Konzepte der Funktionalen Sicherheit in Antriebssystemen
Concepts of functional safety integrated in drive systems

Dipl.-Ing. Martin Grosser, Lenze AG, Aerzen, Deutschland, grosser@lenze.de

Kurzfassung

Die antriebsintegrierte Sicherheitstechnik in Kombination mit fehlersicheren Kommunikationsnetzwerken bietet neue Lösungsansätze, die es ermöglichen, Gefahrenpotentiale am Ort ihrer Entstehung besser zu sichern und somit zu weiteren Kosteneinsparungen und Produktivitätssteigerungen beitragen. Der vorliegende Beitrag gibt einen Überblick über den Stand der Sicheren Antriebstechnik und beleuchtet die am Markt gängigen Arten der technischen Realisierung.

Summary

Drive-based Safety in combination with fail safe communication networks offer new approaches for a better management of risk potential directly at the source of its accruement. Positive effects are potentials in cost savings and an increase in productivity. This technical paper will inform about the state of the art in drive-based safety and will give an overview about the available technical realisation on the market.

1 Prinzipieller Aufbau eines sicheren Antriebssystems

Bevor die heutigen technischen Lösungen beschrieben werden, ist es notwendig sich den prinzipiellen Aufbau eines sicheren Antriebssystems anzuschauen. Ein solches System besteht aus einem Elektromotor der bei höheren Anforderungen an die Regelgüte bzw. Dynamik mit einem Drehgeber zur Erfassung der Motorrotorlage und der Drehzahl ausgestattet ist, einem Antriebsregler bestehend aus Leistungselektronik und Steuerelektronik, einer Steuerelektronik für die Ausführung der Sicherheitsfunktionen, sichere und nicht sichere digitale Ein- und Ausgänge sowie einem Kommunikationssystems, das häufig über ein Bussystem ausgeführt ist.

2 Sicherheitsgerichtete Abschaltung

Zu den wichtigsten Sicherheitsfunktionen eines Antriebs gehört die sichere Abschaltung der Bewegung. Diese wird bei nahezu allen Maschinen und Anlagen benötigt, wenn sich eine Person im gefahrvollen Arbeitsbereich befindet. Hier gilt es, unter allen Umständen eine Bewegung zu verhindern, die zu einer eventuellen Verletzung führen kann. In den meisten Fällen reicht hierbei die sichere Abschaltung des Moments, bei der der Antrieb von seiner Leistung getrennt wird.
Wie im Bild 1 gezeigt, reicht es für diese gewünschte Funktion, die Leistungselektronik daran zu hindern, den Motor weiter zu betreiben. Allerdings verweilt der Antrieb bei einer Abschaltung der Leistung ohne jegliches Moment. Der Antrieb kann daher durch äußere Einwirkung in Rotation versetzt werden. Wenn man diese Funktion beispielsweise bei einem Kran verwendet, der über keine Bremse verfügt, beschleunigt die Last erst recht und Unfälle sind nicht auszuschließen. Die einfache Abschaltung des Moments birgt zudem den Nachteil, dass der Antrieb austrudelt. Beim Betrieb von Systemen mit hohen Trägheitsmomenten (z.B. Zentrifugen) dauert das Erreichen des Stillstands mitunter recht lange.

