SPS MAGAZIN
SONDERAUSGABE 3/2019
www.sps-magazin.de

INDUSTRIAL COMMUNICATION JOURNAL

ICJ

ETHERNET WIRELESS SECURITY

Systeme vor unbekannten Angriffen schützen

Industrielle IT-Sicherheit gewährleisten

Seite 6

SIEMENS

Titelbild: Siemens AG

VIEL MEHR ALS NUR GESCHWINDIGKEIT
Kombination von OPC UA und TSN
Seite 20

PRIVATES LTE-NETZ ODER BESSER 5G?
Wireless-Kommunikation in der Fabrik
ab Seite 36

ALTE SPS-SYSTEME VS. DIGITALISIERUNG
Tipps zur Absicherung der Produktion
Seite 45

sps

smart production solutions

30. Internationale Fachmesse
der industriellen Automation

Nürnberg, 26. – 28.11.2019
sps-messe.de

Bringing Automation to Life

Praxisnah. Zukunftsweisend. Persönlich.

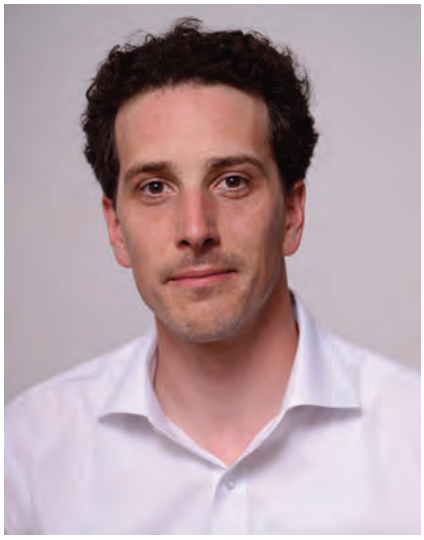
Finden Sie praxisnahe Lösungen für Ihren spezifischen Arbeitsbereich sowie Lösungsansätze für die Herausforderungen von morgen.

Registrieren Sie sich jetzt! sps-messe.de/eintrittskarten

30 %
Rabattcode:
SPS19BESV11

mesago
Messe Frankfurt Group

Das Thema IT- und Datensicherheit ist in der Industrie angekommen. Und das ist gut so. Denn einerseits werden industrielle Anlagen immer interessanter für Cyberkriminelle. Andererseits werden bei Steuerungen zunehmend Schwachstellen publik, die sich als Einfallstor hätten nutzen lassen.



Mathis Bayerdörfer,
Chefredakteur SPS-MAGAZIN

Nicht schwächeln!

Spannende Sicherheitskonzepte und Maßnahmen, mit denen sich die Fertigung schützen lässt, finden sich auch wieder in dieser Ausgabe des INDUSTRIAL COMMUNICATION JOURNALs. So gibt z.B. Siemens im Rahmen der Titelstory einen detaillierten Einblick in die Absicherung von Industrienetzen mit dem Defense-in-Depth-Ansatz (Seite 6ff).

Der Konzern hat sein Security-Angebot in den vergangenen Jahren stetig ausgebaut. Damit trägt er auch dem eigenen Verständnis als Industrial-IoT-Anbieter Rechnung, der die Anbindung der Produktion an die Cloud propagiert. Deren Mehrwerte würden Maschinenbauer und Produktionsunternehmen schon gerne nutzen – sind bei der Umsetzung aber oft verhalten und zögerlich. Schließlich hängt das Damoklesschwert der Cyberattacken und Industriespionage über den Köpfen der potenziellen Cloudnutzer. Doch welcher Anteil dieser Gefahr ist real und welcher nur gefühlt?

Fest steht, dass die Angriffsmöglichkeiten steigen, wenn SPSen online angebunden sind. So hat McAfee – übrigens ein Kooperationspartner von Siemens – kürzlich eine Zero-Day-Schwachstelle bei der Ausführung von Remote-Code in den Industriesteuerungen von Delta Controls aufgedeckt. Mit ihr hätten Hacker die Kontrolle über das Betriebssystem der gesamten Anlage gewinnen können. Auch der IT-Sicherheitsanbieter Tenable hat jüngst eine industrierelevante Sicherheitslücke gefunden: in der Automatisierungsumgebung TIA-Portal von Siemens, mit der unter anderem die S7-SPSen programmiert werden. Es ist also die gleiche Gerätefamilie betroffen wie damals bei Stuxnet – quasi der Mutter aller Industrie-Malware. Auch in diesem Fall wäre es Angreifern möglich gewesen, administrative Tätigkeiten auszuführen, Schadcode auf benachbarte Steuerungen zu verteilen oder unbemerkt Daten abzugreifen.

„Die Bedrohung für diese Systeme darf nicht unterschätzt werden", unterstreicht Tenable-CTO Renaud Deraison und liegt damit vollkommen richtig. Mehr noch: Schlicht und einfach sträflich handelt, wer dem Thema heutzutage zu wenig Aufmerksamkeit schenkt und sich nicht ausreichend mit entsprechenden Sicherheitskonzepten und Lösungen beschäftigt.

In diesem Sinne wünsche ich eine interessante Lektüre.

Mathis Bayerdörfer
mbayerdoerfer@tedo-verlag.de

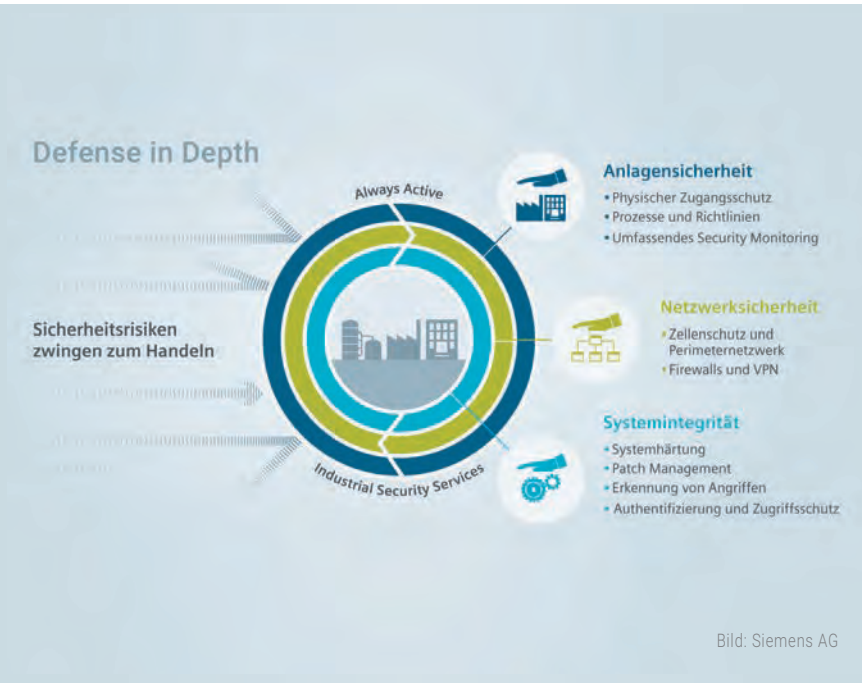


Bild: Siemens AG

TITELSTORY

6 Mit Netzwerk-Management zu mehr Sicherheit

Jedem Security-Update folgen neue Softwareschwachstellen, jeder Schutzmechanismus deckt neue Angriffsvektoren auf – auch in der Industrie. Bereits seit dem erstmaligen Auftreten einer Schadsoftware besteht ein Wettrennen und oft stellt sich die Frage, wie sich ein effektiver Schutz überhaupt etablieren lässt. Die Antwort darauf findet sich im nahtlosen Zusammenspiel mehrerer Maßnahmen.

