Sicherheitstechnik gibt der Gefahr keine Chance

R. Berlin , Berlin; *L. Opitz,* Leipzig

Stromkreise, die der Sicherheit dienen, bereiten Konstrukteuren, Installateuren und Betreibern von Industriemaschinen sowie ihren Sicherheitsbeauftragten immer wieder Kopfzerbrechen. Die Verantwortung auf diesem Gebiet ist groß. Bei dem stetig steigenden Produktionstempo und der zunehmenden Komplexität von Anlagen können bereits kleine Fehler in den elektrischen Steuerungen unangenehme Folgen für Mensch, Umwelt, Maschine und die Wirtschaftlichkeit haben. Der folgende Bericht beschreibt auf der Grundlage wesentlicher europäischer und deutscher Normen am Beispiel von ET 200S-SIGUARD der Siemens AG die Lösung des Problems.

In den europäischen Normen (EN) ist analog zur deutschen DIN EN 60204 (VDE 0113) die Sicherheit einer Maschine derart definiert, daß bei der Ausführung ihrer Funktionen keine Verletzungen oder Gesundheitsschädigungen des Bedienungspersonals verursacht werden dürfen. Als Maschine im weitesten Sinne dieser Normen wird die „ ...Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist..." bezeichnet. Die dazu erforderliche zusätzliche Sicherheitstechnik soll ohne Einschränkung der Produktion die Gefährdung beim Umgang mit solchen Maschinen so gering wie möglich halten. Diese Forderungen sind gleichermaßen in allen Ländern der Europäischen Union (EU) zu berücksichtigen. Der einheitliche europäische Binnenmarkt ab 01.01.1993 führte deshalb auf Basis der Maschinenrichtlinie 98/37/EG zur Harmonisierung der Normen und Vorschriften aller EU-Mitgliedstaaten. Diese Vorschrift war dazu durch jeden Mitgliedstaat in nationales Recht umzusetzten.

Autoren

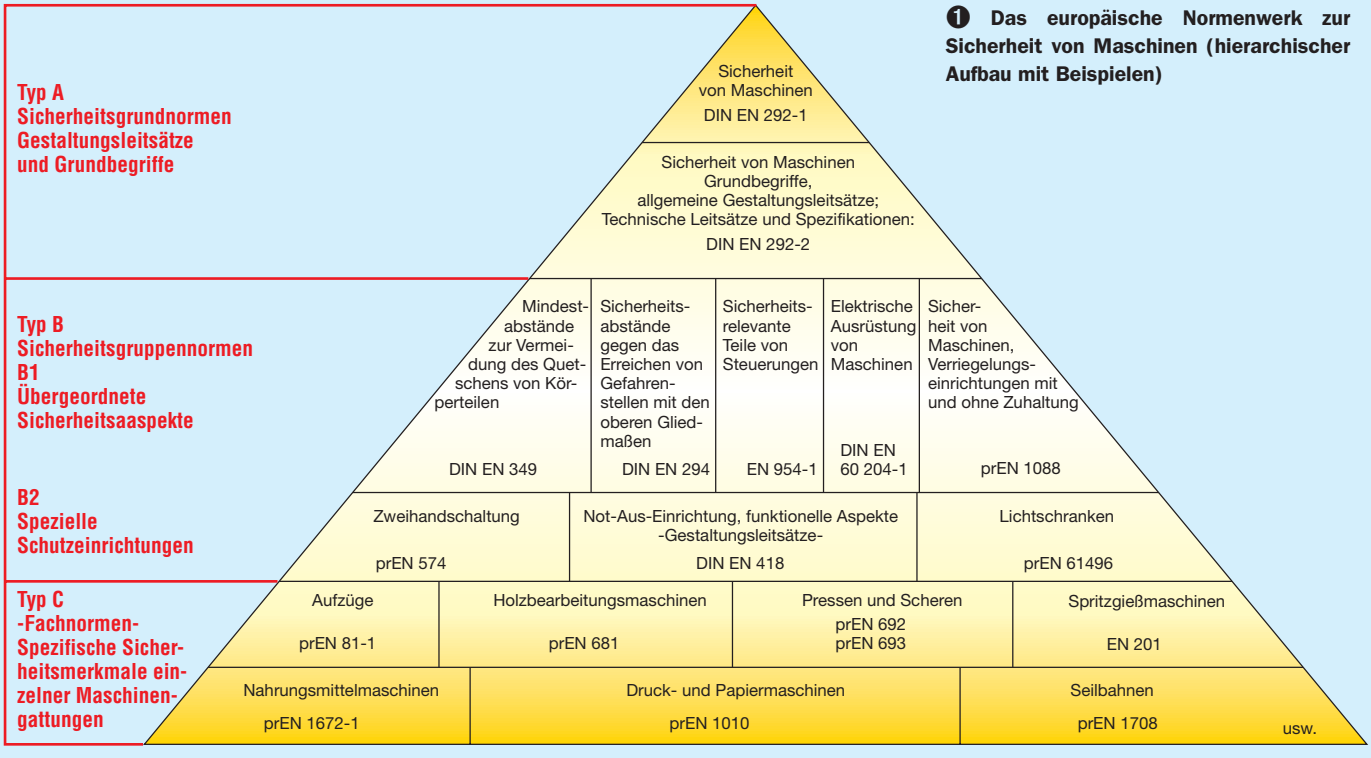
Dipl.-Ing. *Reiner Berlin* und Dipl.-Ing. *Lothar Opitz* sind Promotoren Niederspannungstechnik bei der Siemens AG Automatisierungs- und Antriebstechnik, Berlin Vertriebsregion Ost.

