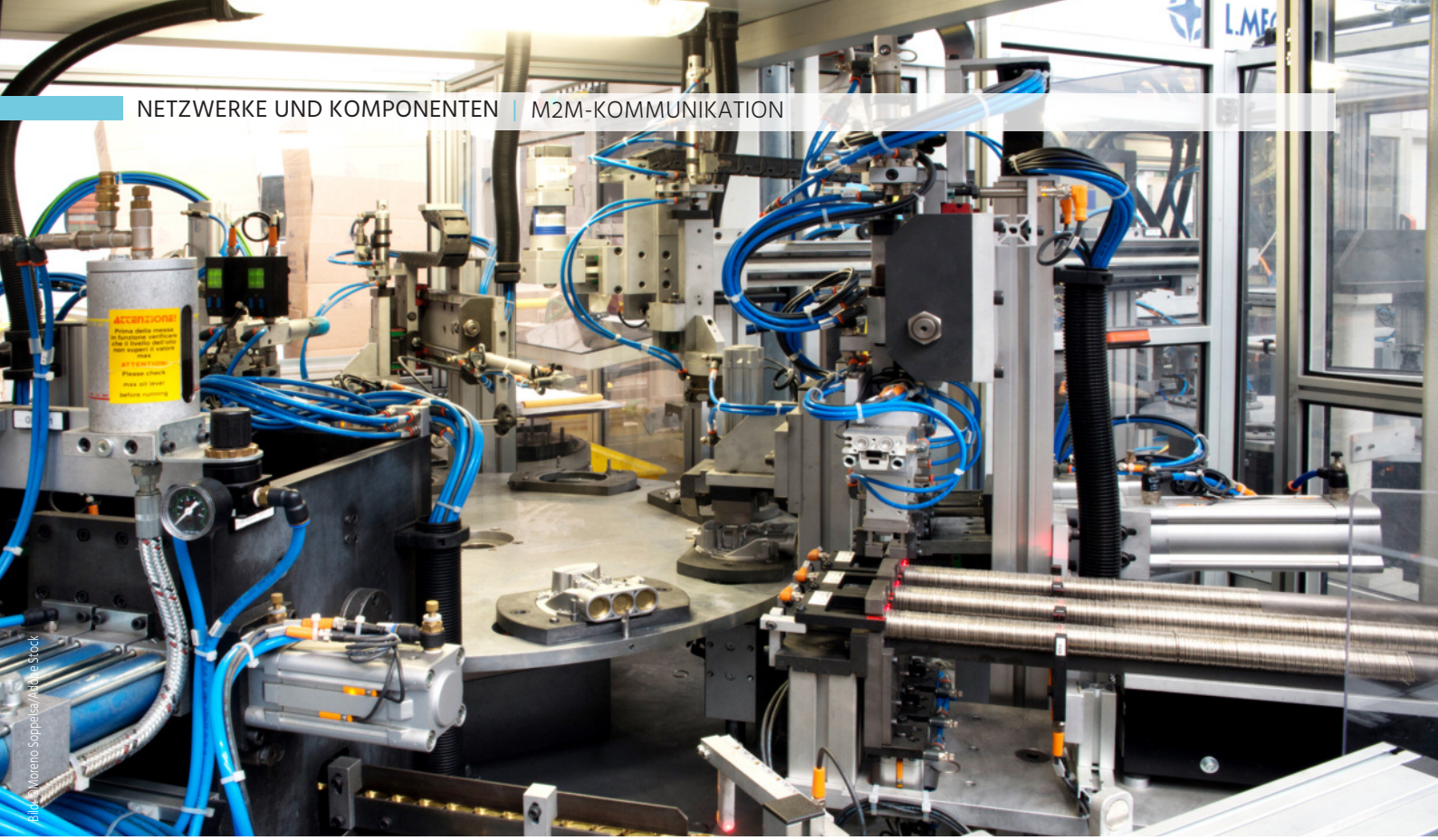

Bild: Moreno Soppelsa/Adobe Stock

HANNOVER MESSE
Halle 6
Stand D02/7

Machine-2-Machine-Kommunikation

Maschinendaten in der Kapsel

Ohne Machine-to-Machine- beziehungsweise Sensor-Aktor-Kommunikation kommen Produzenten auf ihrem Weg zur Industrie 4.0 an Grenzen. Ohne IT-Sicherheit im Netzwerk aber auch. Zwar lässt sich der Transfer von Produktionsdaten auch vertikal absichern, aber eine sinnvolle Abgrenzung von Anlagen, Zellen und Linien spart unnötigen Aufwand und verringert Risiken.