Titelanzeige: Siemens AG

MARKT – TRENDS – TECHNIK

PROTOKOLLE UND STANDARDS

Bild: Sigmatek GmbH & Co. KG

Das Industrial-Ethernet-Protokoll Varan sorgt für zuverlässige Qualität beim Arbeitsergebnis von Hochleistungs-Stickmaschinen.

KOMPONENTEN UND LÖSUNGEN

WIRELESS UND REMOTE

SICHERHEIT

SERVICE

Einstieg in die Highend-Messtechnik: Präzise, schnell, robust

Basic-Serie ELM3x0x
24 Bit
50 kSps pro Kanal
simultan
25 bzw. 100 ppm @ 23 °C

Economy-Serie ELM3x4x
24 Bit
1 kSps pro Kanal
multiplexed
100 ppm @ 0...50 °C

www.beckhoff.de/messtechnik

Mit den EtherCAT-Messtechnik-Modulen der ELM-Basis- und Economy-Serie erweitert Beckhoff das Spektrum der systemintegrierten und hochskalierbaren Highend-Messtechnik. Die Economy-Serie ELM314x ergänzt dabei die Basisserie um die Sampleklasse 1 kSps bei niedrigen Kanalkosten.

Basic-Serie
- Eingangsbeschaltungen: Spannung 20 mV … 60 V, Strom 20 mA, IEPE, DMS, RTD/TC

Economy-Serie
- Eingangsbeschaltungen: Spannung 1,25 … 10 V, Strom 20 mA

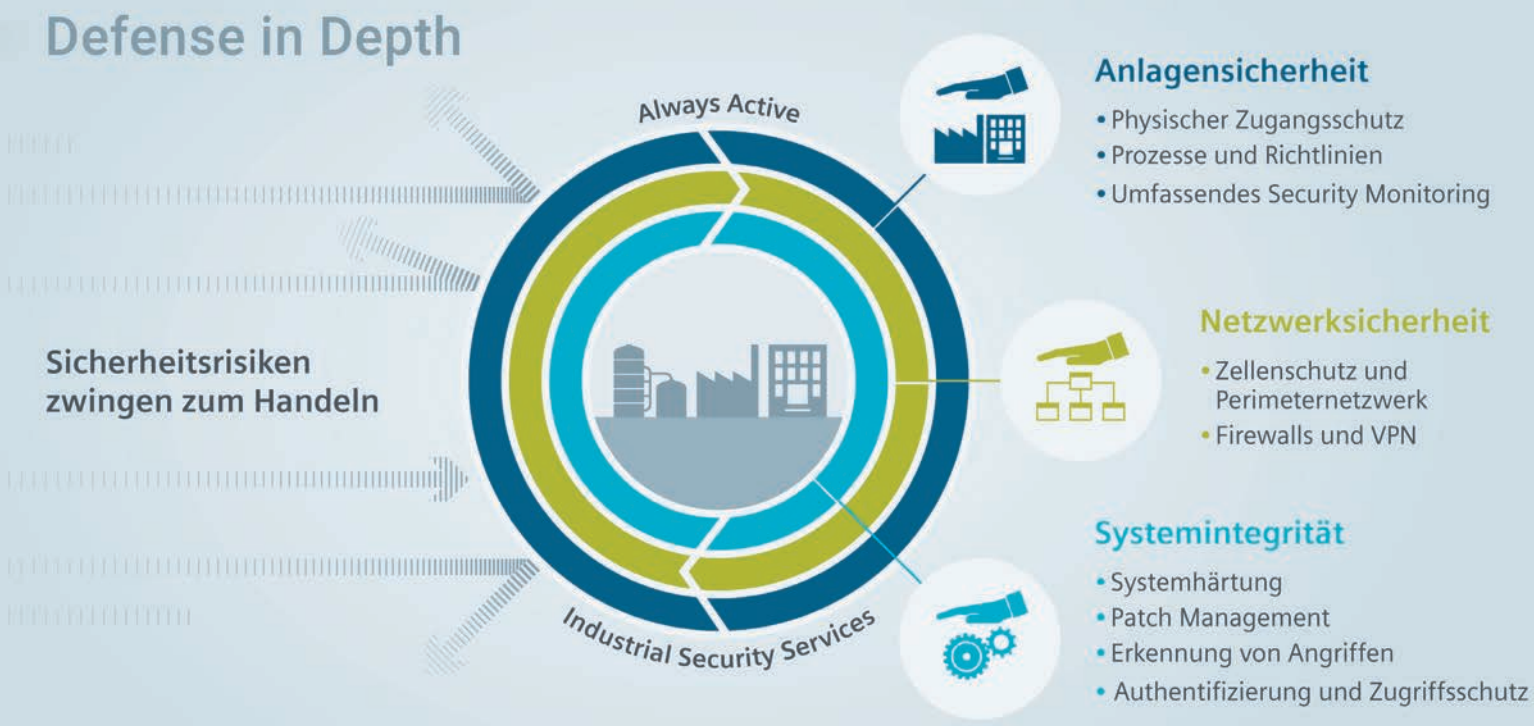
Alle verfügen über:
- umfangreiche variable Filterfunktionen
- TrueRMS Berechnung und Differentiator/Integrator
- Standard EtherCAT Interface zum Betrieb an jedem EtherCAT Master

New Automation Technology **BECKHOFF**

Industrielle Systeme vor Cyber-Angriffen schützen

Mit Netzwerk-Management zu mehr Sicherheit

Jedem Security-Update folgen neue Softwareschwachstellen, jeder Schutzmechanismus deckt neue Angriffsvektoren auf – auch in der Industrie. Bereits seit dem erstmaligen Auftreten einer Schadsoftware besteht ein Wettrennen und oft stellt sich die Frage, wie sich ein effektiver Schutz überhaupt etablieren lässt. Die Antwort darauf findet sich im nahtlosen Zusammenspiel mehrerer Maßnahmen.



Das tiefengestaffelte Industrial-Security-Konzept von Siemens ist durch unterschiedliche Maßnahmen und Mechanismen auf mehreren Ebenen für einen umfassenden Schutz vor Cyberbedrohungen ausgelegt.