Das europäische Normenwerk

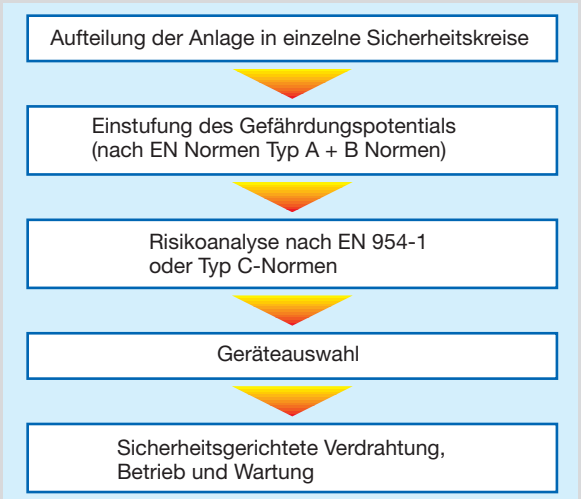
Das europäische Normenwerk der CEN für die Sicherheit von Maschinen gliedert sich hierarchisch in A-, B- und C-Normen. Die Typ-A-Normen, die Sicherheitsgrundnormen, gelten für alle Maschinen verbindlich und enthalten Grunddefinitionen. Zum Typ-B zählen die Gruppennormen mit sicherheitstechnischen Aussagen für mehrere Arten von Maschinen. Die Typ-C-Normen schließlich sind Fach- bzw. Produktnormen, die maschinenspezifische Anforderungen berücksichtigen. Bild ❶ zeigt den Aufbau des europäischen Normenwerkes für die Sicherheit von Maschinen mit den darin enthaltenen harmonisierten Vorschriften. Sie bilden die Richtschnur, die von der Konstruktion bis zur Inbetriebnahme einer Maschine anzulegen ist.

Die konzeptionelle Grundlage sicherer Anlagen bildet die Risikoanalyse/-beurteilung nach den Sicherheitsgrundnormen (Typ-A) EN 292 und EN 1050. Die Bewertung des Risikos erfolgt über einen sogenannten Risikographen nach EN 954-1, wenn für die betreffende Maschinengattung keine Typ-C-Normen vorhanden sind. Die Eckpunkte dieser Risikobeurteilung sind im Bild ❷ dargestellt.

