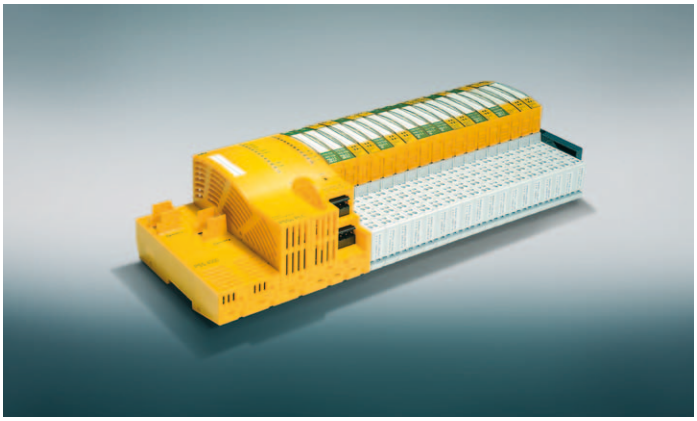
Doppelt sicher: Safety + Security!

Abgesicherte Kommunikation in Industrie 4.0 braucht standardisierte Features aus beiden Sicherheits-Welten



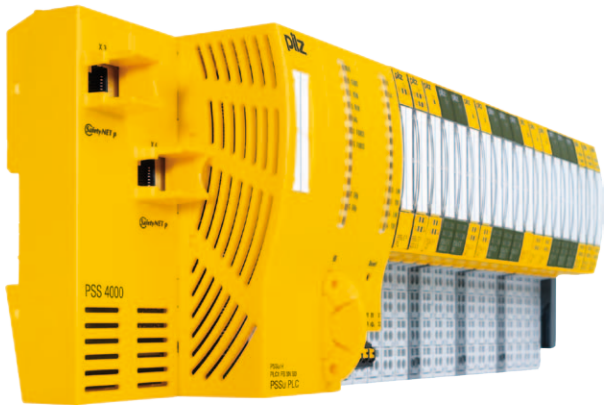


Bild 1a/b: Die Steuerungen PSSuniversal PLC sind die „Allrounder" im Automatisierungssystem PSS 4000. In Kombination mit anderen Komponenten bieten sie neue Lösungsansätze, z. B. die sichere Erfassung von Positionen

Mit zunehmenden Vernetzung von Maschinen treffen in Bezug auf das Thema Sicherheit zwei Welten aufeinander: Die Welt der Automatisierung verschmilzt mit der IT-Welt aus dem Anwendungsfeld der Büroumgebungen. Die jeweiligen Sichtweisen auf das Thema Sicherheit unterscheiden sich jedoch deutlich: die international verwendeten Begriffe „Safety" für Maschinensicherheit und „Security" für IT-und Datensicherheit helfen zunächst in der grundlegenden Differenzierung. Die Herausforderung liegt aber darin, die Anforderungen beider Welten zu passenden und praktikablen Lösungen zu standardisieren, um letztendlich eine abgesicherte Kommunikation zu gewährleisten.

Sicherheitsziele

In verknüpften Safety und Security-Lösungen muss der Nutzen für jeden Anwenderkreis und der Mehrwert von Sicherheit im Vordergrund stehen. Maschinenbauer, Systemintegratoren, aber auch Betreiber, müssen mit ihren Sicherheitsbedürfnissen und ihren individuellen Handlungsmöglichkeiten wahrgenommen werden. Die neuen Sicherheitsziele umfassen beispielsweise den Schutz von Produktionsdaten, Produkt- und Plagiatsschutz, Schutz von Know-how, Zugangsschutz, Integritätsschutz oder die Fernwartung.

Dabei ist die Ausgangslage auf dem Weg zur Industrie 4.0 hinsichtlich Sicherheit je nach Bereich völlig unterschiedlich. Neben den technischen Herausforderungen – wie beispielsweise die Schaffung einheitlicher Standards – werden deshalb erfolgreiche Sicherheitslösungen auch vor betriebswirtschaftliche, psychologische und die Ausbildung betreffende Herausforderungen gestellt.