„Ooops, your files have been encrypted!" – mit diesen Worten hat noch vor wenigen Jahren ein berühmtes Schadprogramm für Schlagzeilen gesorgt. Obwohl weder die Art der Bedrohung noch die verwendete Technologie von großer Innovationskraft geprägt waren, erreichte diese Malware binnen weniger Tage traurige Berühmtheit. Weitere namhafte Würmer und Viren, wie Blaster, Sasser oder MyDoom, haben bereits vor über 15 Jahren Schäden in Milliardenhöhe verursacht. Große Bekanntheit erlangte auch der Virus Stuxnet, der durch sein primäres Infektionsziel die Betreiber industrieller Anlagen in Atem hielt. Wenn man heute nach berühmten Schadprogrammen fragt, werden viele wahrscheinlich die Ransomware WannaCry nennen. Und das obwohl andere Würmer entweder deutlich mehr Geräte infiziert, größeren wirtschaftlichen Schaden angerichtet oder gar raffiniertere Angriffsvektoren genutzt haben. Was also war anders? Was hat WannaCry zu jener Bekanntheit verholfen? Die Beantwortung dieser Frage ist ziemlich vielschichtig. Entscheidende Aspekte waren aber wohl die schnelle Ausbreitungsrate sowie die Art der infizierten Geräte. Binnen weniger Stunden hatte sich die Ransomware in über 150 Ländern auf verschiedenen Computersystemen ausgebreitet und die darauf abgelegten Daten verschlüsselt. Es waren nicht nur Privatanwender und industrielle Unternehmen betroffen, sondern auch öffentliche Einrichtungen wie Krankenhäuser oder Anzeigetafeln im Fernverkehr. Dadurch hat dieser Vorfall die Angreifbarkeit unserer vernetzten Infrastruktur offengelegt. Und

Bilder der Doppelseite: Siemens AG

obwohl die Ausbreitung relativ schnell gestoppt werden konnte, blieb der fade Beigeschmack leicht anzugreifender Systeme sowie die Furcht vor neuen, vielleicht noch effektiveren Bedrohungen. Wie aber kann sich der Anwender nun wirkungsvoll gegen neue, heute noch unbekannte Angriffe schützen?

Defense in Depth – die Grundlage

Der sicherlich wichtigste Schritt ist es, sich auch in industriellen Umgebungen mit dem Thema Cybersecurity zu befassen und die Furcht vor dem Unbekannten zu verlieren. So lässt sich mit professioneller Unterstützung ein wirkungsvoller Ansatz für mehr Sicherheit durch eine sogenannte tiefengestaffelte Verteidigung etablieren. Die ist häufig auch unter dem Begriff Defense in Depth bekannt. Das Prinzip dahinter besagt, dass einem möglichen Angriff verschiedene, unabhängig voneinander arbeitende Schutzmaßnahmen entgegengebracht werden sollen. Mit diesen soll der Angriff entweder sofort gestoppt oder im Zusammenspiel genug Zeit für entsprechende Gegenmaßnahmen gewonnen werden. Wenn auch die Automatisierungskomponenten bereits während deren Entwicklungsphase Security-Aspekte hinreichend berücksichtigen, kann das Konzept auf einem tragenden Fundament verankert werden. Aus diesem Grund ist der sichere Produktlebenszyklus gemäß IEC62443 bei Siemens Digital Industries fester und zertifizierter Bestandteil des Entwicklungsprozesses. Die Prozessanforderungen und das Konzept der tiefengestaffelten Verteidigung inklusive der gängigen Mechanismen wie Firewalls oder weiterführender Anwendungen zur Angriffserkennung sind im Standard IEC62443 bzw. in einschlägiger Literatur ausführlich beschrieben. Ergänzend sind einige weitere Lösungen verfügbar, um Produktionssysteme vor Cyber-Angriffen zu schützen.

Angriff nach bekannten Mustern

Obwohl über alle möglichen Angriffsvektoren und ausnutzbaren Schwachstellen heute nur spekuliert werden kann, folgen einige Aspekte im zeitlichen Verlauf der meisten Angriffswellen einem bekannten Muster. Nachdem erste Infektionen sehr überraschend zugeschlagen haben, werden Security-Experten weltweit aktiv. Sie beginnen das Verhalten und die Funktionsweise der Schadsoftware so schnell wie möglich zu analysieren und versuchen wirkungsvolle Gegenmaßnahmen einzuleiten. Diese reichen z.B. von ersten Empfehlungen zum Eindämmen infizierter Systeme, über neue Signaturen für Virenscanner oder Deep-Packet-Inspection-Firewalls bis hin zu Security-Updates betroffener Anwenderprogramme. Da jene spezifischen Gegenmaßnahmen jedoch erst ausgerollt werden können, nachdem die Schadsoftware erkannt und analysiert wurde, wird weiterhin darauf gesetzt, die Erstinfektion mit den bereits vorhandenen Maßnahmen der tiefengestaffelten Verteidigung abzuwehren. Bevor sich das Angriffsmuster verändert, wie es bei sogenannten polymorphen Angriffen gängig ist, oder falls es trotz präventiver Schutzmechanismen zu einer Infektion einzelner Systeme gekommen ist, sollten lokale Ausbreitungswege unterbunden und genutzte Schwachstellen dauerhaft geschlossen werden. In beiden Fällen zeigt die Verwendung eines zentralen Netzwerk-Managementsystems Vorteile und hilft dabei die dafür nötige Transparenz im Netzwerk zu erreichen.

Schwachstellen identifizieren

Nach den ersten Analysen der Security-Experten veröffentlichen Produkthersteller wie Siemens entsprechende Security Alerts. Sie informieren darüber, ob Produkte von einer Schwachstelle betroffen sind. Unter Zuhilfenahme des Netzwerk-Managements lassen sich im ersten Schritt die jeweiligen Assets – also die Komponenten und Teilnehmer des Netzwerkes – ohne großen Aufwand auflisten und mit den Informationen der Security Alerts abgleichen. Bei möglichen Übereinstimmungen können nun weitere Eindämmungsmaßnahmen im Produktionsnetz ergriffen werden, bis Security-Updates der Produktlieferanten für die betroffenen Komponenten letztlich zur Verfügung stehen. Die identifizierten, angreifbaren Komponenten müssen besonders vor der Bedrohung geschützt werden, indem die Ausbreitung der Schad-

Mit einem Zellenschutzkonzept und Industrial-Security-Appliances aus dem Programm Scalance S lassen sich einzelne Produktionsbereiche effektiv vom Anlagennetzwerk trennen und schützen.

software über offene Ports diverser Protokolle und Netzwerkdienste im lokalen Netzwerk eingeschränkt wird. Folglich wäre der nächste Schritt, jene Protokolle und Netzwerkdienste durch Firewalls zu blockieren. Während sich dieses Vorgehen am Zonenübergang von der Büro- zur Fertigungsumgebung noch relativ mühelos umsetzen lässt, zeigt sich bereits an den Fertigungszellen eine gewisse Komplexität. Die zusätzlichen Regeln müssen an vielen Firewalls angewendet werden und dürfen bei einigen Zellen gegebenenfalls nur temporär oder gar nicht aktiv geschaltet werden, um den Produktionsprozess nicht zu beeinflussen. Möchte man zudem als weitere Maßnahme auch sekundäre Systeme, wie Archivierungsserver im Rahmen einer Notfall-Policy zeitweise komplett vom Anlagennetzwerk trennen, indem neben den Ports ganze Schnittstellen am Switch oder Router deaktiviert werden, wird das Ausmaß der Komplexität schnell deutlich. Kombiniert man aber Firewall- und Netzwerkmanagement in einem System, bieten sich dem Anwender einfache und flexible Varianten. Er kann die Kommunikationsbeziehungen zwischen den Netzwerkzellen begrenzen und die Produktion z.B. mit eingeschränkten Diagnose- oder Zugriffsmöglichkeiten weiterhin am Laufen halten.

