Bilder: Schmersal

Maschinensicherheit – maßgeschneidert!

von Tobias Thiesmann

Sicherheitsfunktionen verlagern sich von der Hard- auf die Software-Ebene. Daher bietet es sich für Maschinenbauer bei Neuentwicklungen an, frühzeitig mit ihrem Zulieferpartner für Sicherheitssysteme zusammenzuarbeiten. Besondere Vorteile ergeben sich aus der Nutzung von OEM-spezifischer Software.

Zu den Entwicklungszielen bei der Projektierung von Schutzeinrichtungen gehören unter anderem die nahtlose Integration von Sicherheitsfunktionen in den Prozess, Transparenz hinsichtlich des Betriebszustandes sowie ein minimierter Installationsaufwand und hohe Konnektivität. Die Verlagerung vieler Sicherheitsfunktionen von der Hard- in die Software sowie der Einsatz von elektronischen Sicherheitsschaltgeräten und Sicherheitssteuerungen schaffen die Voraussetzung dafür, diese Ziele gut erreichen zu können.

Individuell statt aus dem Katalog

Liegen die konkreten Anforderungen einer Applikation jenseits des ‚Mainstream' (aber nicht nur dann), hilft eine kundenspezifische Anpassung der Sicherheitsfunktionen das Zusammenwirken von Maschinensicherheit und Prozess zu optimieren. Bei Schmersal hat sich diesbezüglich mit individuellen Software-Bausteinen sowohl für programmierbare Sicherheitssteuerungen als auch für parametrierbare Sicherheitskleinsteuerungen ein Lösungspfad etabliert, da diese ab Werk mit kundenspezifischer Software ausgeliefert werden können.

Event-Tipp

Schmersal ist Aussteller auf der SPS von 8. bis 10. November in Nürnberg:
Halle 9, Stand 460

Entwickelt und projektiert werden solche kundenspezifischen Sicherheitslösungen von einem Projektteam bei Schmersal im Geschäftsfeld ‚Systeme und Lösungen'. Nachfolgend einige Beispiele aus der Praxis.

Kompaktsteuerung ersetzt 13 Relaisbausteine

Ein Unternehmen, das Lebensmittelmaschinen herstellt und eine neue Maschinenbaureihe entwickelte, konsultierte Schmersal mit dem Ziel, die Auswahl der sicherheitstechnischen ‚Hardware' zur Überwachung mehrerer Schutztüren und Klappen an einer Schneidanlage zu optimieren und auch zu konsolidieren. Die Herausforderung bestand darin, die insgesamt 13 verschiedenen Typen von Sicherheitsauswertungen zu vereinheitlichen, die in diversen Produktreihen des Maschinenbauers verbaut waren. Auslöser dafür war ein Mix aus Anforderungen an die Verfügbarkeit, gestiegenen Sicherheitsstandards sowie Abkündigungen seitens der Hersteller.

In Zusammenarbeit mit Schmersal wurden die Funktionen dieser 13 Sicherheitsbausteine in einem Gerät vereint: der Sicherheitskompaktsteuerung ‚Protect Select', genauer gesagt, der OEM-Version mit kundenspezifischen Software-Modulen. So kann nun eine einzige Version der Kompaktsteuerung in sämtlichen Produktbaureihen eingesetzt werden – ohne Einschränkung der Funktionalitäten. Im Zuge des Projektes wurden die Sicherheitskennwerte ermittelt und alle Anforderungen der Maschinensicherheit berücksichtigt. Dem Anwender der Maschine stehen unter anderem verbesserte Diagnosemöglichkeiten im Fehlerfall und bei Unregelmäßigkeiten zur Verfügung.

Kundenspezifische Stillstandsüberwachung

Ein Hersteller von Brotschneidemaschinen für Supermärkte suchte nach einer Lösung für die Überwachung und Integration der Sicherheitseinrichtungen Stillstandsüberwachung der Schneidvorrichtung, Zuhaltung der Schutzhaube, sensorische Überwachung der Schutzhaube sowie Not-Halt. Im Wettbewerb mehrerer Anbieter konnte sich Schmersal auch hier mit dem Konzept der Sicherheitskompaktsteuerung ‚Protect Select' in einer OEM-Version durchsetzen. Das Konzept mit kundenspezifischer Software trägt allen individuellen Anforderungen des Maschinenherstellers Rechnung. Die Steuerung lässt sich universell für mehrere Baureihen einsetzen, ermöglicht umfassende Diagnosefunktionen und bietet im Vergleich zu einer herkömmlichen Stillstandsüberwachung erhebliche Kostenvorteile.

