



Wechsel zur Sicherheitssteuerung erleichtert

Zustimmprinzip zur Erstellung der Sicherheitslogik

Programmierbare Sicherheitssteuerungen sind in mittleren bis großen Automatisierungslösungen auf dem Vormarsch. Diejenigen, die noch an verdrahtete Sicherheitstechnik glauben, kommen angesichts der Einsparungspotentiale und Diagnosemöglichkeiten zusehends ins Wanken. Wie bei der Einführung der SPS, wird es Unverbesserliche geben, die um jeden Preis an existierender Technik festhalten wollen. Aber auch diese werden auf Dauer nicht dem Preisdruck und dem Kundenwunsch nach schnellster Diagnose im Falle eines Stillstandes standhalten. Eine einfache und effektive Methode auf programmierbare Sicherheitstechnik umzusteigen, bietet das sogenannte Zustimmprinzip. Damit ist die Erstellung der Sicherheitslogik nicht schwieriger, als einen Stromlaufplan zu entwickeln.

STEFFEN SCHLETTE



Dipl.-Ing. STEFFEN SCHLETTE,
KW-Software GmbH

Zustimmprinzip für moderne Sicherheitssteuerungen

Der Druck auf Anbieter von Automatisierungslösungen, programmierbare Sicherheitsfunktionen anzubieten, erhöht sich zusehends. Leider ist das Entwickeln eines sicherheitsrelevanten Produktes auf Grund der einzuhaltenden Normen und der Zertifizierung aufwendiger und teurer als ein Standardprodukt. KW-Software hat deshalb die sichere grafische Programmieroberfläche

SafePROG mit der sicheren Laufzeitumgebung SafeOS entwickelt, die auf die Hardware und das Bussystem einer neuen Sicherheitssteuerung angepasst werden kann. Die Programmieroberfläche bietet u.a. die Möglichkeit, im so genannten Zustimmprinzip zu programmieren. Dabei wird gedanklich der sichere Anteil einer Anlage, wie zum Beispiel eine Not-Aus Schaltung aus der Verdrahtungstechnik in das Programmiersystem übertragen. Die Programmierung der normalen Automatisierungsfunktionen bleibt so, wie sie heute schon ist. Der heutige SPS-Programmierer

muss sich bezüglich seiner erlernten Fähigkeiten und erprobten Vorgehensweisen bei der Programmierung einer Anlage kaum umstellen. Es ändert sich lediglich der Typ der Schnittstelle zu der Sicherheit von Hardware auf Software.

Die obere Hälfte von Abb.1 zeigt eine klassische Not-Aus-Schaltung, die auf die Spannungsversorgung der SPS-Ausgänge wirkt. Ein Auslösen der Not-Aus-Funktion bewirkt ein komplettes Abschalten der Ausgangskreise. Natürlich ist anstelle der Schützschialtung auch ein elektronisches Not-Aus-Gerät einsetzbar.

In der unteren Hälfte von Abb.1 wurde die Verdrahtung durch eine Zustimmsicherheitssteuerung ersetzt. Diese ist in der Lage, jeden Ausgang separat abzuschalten, den ausgelösten Not-Aus-Schalter zu identifizieren oder, im Falle von Hardwareschäden, den entsprechenden Schaden – wie zum Beispiel Drahtbruch – zu melden.

Die SPS arbeitet in diesem Fall in gewohnter Weise, indem sie Eingänge verarbeitet und Ausgänge setzt. Es handelt sich hierbei allerdings um sichere Ausgänge, die ebenfalls von der Sicherheitssteuerung angesprochen werden können. Jetzt kommt das Zustimmprinzip ins Spiel. Genauso, wie das Schütz K1 in Abb.1 je nach Zustand den Betrieb der Lasten erlaubt oder verweigert, erlaubt oder verweigert die Sicherheitssteuerung den Betrieb der Lasten in gleicher

Weise (Abb. 2).

Im Sicherheitsprogramm wird der Funktionsbaustein ‚Not-Aus‘ mit den Eingangssignalen der entsprechenden Taster und Schalter verbunden. Zusätzlich wird der Funktionsbaustein mit demselben sicheren Ausgang verknüpft, auf den auch die SPS wirkt. Der sichere Ausgang hat eine eigene Intelligenz und schaltet nur dann durch, wenn die SPS und die Sicherheitssteuerung ein ‚1‘-Signal auf diesen Ausgang legen.