Updates zentral einspielen

Für einen nachhaltigen Schutz müssen die angreifbaren Komponenten letztlich dauerhaft vor dieser spezifischen Bedrohung geschützt werden. Dazu müssen die von den Herstellern bereitgestellten Software- und Firmwareupdates zeitnah eingespielt werden. Je nach Netzwerk- und Systemarchitektur kann dies bereits während des laufenden Betriebs oder in einem Wartungszyklus der Produktion erfolgen. In beiden Fällen kann der Aufwand enorm sein. Bei Computersystemen in geschlossenen Domänen hat sich daher eine zentrale Variante über sogenannte Update-Server etabliert. Um diese Vorzüge ebenso bei industriellen Infrastrukturkomponenten wie Switches, Router oder Firewalls genießen zu können, bedarf es erneut eines zentralen Netzwerkmanagements, mit dem Firmwareupdates übergreifend eingespielt werden können. Ist die Schwachstelle auf allen Komponenten behoben, können die zuvor gesetzten restriktiven Firewall-Regeln und die abgekoppelten Systeme wieder in den normalen Betrieb zurückgesetzt werden. Dadurch kann das gesamte Produktionsnetz wieder im vollen Umfang mit Datenarchivierungen oder weiterführenden Diagnosen wie gewohnt genutzt werden.

Ausbreitung von Schadsoftware eindämmen

Reflektiert man die gewonnen Erkenntnisse auf die Verbreitung von WannaCry, erkennt man sehr deutlich das Potenzial eines Netzwerk-Managementsystems. Während die Erstinfektion zwar nicht verhindert worden wäre, hätte die Ausbreitung im lokalen Netzwerk im Vorfeld soweit eingedämmt werden können, bis das bereits vorhandene Security-Update auf verwundbaren Systemen ausgebracht worden wären. Ein modernes Managementsystem steht also nicht nur für rein administrative oder diagnostische Einsatzzwecke. Vielmehr unterstützt es ebenso im Rahmen einer tiefengestaffelten Verteidigung und im Zusammenspiel mit Firewalls und weiteren Security-Komponenten die Anlagenverfügbarkeit auch in Bedrohungslagen aufrechtzuerhalten. Gerade vor dem Hintergrund kontinuierlich zunehmender Cyberangriffe und stetig variierender Angriffsszenarien kann es den entscheidenden Vorteil bieten. ■

Transparenz und detaillierte Informationen über die Teilnehmer eines Netzwerkes sind ein Schlüsselfaktor, um Security-Maßnahmen effektiv und zielgerichtet einsetzen zu können.

Bild: Siemens AG

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/9595

Peter Schönemann, Systemmanagement Industrial Security
Siemens AG
www.siemens.de/industrial-security

Erstes Plug Fest für Safety over Ethercat (FSoE)

ETG hat kürzlich sein erstes Safety-over Ethercat Plug Fest durchgeführt. Hersteller von Ethercat-Safety-Master- und -slave-Systemen haben die Interoperabilität ihrer Safety-over-Ethercat-Geräte (FSoE) getestet und ausgetauscht. Neu bei dem Fest war der Schwerpunkt nur auf FSoE-Mastern als sichere Steuerung für dezentrale und zentrale Lösungen sowie auf FSoE-I/O-Geräten. Insgesamt waren 36 Teilnehmer von 18 unterschiedlichen Firmen gekommen. Neben neun Mastern und 15 Slave-Geräten waren auch ein Stack sowie ein Tool im Einsatz. Das Ethercat-Protokoll bei Geräten ohne Safety-Funktion diente lediglich als Transport-Layer. Zudem wurden sichere Antriebe getestet, deren Funktionen mit Unterstützung des Profils ETG.6100 umgesetzt werden. Das Profil dient zur Vereinheitlichung der Funktionsweise und Parameter für antriebsintegrierte Sicherheitsfunktionen.

Ethercat Technology Group
www.ethercat.org

Spezifikation von Profinet mit TSN abgeschlossen

Ethernet TSN wurde mit der aktuellen Spezifikation V2.4 als zusätzliche Layer2-Technik in die Profinet-Architektur integriert. Die Spezifikationsarbeiten sind laut Nutzerorganisation abgeschlossen und die drei Teile des Dokuments stehen zum Download bereit. Damit sollen sowohl Hersteller als auch Anwender die Vorteile von TSN interoperabel umsetzen können, wie zukunftssichere IEEE-Ethernet-Technik mit höherer Bandbreite, Deterministik, flexible Netzwerkkonfiguration und große Prozessorvielfalt. Dabei bleibt die Anwenderschnittstelle, d.h. die Nutzung von I/O-Daten, Diagnose und Parametrierung unverändert, da die neuen TSN-Mechanismen im Wesentlichen in den unterlagerten Kommunikationsschichten wirken. Zum einfachen Verständnis der Funktionsweise ist auch eine Guideline verfügbar, welche die Grundlagen von TSN erklärt. Gerätehersteller können sich der Stacks oder Module bedienen ohne wie bisher die Details verstehen oder selbst implementieren zu müssen.

Profibus Nutzerorganisation e.V. (PNO)
de.profibus.com

Zusammenarbeit von Peak und Emsa

Peak-System und Emsa haben ihre Partnerschaft vertieft, um gemeinsame CANopen-, CANopen-FD- und J1939-Lösungen anzubieten. Aufbauend auf dieser Partnerschaft ist Peak nun Gesellschafter und Partner von Emsa geworden. Dadurch sollen Entwicklungsprozesse rationalisiert werden, die sowohl CAN-Hard- als auch -Software betreffen. Aktuelle Projekte umfassen generische CANopen-FD-Ein- und Ausgabegeräte, CANopen-FD-Protokollbibliotheken, Sicherheitsoptionen für CAN sowie Diagnose- und Testsysteme für CANopen (FD) und J1939.