Je nach Schwere der Verletzung in Abhängigkeit von Häufigkeit bzw. Dauer der Gefährdung sowie der Möglichkeit, diese Gefahr zu vermeiden, ergeben sich nach EN 954-1 die Kategorien B;1; 2; 3 und 4. Sie definieren die grundlegenden Anforderungen der komplexen Steuerung einer Ma-



❶ **Das europäische Normenwerk zur Sicherheit von Maschinen (hierarchischer Aufbau mit Beispielen)**



❷ **Risikoanalyse nach EN 954-1**

schine. Die mit Bild ❸ charakterisierten Anforderungen dieser Kategorien enthält vollständig der Abschnitt 6 der EN 954-1.

Stillsetzen als Schwerpunkt der Sicherheit

Von den sicherheitsbezogenen Funktionen
- Stillsetzen
- Handlungen im Notfall
- Geschwindigkeitsbegrenzung
- Positionsbegrenzung
- Geschwindigkeitsabweichung u. ä.

wird die Funktion „Stillsetzen" näher betrachtet. Gefährdungen an Maschinen entstehen nämlich in der Regel durch Drehbewegungen von Antrieben. Und im Notfall müssen somit diese Antriebe sicher stillgesetzt werden. Die EN 60204-1 (vergleichbar mit VDE 0113 Teil 1) definiert für das „Stillsetzen" drei Stopp-Kategorien (andere Funktionen kennzeichnen bis zu 4 Kategorien).

Stopp-Kategorie 0
- Stillsetzen durch sofortige Abschaltung der Energiezufuhr
- Elektromechanische Bauteile sind vorgeschrieben.
- Elektronische Betriebsmittel sind erlaubt [1].

Stopp-Kategorie 1
- Die Energiezufuhr wird solange beibehalten, bis der Antrieb elektrisch in den Stillstand abgebremst ist.
- Elektromechanische und elektronische Betriebsmittel sind erlaubt [1].

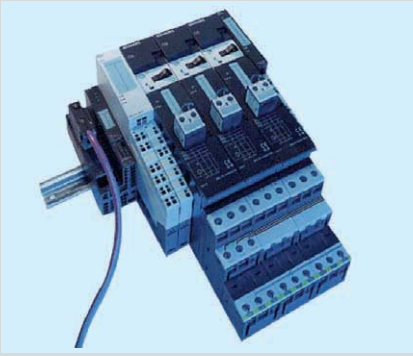
Stopp-Kategorie 2
- Gesteuertes Stillsetzen
- Bei Maschinenstillstand bleibt die Energiezufuhr erhalten.
- Jede Maschine muß mindestens mit Stopp-Kategorie 0 ausgerüstet sein
- Stopp-Funktionen müssen durch Entregen wirksam werden.

Für Sicherheitssteuerungen sind die Stopp-Kategorien 0 und 1 erlaubt. Bisher galt, daß eine Not-Aus-Einrichtung der Stopp-Kategorie 0 mit festverdrahteten, elektromechanischen Bauteilen erfolgen muß.
Die Stopp-Kategorien 1 und 2 sind aus si-

1) NEU: nach DIN EN 60204-1 11/99 Nationales Vorwort November 1998
" ... damit ist auch klargestellt, daß elektronische Betriebsmittel für Not-Aus-Einrichtungen - unabängig von der Stopp-Kategorie - angewendet werden dürfen, wenn diese die gleiche Sicherheit erfüllen, wie nach EN 60204-1 gefordert...."