Mit diesem Vorgehen erreicht man, dass ein Sicherheitsprogramm von dem normalen SPS-Programm vollständig entkoppelt ist. Die SPS kann auf Grund von Programmierfehlern oder äußeren Einflüssen, wie EMV, ‚verrückt‘ spielen und sicherheitsrelevante Ausgänge setzen, ohne dass die Sicherheit in der Maschine gefährdet ist. Sollte ein Ausgang gesetzt werden, der zum Beispiel eine für Menschen gefährliche Bewegung auslöst, während die entsprechende Schutztür offen ist, erkennt die Sicherheitssteuerung die Verletzung der Sicherheit und überstimmt die SPS, indem der Ausgang zurück-

gesetzt wird, solange die Schutztür offen ist. Es gibt für die grundlegenden Sicherheitsfunktionen Standardfunktionsbausteine wie zum Beispiel Not-Aus, Schutztür, Zweihandschaltung oder Betriebsartenwahlschalter. Leider sind

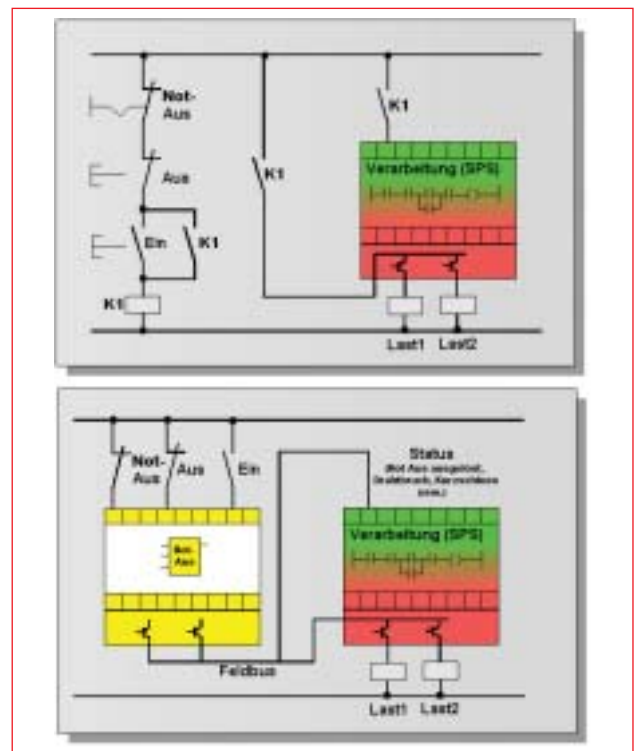


Abb.1: Vergleich Schützschialtung und Sicherheitssteuerung

Anzeige

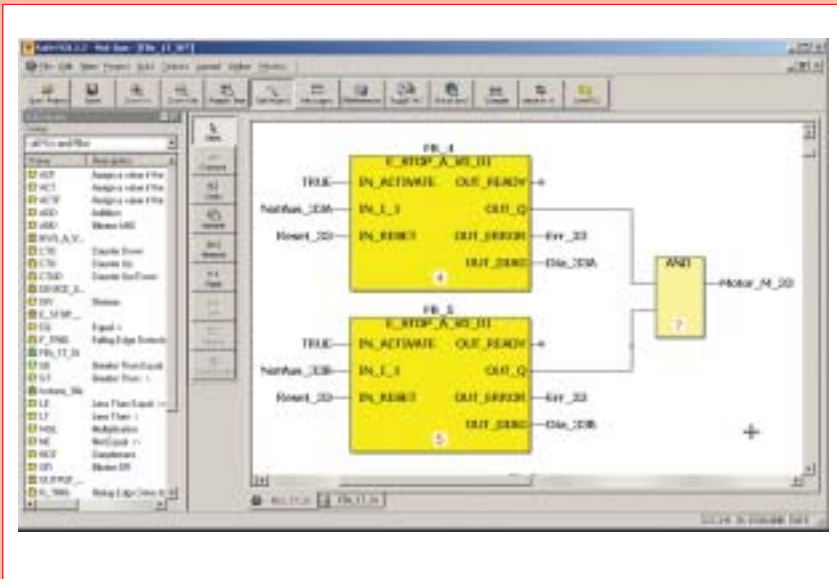


Abb.2: Sichere Funktionsbausteine in SafePROG

Kategorie (EN 954-1)	SIL (IEC 61508)
B	0
1-2	1
2-3	1
3	2
4	3
-	4

Abb.3: Zuordnung von Kategorie auf SIL: Dies ist ein Anhaltspunkt, eine direkte Zuordnung ist nicht möglich.

derzeit diese Bausteine von Sicherheitssteuerung zu Sicherheitssteuerung unterschiedlich, es gibt aber momentan Bestrebungen der PLCopen, diese Bausteine zu standardisieren. Im einfachsten Fall werden diese dann im Sicherheitsprogramm mit den entsprechenden Eingangs- und Ausgangsklemmen verbunden und die gewünschte Funktion ist einsatzbereit. Sehr einfache Sicherheitssteuerungen setzen nahezu ausschließlich auf dieses Prinzip, dass sicherlich für viele Einsatzzwecke ausreichend ist.