So existieren etwa heute noch keine geeigneten, durchgängig standardisierten Betriebsplattformen in der Industrie, um ausreichende Sicherheitslösungen zu implementieren. Ein Ausbau oder eine Aktualisierung bestehender Infrastrukturen ist oft nur begrenzt möglich, zumal viele Lösungen ursprünglich für andere Branchen entwickelt wurden.

Zudem sind Sicherheitsfragen auch immer Fragen des Sicherheitsbewusstseins: Es existieren auch (noch) zu viele unterschiedliche Sensibilisierungsgrade hinsichtlich der Sicherheit in den einzelnen Branchen. Insbesondere angesichts der in Industrie 4.0 zunehmenden Vernetzung und damit auch Kooperation mehrerer Partner in Wertschöpfungsnetzen ist ein Abgleich von Erfahrungen und der entscheidenden Akzeptanzfaktoren zwingend erforderlich.

Industrie 4.0 hat bereits begonnen

Letztendlich geht es um die Steigerung der Wettbewerbsfähigkeit der Industrie. Dafür benötigt diese nicht erst morgen Maschinen und Anlagen, mit denen sie flexibel, ressourcenschonend und effizient möglichst individuelle Produkte produzieren kann.

Um flexibel und schnell auf veränderte Anforderungen in der Produktion eingehen zu können, wird ein modularer Aufbau von Maschinen und Anlagen immer wichtiger. Damit lassen sich zudem Engineering-Prozesse vereinfachen sowie die Wiederverwendbarkeit der einzelnen Einheiten steigern. Allerdings werden dafür Automatisierungssysteme benötigt, die in der Lage sind, die in den mechatronischen Einheiten verteilte Intelligenz zentral und anwenderfreundlich zu steuern. Anlagen lassen sich dann in übersichtliche, selbstständig arbeitende Einheiten zerlegen.

Dagegen können mit zentralistisch ausgelegten SPS-Steuerungen, wie sie heute im Einsatz sind, die Vorteile einer Modularisierung nicht komplett ausgeschöpft werden: Änderungen in einzelnen Anlagenteilen verursachen einen überproportional hohen Aufwand auf der Steuerungsebene, da dann alle Programmstrukturen und die Kommunikationsbeziehungen der Module untereinander an zentralen Stellen der Steuerung verändert werden müssen.

Für die Automatisierung der Zukunft sind daher Lösungen gefragt, die zum einen in der Lage sind, Steuerungsintelligenz zu verteilen und zum anderen gleichzeitig gewährleisten, dass die notwendige Vernetzung mehrerer Steuerungen für den Anwender einfach zu handhaben bleibt. Mit dem Automatisierungssystem PSS 4000 verfolgt Pilz konsequent diesen mechatronischen Ansatz: PSS 4000 und das Echtzeit-Ethernet SafetyNET p gehen konsequent den modularen und verteilbaren Ansatz, der es erlaubt, bereits heute die Vorteile einer dezentralen Steuerungsstruktur zu nutzen.

Maschinensicherheit gewährleisten bei dezentraler Kommunikation?

Industrie 4.0 bedeutet extrem vernetzte Systemstrukturen mit einer Vielzahl beteiligter Menschen, IT-Systeme, Automatisierungskomponenten, Maschinen. Die Folge: neue Herausforderungen bei Modularisierung, Vernetzung und Verte-

Autor:

Armin Glaser, Leiter Produktmanagement, Pilz GmbH & Co KG

lung von Steuerungsfunktionen in immer kleinere Teilfunktionen.

Durchgängige Komplettlösungen im Verbund mit moderner, programmierbarer Sicherheitstechnik, die im Vergleich zur klassischen relaisbasierten Sicherheitstechnik wesentlich flexibler ist, ist eine Antwort. Man spricht hier von dynamischer Sicherheit. Diese erlaubt es beispielsweise, dass Roboter nicht gleich hart gestoppt werden müssen, wenn sich ein Mensch nähert, sondern mit reduzierter (und damit weniger gefährlicher) Geschwindigkeit weiter arbeiten können.