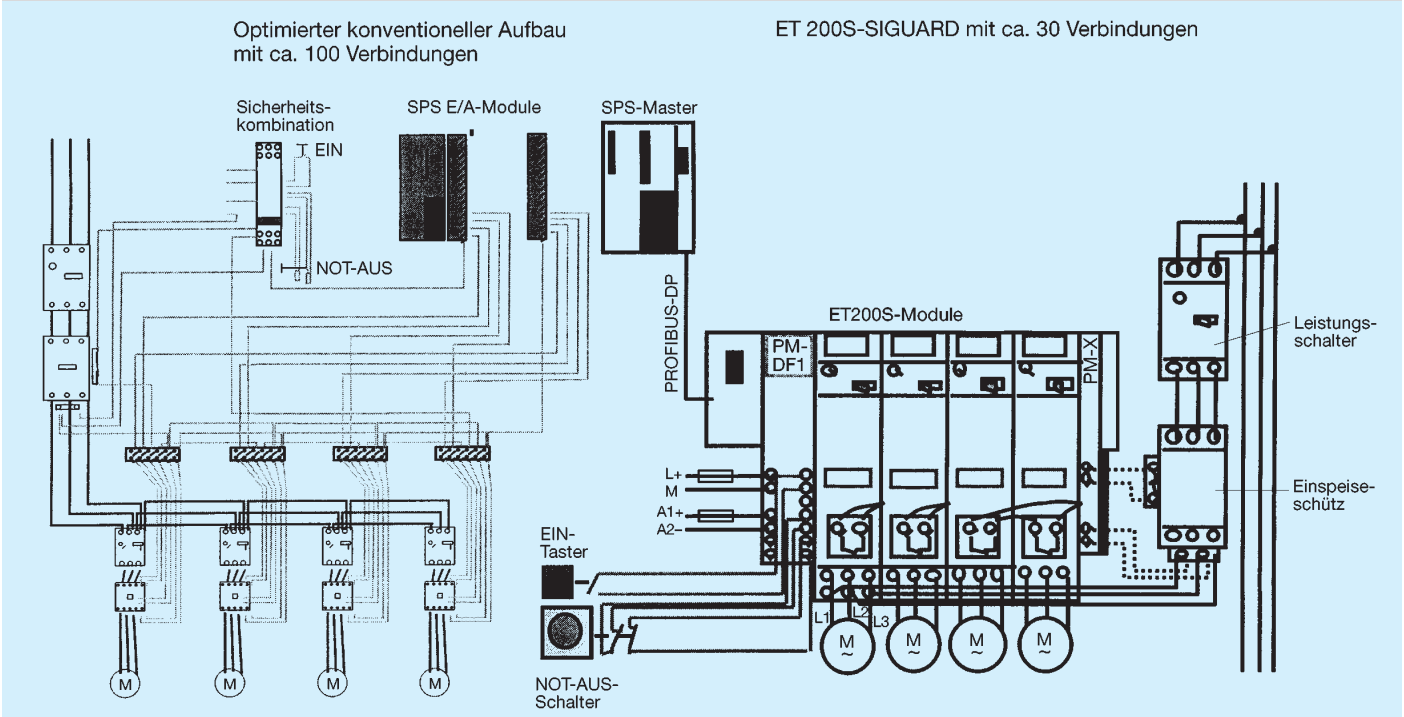
Kategorie	Kurzfassung der Anforderungen	Systemverhalten	Prinzip
B	Die Steuerung muß so konzipiert sein, daß sie den zu erwartenden Einflüssen standhalten kann	Ein Fehler kann zum Verlust der Sicherheitsfunktion führen	Überwiegend durch die Auswahl von Bauteilen charakterisiert
1	Anforderung von B muß erfüllt sein; Verwendung von sicherheitstechnisch bewährten Bauteilen und Prinzipien	Wie Systemverhalten von B, jedoch mit höherer sicherheitsbezogener Zuverlässigkeit	
2	Anforderung von 1 muß erfüllt sein; zusätzliche Prüfung der Sicherheitsfunktion in geeigneten Zeitabständen	Ein aufgetretener Fehler wird erst bei der nächsten Prüfung erkannt	Überwiegend durch die Struktur der Steuerung charakterisiert
3	Anforderung von 1 muß erfüllt sein; ein einzelner Fehler darf nicht zum Verlust der Sicherheitsfunktion führen	Die Sicherheitsfunktion bleibt beim Auftreten einzelner Fehler immer erhalten	
4	Anforderung von 3 muß erfüllt sein; der einzelne Fehler muß vor oder bei der nächsten Aufforderung an die Sicherheitsfunktion erkannt werden	Wenn Fehler auftreten, bleibt die Sicherheitsfunktion erhalten. Die Fehler werden erkannt	

