SICHERE PRESSENAPPLIKATIONEN

Viele Hersteller von Sicherheitssteuerungen bieten Programmiersysteme mit Bausteinbibliotheken gemäß der PLCopen Safety an. Die gleichnamige herstellerübergreifende Arbeitsgruppe ergänzt nun die Spezifikation um weitere Funktionsbausteine für Pressenapplikationen.

TEXT: Jochen Ost, Bosch Rexroth **FOTOS:** Bosch Rexroth www.AuD24.net/PDF/ADK9017440

Mit Ablösung der EN 954 durch die ISO 13849 beziehungsweise durch die IEC 62061 ist neben der Bewertung der Ausfallwahrscheinlichkeit und der Berücksichtigung systematischer Fehler sowie Fehler gemeinsamer Ursache insbesondere das Thema Software in den Fokus sicherheitstechnischer Anforderungen gerückt. Sicherheitssteuerungen arbeiten Programme zwar sicher ab, allerdings ist ihre Zertifizierung mit SIL 3 (Safety Integrity Level) oder PL e (Performance Level) kein Garant dafür, dass die Anwendung auch korrekt programmiert wurde.

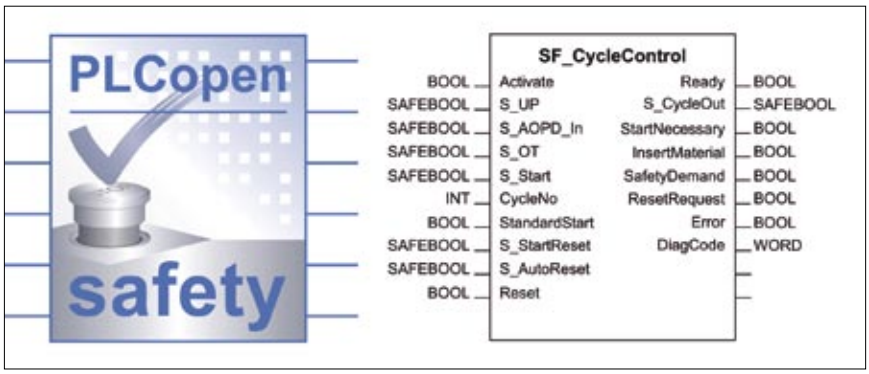
Wird beispielsweise eine Sicherheitsfunktion durch eine einfache ODER-Verknüpfung auf unzulässige Weise überbrückt, also vorübergehend außer Kraft gesetzt, besteht Gefahr für Mensch und Maschine. Das gilt auch dann, wenn Komponenten eingesetzt werden, die über entsprechende Zertifikate und Prüfsiegel verfügen. Um solchen Anwendungsfehlern vorzubeugen, stellen die neuen Normen qualitative Anforderungen an den kompletten Software-Entwicklungsprozess. Diese lassen sich mit je einfacher, desto sicherer auf einen gemeinsamen Nenner bringen.

Dem steht gegenüber, dass sich die Sicherheit im Maschinen- und Anlagenbau kontinuierlich weiterentwickelt. Während die Funktionalität von Maschinen wie Produkten steigt, soll die Komplexität der Programmierung jedoch nicht zunehmen. Ziel muss es also sein, Anwender so zu unterstützen, dass sie Sicherheitsfunktionen in der Praxis mit der gebotenen Einfachheit programmieren und umsetzen können.

Fehlerquellen aus drei Bereichen

Mögliche Fehlerquellen bei der Programmierung von Sicherheitssteuerungen lassen sich folgenden Ursachen zuordnen: mangelhafte Spezifikation, Modifikationen, zu komplexe Programme und Herabsetzung der Sicherheitsintegerität, also der Wirksamkeit von Sicherheitsfunktionen.

Mangelhafte Spezifikation bedeutet, dass die Funktion, die es umzusetzen gilt, nicht vollständig definiert wird. Im Zuge der Umsetzung kann es deshalb zu Interpretationen kommen, die nicht zwangsläufig mit dem ursprünglich Gewollten übereinstimmen müssen. Die Folge ist, dass verschiedene Betriebs-



PLCopen-Safety-Funktionsbaustein für Pressen: SF_CycleControl zur Steuerung einer Presse durch eine nicht-trennende Schutzeinrichtung bei zyklischem Eingriff

zustände nicht berücksichtigt, Fehlerverhalten nicht definiert und eindeutige Leistungskriterien nicht festgelegt werden.

Modifikationen sind während der Konstruktion keine Seltenheit, denn auch eine Serienmaschine ist in der Regel keine echte Serienmaschine. Spezifische Änderungen für den Endkunden werden insbesondere mit Blick auf die funktionelle Sicherheit oftmals unter Zeitdruck kurz vor Maschinenübergabe vorgenommen. Dabei wird weder analysiert, welchen Einfluss diese Änderungen auf die gesamte Anwendung haben, noch werden sie immer durchgängig dokumentiert. Bei Verdrahtungsfehlern etwa ist nicht selten die Argumentation zu hören, dass diese durch eine entsprechende Anpassung in der Software viel einfacher zu beheben seien. Kommt es allerdings irgendwann zu einem Austausch der Bauteile und werden diese dann korrekt angeschlossen, besteht Gefahr für Mensch und Maschine.