Intelligente Sensoren und Aktoren in verteilten Systemen werden dabei immer mehr die Funktionen von Steuerungen übernehmen und zu einer besseren Interaktion von Maschinenmodulen untereinander und von Mensch und Maschine führen. Sichere Motion-Controller, die synchron und sicher über Echtzeit-Ethernet gekoppelt sind, tragen bereits lokale Steuerungs- und Auswertefunktionen. Auch mit intelligenten Kamerasystemen zur dreidimensionalen sicheren Raumüberwachung und kamerabasierten Schutz- und Messsystemen markiert beispielsweise Pilz den Weg in diese Richtung.

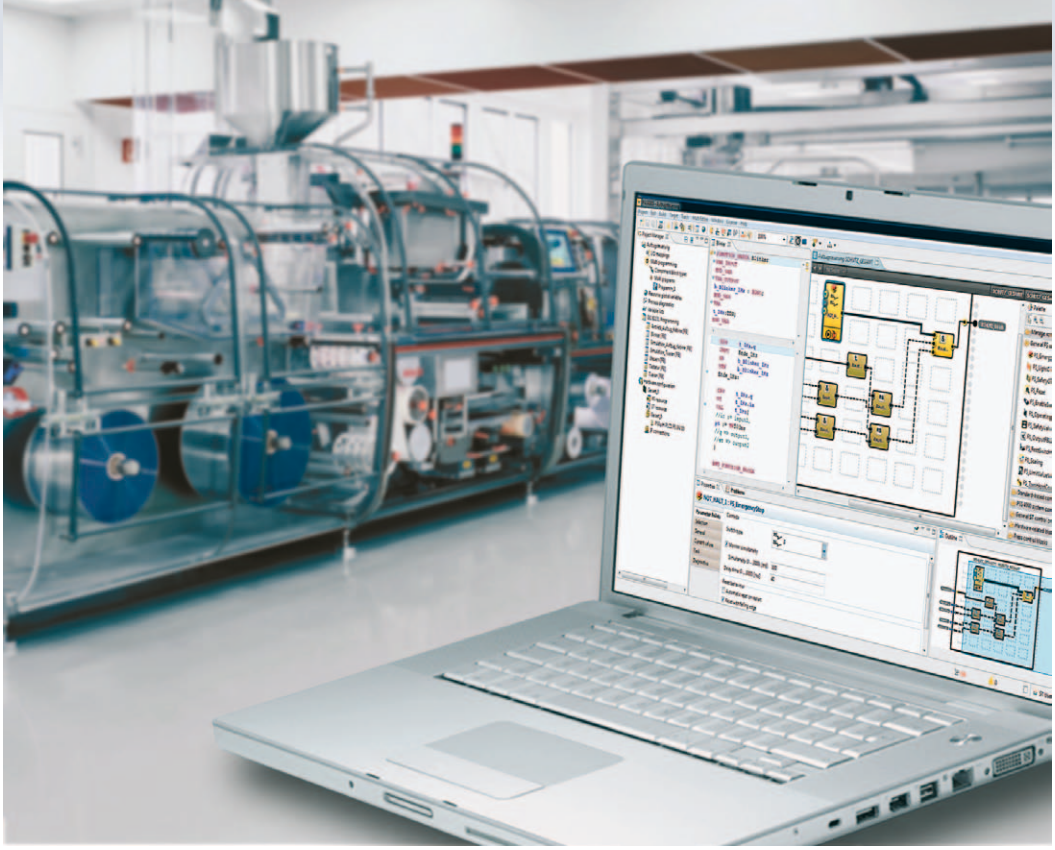


Bild 2: Die Softwareplattform PAS 4000 im Automatisierungssystem PSS 4000 ermöglicht ein einfaches Handling mit Blick auf Projektierung und Programmierung. Datenschnittstellen sind so angelegt, dass der Austausch von Informationen in allen Phasen gewährleistet ist

Safety mit Security = abgesicherte Kommunikation

Gleichzeitig steigt mit erhöhter Kommunikation auch der Bedarf an abgesicherter Kommunikation: Safety (Maschinensicherheit) und Security (Betriebssicherheit) inklusive. Eine Grundlage ist die Schaffung standardisierter Mechanismen in der Kommunikation. Wenn die Anforderungen beider Welten berücksichtigt sind, entstehen praktikable, akzeptierte Lösungen, die auch vom Markt nachhaltig akzeptiert werden.