Bild: Peak-System Technik GmbH

Peak-System Technik GmbH
www.peak-system.com

Helmut Halmburger von Wachendorff referierte über die Cloud-Basis für Industrie-4.0-Anwendungen.

Wachendorff IIoT-Konferenz Flexthink

Keep calm...

...and think of IIoT. So lautete das eingängige Motto der diesjährigen Wachendorff Flexthink-Konferenz. Bei Außentemperaturen nahe der 40°C war dies für die Teilnehmer jedoch nicht immer uneingeschränkt möglich. Dennoch sorgten informative Vorträge, ein abwechslungsreiches Rahmenprogramm und – nicht zuletzt – klimatisierte Räumlichkeiten für ein sehr gutes Fazit.

Wachendorff Prozesstechnik und HMS Industrial Networks haben sich also wieder mächtig ins Zeug gelegt, um Kunden und Interessenten der Fernwartungslösung Ewon & Talk2M einen Tag voller Impulse in Sachen Digitalisierung und datenbasierter Geschäftsmodelle aufzubereiten. An vier Orten (Groß Meckelsen bei Hamburg/Bremen, Bad Salzuflen bei Bielefeld, München und Böblingen) nahmen Ende Juni/Anfang Juli in Summe mehr als 100 Personen die Einladung an und folgten einem abwechslungsreichen Programm. Helmut Halmburger, Produktmanager von Wachendorff Prozesstechnik, und Horst Lange (HMS/Ewon) ist es gelungen Top-Referenten mit spannenden Inhalten für eine aktive Teilnahme an dieser IIoT-Konferenz zu begeistern. Beide steuerten auch eigene Vorträge bei, die ebenfalls auf großes Interesse und Zustimmung trafen.

Abwechslungsreiches Vortragsprogramm

So referierte Lange, Manager IIoT Strategy bei HMS, über die Phasen der Industrie-4.0-Evolution – vom einfachen Fernzugriff zur Kostenersparnis bis zum rentablen Servicemodell. Klein anfangen, evaluieren im definierten Rahmen, das große Ganze im Auge behalten und entsprechend hochskalieren bzw. weiterentwickeln zur richtigen Zeit war hier das Fazit. Neben einem Ausblick zur Ewon-Roadmap stellte Lange auch die Vorteile von strategischen Partnerschaften, die bei der Zusammenarbeit von verschiedenen Kommunikations- und Anwendungsplattformen zum Tragen kommen. So stellte Lange gemeinsam mit Halmburger dar, wie die Leistungen der Firma Wachendorff das Produktportfolio von HMS und Ewon flankieren: Hierzu zählen FAE-Dienstleistungen, zahlreiche Optionen hinsichtlich kundenspezifischer Anpassungen und bedarfsgerechte Schulungen. Als Gastreferent war u.a. Percy Ralf eingeladen, Gründer und Vorstand der Net.ag, der eine abwechslungsreiche Bestandsaufnahme von Industrie 4.0 im deutschen Mittelstand lieferte, inkl. Herausforderungen, kritischen Faktoren und einem Ausblick auf das, was die Zukunft bringt. Weiter bot Lars Stuke von der IoT-Plattform Cumulocity eine eindrucksvolle Live-Demo einer Data-Mailbox-Verbindung in die Cloud. Mit besonders hohem Interesse wurde der Vortrag von Stefan Hoppe, Präsident und Executive Director der OPC Foundation, erwartet, der über die Möglichkeiten von OPC UA als Framework für den sicheren, robusten Austausch von Informationen referierte.

Flexibles Denken als Grundvoraussetzung für ein erfolgreiches IIoT-Projekt.

Zufriedene Gesichter

Die Erwartungen der Teilnehmer an die Veranstaltung wurden in den meisten Fällen voll ‘erfüllt’ oder sogar ‘übertroffen’, das zeigte die Auswertung der Feedbackbögen. Auch die Übertragbarkeit der vermittelten Inhalte in die tägliche Praxis wurde von den Teilnehmern ausdrücklich bescheinigt und gelobt. Darüber hinaus trug nicht zuletzt das von HMS veranstaltete Rahmenprogramm zur Zufriedenheit der Teilnehmer bei: Grill-Seminare und eine VIP-Arena-Besichtigung standen auf dem Programm. Bei so viel Zuspruch wird es wahrscheinlich auch im Jahr 2020 wieder zu ähnlichen Veranstaltungen kommen, wie Wachendorff und HMS verlauten lassen. *(bfi)* ■

Wachendorff Prozesstechnik GmbH & Co. KG
www.wachendorff.de

Neue Version des Klassifizierungsstandards eCl@ss vorgestellt

Die Version 11.0 des Klassifizierungsstandards eCl@ss ist kürzlich erschienen. Stefan Mülhens, Geschäftsführer von AmpereSoft, bezeichnet das neue Release als „Meilenstein auf dem Weg zu Industrie 4.0“. Wichtigste Neuerung sei die Möglichkeit, neben physikalischen Angaben auch die Funktionen eines Produktes mit dem Standard abzubilden. „Daraus entsteht ein großes Potenzial für einen reibungslosen und automatisierten Produktionsprozess“, so Mülhens. Denn: Die noch genauere Beschreibung der Produktdaten ermöglicht einen entsprechend detaillierten Engineering-Prozess. Mit Version 11.0 kommt auch die Entwicklung von SemAnz40 einen Schritt voran. Dieses Projekt, an dem der eCl@ss-Verband mit Partnern aus Forschung und Industrie arbeitet, zielt auf eine semantische Basis für den Informationsaustausch in M2M-Anwendungen ab, die gewährleistet, dass die bereitgestellten Produktdaten von jeder Maschine gleich interpretiert werden. „Standards sind der Schlüssel zu Industrie 4.0“, betont Mülhens. „Deshalb engagieren wir uns bereits seit vielen Jahren um die Etablierung von Standards wie eCl@ss und AutomationML.“ In der jüngeren Vergangenheit sei die Anzahl positiver Praxisbeispiele spürbar gestiegen, wodurch sich der Druck auf Nachzügler erhöhe. „Mit dem 11.0-Release und den darin enthaltenen Verbesserungen verschärft sich diese Situation noch einmal.“ Unternehmen, die noch immer auf eCl@ss als Produktdatenstandard verzichten, würden in Zukunft abgehängt. Weil die konkrete Umsetzung in den unterschiedlichen IT-Landschaften gerade in der Initialphase herausfordernd sein kann, stehen Unternehmen bei der Einführung eCl@ss-Partner wie AmpereSoft zur Seite, die Software-Tools für die Pflege und Nutzung sowie Beratungs- und Unterstützungsleistungen anbieten.