❸ Kurzfassung der Anforderungen der Kategorien für die sicherheitsbezogenen Teile von Steuerungen



❹ ET 200S-Motorstartermodul für 5,5 kW

❺ Aufbau einer sicherheitsgerichteten ET 200S-SIGUARD mit vier Verbraucherabzweigen in der Kategorie 4 nach EN 954-1



cherheits- oder funktionstechnischen Erfordernissen notwendig.

EN 60204-1 (Elektrische Ausrüstung von Maschinen) verlangte die Realisierung mit elektromechanischen Komponenten, da „einfache (programmierbare)" Systeme (noch) nicht sicher genug waren. Diese Regelung wird neuerdings ergänzt durch das europäische Vorwort[1)] zu dieser Norm, daß dem Stand der Technik Rechnung trägt. Darin ist festgehalten, daß bei Anwendung funktionssicherer elektronischer und programmierbarer elektronischer Komponenten mit diesen ebenfalls das NOT-HALT für alle Kategorien realisiert werden kann. Voraussetzung ist ihre Zertifizierung nach IEC 61508 bzw. EN 954-1.

In den Kategorien sind die grundlegenden Anforderungen zur Gestaltung von Sicherheitsschaltungen festgelegt. Dabei gilt: Mit größerer Ziffer der Sicherheitskategorie steigt der Umfang der zutreffenden Maßnahmen. Während bei einer Kategorie 1 das Auftreten eines Fehlers in der Sicherheitsschaltung zum Verlust der Sicherheitsfunktion führen darf, bleibt bei der Kategorie 4 beim Auftreten eines Fehlers in der Sicherheitsschaltung die Sicherheitsfunktion erhalten. Die Defekte müssen immer rechtzeitig erkannt werden, um einen Verlust der Sicherheitsfunktion zu verhindern.

Sicherheitsschaltungen mit ET200S-SIGUARD

Zur Realisierung von Sicherheitsschaltungen, welche die Sicherheitskategorien 1 bis 4 erfüllen, bietet die Siemens AG ein komplettes Geräteprogramm SIGUARD. Das jüngste Kind in dieser Familie sind die SIMATIC ET 200S-Motorstarter mit integrierter Sicherheitstechnik. Diese Motorstarter sind in das „Dezentrale Peripheriesystem ET 200" integriert. ET200 ist ein intelligentes, dezentrales Peripheriegerätesystem, das über den Profibus mit der elektronischen Steuerung verbunden ist [1].

Die Variante ET 200S erfüllt die Forderungen der Praxis hinsichtlich Technik, Funktionalität und Benutzerfreundlichkeit nun vollständig. Eine ET 200S-Station läßt sich in beliebiger Kombination aus Ein-/Ausgabe-, Technologie- und Verbraucherabzweig-Modulen aufbauen.

Erstmals erlaubt das System bei Schutzart IP20 (also im Schaltschrank), komplette Motorabzweige bis 5,5kW bei 400 VAC (Bild ❹), sei es ein Direkt- oder ein Wendestarter, direkt über den PROFIBUS-DP anzusteuern.

Was macht die ET 200S für die Sicherheitstechnik so interessant?