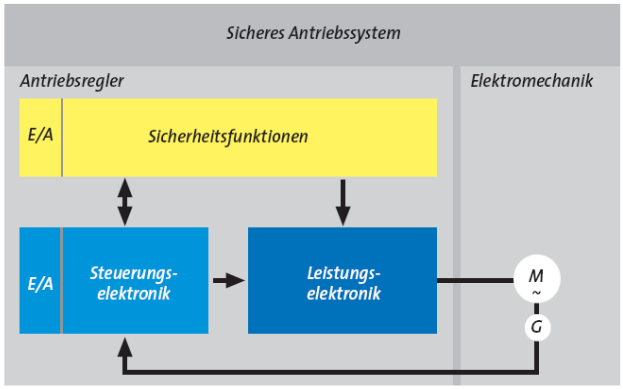

Bild 1 Prinzipieller Aufbau eines sicheren Antriebssystems

Daher fordern die Anwendungen unterschiedliche Abschaltstrategien, die aus der Sicherheitsbetrachtung resultieren. Hierbei werden nach der Norm IEC 61800 Teil 5.2 [1] drei unterschiedliche Funktionen beschrieben, die im Endeffekt zum Stopp des Antriebs führen:
➲ Die Funktion STO (Safe Torque Off, deutsch: Sicherer Halt) unterbindet nach seiner Anforderung die Zuführung eines Moments zum Antrieb. Dieses kann entweder durch die Unterbrechung der Energie oder durch die Abschaltung

der zur Kommutierung notwendiger Impulsmuster geschehen. Die Funktion fordert keine Unterbrechung der Versorgung.

➲ Die Funktion SS1 (Safe Stop 1, Stopp-Kategorie 1 nach EN 60204 [2]) bremst den Antrieb mit der Antriebsenergie ab und unterbricht dann die Zuführung des Moments, sofern die Ruhelage erreicht ist. Sofern keinerlei externe Kräfte wirken, wird der Stillstand erheblich schneller erreicht als bei der Funktion STO.

➲ Die Funktion SS2 (Safe Stopp 2 auch „Sicherer Betriebshalt“, Stopp-Kategorie 2 nach EN 60204) beginnt wie die Funktion SS1. Allerdings verweilt der Antrieb nach Erreichen der Ruhelage in Regelung. Der Stillstand wird somit stabilisiert.

3 Sicherheitsgerichtete Abschaltung des Antriebs

Die Abschaltung eines Antriebs durch Unterbrechung der Versorgung stellt heute nicht mehr den Stand der Technik dar. Die benötigen Unterbrecher (Schütze) verhalten sich in der Regel sehr träge und benötigen nicht selten 50 msec. bis sie den Stromfluss sicher beenden. In diesem Zeitraum kann ein hochdynamischer Antrieb bereits eine gefahrvolle Drehzahl errecht haben. Ein erheblich besseres Prinzip besteht darin, die Impulsmuster über Optokoppler abzuschalten Bild 2.

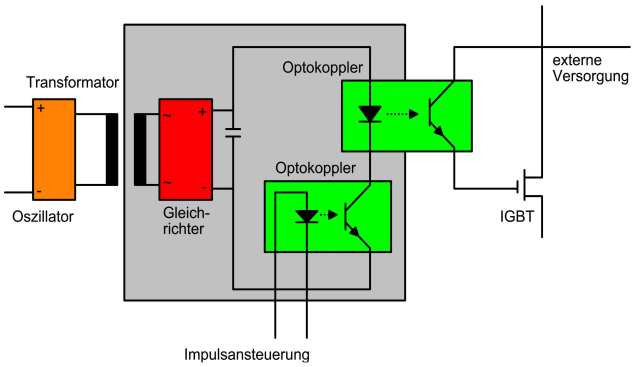

Bild 2 Sichere Abschaltung durch Sperrung der Spannungsversorgung der Optokoppler

Die Schaltung besteht aus einem primärseitigen Oszillator, der einen Transformator versorgt. Der Transformator erzeugt sekundärseitig eine Wechselspannung, die nach einer Gleichrichtung und Siebung zur Versorgung der Optokoppler dient. Die Optokoppler übertragen die notwendigen Signale zur Ansteuerung der IGBT. Wenn die Spannung am Eingang ausbleibt, so erhält der galvanisch isolierte Kreis mit den Optokopplern (grau gezeichnet) keine Versorgung und das Impulsmuster zur Ansteuerung der IGBT erlischt. Die im Bild 2 dargestellte Schaltung stellt die Grundfunktion für alle weiteren Sicherheitsschaltungen dar. So kann eine Sicherheitslogik den funktionalen Teil des Antriebs vollkommen unabhängig in kurzer Zeit unterbrechen und so einen sicheren Zustand herbeiführen (Hinweis: Das Bild 2 zeigt nur eines der zahlreichen Prinzipien).