Installation von Sicherheitsschaltgeräten

Auch bei der Installation und Integration von Sicherheitsschaltgeräten im Feld ergeben sich Vorteile, wenn die Sicherheitstechnik individuell angepasst wird, wie das dritte Beispiel belegt: Ein Hersteller von Verpackungsmaschinen überwacht die Schutztüren einer Maschinenbaureihe unter anderem mit Sicherheitszuhaltungen (AZM 300), Sicherheitssensoren (RSS 260) sowie Befehlsgeräten und Not-Halt. Das Application Engineering von Schmersal schlug die Anschaltung dieser (Sicherheits-) Schaltgeräte über eine ‚Safety Fieldbox' vor. Sie ermöglicht die Anschaltung von bis zu acht Sicherheitsschaltgeräten verschiedener Bauarten im Feld. Sowohl die sicherheitsgerichteten als auch die betriebsmäßigen Signale werden gesammelt und via Profinet/Profisafe mit übergeordneten Steuerungen verbunden. Künftig werden Anwendern auch Ausführungen mit Anbindung an Ethernet/IP, CIP Safety und Ethercat FSoE zur Verfügung stehen. So profitiert der Maschinenbauer von vereinfachter Installation und der Anwender unter anderem von schneller Diagnose im Fehlerfall.

Auswege aus der Materialknappheit

Eine neue Aufgabe für das Team ‚Systeme und Lösungen' hat sich erst in den letzten Monaten ergeben. Anlass ist die anhaltende Knappheit elektronischer Bauelemente. Sie führt bei Schmersal dazu, dass gerade die neuesten Generationen von elektronischen Sicherheitsschaltgeräten zeitweise nicht in den Stückzahlen produziert werden konnten und können, die der Markt benötigt.

Die Aufgabe lautet also: Suche nach Alternativlösungen, die aus Sicht des Maschinenbauers möglichst wenig Änderungen

Die programmierbaren Sicherheitssteuerungen Protect PSC1 sind Basis vieler Sicherheitslösungen – auf Wunsch mit kundenspezifischer Software.

erfordern und aus Sicht des Anwenders die volle Funktionalität bieten. Mit etwas Engineering-Aufwand und genauer Analyse des Bedarfs lässt sich das gut bewältigen – zumal teilweise baugleiche Schalter mit anderem Wirkprinzip zur Verfügung stehen. Ein Beispiel: Zu den Sicherheitssensoren vom Typ RSS16 mit sicherer RFID-Technik (und Mikrocontroller) gibt es als Alternative (ohne Mikrocontroller) den Magnetsicherheitssensor BNS16 und den elektromechanischen Sicherheitsschalter AZ16. Im Einzelfall muss jedoch durch Sicherheitsberechnungen ermittelt werden, welche Lösung tatsächlich in Frage kommt – um dann leider festzustellen, dass sich nicht alle nötigen Eigenschaften 1:1 realisieren lassen.

Ein Beispiel aus der Beratungspraxis: Bei ein und denselben Anwendungsfall (Zykluszeit 1000 s = 12.672 Betätigungen pro Jahr, drei Geräte in Reihe) ergaben sich für den RFID-Sicherheitssensor RSS260 ein maximaler Performance Level (PL) e und ein hoher Diagnosedeckungsgrad (DC). Beim elektromechanischen Sicherheitsschalter AZ16 wurde Performance Level d und ein niedriger DC ermittelt. Für den BNS260 wurden PL c und kein DC errechnet. Gründe dafür

Die Sicherheitskleinsteuerung Protect Select gibt es in OEM-Varianten mit kundenspezifischer Programmierung.

sind Verschleiß (der bei den RFID-basierten Sicherheitssensoren nicht auftritt), Fehlermaskierungen und fehlende Selbstüberwachungsfunktionen (auf Kurzschluss oder Querschluss oder ähnliches). Darüber hinaus wirkt sich hier die Reihenschaltung negativ auf den Performance Level aus. Allerdings kann der Konstrukteur die Möglichkeit nutzen, bestimmte Funktionen (zum Beispiel die Selbstüberwachung auf Kurzschluss und Querschluss) in die Auswertung zu verlagern, zum Beispiel in den Sicherheitsrelaisbaustein.
Wie die Beispiele zeigen, kann die frühzeitige Zusammenarbeit mit Experten von Sicherheitssystemen Vorteile bei der Konstruktion neuer oder der Optimierung vorhandener Maschinenbaureihen bringen. Dies gilt dann, wenn der Einsatz kundenspezifischer (Sicherheits-) Software geprüft wird. ik

Eine Frage der Sicherheit

In Sachen Safety-Zertifizierung herrscht oft Unsicherheit seitens der Anwender. Zu aktuellen Fragestellungen bezieht Tobias Thiesmann, System- und Lösungsmanager bei der Schmersal Gruppe, Stellung.

