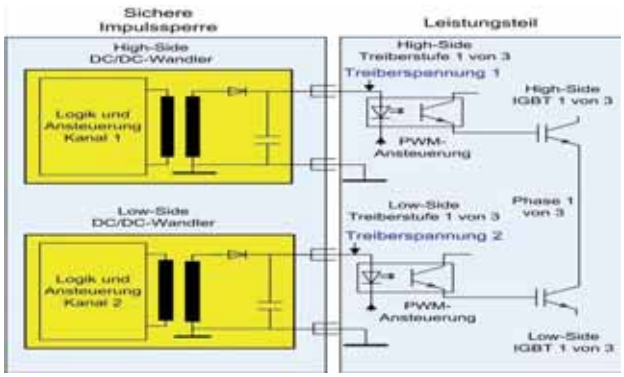


Typische Anordnung in einem sicheren Antriebskonzept.



Sichere Impulssperre mit Not-Halt-Funktion.

Ein in der Sicherheitstechnik etabliertes Prinzip zur sicheren Abschaltung eines Antriebes ist die Impulssperre [2], [9], [10]. Das Wirkprinzip besteht darin, die Versorgungsspannung der für die Kommutierung zuständigen Optokoppler der Treiberstufe zweikanalig und sicher zu unterbrechen (Treiberspannungen 1 und 2). Das Funktionsprinzip einer zweikanaligen Impulssperre ist im Bild 2 dargestellt.



Prinzip sichere Impulssperre.

Die Auswertung sicherer Eingänge und die Überwachung aktiver sicherheitsrelevanter Steuerungsparameter erfolgt durch eine zweikanalige Logik. Das grundlegende Prinzip der sicheren Abschaltung besteht in der transformatorischen Kopplung dynamischer Signale. Die Ansteuerung der dargestellten Übertrager besteht im Wesentlichen je Kanal aus einem Generator, der nur dann eine Wechselspannung erzeugt, wenn die Sicherheitsfunktionen fehlerfrei ausgeführt werden und die Funktion Safe Torque Off (STO] nicht ausgelöst wurde. Wird durch das Sicherheitsmodul eine Verletzung der parametrierten Sollwerte festgestellt, wird die Erzeugung der Generatorspannung eingestellt. Die Logik des Sicherheitsmoduls muss so ausgelegt werden, dass das System bei fehlerhafter Logik durch Abschaltung der Treiberspannungen in den sicheren Zustand geführt wird. Eine derartige Schaltungstechnik erfüllt die Anforderungen nach PL-e.

Die Logik kann für komplexe Sicherheitsfunktionen z.B. durch Mikrocontroller oder FPGAs realisiert werden. Einfache Funktionen, wie z. B. die direkte Auslösung der Funktion STO, können als reine Hardwarelösung umgesetzt werden [2], [3].
In diesem Fall wird z. B., wie in Bild 3 dargestellt, ein auf Hardware basierender Oszillator durch eine externe Spannungsversorgung über ein Not-Halt-Gerät versorgt.

Die Schaltung wird ausschließlich mit Energie versorgt, wenn die Kontakte des Not-Halt-Gerätes geschlossen sind. Mit der Betätigung des Not-Halt-Gerätes wird der Eingang der Schaltung vollständig energielos geschaltet. Die Folge ist, dass keine Energie auf die Sekundärseite des Übertragers gelangen kann. Die Schaltung weist die Eigenschaft auf, dass jeder sicherheitsrelevante Bauteilefehler automatisch in den sicheren Zustand führt. Da es sich um ein etabliertes Fail-Safe-Prinzip handelt, sind keine weiteren Diagnosemaßnahmen erforderlich. Die Versorgung des Not-Halt-Gerätes mit unterschiedlichen Potenzialen ist nützlich, um Leitungskurzschlüsse in der externen Verdrahtung zu detektieren.

Durch das dargestellte Schaltungsprinzip der sicheren Impulssperre lässt sich unter Berücksichtigung weiterer sicherheitsrelevanter Aspekte eine sichere Abschaltung bis Performance Level e realisieren.

Zwei- oder mehrkanalige Strukturen

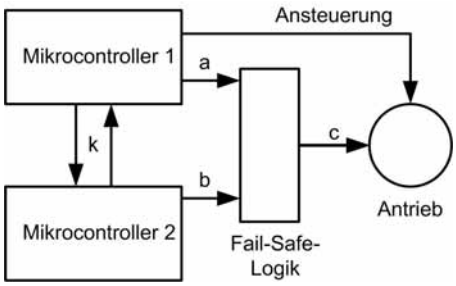
Die notwendigen Sicherheitsfunktionen für sichere Anwendungen innerhalb der Antriebstechnik sind in der Norm IEC 61800 (speziell im Teil 5.2) dargestellt. Hierbei gibt es eine ganze Reihe von Funktionen, die man nur noch durch das Zusammenwirken zweikanaliger Systeme realisieren kann, sofern die Anforderungen eine PL-Wert von „d“ oder gar „e“ entsprechen. Diese sind beispielesweise:

- Sicherer Halt nach Stopp-Kategorie 0 bei direkter Abschaltung der Impulsmuster ohne Verwendung von Optokopplern
- Sichere Kontrolle der Abschaltung nach Stopp-Kategorie 1 (Kontrolle der Zeit oder Kontrolle der Bremsfunktion)
- Stillsetzung nach Stopp-Kategorie 2
- Alle komplexeren Funktionen (Schleichgang, Tipp-Betrieb, Reduziertes Schrittmaß, …)

Eine Zweikanaligkeit lässt sich durch den Aufbau von 2 Mikrocontrollern und einer Fail-Safe-Logik realisieren. Um Common-Cause-Fehler weitgehend ausschließen zu können, verwendet man zwar identische Controller, diese sollten jedoch mit unterschiedlicher Software ausgestattet sein (homogene Hardware, diversitäre Software) [8].

Das folgende Bild 4 gibt das Prinzip wieder. Die Zweikanaligkeit ist durch zwei Mikrocontroller aufgebaut, die sich über einen Kommunikationskanal unterhalten (k). Der obere Mikrocontroller ist direkt für die Ansteuerung des Antriebs zuständig. Beide Mikrocontroller

wirken unabhängig auf die Fail-Safe-Logik (a, b). Diese kann den Antrieb jederzeit abschalten (z. B. durch eine Impulsmustersperre). Der zweite Mikrocontroller arbeitet in dieser Technik als Zustimmschaltung für den ersten Mikrocontroller. Im Fehlerfall erfolgt eine Abschaltung nach STO. Dieses Verhalten kann dazu führen, dass der Antrieb im Fehlerfall austrudelt oder (bei hängenden Lasten) sogar beschleunigt.



Zweikanalige Ansteuerung mit Fail-Safe-Logik.

Mit einer zweikanaligen Struktur lassen sich im Prinzip alle weiteren Sicherheitsfunktionen ausführen:

- Sicherer Betriebshalt nach Stopp-Kategorie 2
- Schleichgang
- Tipp-Betrieb
- Reduzierte Geschwindigkeit
- Reduzierter Weg
- Sichere Absolutlage.
- Zustimmbetrieb

Antriebshersteller bieten oftmals Standardantriebe an, bei denen sich Sicherheitsmodule hinzufügen lassen, wenn man den Antrieb für Sicherheitstechnik einsetzen möchte. Sobald das Sicherheitsmodul gesteckt wird, kontrolliert es intern den funktionalen Ablauf der gewünschten Funktion. Im Versagensfall greift die Sicherheitslogik ein und schaltet die Impulsmuster ab.

Synchronisierte Motoren als Getriebeersatz

Modere Maschinen ersetzen mechanische Getriebe durch Einzelantriebe, die elektronisch miteinander gekoppelt werden. Diese Technik bringt ganz erhebliche Vorteile mit sich. Zum einen vermögen elektronische Getriebe komplexe Funktionen ausführen, die bei rein mechanischen Einheiten kaum vorstellbar sind. Zum anderen lassen sich die gekoppelten Bewegungsfunktionen rasch verändern (durch die Parametrierung der Software), ohne den Umbau eines Getriebes durchführen zu müssen. Darüber hinaus werden Vibration und hohe Geräuschemissionen vermieden. Allerdings erkauft man sich die erhöhte Flexibilität durch ein eventuelles unsicheres Verhalten, wenn es um die Funktionen der Maschineneinrichtung geht. Bei der Verwendung eines einzigen Antriebs mit einem oder mehreren Getrieben folgen alle Bewegungen lediglich dem Antrieb selbst (Hauptantrieb). In größeren Maschinen wird die Erregung aller Bewegun- →

Siemens Automation Innovation Tour.

Innovativ denken! Mit Sicherheit profitieren.

Wo/Wann:

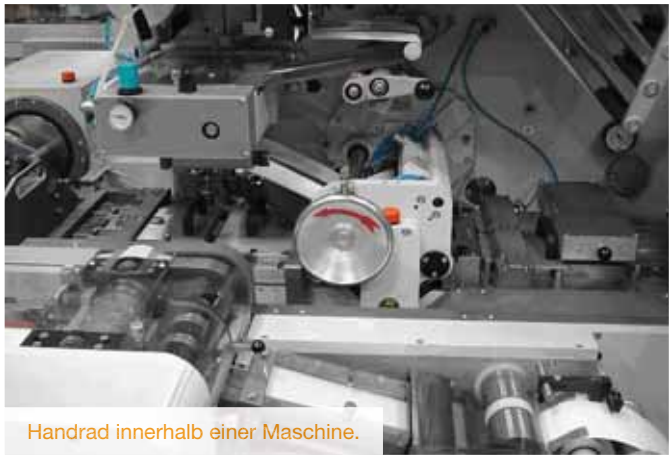
Graz: 4. Mai
Klagenfurt: 5. Mai
Linz: 7. Mai
Wien: 25. Mai
Salzburg: 26. Mai
Innsbruck: 27. Mai
Dornbirn: 28. Mai