4 Mehrkanaligkeit zur Erfüllung der Sicherheitsanforderungen

Nach der Sicherheitsnorm IEC 61508 [3], die auch in allen wesentlichen Teilen in der IEC 61800 [4] übernommen wurde, sind insgesamt 4 Kenngrößen angegeben, die eine Eignung für eine geforderte Sicherheitsklasse ermöglichen. Diese Kenngrößen sind:

➲ Struktur des Systems
➲ Ausfallrate der verwendeten Bauteile
➲ Diagnosedeckungsgrad
➲ Fehler gemeinsamer Ursache

Die folgende Tabelle 1 stellt diesen wichtigen Zusammenhang dar.

Anteil der sicheren Ausfälle (SFF)	Hardwarefehlertoleranz		
	0	1	2
< 60%	Nicht erlaubt	SIL 1	SIL 2
60% bis 90%	SIL 1	SIL 2	SIL 3
90% bis 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Tabelle 1 Zusammenhang Hardwarefehlertoleranz und Aufdeckung von Fehlern durch Tests

Die Hardwarefehlertoleranz (HFT) gibt im Prinzip die Architektur des Antriebssystems wieder. Bei einer Hardwarefehlertoleranz von 1 darf ein Fehler niemals zum Sicherheitsrisiko führen. In der Regel sind hier nur zweikanalige Strukturen tauglich. Die Safe Failure Fraction (SFF) ist eine prozentuale Angabe aller Fehler, die einerseits in den sicheren Zustand führen oder durch interne Tests aufgedeckt werden, bevor sie sich gefahrvoll auswirken. Beispielsweise kann man bei einem Wert von 80% für SFF mit einer zweikanaligen Struktur (HFT = 1) SIL 2 erreichen.

Für die Ausfallraten und die Versagenswahrscheinlichkeiten gibt die Norm IEC 61508 ebenfalls konkrete Werte an. Die folgende Tabelle 2 zeigt eine Übersicht.

SIL	PFH (pro Stunde)	PFH (pro Anforderung)
4	10^{-9} bis < 10^{-8}	10^{-5} bis < 10^{-4}
3	10^{-8} bis < 10^{-7}	10^{-4} bis < 10^{-3}
2	10^{-7} bis < 10^{-6}	10^{-3} bis < 10^{-2}
1	10^{-6} bis < 10^{-5}	10^{-2} bis < 10^{-1}

Tabelle 2 Tolerierbare gefährliche Ausfallraten in Abhängigkeit der Sicherheitseinstufung

Wie aus der Tabelle 2 zu entnehmen ist, ergibt sich für SIL 2 ein Wert von < 10^{-6}/h für PFH und < 10^{-2} für PFD. PFH

(Probability Failure per Hour) ist die Ausfallrate pro Stunde. Ein Wert von 10^{-6}/h garantiert, dass höchstens alle 100 Jahre ein gefahrvoller Ausfall eintreten kann. Der PFD-Wert (Probability Failure per Demand) gibt an, bei welcher Anzahl an Sicherheitsanforderungen höchstes mit einem Versagen zu rechnen ist.
Die Tabelle 1 zeigt, dass man im Prinzip bei höheren Sicherheitsanforderungen (ab SIL 3) stets eine mehrkanalige Struktur benötigt. Eine einkanalige Lösung würde einen SFF-Wert von > 99% fordern. Diese ist aber technisch kaum realisierbar. Daher haben sich bei allen Antrieben Sicherheitsstrukturen etabliert, die 2 oder 3 Prozessoren benötigen. Im Folgenden sind die gängigen Verfahren im Detail beschrieben.