Es stößt aber immer dann an seine Grenzen, wenn komplexe Sicherheitsbedingungen programmiert werden sollen. Vorstellbar ist zum Beispiel eine Maschine, die von zwei Personen mit Teilen beschickt wird. Jede Person kann an der Maschine über eine Zweihandschaltung eine

gefährbringende Bewegung, zum Beispiel eine Pressung, auslösen. Tatsächlich wird die Bewegung aber erst dann ausgelöst, wenn beide Personen ihre jeweilige Zweihandschaltung innerhalb einer bestimmten Zeitspanne betätigen. Da es sich bei der Bewegung nicht um das simple Anschalten eines Motors handelt, sondern um eine komplexe Bewegung, die nur von der SPS durchgeführt werden kann, muss diese von der Sicherheitssteuerung ein entsprechendes Signal bekommen, um die Bewegung durchführen zu können. Lässt eine der Personen die Zweihandschaltung los, würde das Zustimmprinzip die Anlage sofort außer Betrieb setzen.

Für derartige Anwendungsfälle bietet SafePROG die Möglichkeit, über selbst definierte Funktions-

bausteine, auch komplexe Logik zu programmieren und diese beliebig oft wieder zu verwenden.

Einsparmöglichkeiten durch Sicherheitssteuerung

Einsparungen im Materialbedarf resultieren durch reduzierten Verdrahtungsaufwand, geringeren Platzbedarf im Schaltschrank und Einsparung von Sicherheitsrelais.

Die erste Frage, die dem Projektierer einer Anlage einfällt, ist – verständlicherweise – ob er diesen Vorteil durch die Einarbeitung in die Programmierungsumgebung nicht wieder verliert.

SafePROG legt einen hohen Wert auf intuitives Arbeiten mit viel Unterstützung durch Program-

Anzeige

mierhilfen. Man sollte auch nicht vergessen, dass sich viele Sicherheitsfunktionen von Anlage zu Anlage wiederholen oder im Serienmaschinenbau gar immer gleich sind. In diesen Fällen kann man bereits programmierte Logik ohne Aufwand wieder verwenden. Verdrahtete Logik muss im Gegensatz dazu in jede Maschine einzeln eingebaut werden.

Wege aus dem Normendschunzel

Für die Konstrukteure von Anlagen und Maschinen mit Sicherheitsfunktionen gilt neben den verbindlichen EG-Richtlinien und harmonisierten

Europasnormen, wie die EN 292, die grundlegende Sicherheitsanforderungen definiert, auch die bekannte EN 954, die sich gezielt mit Anforderungen an die sicherheitsgerichteten Teile einer Maschinensteuerung auseinandersetzt und diese in die Kategorien 1-4 unterteilt. Anbieter von Sicherheitssteuerungen entwickeln ihre Produkte aber inzwischen ausschließlich nach der neueren IEC 61508, die auf die Kategorien der EN 954 nicht eingeht, sondern SIL (Safety Integrity Level) beschreibt.

SafePROG und SafeOS erfüllen die strengen Auflagen der IEC 61508 bereits. Diese Norm wird wohl auch in der Welt des Maschinenbaus ihren Platz einnehmen. Momentan hat sie aber noch nicht die gleiche Bedeutung wie die EN 954 erreicht. Bis das soweit ist, muss der Konstrukteur entscheiden, ob ein Sicherheitssystem der von ihm einzuhaltenden Kategorie entspricht.

In vielen Fällen handelt es sich dabei um die Kategorie 4, d.h. alle Sicherheitsfunktionen müssen doppelt ausgeführt werden. Um diese Kategorie mit einer Sicherheitssteuerung erfüllen zu können, muss die Sicherheitssteuerung und alle dazugehörigen Teile, wie z.B. sichere I/O-Feldbusmodule, baumustergeprüft sein und es muss dafür eine Programmierumgebung bereit gestellt werden, die für das Programmieren nach SIL 3 freigegeben ist.

Da es an der Schnittstelle von der Programmierumgebung zu der Sicherheitssteuerung keinen Standard gibt, liefert jeder

Hersteller eine passende Programmierumgebung mit. Das eine Sicherheitsfunktion doppelt ausgeführt werden muss, heißt nicht, dass die Sicherheitssteuerung sowie alle sicheren I/O-Module doppelt vorhanden sein müssen. Die Dopplung wird in der Regel über geschickte Maßnahmen in den Geräten und im Feldbus selbst erreicht. Bessere Systeme können sichere I/O-Module sogar in den ganz normalen Feldbus integrieren und erfordern keinen eigenen Sicherheitsbus.

Das bietet neben dem weiteren Einsparungspotenzial die Möglichkeit, existierende Anlagen

mit einer Sicherheitssteuerung zu modernisieren.

Diesen Beitrag als PDF und weiterführende Informationen (ähnliche Beiträge, technische Daten, Direktlinks zum Hersteller etc.) auf www.aud24.net.

Beitrag als PDF per ‚more@click‘:



Anzeige