Der Bereich Safety – Maschinensicherheit - zeichnet sich bereits durch große Investitionssicherheit und Rechtssicherheit aus. Das liegt auch an der Ordnung durch Normen und Standards. So sind Dinge wie ein Safety Integrity Level klar definiert und eine Einteilung in Gefährdungsklassen und Risikoabschätzungen möglich. Für das Zusammenspiel von Safety und Security – also Betriebssicherheit – werden in Zukunft spezielle Indikatoren benötigt, etwa für die Standardisierung.

Von besonderer Bedeutung wird es zudem sein, bei der Entwicklung von Lösungen von Anfang an die Bedürfnisse des Anwenders zu berücksichtigen, zum Beispiel mit Blick auf die Benutzerfreundlichkeit.

Denn, wenn Internet-Technologien in Produktionsprozessen eingesetzt werden, damit zukünftig flexibler und effizienter produziert werden kann, dann findet nicht nur zwischen den teilweise autonom agierenden technischen Systemkomponenten ein reger und in der Regel auch zeitkritischer Daten- und Informationsaustausch statt, es sind ebenso wesentlich mehr Akteure entlang der Wertschöpfungskette beteiligt.

■ *Pilz GmbH & Co. KG*
www.pilz.de

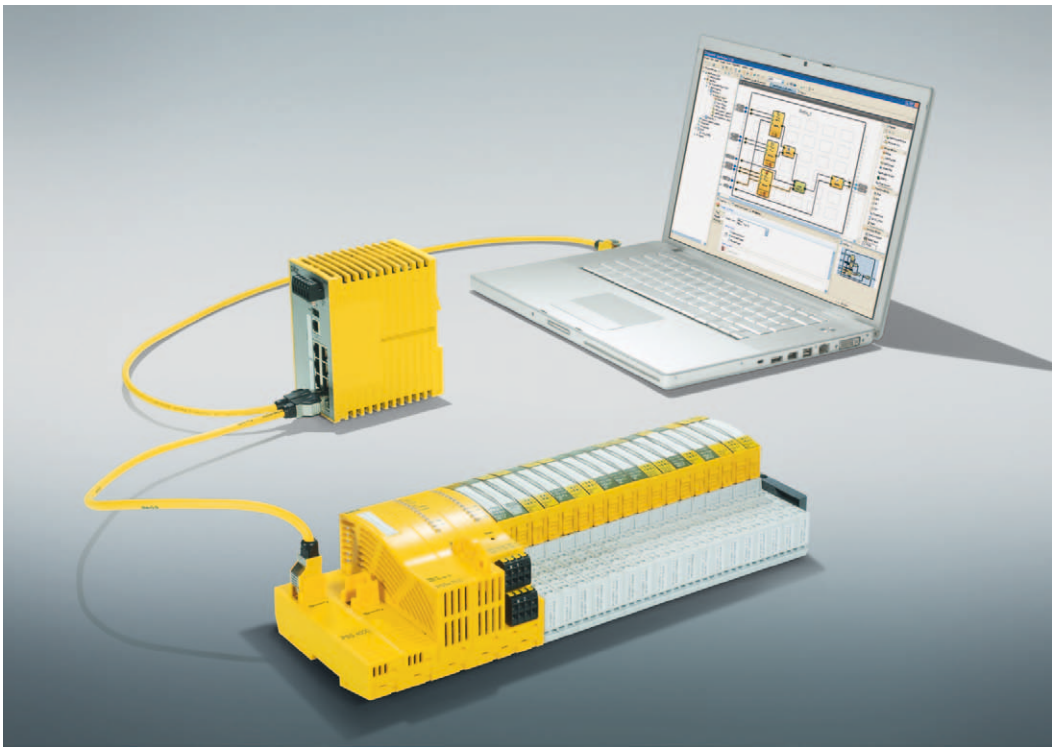


Bild 3: Das Automatisierungssystem PSS 4000 für Standard und Sicherheit besteht aus verschiedenen Hardware- und Software-Komponenten sowie dem Echtzeit-Ethernet SafetyNET p. PSS 4000 erlaubt eine konsequente Verteilung von Steuerungsfunktionen, Prozess- und Steuerungsdaten