5 Konkreter Aufbau

Die Sicherheitsfunktion ist bei modernen sicheren Antrieben direkt integriert. Wie Bild 3 darstellt, besteht die Antriebsregelung selbst aus einem Funktionsteil und einem Sicherheitsteil. Der Funktionsteil führt alle notwendigen Bewegungen des Antriebs aus. Dagegen überwacht der Sicherheitsteil stetig die richtige Abarbeitung des Funktionsteils. Im einwandfreien Betrieb stimmt der Sicherheitsteil immer dem Funktionsteil zu. Die Optokoppler werden hierzu dauerhaft aktiviert und die Impulsmuster erzeugen eine Rotation des Antriebs. Sobald der zweikanalige Sicherheitsteil jedoch eine unzulässige Funktion aufdeckt, erfolgt eine sofortige Unterdrückung der Optokoppler-Freigabe und die Impulsmuster verschwinden. Der Antrieb wird instantan momentenfrei geschaltet.

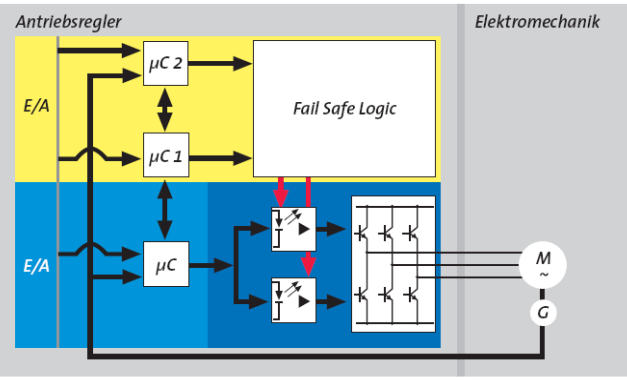

Bild 3 Interner Aufbau eines zweikanalig ausgeführten sicheren Antriebssystems mit 3 Prozessoren

6 3-Prozessor-Lösung

Die im Bild 3 gezeigte Architektur verfügt insgesamt über 3 Prozessoren. Der untere µC stellt den funktionalen Teil der Antriebsregelung dar, der oftmals durch einen DSP (Digital Signal Processor) repräsentiert wird.
Das technische Verfahren basiert auf der vollständigen Trennung zwischen der funktionalen Antriebsfunktion und dem Sicherheitsteil. Da der (im unteren Teil gezeichnete) Regler nicht zum Sicherheitsteil hinzugezählt wird, werden alle möglichen Fehler unterstellt. Die Gewährleistung der geforderten Sicherheit erfolgt ausschließlich über den (oben gezeigten) Sicherheitskern, der – entsprechend der Norm – zweikanalig ausgeführt ist. Die Erfüllung der Sicherheitsfunktion erfolgt über das Zustimmprinzip, bei dem die beiden sicherheitsgerichteten Mikrocontroller lediglich die Funktion des Antriebsprozessors überwachen. Sie greifen so lange nicht ein, bis sie eine Fehlfunktion des Antriebsprozessors aufdecken. Die notwendige Abschaltung im Fehlerfall geschieht dann über die sichere Optokopplersperre.

7 2-Prozessor-Lösung

Etwas preisgünstiger gegenüber der soeben vorgestellten Lösung ist freilich eine 2-Prozessor-Lösung. Hier überwacht nur ein einziger Mikrocontroller den Antriebsregler wie im Bild 4 dargestellt.

