12. April 2012

openSAFETY-Initiative zielt auf Vereinheitlichung industrieller Sicherheitsprotokolle ab

von David Humphrey am 12.04.2012 13:24

Zusammenfassung

Einer der wesentlichsten Automatisierungstrends der letzten Jahre ist die Transformation der Maschinensicherheitstechnik von hart verdrahteten Einzelkomponenten hin zu hoch entwickelten Netzwerksystemen. Heute verbinden moderne Sicherheitslösungen intelligente Sicherheitsgeräte über offene Netzwerke. Sicherheitsinformationen werden über sichere Protokolle ausgetauscht. Diese implementieren Maßnahmen zur Sicherstellung eines Ausmaßes an Datenintegrität, das ausreicht, um die Anforderungen internationaler Sicherheitsstandards zu erfüllen.

Parallele Entwicklungen mündeten zum Bedauern der industriellen Anwender in einer Vielzahl inkompatibler Lösungen. Nun ist jedoch eine Initiative im Gang, ein einzelnes Sicherheitsprotokoll - openSAFETY – über die gängigsten ethernetbasierten Netzwerke hinweg zu standardisieren. Das wäre ohne Rückendeckung von großen Endanwender und Unterstützung durch einen Branchenverband ein viel schwierigeres Unterfangen. Dieser ARC View blickt hinter die Kulissen dieser Initiative.

Die Evolution von vernetzter Sicherheit

Im letzten Jahrzehnt ebneten konvergierende Sicherheitsstandards den Weg für die Entwicklung integrierter Sicherheitslösungen, deren Komponenten mit anderen intelligenten Geräten über industrielle Netzwerke kommunizieren. Das führt zu einer Vielzahl von Kundennutzen wie flexibleren Architekturen, eine größere Informationsmenge für die Diagnose von Sicherheitsabschaltungen und Integration sicherer und nicht sicherer Geräte in einer einzigen Netzwerkumgebung.

Mit der steigenden Verbreitung ethernetbasierter industrieller Netzwerke wurden Sicherheitsprotokolle implementiert und von der jeweils verantwortlichen Nutzerorganisation zertifiziert. Zurzeit sind die am meisten verbreiteten Netzwerke mit Sicherheitsprotokoll Profinet (PROFIsafe), EtherNet/IP (CIP Safety), POWERLINK (openSAFETY) und EtherCAT (Safety over EtherCAT). Zu den Nutzen der Verwendung von Netzwerkintegrierter Sicherheit gehören:

- Die Beseitigung unflexibler hart verdrahteter Systeme,
- Mittels flexibler Topologie – Geräte können einfach hinzugefügt oder entfernt werden – schnelles Umkonfigurieren bestehender Netzwerke,
- Fernkonfiguration und Entstörung vernetzter Sicherheitsgeräte,

•Zugriff auf Geräte-Statusdaten für schnelle Diagnose (nützlich für die Analyse von Notfallabschaltungen)

Die openSAFETY-Initiative

Das Protokoll von openSAFETY war ursprünglich von der Ethernet POWERLINK Standardization Group (EPSG) für Ethernet POWERLINK entwickelt worden. Nachdem einige Schlüsselkunden Interesse an der Verbindung zu anderen Sicherheitssteuerungen bekundet hatten, lancierte EPSG die gegenwärtige Initiative zur Ertüchtigung von openSAFETY für andere Industrial-Ethernet-Varianten wie Profinet, EtherNet/IP, Modbus TCP und Sercos III. Die EPSG spezifizierte die Proof-of-concept-Tests, ihre Mitgliedsunternehmen B&R und Schneider Electric führten die Labortests durch.

Zur Implementierung von openSAFETY auf anderen Netzwerken nutzt die EPSG die Tatsache aus, dass die meisten Netzwerke ein schichtenbasiertes Netzwerkmodell unterstützen. Die openSAFETY-Applikationsschicht kapselt Sicherheitsmeldungen über ein Netzwerk in einer netzwerkagnostischen Weise ein. Das ermöglicht die völlige Unabhängigkeit von der darunter liegenden Transportschicht, das ermöglicht einer gemeinsamen Anwendung die Nutzung einer Vielfalt an Netzwerken.

Endbenutzer sehen Nutzen eines einzigen Sicherheitsprotokolls

Obwohl Sicherheitsprotokolle die nahtlose Kommunikation kritischer Sicherheitsinformationen von Gerät zu Gerät ermöglichen, sind viele Endkunden in der realen Welt weiterhin mit einem Dilemma konfrontiert. Allen Anstrengungen zur Standardisierung industrieller Autmatisierungsarchitekturen über verschiedene Werke hinweg sind in vielen Produktionsstätten immer noch mehrere Marken inkompatibler Systeme im Einsatz, oft innerhalb derselben Fabrik oder sogar in derselben Produktionsstraße. Während Informationen aus unterschiedlichen Systemen über offene Standards wie OPC ausgetauscht werden können, verhindern abweichende Sicherheitsprotokolle einen schnellen und sicheren Austausch sicherheitsrelevanter Informationen zwischen unterschiedlichen Geräten.

