

Serie I:

Sicherheitstechnik

im Maschinen und Anlagenbau | Teil III



Software unter dem Gesichtspunkt der neuen Maschinenrichtlinie



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

Es ist kaum 15 Jahre her, dass die einschlägigen Normen noch jegliche Anwendungen von programmierbaren oder softwarebehafteten Systemen für Sicherheitsfunktionen ausschlossen. So galt die Software als allgemein fehlerträchtig und damit als vollkommen ungeeignet, Sicherheitsfunktionen zu lösen. Doch seit dieser Zeit hat sich bei allen Maschinen- und Anlagenapplikationen die Kenntnis verbreitet, dass gerade der Software die Aufgabe zukommt, Sicherheitsfunktionen mit hoher Qualität auszuführen. Mehr noch – ohne Software besteht kaum die Möglichkeit, Sicherheitsfunktionen zu testen, und damit wäre eine Erfüllung der Anforderungen aus der neuen Maschinenrichtlinie für gehobene Anforderungen kaum realisierbar.

Autor: Dr. Peter Wratil / innotec

Im Gegensatz zu der alten, in der MRL gelisteten Norm EN 954 fordert die neue Norm ISO 13849 einen gewissen Diagnosedeckungsgrad (DC: Diagnostic Coverage), der dazu benötigt wird, die Sicherheitsfunktion stetig zu testen. Ein evtl. Ausfall eines Sicherheitssystems wird so erkannt, bevor es bei einer Anforderung versagt. In geeigneter Weise erbringt der stetige Test durch die Software einerseits den Nachweis, dass die Sicherheit noch gegeben ist, und andererseits informiert die Software darüber, dass ein System ausgefallen ist und damit ausgetauscht werden muss. Die Software wird damit nicht nur zum Schlüssel für mehr Sicherheit, sondern vermag auch die Verfügbarkeit anzuheben. In dem Bestreben nach einer möglichst hohen Maschinenauslastung ist sie daher nicht mehr wegzudenken.

Einheiten der Software bei Sicherheitssystemen

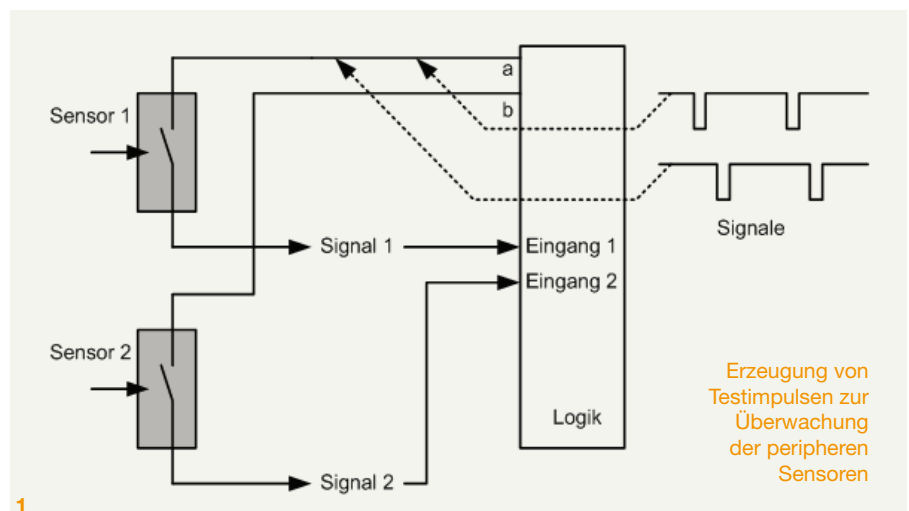
Wenn man bei Sicherheitssystemen von Software spricht, so muss man sich stets vergegenwärtigen, dass es zwei unterschiedliche Sorten von Programmen gibt. Zunächst enthält jede intelligente Sicherheitskomponente oder jedes Sicherheitssystem eine interne (embedded) Software, die alle Grundfunktionen zum Erreichen der geforderten Sicherheit enthält. Dieses Programm ist zumeist fest mit der Hard-

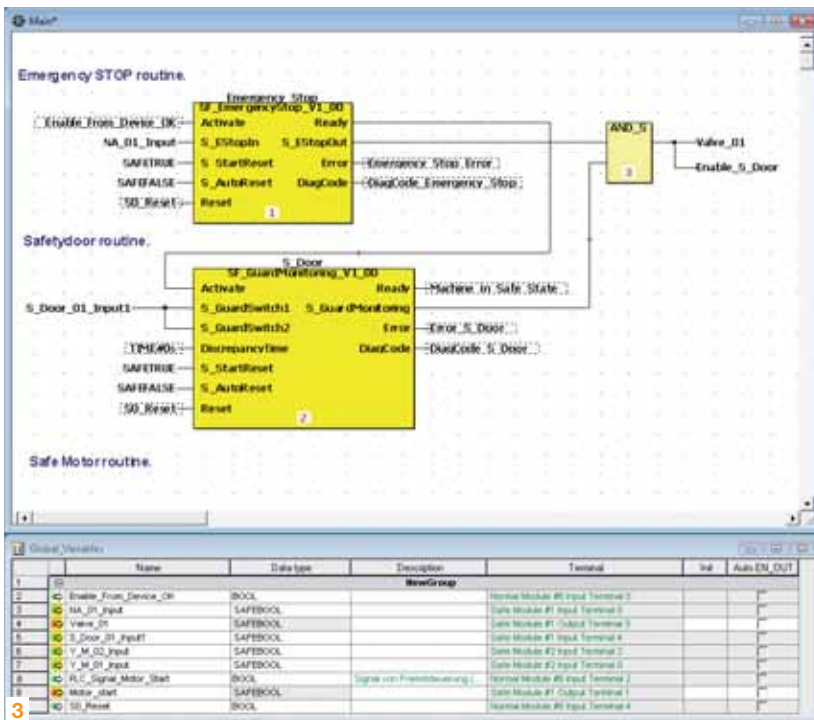
ware verankert und lässt sich nicht später (nach Auslieferung der Einheit) verändern. Oftmals wird die Hardware zusammen mit der internen Software auch als Firmware bezeichnet. Diese Firmware führt für alle in der Hardware vorhandenen Komponenten Sicherheitsfunktionen durch. So werden hier die Eingangsabbilder der Sensorzustände geholt und deren berechnete Werte an die Ausgänge weitergeleitet. Zusätzlich führt diese Software alle notwendigen Tests durch, die garantieren, dass die Sicherheit noch erfüllt ist. Zu diesen Tests gehören insbesondere folgende Funktionen:

- Test der richtigen Funktionsweise der Ein- und Ausgänge,
- Test der Verarbeitungseinheit(en) wie z. B. CPU,

- Prüfung der Speichermedien (z. B. Flash, RAM oder ROM),
- Nachweis der Richtigkeit aller Übertragungsstrecken (z. B. Bustransfers).

Die genannten Testfunktionen laufen parallel zum eigentlichen Programmablauf ab, sodass das gesamte System in einem Zeitintervall von wenigen Sekunden bis zu einigen Stunden vollständig geprüft wird. Bei der Identifikation eines Fehlers führt die Einheit eine Sicherheitsfunktion durch, die in der Regel eine Abschaltung nach sich zieht. Intelligente Einheiten sind zusätzlich noch in der Lage, die externe Anschlussstechnik zu überwachen. Wie Bild 1 darstellt, stellen hochwertige Einheiten bereits Spannungen zur Verfügung, an die der Anwender seine elektromechani-





Beispiel einer Programmierung mit Funktionsbausteinen (Bild: KW-Soft)

Black-Box-Tests zu verwenden. Auch statistische Tests fallen unter die Kategorie der Black-Box-Tests. Bei der Methode des White-Box-Tests sind dem Tester die internen Details des Codes bekannt. Durch geschickte Testspezifikationen kann er jede einzelne Reaktion und jeden Ablauf genau nach verfolgen. Der White-Box-Test wird häufig auch von der Person durchgeführt, die den Programmcode entwickelt hat.

Verwendung von Funktionsblöcken

Damit es dem Anwender leicht fällt, seine Applikation möglichst fehlerfrei zu entwickeln, stellen die Hersteller von Sicherheitssystemen oftmals Hochsprachenelemente zur Verfügung, die selbst bereits hinreichend getestet sind und damit nur zu einer Gesamtfunktion kombiniert werden müssen. Da die Editoren für die Erstellung dieser Funktionsbausteine bereits den größten Teil der Fehler abfangen, werden gravierende Unstimmigkeiten bereits im Vorfeld ausgeräumt.

Wie man in Bild 3 sieht, lassen sich spezifische Funktionsblöcke innerhalb eines Editors aufrufen und in geeigneter Weise miteinander kombinieren,

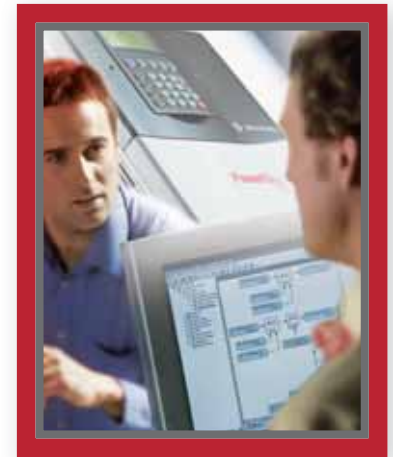
sodass die gewünschte Sicherheitsfunktion entsteht.

Bei einigen Programmen stehen direkt Simulatoren zur Verfügung, die auch solche Zustandsveränderungen erlauben, welche man in der Realität nur schwer nachbilden kann. Nicht zuletzt dient die Verwendung von Programmier-Tools mit deren integrierten Dokumentationsfunktionen zur Ablage der gefundenen Sicherheitsfunktion.

Fazit

Software enthält im Gegensatz zur Mechanik oder Elektronik keinerlei sporadische Fehler. Die Software ist ausschließlich von systematischen Fehlern geprägt, deren Ursache in einer fehlerhaften Programmierung zu suchen ist. Damit die gesamte Sicherheitsfunktion entsprechend den Anforderungen der Normen möglichst fehlerfrei zum Einsatz kommt, sind besondere Maßnahmen für deren Erstellung gefordert.

Der Programmierer muss fundierte Techniken beherrschen und so einsetzen, dass Fehlfunktionen nicht zu Risiken für das Leben und die Gesundheit des Menschen führen.



WIE ANSPRUCHSVOLL IHRE ANFORDERUNGEN AUCH SIND, UNSERE INTELLIGENTE MOTORSTEUERUNG BIETET DEN OPTIMALEN ANTRIEB.

Vom einfachen Drehzahlregler bis zu komplexen Moment- oder Positionsregelungen, Rockwell Automation unterstützt Sie mit Applikationswissen, Industrieerfahrung und einer kompletten Familie von Frequenzumrichtern. Von 0,25 kW bis 25 MW: PowerFlex Antriebe sind optimal für Ihre Anwendungen.

POWERFLEX DRIVES
www.rockwellautomation.at



Rockwell Automation

ALLEN-BRADLEY • ROCKWELL SOFTWARE