AmpereSoft GmbH
www.amperesoft.net

Modul für 40GBit-Ethernet

Das Network-Modul der Windows-Erweiterung RealTime Suite von Kithara ermöglicht eine Echtzeit-Netzwerkkommunikation bis zu 40GBit/s. Mithilfe des Intel-Controllers XL710 lässt sich gegenüber den vorher möglichen 10Gbit/s die Datenrate mit der Windows-Echtzeit-Erweiterung vervierfachen. Karten mit dem Controller verfügen über Anschlüsse für den Enhanced Quad Small Form-factor Pluggable Transceiver (QSFP+), einer Erweiterung des SFP+. Damit lässt sich neben der gleichzeitigen Nutzung von vier 10GBit/s-Kanälen auch ein Kanal für 40GBit/s verwenden.

Kithara Software GmbH
www.kithara.de

Erweitertes Beleuchtungskonzept für Bediensysteme

Griessbach hat sein Portfolio an Beleuchtungsoptionen für Bedien- und Eingabesysteme erweitert. Die neuen Funktionen lassen sich variabel für kundenspezifische Bedienlösungen adaptieren und können auch standardmäßig in CAN-Tastermodule integriert werden. Zur Symbolhinterleuchtung sind die Module nun mit RGB-LEDs in frei wählfarben Farben ausgestattet. Das erweiterte Beleuchtungskonzept umfasst eine umlaufende Ring- oder Segmentbeleuchtung für jedes Tasterfeld. Mithilfe von Ampelfarben wird der Status signalisiert, um Warn- oder Alarmsignale direkt am Taster kenntlich zu machen.

Griessbach GmbH
www.griessbach.de

PC-CAN-ADAPTER FÜR WINDOWS UND LINUX

Mit dem SimplyCAN bietet HMS unter der Marke Ixxat einen PC-CAN-Adapter an. Er enthält eine intuitiv zu nutzende API-Schnittstelle und kann laut Hersteller schnell und einfach integriert werden. Der Adapter ist für den mobilen und stationären Einsatz mit galvanisch isolierter CA-High-Speed-Schnittstelle und Sub-D9-CAN-Anschluss ausgelegt. Er wird automatisch als USB-COM-Schnittstelle erkannt und erfordert unter Windows 10 und Linux für den Betrieb der Hardware keine Treiberinstallation. Kundeneigene Anwendungen auf Basis des Adapters können somit direkt genutzt werden, z. B. für die Diagnose, Konfiguration oder Inbetriebnahme. Die Anbindung von eigenen Programmen erfolgt mittels einfacher Funktionen, die über ein kompaktes API bereitgestellt werden. Es werden die Programmiersprachen C, C# und Python unterstützt.

Der Adapter SimplyCAN kann einfach in Kundenanwendungen integriert werden.

HMS Network
www.hms-networks.de

Edge Controller kombiniert I/O- und serielle Konnektivität mit Netzwerkverbindungen

Mit dem BB-400-NeuronEdge-Controller von Brainboxes können Anwender I/O- und serielle Konnektivität mit verschiedenen Netzwerkverbindungen kombinieren.

Der Controller BB-400 NeuronEdge von Brainboxes kombiniert I/O- und serielle Konnektivität mit verschiedenen Netzwerkverbindungen, wie Bluetooth oder WLAN. Im kompakten DIN-Mount-Design befindet sich ein Raspberry-Pi-Compute-Modul und ein Arduino. Der PI wird durch ein industrietaugliches Power-Management-System unterstützt und der Arduino ist für Edge Computing verantwortlich. Gesteuert wird das Gerät über eine Open-Source-Software. Der Controller empfängt, sortiert und sendet Daten in der Peripherie des Netzwerkes. So soll er helfen, Reaktionszeiten zu verbessern und Ausfallzeiten zu reduzieren. Er ist mit vielen Hardware-Schnittstellen ausgestattet und kann über Ethernet mit zwei Ports, Bluetooth, I/O mit acht Lines, WLAN, NFC, USB und RS232/422/485 mit unterschiedlichen Geräten und Maschinen kommunizieren. Die Übertragungsrate beträgt 100MBit/s. Der Controller verfügt über zwei redundante Anschlüsse von 5 bis 30VDC und integriertes UPS.

Brainboxes Limited
www.brainboxes.com

Bereit für Datenkommunikation von morgen

Alles für industrielle Netzwerke

Industrielle Netzwerke werden immer komplexer. Mit vollständigen Lösungen für die industrielle Datenkommunikation von morgen ist Phoenix Contact Ihr langfristiger Partner, um die Herausforderungen der Digitalisierung in die Praxis umzusetzen.

Mehr Informationen unter Telefon +49 5235 3-12000 oder **phoenixcontact.de**

PHOENIX CONTACT
INSPIRING INNOVATIONS

ION11-18.000.L1

Firewall für Geräte und Maschinen im eigenen Netzwerk

Die Microfirewall soll potentiell anfällige oder nicht vertrauenswürdige Geräte und Maschinen in eigenen Netzwerksegmenten isolieren.

Die Firewall Microwall Gigabit von Wiesemann & Theis isoliert potentiell anfällige oder nicht vertrauenswürdige Geräte und Maschinen in eigenen Netzwerksegmenten, wie IoT-Devices, Smart-Home-Assistenten und CNC-Fräsen. Jeder Funktionseinheit wird ein eigenes Netzwerksegment in Form einer sicheren Insel zugewiesen. Der erlaubte Datenverkehr wird auf die unbedingt notwendigen Fälle für den Betrieb eingeschränkt. So sollen sich Angriffe auf offene TCP- oder UDP-Ports sowie unerwünschte Datenverbindungen effektiv unterbinden lassen. Geräte auf der gleichen Insel können weiterhin ungehindert miteinander kommunizieren. Die Konfiguration des Zwei-Port-Firewallrouters erfolgt einfach über eine webbasierte Benutzerschnittstelle. Nach erfolgter Einrichtung kann die Konfigurationsoberfläche dauerhaft deaktiviert werden, sodass für eine Neukonfiguration ein physikalischer Zugriff auf das Gerät notwendig ist.

Wiesemann & Theis GmbH
www.wut.de

Switch mit 16 Fast-Ethernet-Ports

Der industrielle Ethernet Switch IFGS-1822TF von Spectra stellt für seine 16 Fast-Ethernet-Ports zwei GBit-Uplink-Ports zur Verfügung. Sie ermöglichen hohe Übertragungsgeschwindigkeiten. Der Uplink kann wahlweise in Kupfer oder Glasfaser (Combo-Port) ausgeführt werden. Der Switch verfügt über einen Temperaturbereich von -40 bis +75°C, ein robustes Metallgehäuse, 6kV-ESD-Schutz und einen Weitbereichsspannungseingang von 12 bis 48VDC. Er erfüllt den EEE-Standard nach IEEE 802.3a und lässt sich auf der DIN-Schiene und an der Wand montieren.