Nestlé S.A., ein führender Lebensmittelerzeuger, sieht wesentliche Vorteile in der Verwendung eines einheitlichen Sicherheitsprotokolls und untersucht aktiv die openSAFETY-Initiative. Die Vorteile für Nestlé umfassen die Verbesserung der Gesamtsicherheit von Produktionsstraßen und die Gesamt-Produktionsmitteleffektivität (overall equipment effectiveness; OEE) wegen der verbesserten Verwaltung von Sicherheitsereignissen auf der Linienebene. Laut diesem Unternehmen muss das Sicherheitsprotokoll nicht bis zur Geräteebene hinab implementiert werden. Für die Steuergeräte von Maschinen und Anlagen ist es ausreichend, unabhängig von Typ oder Marke der verwendeten Steuerung ein einziges Protokoll über ein Standard Ethernet TCP/IP Netzwerk zu verstehen und darauf zu reagieren.

Laut Nestlé vermindert das Nicht-Vorhandensein eines gemeinsamen Sicherheitsprotokolls zwischen Maschinen den Mehrwert einer integrierten Produktionsstraße. Alle darin zusammengefassten Maschinen müssen in der Lage sein, auf ein Sicherheitsereignis zu reagieren, egal wo es eintritt. So können zum Beispiel andere Maschinen in Abhängigkeit von der Schwere der Sicherheitsverletzung abgeschaltet oder im Interesse eines beschleunigten Wiederanlaufs in einen Ruhezustand gebracht werden (Heizbacken bleiben eingeschaltet, Achsen bleiben synchronisiert, etc.). Der Schlüssel ist dabei, die Balance zwischen Energieverbrauch und Wiederanlaufeffizienz zu treffen und zugleich sichere Bedingungen für Maschinen und Personal aufrecht zu erhalten. Durch Verwendung eines einzigen Sicherheitsprotokolls erwartet sich Nestlé eine Verbesserung von Arbeitnehmer- und Maschinensicherheit sowie der OEE.

Neben Nestlé prüft eine Vielzahl anderer Anwender die openSAFETY-Initiative. Zu ihnen gehören Pactiv, ein amerikanischer Hersteller von Lebensmittelverpackung und Rügenwalder Mühle, ein deutscher Fleischverarbeiter. Andere Lebensmittel- und Getränkeerzeuger wie Kraft Foods, Pepsico, Arla Foods und M&M Mars nehmen ebenfalls die potentiellen Vorteile der Technologie unter die Lupe.

OMAC und PackSafety

Das Konsortium Organization for Machine Automation and Control (OMAC) erstellt hardwareunabhängige Richtlinien für offene Steuerungen in Verpackungsmaschinen und Werkzeuge. OMACs verschiedene Arbeitsgruppen definieren Anforderungen und geben Richtlinien zu Themen heraus, die von Bezeichnungskonventionen bis Maschinenkonnektivität reichen.

Letztes Jahr gründete die OMAC das PackSafety-Komittee und gab ihm die Aufgabe, Sicherheitsanforderungen zu identifizieren, die sich als OMAC-Richtlinien für Maschinenhersteller eignen. Fabrice Bertin von Nestlé ist Vorsitzender der Arbeitsgruppe, der Vertreter anderer großer Endanwender wie Pepsico ebenso angehören wie einige Maschinenhersteller.

Zu Beginn des Jahres 2012 definierte das PackSafety-Komittee zwei Hauptziele: 1) Maximierung der Effizienz im sicheren Betrieb durch Verwendung der neuesten Sicherheitstechnologie und 2) Reduktion des Integrationsaufwandes für Produktionsstraßen durch Erstellung von Sicherheits-Schnittstellendefinitionen. Das Komitee setzte zudem Meilensteine wie die Veröffentlichung eines ersten Spezifikationsentwurfs bis Ende 2012. Höchste Priorität hat wahrscheinlich die Evaluierung eines einzigen Sicherheitsprotokolls.

Politik der Sicherheit

Die Feldbuskriege der Vergangenheit haben eines gezeigt: Während Branchenkonsortien echten Nutzen durch offene Technologien bringen, werden diese weiterhin von kommerziellen Interessen getrieben. openSAFETY ist da keine Ausnahme. Es wird nicht einfach sein, Automatisierungshersteller davon zu überzeugen, mit ihren Schlüsselprodukten ein zusätzliches Sicherheitsprotokoll zu unterstützen. Andererseits neigen dieselben Hersteller dazu, gut zuzuhören, wenn es um den Bedarf großer, globaler Kunden geht, abgestützt auf Industriestandards oder Richtlinien.

Die EPSG ihrerseits sagt, sie ist bereit, Automationsherstellern zu helfen, wenn diese bereit sind, diesen Weg zu gehen. Diese Unterstützung zielt darauf ab, Kosten und Aufwand für die Implementierung von openSAFETY zu reduzieren, indem keine Lizenzgebühren anfallen (open source), rechtliche Hindernisse auszuräumen (kein Vetragsabschluss erforderlich) und technische Elemente bereitzustellen (verfügbarer TÜV-zertifizierter Stack für openSAFETY Master und Slave). Die Last, das möglich zu machen, liegt bei großen Endanwendern, die ihre traditionellen Automatisierungslieferanten davon überzeugen müssen, diesen neuen Standard zu unterstützen.

Schlusswort

In mancherlei Hinsicht stellt die openSAFETY-Initiative eine Herausforderung an die Automatisierungsbranche dar. Während diese über offene Technologien spricht, sind unsere nicht annähernd so offen und allgegenwärtig wie diejenigen in der IT-Welt. Bei so vielen Ausprägungen industrieller Netzwerktechnik könnte die Entscheidung für ein einziges, allgegenwärtiges Sicherheitsprotokoll tatsächlich einen Schritt in die Richtung echter Offenheit darstellen.