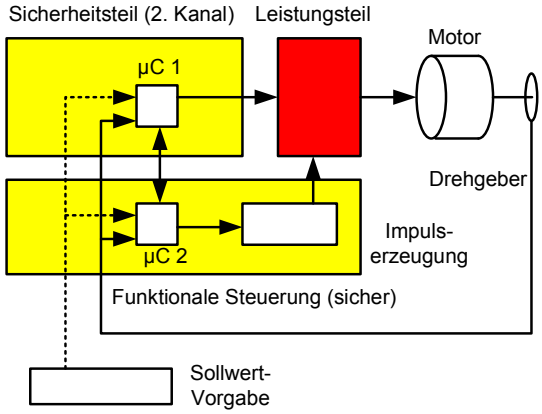

Bild 4 Überwachung des Antriebes mit nur einem zusätzlichen Controller

Die von der Hardware her abgespeckte Lösung funktioniert genauso wie die 3-Prozessor-Variante. Auch hier überwacht der Sicherheitskern den Antriebsteil und führt im Fehlerfall eine Abschaltung durch. Allerdings muss nun der Antriebscontroller in die Sicherheitsfunktion mit einbezogen werden, da er den verbleibenden zweiten Kanal darstellt. Die beiden Controller sind nun auch über eine direkte Schnittstelle miteinander verbunden, damit alle internen Fehler durch gegenseitige Tests aufgedeckt werden. Entsprechend der Tabelle 1 muss auch er nun einen SFF-Wert von > 90% mitbringen, wenn man eine Sicherheitsanforderung nach SIL 3 realisieren möchte. Während seiner Antriebsverarbeitung muss er beispielsweise folgende Einheiten testen

- Sich selbst (CPU-Test)
- Speichermedien
- Eingabe und Ausgabe
- Netzwerke (falls vorhanden)
- Zeiterwartung zum anderen Controller

Sicherheitsfunktionen lassen sich relativ leicht als Zusatzfunktionen integrieren. Allerdings kosten sie Verarbeitungszeit, die nun nicht mehr der Antriebsfunktion zur Verfügung stehen. Etwas schwerwiegender ist allerdings

der Umstand, dass nun neben dem Sicherheitscontroller auch der Antriebscontroller nach den Sicherheitskriterien der Norm programmiert werden muss. Das bedeutet stets, dass jedes Programm, jede Routine oder jegliche Funktion den strukturierten Vorgaben entsprechen muss. Die Verwendung eines hinzugekauften Stacks für eine Netzwerkfunktion ist in der Regel nicht möglich. Jede Änderung muss sicherheitsrelevant durchgeführt und vollständig gestestet werden.
Damit mag eine 2-Controller-Lösung vielleicht bei der reinen Betrachtung der Hardware etwas preisgünstiger sein, aber die Flexibilität ist eher eingeschränkt.

8 Lösung mit 1 oder 2 Drehgebern

Die in der Tabelle 1 vorgestellten HFT-Werte beziehen sich prinzipiell auf den gesamten Kanal. Fehler passieren nicht nur in den Controllern, sondern auch bei der Messwerterfassung. Das lässt sofort den Schluss zu, dass man für Sicherheitssysteme auch noch einen zweiten Encoder benötigt, der zusammen mit dem bereits vorhandenen den zweiten sicheren Kanal vervollständigt Bild 5.