Safety integrated

Auf kürzestem Weg zur sicheren und produktiven Maschine, konform mit den neuesten Normen? Siemens Safety Integrated macht es möglich. Wie? Live und hautnah. Besuchen Sie uns. Es lohnt sich mit Sicherheit! **www.siemens.at/safety-tour**

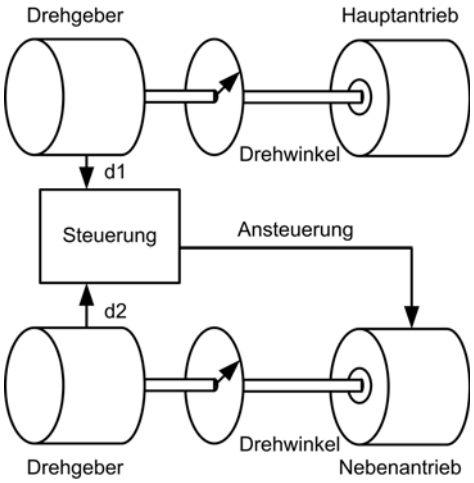
Answers for industry. SIEMENS

gen über eine einzige Welle als „Königswelle“ bezeichnet. Sofern der Hauptantrieb momentenlos ist, verweilen auch alle anderen Wellen in Ruhe. Eine Bewegung kann über die Betätigung eines Handrads manuell erfolgen, wobei sich dann alle am Getriebe angeschlossenen Wellen synchron mitbewegen. Ein Maschineneinrichter kann auf diese Weise durch Drehen am Handrad alle anderen Bewegungen verfolgen. Sobald man das Handrad nicht mehr dreht, stehen auch alle anderen Wellen. Bild 5 zeigt einen Maschinenausschnitt mit einem Handrad.



Handrad innerhalb einer Maschine.

Elektronisch gekoppelte Getriebe bestehen nun aber nicht aus einem einzelnen Antrieb mit einer Königswelle, sondern aus zahlreichen Einzelantrieben.



Aufbau eines elektronischen Getriebes.

Wie Bild 6 darstellt, führt die Steuerung die Bewegungsfunktion zwischen den beiden Antrieben durch. Dabei gibt der Hauptantrieb die Grundbewegung vor, die über den oberen Drehgeber zum Eingang der Steuerung führt (d1). Der untere Drehgeber ist fest mit dem Nebenantrieb verbunden. Dieser wird von der Steuerung, entsprechend der Getriebefunktion, nachgeregelt. Hierzu wird dessen Position ebenfalls zur Steuerung geleitet (d2). Wenn man sich innerhalb der Maschine zu schaffen macht, schaltet man den Hauptantrieb ab und verwendet zu dessen Bewegung ein Handrad. Der Nebenantrieb bleibt weiterhin in Regelung und folgt der Bewegung des Handrads. Hierdurch kann man die Bewegungen der Maschine gezielt ausführen. Beispielsweise lässt sich ein eingeklemmtes Papierstück oder eine verknickte Cellophanfolie manuell entfernen (Bild 7).

Entfernen einer Folie durch manuellen Eingriff.

Wenn während des manuellen Eingriffs die Steuerung versagt, kann der Nebenantrieb spontan anlaufen, ohne dass der Hauptantrieb erregt wurde. Wie Bild 7 zeigt, kann es in diesem Fall zu einem Einzug der Finger oder der Hand zwischen den Zuführrollen kommen. Eine Verletzung ist dann leicht möglich. Derartige Fehler sind stets auszuschließen, indem man sicherheitsgerichtete Techniken mit einer zweikanaligen Struktur verwendet.

Literaturangaben und Hinweise

[1] Birolini: Zuverlässigkeit von Geräten und Systemen, Springer-Verlag 1996, ISBN: 3-540-60997-0

[2] BIA-Report 4/97: Maschinen- und Gerätesicherheit, Seite 106 ff: Schutz gegen unerwarteten Anlauf bei Servoantrieben, ISBN 3-88383-449-1

[3] BIA-Report 6/98: Maschinen- und Gerätesicherheit, Seite 135 ff: Sicherheitgrichtete Funktionen elektrischer Antriebssysteme in Maschinen, ISBN 3-88383-510-2

[4] EN 61508, VDE 0803: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme, Version November 2002, DIN (Kapitel 1-7)

[5] ISO 13849, Safety of Machinery – Safety related parts of control systems

[6] DKE-AK 226.03: Grundzüge der Sicherheitsfunktionen in Antriebssystemen

[7] IEC 61800 Part 5-2: Safety related drives, requirements

[8] P. Wratil, M. Kieviet: Sicherheitstechnik für Komponenten und Systeme, Hüthig-Verlag, 2007, ISBN 3-7785-2984-6

[9] P. Wratil: Technology of safe Drives, IEEE-Publication, 5th International IEEE conference on Industrial Informatics, Vienna 2007, ISBN 1-4244-0864-4

[10] T. Wedemeyer: Sichere Antriebskonzepte, SPS-Magazin, Ausgabe 5, 2008

In der nächsten Ausgabe

Programmierbare und parametrierbare Systeme nach der neuen MRL.