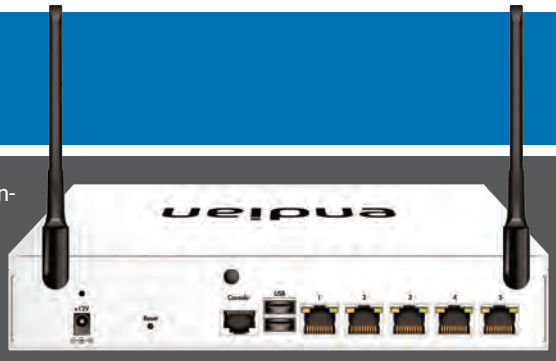
Spectra GmbH & Co. KG
www.spectra.de

Funkempfänger für codierte Signale

Mit dem Funkempfänger LevelView.WLAN von RCT lassen sich codierte Funksignale ins globale Netz weiterleiten. Er kann einfach mit handelsüblichen Routern verbunden werden. Alarmmeldungen zu eingestellten Grenzwerten werden wahlweise per Email oder Push-Benachrichtigung zum Betreiber der Tanks weitergeleitet. Der Empfänger besteht z.B. aus einem WLAN-Modul mit integrierter Antenne, einer 32Bit-ARM-CPU und einem 868-MHz-Transmitter-Modul mit externer Antenne.

RCT Remote Control Technology GmbH
www.rct-monitor.com

Securitygateway mit WLAN-Ausstattung



Die All-in-One-Lösung Endian UTM Mercury 50 ist ab sofort auch als leistungsstarke Wireless-Version verfügbar. Neben den bisherigen Sicherheitsfunktionen ist das Securitygateway zusätzlich mit einer Karte und zwei Antennen ausgestattet. Damit können bis zu vier separate Wireless-Netzwerke mit unterschiedlichen Verschlüsselungstypen eingerichtet werden, wie WPA2 Personal oder WPA2 Enterprise. Die Lösung erfüllt so die Anforderungen an ein sicheres WLAN und kann einfach bis zu zwei Access-Points ersetzen. Anwender können mehrere Wireless-Netzwerke unterschiedlicher Verschlüsselungstypen erstellen und somit das WLAN mit der Öffentlichkeit teilen. Die intuitive Bedienbarkeit sowie die Verfügbarkeit als Hard-, Software oder On-Premises-Lösung sorgt für hohe Flexibilität. Durch den Authentifizierungsschritt wird der WLAN-Zugang externer Gäste mitverfolgt und zusammen mit Traffic-Protokollen und Kontaktdaten gemeldet. Alle Daten werden intern auf der Festplatte der Appliance gespeichert und stehen damit jederzeit zur Verfügung.

Endian SRL
www.endian.com

Individuell konfigurierbare Temperierlösung

Der Dreipunkt-PID-Regler R4100 ist für den Einsatz in Temperierapplikationen ausgelegt. Das 3,5"-große, farbige Touch-LCD-Display stellt wesentliche Funktionen übersichtlich dar, um Temperaturverläufe besser zu erkennen. Der integrierte Programmregler fährt das eingestellte Temperaturprofil ab. Bis zu acht unterschiedliche Temperaturprofile bzw. -programme kann der Benutzer im Detail konfigurieren und individuell auf Programmtasten legen. Ein Algorithmus sorgt für eine genaue Regelung und Rampenverläufe können frei konfiguriert werden. Der integrierte Webserver erlaubt den Fernzugriff über LAN oder WLAN mit Endgeräten wie Smartphone, PDAs oder PCs. Anwender können nach Eingabe der IP-Adresse das System einfach von anderen Arbeitsplätzen aus steuern oder beobachten. Der Regler besteht aus einer Controller- und einer abgesetzten IO-Hutschienen-Baugruppe.

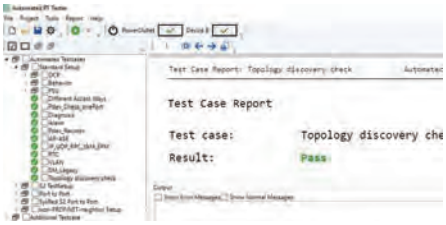
Elotech Industrieelektronik GmbH
www.elotech.de

Modulserie für extreme Temperaturen

Die UT-Varianten der Modulserie ET-7000 von ICPDAS ermöglichen einen sicheren Betrieb bei Umgebungstemperaturen von -40 bis +75°C. Die Anbindung des ET-7042-Moduls an überlagerte Systeme erfolgt über das Modbus-TCP-/UDP-Protokoll. Der integrierte Webserver ermöglicht die einfache Parametrierung des Moduls, wie die Einstellung der Einschaltwerte oder der Safe Values. Die Stromversorgung erfolgt direkt über das Ethernet-Kabel. Anwender können über die Funktion I/O Pair Connection schnell einen flexiblen Feld-Multiplexer erstellen. Zusätzliche Sicherheit bieten der Überspannungsschutz und die Kabelbrucherkennung.

ICPDAS-Europe GmbH
www.icpdas-europe.com

Tester für die Qualitätsabsicherung



Der Automated RT Tester von PI ist für die Qualitätsabsicherung entwickelt worden. Er soll zuverlässig und reproduzierbar typische Fehler bei der Anpassung neuer Geräte ermitteln. Der Tester wurde in enger Abstimmung mit Standardisierung, Qualitätsgremien und Technologie-Suppliern nach aktuellen Vorgehensmethoden entwickelt. So prüft er z.B. in einem Nachtlauf das täglich erstellte Coding, um eine schnellstmögliche Rückmeldung über die Zertifizierbarkeit zu bekommen. Er kann auch als Basis für die eigene Testfallentwicklung genutzt werden. Eigene Testsequenzen können selbst mittels C# ergänzt werden.

Profibus Nutzerorganisation
www.profibus.de

App zur Berechnung von Registerwerten für CAN- und CAN-FD-Controller

Peak-System hat ein Bit Rate Calculation Tool für iOS, Android und Windows veröffentlicht. Das kostenlose Tool ermittelt die Registerwerte eines CAN-, CAN-FD- oder SJA1000-Controllers für benutzerdefinierte CAN- und CAN-FD-Bitraten. Anwender können die Ergebnisliste anhand verschiedener Parameter wie Taktfrequenzen und Sample Point anpassen. Um nahe liegende Ergebnisse mit in die Auswertung aufzunehmen, kann eine Toleranz von bis zu fünf Prozent bestimmt werden. Die Bit-Timing-Werte BRP, TSEG1, TSEG2 und SJW der Ergebnisse können gespeichert und plattformübergreifend geladen werden. Android- und iOS-Nutzer können die Resultate via E-Mail versenden und Windows-User können die Werte einfach in die PCAN-Basic API und darauf aufbauende Applikationen übernehmen. Die App ist besonders für das Planen und Verbessern klassischer CAN- und moderner CAN-FD-Netzwerke geeignet.