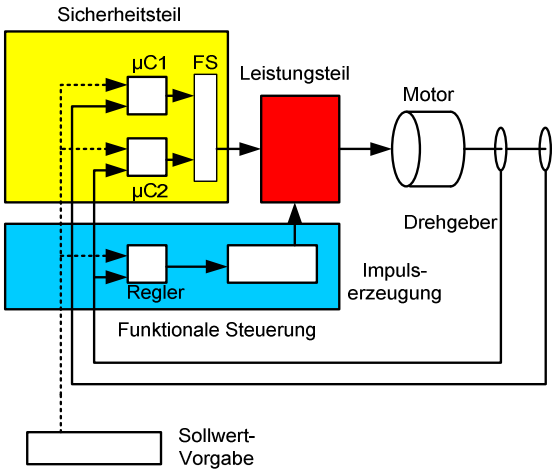

Bild 5 Verwendung von 2 Encodern oder Drehgebern

Diese Anforderung lässt sich auch mit einem einzigen Drehgeber abdecken, wenn dieser eine getrennte Sinus- und Cosinus-Spur zur Verfügung stellt, und die nachgeschaltete Logik die Daten fehlerfrei verarbeiten kann. Der Grund hierfür besteht darin, dass Sinus/Cosinus-Encoder selbst eigensicher sind, da man durch die Funktion $\sin^2+\cos^2=r^2$ jederzeit die richtige und unabhängige Winkelerfassung nachweisen kann Bild 6. Ein weiterer Punkt der bei Verwendung von nur einem Gebersystem einer genaueren Betrachtung zu unterziehen ist, ist die Geberwellen Verbindung mit dem Elektromotor. Hier ist eine Redundanz per Definition kaum möglich und es gilt durch eine erhebliche Überdimensionierung der Verbindung einen durchgängig sicheren Antriebsstrang zu gewährleisten. Während heute die Verwendung von Encodern, die keiner speziellen sicherheitstechnischen Bewertung unterzogen wurden, noch dem Stand der Technik entsprechen, ist mittelfristig aufgrund der sich ändernden Normenlage doch deutlich absehbar, dass zunehmens Sicherheits-Gebersysteme zum Einsatz kommen werden.

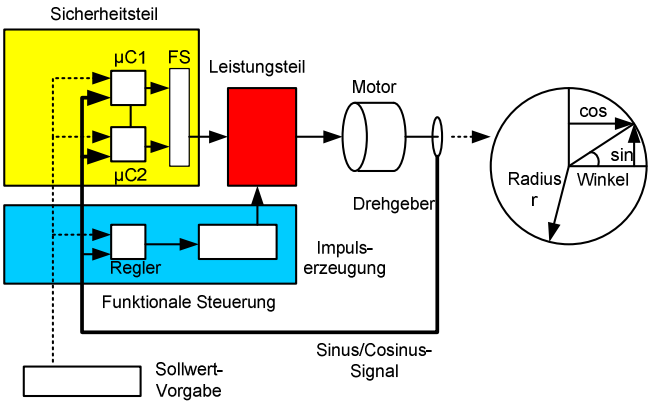

Bild 6 Verwendung von nur einem Encoder

9 Regelung über Softwaremodell

Die Zweikanaligkeit muss nicht unbedingt aus zwei Hardware-Funktionen bestehen. So sind auch Lösungen verfügbar, die nur einen Prozessor enthalten, der ein Regelungsprogramm „zweifach“ in diversitärer Form durchläuft. Hierbei wird die funktionale Regelung mit einem Simulationsprogramm verglichen. Sofern die Hardware-basierte Verarbeitung zu identischen Größen wie die Software-basierte Simulation führt, geht man davon aus, dass der Antrieb die gewünschte Funktion ausführt Bild 7.

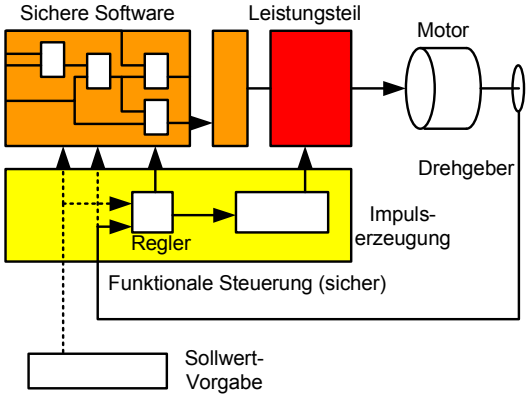

Bild 7 Zweikanaligkeit durch Software-Modell

Grundsätzlich ist eine derartige Lösung als sicherer einzustufen als eine einkanalige Variante. Dennoch erfüllt sie nicht die Anforderungen nach einem HFT-Wert von 2. Um hier eine hinreichende Sicherheit zu gewährleisten sind noch zahlreiche Zusatzelemente notwendig, die eine Unabhängigkeit der Hard- und Softwareverarbeitung garantieren. Es muss zu jeder Zeit sichergestellt sein, dass die Hardware alleine keine Blockade der Sicherheitsfunktion auslösen kann. Ferner gilt es alle „Fehler gemeinsamer Ursache“, die aus der einkanaligen Hardware erwachsen, auszuschalten.