Herr Thiesmann, aufgrund der Lieferengpässe kommt es zu Reengineering und auch alternativen Lösungen. Welche Auswirkungen hat das auf die Sicherheitszertifizierung nach den Safety-Standards? Wie lässt sich eine erneute Zertifizierung verhindern?
Tobias Thiesmann: Gezielt kann man in diesem Fall wenig verhindern. Wenn die alternativen Bauteile innerhalb der vorgegebenen Spezifikation sind und über die gleiche Bauform verfügen, bewerten wir es intern und melden die Änderung beim zuständigen Notified Body. Muss eine wesentliche Änderung durch das alternative Bauteil durchgeführt werden, wie zum Beispiel eine Layout-, Schaltungs- oder Software-Änderung, müssen diese Änderungen beim Notified Body neu geprüft werden – bis hin zur Neuzertifizierung.

Tobias Thiesmann
ist System- und Lösungsmanager bei der Schmersal Gruppe in Wuppertal.

Immer mehr Safety-Funktionen werden in Software abgebildet. Worauf sollte der Anwender bei der Realisierung achten?
Sicherheitsfunktionen in Software abzubilden ist grundsätzlich kein Problem. Allerdings sollte diese Software auf einer Hardware laufen, die für den Einsatz im Bereich funktionaler Sicherheit geeignet ist. Das erkennt man in der Regel schon daran, dass der Hersteller die entsprechenden Kennwerte angibt – also Safety Integrity Level, Performance Level oder Sicherheitskategorie. Aber auch die Software selbst muss bestimmte Anforderungen erfüllen. Einen Einstieg bieten hier die Normen ISO 13849-1 und 13849-2. Meistens wird programmierbare Hardware, die es erlaubt, Sicherheitsfunktionen in Software abzubilden, seitens des Herstellers mit einer geeigneten Programmierumgebung ausgeliefert. Nach Erstellung der Software muss außerdem eine Validierung vorgenommen werden, die gewährleistet, dass die Implementierung der Software den Anforderungen zum Beispiel aus der Risikobeurteilung genügt.

Auf Safety-Steuerungen kommt auch Software von Anwendern zum Einsatz. Was heißt dies bezüglich der Einhaltung der Safety-Zertifizierung?
Die vom Hersteller angegebenen Sicherheitsparameter gelten in der Regel nur für die Hard- und Firmware der Sicherheitsteuerung. Die Anwendersoftware liegt - wie der Name schon nahelegt – in der Verantwortung des Erstellers, also des Anwenders. Softwarefehler im engeren Sinne werden hierbei zwar oft über die Programmierumgebung abgefangen – die eigentliche Programmlogik bleibt bei dieser Prüfung aber außen vor. Das heißt: Nicht alles, was kompiliert ist, ist auch funktional sicher.
Zusätzlich zur Verwendung sicherer Hardware und einer geeigneten Programmierumgebung muss der Anwender durch Validierung die Eignung der Software dokumentieren. Neben der Eignung der Steuerung spielen nämlich auch Fragestellungen in Bezug auf die konkrete Applikation zur Erreichung bestimmter Sicherheitskennwerte eine Rolle – zum Beispiel Schutz gegen unerwarteten Wiederanlauf oder das Einbinden der Rückführkreise.

Schmersal steht Anwendern beratend zur Seite. Welche Fragen tauchen dabei immer wieder auf? Wo sehen Sie den größten Handlungsbedarf?
Die erste Fragestellung ist oft die Auswahl der richtigen Hardware für eine konkrete Aufgabenstellung. Daran schließt sich dann häufig die Beratung der Kunden bei der Integration der Sicherheitslösung in die Applikation an. Was oftmals auf der Strecke bleibt, ist allerdings die Nutzung von Synergieeffekten. Eine moderne, programmierbare Sicherheitslogik bietet häufig die Möglichkeit, Sicherheitslösungen zu vereinheitlichen und auch weitere Funktionen wie etwa Schnittstellen zur Dokumentation sowie zur Diagnose und Kommunikation. Dieses Potenzial wird gern verschenkt, weil es dem Anwender nicht unmittelbar neuen Umsatz bringt und man deshalb ‚alles so lassen will, wie es ist'. Die langfristige Steigerung der Produktivität bleibt damit leider oft auf der Strecke. ik