Die Vernetzung der Komponenten im Fertigungsnetz sowie die Öffnung des Produktionsnetzes in Richtung Office-IT führen dazu, dass vermehrt auch Datenverkehr in die Produktion fließen kann, der dafür nicht vorgesehen ist. Andersherum kommt es vor, dass direkt von einem Steuerungs-PC im Produktionsnetz ein Zugriff auf das Internet möglich ist. Dadurch kann es zu unerwünschten Kommunikationsbeziehungen kommen, für die nur unzureichende Sicherungsmaßnahmen bestehen.

Status Quo Anlagenschutz

Um Anlagenerweiterungen zu schützen, werden häufig neuere Protokolle entwickelt. Diese können sich aber als ungeeignet erweisen, da sie auf die vorhandene Technik nicht anwendbar sind. Eine Möglichkeit, Altsysteme vor Missbrauch zu schützen ist wiederum, sie weitestgehend vom restlichen Netzwerkverkehr zu isolieren. Daraus ergeben sich jedoch Anforderungen hinsichtlich der Gewährleistung der Authentizität als auch von Integrität der Steuerungsdaten. Eine besondere Herausforderung im üblichen Mischbetrieb von Bestandsanlagen und neuer Technik stellen die neuen Anlagen dar: Auch wenn diese den aktuellen Stand der Technik aufweisen sollten, liefern Anlagenbauer oft teils veraltete oder nicht mehr vom Hersteller unterstütze Systeme mit aus und untersagen dem Betreiber zudem, diese Bestandteile der Anlage während der Garantiezeit zu verändern. Dadurch kann es passieren, dass der Altbestand besser abgesichert ist als neue Anlagen. Dies resultiert unter anderem daraus, dass versucht wird, bestehende Systeme im stabilen Betrieb abzusichern, während neuen Anlagen im fragilen Anlauf-Prozess keinerlei Änderungen zuzumuten sind.

Abschottung ist keine Lösung

Eine Schutzmöglichkeit wäre die Rückkehr zu einem geschlossenen Produktionssystem und sowohl alte als auch neue Systeme mit zusätzlichen Gateways oder Firewalls so voneinander abzuschotten, dass keine problematischen Netzwerkzugriffe möglich sind. Dies widerspricht jedoch dem Industrie-4.0-Ansatz, der einen weitreichenden Datenaustausch beschreibt – sogar über die Grenzen der Organisation hinweg. Dabei hat sich eine vollständige Kontext- und Datenflussana-

IT&Production

Auszug aus IT&Production, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 4/2018.

lyse für die Kommunikation innerhalb der Produktion und über deren Grenzen hinweg sowie die Erarbeitung entsprechender Maßnahmen zur sicheren Bereitstellung der Daten etabliert.