Komplexität beispielsweise in Form von Spaghetti-Codes, Programmsprüngen, absoluten Adressierungen oder mangelhaften Kommentierungen führt zu kaum noch nachvollziehbaren Programmen, ohne dass die Applikation dies eigentlich erfordert. Probleme, die daraus entstehen, sind somit quasi hausgemacht.

Eine herabgesetzte Sicherheitsintegrität kann aus der Verknüpfung von Prozess- und Sicherheitssignalen resultieren, indem nicht-sicherheitsgerichtete Signale sichere Ausgänge kontrollieren. Dies ist nicht nur bei der bereits erwähnten ODER-Verknüpfung zu berücksichtigen, sondern generell bei der Schaltung von Funktionsbausteinen und Sicherheitsausgängen.

Normgerechte Programmierung vereinfachen

Die Arbeitsgruppe PLCopen Safety setzt gerade bei den beiden letztgenannten Fehlerquellen an. Seit einigen Jahren arbeiten nahezu alle Hersteller von sicherheitsgerichteten Steuerungen daran, die normgerechte Programmierung von Sicherheitsfunktionen so einfach wie möglich zu machen, um Fehler von vornherein zu vermeiden. So entstand bereits 2005 die umfangreiche Spezifikation Safety Functionality: Part 1 – Concepts and Function Blocks. Sie wurde unter der Schirmherrschaft des Instituts für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (damals noch BGIA) und der Mitwirkung des TÜV Rheinlands erarbeitet.

Grundelemente sind dabei die Einschränkung des Sprach- und Funktionsumfangs sowie Maßnahmen zur Sicherstellung der Sicherheitsintegrität bei Verknüpfung von sicherheits- und

Sicherheit an Pressen: PLCopen-Safety-Bausteine zur einfachen Implementierung sicherheitsrelevanter Applikations-Software

nicht sicherheitsgerichteten Signalen. Hierzu definierte PLCopen das Datenattribut SAFE, das es dem Engineering-Tool beziehungsweise dem Compiler ermöglichen soll, unzulässige Verknüpfungen und Unverträglichkeiten zwischen Datentypen aufzudecken.

Neben den allgemeinen Festlegungen wurden zwanzig elementare Funktionsbausteine definiert. Die Spezifikation legt den Grundstein für alle weiteren Arbeiten. Part 2 – User Guidelines beschreibt die Anwendung der Bausteine in Form von Applikationsbeispielen während Part 3 – Extensions eine Erweiterung der in Teil 1 definierten Bausteine darstellt.

Einfache Integration in die Ablaufsteuerung

Weiterführendes Ziel ist es jedoch, auch branchenspezifische Funktionsbausteine zur Verfügung zu stellen. Mit Blick auf das hohe Gefährdungspotenzial von Pressenapplikationen erarbeitet die Nutzerorganisation aktuell Bausteine, die die typischen Funktionen von Pressenapplikationen abdecken und als Part 4 – Extensions for Presses veröffentlicht werden. Dazu gehören unter anderem Bausteine zur Überwachung der Schutzeinrichtungen und der Aktoren sowie Funktionsbausteine zur Steuerung der einzelnen Betriebsarten.

Nachdem elektrische Aktoren bereits in Teil 1 Berücksichtigung fanden, stehen hydraulische Aktoren im Mittelpunkt. Es gilt, sowohl das Schaltverhalten der Ventile – ob als Einfach-, Doppel- oder Pressensicherheitsventil – als auch Geschwindigkeit und Richtung von hydraulischen Achsen zu überwachen. Letztere lassen sich mit den Funktionsbausteinen SF_SpeedMonitoring und SF_DirectionMonitoring umsetzen. Ein weiteres Beispiel für einen pressenspezifischen Funktionsbaustein ist SF_CycleControl. Dieser steuert die Presse durch Interaktion mit der nicht trennenden Schutzeinrichtung, wenn zyklische Eingriffe in den Gefahrenbereich erforderlich sind.

Durch die Funktionsbausteine kann der Anwender Sicherheitsfunktionen auf einfache Weise in die Ablaufsteuerung einbinden. In Kombination mit den PLCopen Safety-Festlegungen helfen sie darüber hinaus Anforderungen an die Software, wie sie die ISO 13849-1 in Kapitel 4.6 definiert, umzusetzen. Das heißt, unter anderem die Voraussetzungen im Rahmen der SRASW (sicherheitsrelevante Anwender-Software) zu erfüllen, die Eignung des Engineering-Tools und der Baustein-Bibliothek sicherzustellen sowie die Sicherheitsintegrität zu gewährleisten.

Für die Implementierung der funktionalen Sicherheit gilt es, Anwendern die normgerechte Programmierung von Sicherheitsfunktionen so einfach wie möglich zu machen, um Fehler von vornherein zu vermeiden. Funktionsbausteine spielen dabei eine wichtige Rolle.

Mit dem vierten Teil der Spezifikation erarbeitet derzeit die unabhängige Nutzerorganisation branchenspezifische Funktionsbausteine für Pressenapplikationen, mit Bausteinen zur Überwachung Sensoren, Aktoren und Bausteinen zur Steuerung der Presse. Sie ermöglichen dem Anwender eine einfache, normgerechte Implementation gemäß den sicherheitsrelevanten Software-Anforderungen, eine Standardisierung von Schnittstellen und eine Minimierung des Aufwands für Verifikation und Validierung. □

> MORE@CLICK ADK9017440