10 Drehgeberlose Sicherheitslösung

Vielfach kommen Antriebe auch vollkommen ohne einen Drehgeber oder Encoder aus. Die notwendigen Ist-Daten der Welle werden in diesem Fall durch die Nachbildung der Rotation aus den vorhandenen Größen der Antriebssteuerung entnommen. So wirken auf den Motor fundamentale Kenngrößen, die eine Rotation bewirken. Diese sind beispielsweise:

- Strom
- Spannung
- Impulsmuster
- Phasenwinkel

Sowohl Asynchron- als auch Synchronmotoren führen aufgrund der Impulsmustererzeugung nur genau definierte Bewegungen aus. Hierbei sind allerdings Synchronantriebe exakter kalkulierbar als Asynchronsysteme. Dennoch kann man durch die Erzeugung der Impulsmuster und der Messung der Kenngrößen mit anschließender Verrechnung auf die Bewegung schließen.

In Bild 8 ist die Methode der Nachbildung eines „virtuellen“ Drehgebers dargestellt.

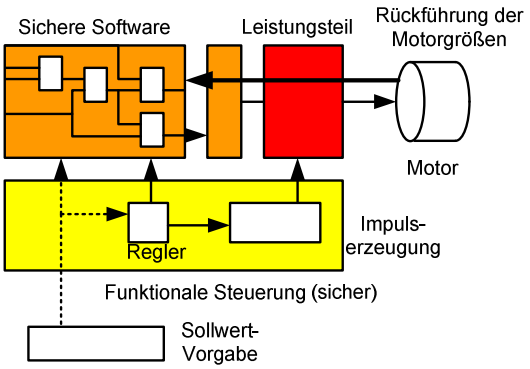

Bild 8 Regelung ohne Verwendung von Drehgebern und Encodern

Der funktionale Controller erzeugt die Impulsmuster zur Kommutierung. Über die Messung der Kenngrößen (z.B. Strom und Spannung) wird auf die Bewegung geschlossen und damit die „virtuelle“ Achse als Regeleingang verwendet.

Diese Methode stößt innerhalb der Sicherheitstechnik allerdings recht rasch an seine Grenzen, wenn es darum geht, den sicheren Betriebshalt zu garantieren. Hierbei steht der Antrieb in der Ruhelage und wird vom System festgehalten. Ohne einen externen Einfluss mag diese Funktion auch sicherheitstechnisch realisierbar sein. Wenn von außen sich jedoch rasch verändernde Kräfte einstellen, so muss das Antriebssystem die Lasten vollständig ausregeln. Kleine Abweichungen der Ruhelage sind nun durchaus möglich. Diese können aber zu unerlaubten Bewegungen beitragen und erfüllen (je nach Anwendung) nicht mehr die geforderte Sicherheit.

11 Ausblick Drive-based Safety

Neuere Marktforschungsergebnisse belegen eindeutig, dass zukünftig sichere Antriebssysteme mehrheitlich zum Einsatz kommen. Dies wird neben Servoantrieben auch Standard und Premium Frequenzumrichter betreffen. Man geht von Anwendungs- Wahrscheinlichkeiten einzelner Sicherheitsfunktionen bis zu 80% aus. Aufgrund der Vielfalt von Anwendungen für sichere Antriebssysteme besitzen die gezeigten Konzepte aus heutiger Sicht alle ihre Berechtigung. Lenze wird konsequent das Angebot an sicheren Antriebssystemen weiterentwickeln und ausbauen. Funktionale Sicherheit integriert im Antriebssystem – wir nennen es „Drive-based Safety“.

12 Literatur

[1] IEC 61508-5:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels

[2] IEC 60204-1:2005, Safety of machinery – Electrical equipment of machines – Part 1: General requirements

[3] IEC 61508-2:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[4] IEC 61800-3, Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods

[5] ISO 13849-1:2006, Safety-related parts of control systems – Part 1: General principles for design