Offen oder proprietär

Beim internen Einsatz von kabellosen Technologien muss zwischen proprietären, also eigenen, und offenen Standards unterschieden werden, wobei sich dabei die Frage nach den übergeordneten Protokollen und angeschlossenen Endgeräten ergibt. Wird auf WLAN gesetzt, sollte auch eine entsprechende Absicherung (IT-Sicherheit) erfolgen. Sind andere Standards der Maschinenkommunikation oder proprietäre Technologien geplant, können diese häufig nur durch ebenso proprietäre Mechanismen abgesichert werden. Bei der Bereitstellung von Daten für Kooperationspartner wurde bisher oft auf Standards wie EDI /EDIFACT gesetzt, was aber häufig zu hohem Aufwand bei der Änderung oder Anpassung der Schnittstellen auf allen Seiten geführt hat. Bei offeneren und flexibleren Anbindungen mit mehr Sicherheitsoptionen können sogenannte APIs (Application Programming Interfaces) helfen. Diese lassen sich oft schneller anpassen und Betreiber sind in der Lage, mehrere Versionen parallel laufen zu lassen, um die Kommunikationspartner bei der Migration nicht unter Druck setzen zu müssen. Der Vorteil der Nutzung von APIs nach außen (published API) liegt also darin, die eher langsamen Entwicklungszyklen in der eigenen Infrastruktur und Produktions-IT von den sich schneller ändernden Anforderungen der Lieferanten oder Kunden abzukoppeln. Intern kann somit weiterhin mit langsameren Verfahren zur SAP-Anbindung gearbeitet werden, während man nach außen auch moderne Apps für Smartphones anbieten kann.

Authentizität durch Zertifikate

Neben der Vertraulichkeit von Informationen spielt auch die Authentizität von Sender und Empfänger eine Rolle. Je nach Leistungsfähigkeit der Kommunikationspartner (in diesem Fall ein Ausschlusskriterium für einfache Sensornetze) können Zertifikate bei der Sicherung der Authentizität helfen. Diese haben sich im privaten Bereich bereits etabliert – etwa beim Onlinebanking. Diese Art der Absicherung kann auch auf Maschinen übertragen werden. Eine entsprechende Speicherausstattung und grundlegende Verschlüsselungsfunktion der Hardware vorausgesetzt, sind Zertifikate derzeit ein sehr sicheres Verfahren zur Absicherung der Maschinenkommunikation. Eine klare Abgrenzung muss jedoch bei Betrachtung der Kommunikation auf Busebene erfolgen: Die dort angewendete Signalisierung kann nicht durch gängige Mittel der IT-Sicherheit geschützt werden, da die Übermittlung der Informationen proprietär erfolgt. Ein Nachteil von Zertifikaten ist jedoch die begrenzte Lebensdauer von etwa ein bis drei Jahren. Zudem basiert die Sicherheit des Gesamtsystems darauf, dass alle beteiligten Partner einer Dritten Partei vertrauen (in dem Fall der die Zertifikate ausgebenden Public-Key-Infrastruktur). Zudem kann im schlimmsten Fall die Kommunikation zusammenbrechen, wenn die jeweiligen Knoten den Ursprung der Zertifikate oder deren Gültigkeit nicht prüfen können. Dies kann insbesondere dann passieren, wenn die Zertifikate der jeweiligen Knoten in der Kette ablaufen oder die Lebensdauer des Vertrauensankers erreicht wird. Kommerzielle Anbieter von Zertifikaten sind daher bereits dazu übergegangen, für solche Einsatzszenarien nur Zertifikate mit erweiterter Lebensdauer von bis zu 30 Jahren einzusetzen.

Absicherung unumgänglich

Eine wirksame Absicherung der M2M-Kommunikation ist unumgänglich. Dazu gilt es, lokale Daten und lokale Kommunikation von dem zu trennen, was den Einflussbereich der Organisation verlassen darf. Als erste Schutzmaßnahme steht also die Abgrenzung der jeweiligen Anlagen, Zellen, Linien und Maschinen untereinander auf dem Plan, damit nur noch der gewünschte Datenverkehr aus der Anlage herauskommen und nur noch validierte Steuerungsinformationen in die Anlage hineingelangen. Zunächst kann dies nur auf Basis einfacher Firewalls und Netzwerkfilter erfolgen, da die zur tieferen Analyse des Verkehrs notwendigen Kenntnisse der Protokolle erst in die Sicherheitstechnik einfließen müssen. Dabei besteht Nachholbedarf, da sich die Stabilität der angeschlossenen Maschinen hinsichtlich Angriffen aus dem Netz bislang als eher unterdurchschnittlich erweist. ■

Die Autoren sind Sebastian Rohr, technischer Geschäftsführer der Accessec GmbH, und Markus Soppa, Research Consultant der Accessec GmbH.

www.accessec.com