Mit dieser Technik lassen sich auch sicherheitsgerichtete, normenkonforme Schaltungen dezentral vor Ort ausführen. ET200S-SIGUARD-Sicherheitskombina-

tionen sind von der Berufsgenossenschaft für Feinmechanik und Elektrotechnik bzw. dem berufsgenossenschaftlichen Institut für Arbeitssicherheit für die höchstmögliche Kategorie 4 nach EN 954-1 zugelassen. Mit einer solchen Gerätetechnik können damit erstmalig direkt an einem Peripheriesystem neben digitalen und analogen Ein-/Ausgaben sowie Standardverbrauchern auch sicherheitsgerichtete Verbraucherabzweige angeschaltet werden.

Bild ❺ veranschaulicht den Aufbau einer Not-Aus-Schaltung Kategorie 4 mit überwachtem Start. Das Powermodul SIGUARD übernimmt sowohl die Spannungsversorgung der Elektronik als auch des Abzweigschützes. Der Not-Aus-Taster (zweikanalig) und der Freigabetaster werden auf das Powermodul verdrahtet. Im Falle einer Not-Aus-Betätigung schaltet die im SIGUARD-Powermodul (PM-D F1) enthaltene Sicherheitsrelais-Kombination sowohl die Spannungsversorgung der dahinterliegenden Abzweigschütze als auch die Steuerspannungsversorgung des Einspeiseschützes über das PM-X (Connection-Modul) ab. Damit wird die Zweikanaligkeit in der Ansteuerung, eine Redundanz im Freigabekreis und eine Senkung der Fehlerwahrscheinlichkeit (Diversität) realisiert. Beide Eigenschaften bilden wichtige Voraussetzungen zum Erreichen der Kategorie 4.

Mit ET 200S-Verbraucherabzweigmodulen lassen sich sowohl einzelne Verbraucher als auch Verbrauchergruppen sicherheitsgerichtet abschalten. Dabei ist es unerheblich, ob es sich um Direkt- oder Wendestarterkombinationen handelt. Desweiteren gestattet das Gerätesystem, die Verbraucher in einzelne Not-Aus-Gruppen zusammenzufassen oder Not-Aus-Kaskaden zu bilden.

Durch die Anwendung der ET 200S-SIGUARD werden moderne Steuerungselektronik und sicherheitsgerichtete Abschaltung von Verbraucherabzweigen miteinander kombiniert, ohne daß dadurch zusätzliche Risiken entstehen. Darüber hinaus reduziert die Anwendung dieser Technik den Verdrahtungsaufwand auf ca. 30% gegenüber herkömmlichen Aufbau mit SPS, E/A-Baugruppe, Sicherheitskombination und Verbraucherabzweig. Der verminderte Verdrahtungsaufwand verursacht weniger Kosten bei Montage und Inbetriebnahme, aber auch geringere Fehlerauftrittswahrscheinlichkeit, was wiederum der Sicherheit dient. Die Gegenüberstellung Bild ❺ verdeutlicht diese vorteilhafte Situation.

Eine Vision wurde verwirklicht

Werner von Siemens in Berlin formulierte bereits im Jahre 1880 „Das Verhüten von Unfällen darf nicht als eine Vorschrift des Gesetzes aufgefaßt werden, sondern als ein Gebot menschlicher Verpflichtung und wirtschaftlicher Vernunft". Diese Vision wurde nun in die Wirklichkeit umgesetzt, indem sich die sicherheitstechnische Kompetenz, angefangen von den klassischen Schaltgeräten für sicherheitsgerichtete Steuerungen über fehlersichere speicherprogrammierbare Steuerungen bis hin zu Antriebslösungen und CNC-Steuerungen, verantwortlich in einer Hand im Geschäftsbereich Automatisierungs- und Antriebstechnik (A&D) befindet. Sie wird unter dem Begriff „Safety Integrated" als ein durchgängiges Gesamtsystem vom Sensor über die Auswertegeräte bis zu den Aktoren und in Zukunft bis zu den Antriebssystemen angeboten.

Literatur:

[1] Safety Integrated – Applikationshandbuch