Peak-System Technik GmbH
www.peak-system.com

4G/5G-PICK-BY-LIGHT-APPLIKATION

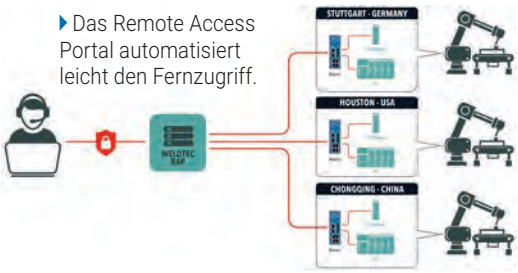
Next Lap hat eine 4G/5G-Pick-by-Light-Applikation für das Gateway SmartController veröffentlicht. Die Plug&Play-Lösung kommt dabei ohne klassische Netzwerkinfrastruktur aus. Mit der 4G/5G-Anbindung werden Pick-by-Light-Prozesse laut Hersteller schneller und einfacher umsetzbar, da sie unabhängig von vorhandener bzw. neuer Netzwerkinfrastruktur implementiert werden können. Das Gateway konnte bisher per 2,4GHz- und 5GHz-WLAN sowie kabelgebunden mit dem Produktionsnetzwerk verbunden werden. Es bildet eine Brücke zwischen IIoT-Hardware im Shopfloor und der AI-Production-Process-Platform IP/1 des Herstellers. Gleichzeitig ist es zu intelligenter Hardware von Drittanbietern, wie Datenbrillen, Scannern, Kameras und fahrerlosen Transportsystemen kompatibel.

Mit der 4G/5G-Pick-by-Light-Applikation bietet NextLap eine Plug&Play-Lösung, die ohne klassische Netzwerkinfrastruktur auskommt.

Next Lap GmbH
www.nextlap.de

Automatisierter Fernzugriff auf Maschinen und Anlagen

Mit dem Remote Acess Portal von Welotec können verschiedene Funktionen für den Fernzugriff auf die Anlage einfach automatisiert werden. So wird automatisch das Routing erzeugt, Firewall-Regeln festgelegt, Zertifikate erstellt und den Routern zugeordnet sowie der Rollout der VPN-Konfiguration durchgeführt. Über die Punkt-zu-Punkt-Verbindung direkt zum gewünschten Gerät haben Anwender nahezu die gleichen Zugriffsmöglichkeiten wie bei der Arbeit vor Ort. Das Portal besteht aus dem Smart Ems, einer Firewall und einer PKI. Durch die integrierte Benutzerverwaltung ist die Verwaltung der Zugriffe auf verschiedene gruppierte Router und Endgeräte möglich.



Das Remote Access Portal automatisiert leicht den Fernzugriff.

Welotec GmbH
www.welotec.com

Signalwandler für bestehende SPS-Architekturen

Red Lion Controls hat eine neue Produktfamilie von Signalwandlern vorgestellt. Die Geräte übersetzen und integrieren Signale in vorhandene SPS-Architekturen und sollen so dem Anwender Eingangskarten zur Aufnahme eines spezifischen Signaleingangs ersparen. Sie sind 6mm breit und wandeln bzw. empfangen Strom, Spannung, Thermoelemente, RTDs, Widerstands- und gepulste Eingangssignale. Sie sind einsetzbar in IIoT-Strategien für die Verbindung von Daten vorhandener Geräte mit zusätzlichen Sensoren oder in Messprozessen, die präzise Sensordaten erfordern.

Red Lion Controls
www.redlion.net/de

Stellungsregler mit Industrial-Ethernet-Schnittstelle

Bürkert bietet die Stellungs- und Prozessregler vom Typ 8692/8693 und 8792/8793 mit Industrial-Ethernet- und Systembusschnittstelle an. Die neuen Regler unterstützen Ethernet/IP, Profinet Conformance Class B (CC-B) sowie Modbus TCP. Die Protokolle ermöglichen verschiedene Diagnosefunktionen, wie Überwachung, Grenzwertdefinition der Betriebsparameter oder Meldungen nach Namur NE107 und verbessern so laut Hersteller die Anlagenverfügbarkeit. Der integrierte Zwei-Port-Switch erlaubt Stern-, Linie- und Ring-Topologien und soll so für eine schnelle und durch MRP und DLR ausfallsichere Kommunikation bis zum Ventil sorgen. Die integrierte BüS-Schnittstelle erlaubt eine unkomplizierte Kommunikation einzelner Sensoren und Aktoren der Geräteplattform EDIP des Herstellers untereinander. Alle Teilnehmer der Plattform lassen sich über das Software-Tool Bürkert Communicator parametrieren und konfigurieren.

Christian Bürkert GmbH & Co. KG
www.buerkert.de/de

Die Stellungs- und Prozessregler vom Typ 8692/8693 und 8792/8793 sind mit Industrial Ethernet ausgestattet.

Neues Release für IoT-Plattform

Bild: ©metamorworks/www.istockphoto.com

Das Unternehmen In-integrierte Informationssysteme hat die Version 8.0 der IoT-Plattform Sphinx Open Online veröffentlicht. Mit dem Release will das Unternehmen die Integration und Verarbeitung großer Datenmengen vereinfachen. Zudem ist die nahtlose Einbindung in vorhandene Docker-Umgebungen sowie der einfache externe Betrieb z.B. in der AWS-Cloud möglich. Die Version bietet neue Funktionen und Schnittstellen, z.B. für das Ladeinfrastrukturmanagement. Das Release kann Mengengerüste

In-integrierte Informationssysteme GmbH
www.in-gmbh.de

FITS: Endspurt der IIoT-Spezifikation

Die FDT Group hat bekannt gegeben, dass die Spezifikation für den FDT-IIoT-Server FITS zur endgültigen Überprüfung für die Mitarbeiter freigegeben ist. Die Grundlagen für das Konzept bilden die FDT-V2.0-Spezifikationen. Der Server stellt den Kern des Konzepts dar, um den die verschiedenen Varianten für die Kommunikation mit den Clients und den Geräten angesiedelt sind. Der neue Standard soll zum Jahresende veröffentlicht werden. Mit ihm können Anbieter für Steuerungs- und Automatisierungssysteme ihr Angebot an intelligenten Lösungen mit den Geschäftsmodellen von FDT weiterentwickeln.

FDT Group
www.fdtgroup.org

FDT IIoT Server Platform

Gateway als Knotenpunkt für Sensoren

Das Gateway Hub-GM100 von In.hub ist mit verschiedenen Schnittstellen ausgestattet und fungiert als smarter digitaler Knotenpunkt für verschiedene Sensoren. Es erfasst einfache Werte wie Temperatur, Luftfeuchte oder Vibration und übernimmt komplexe sicherheitsrelevante proaktive Aufgaben der Maschinendiagnostik, Predictive Maintenance sowie Prozessoptimierung. Intern greift es auf Ubuntu LTS zurück. Für die Verarbeitung und Aufbereitung der erfassten Sensordaten kommt das einfache Baukastenprinzip von IBM Node-Red zum Einsatz. Es ist browserbasiert, einfach bedienbar und ermöglicht ein nahezu unbegrenztes Handling der Messdaten. Alternativ steht Anwendern das Siineos (Smart Industrial Internet Embedded Operating System) zur Auswahl. Das System besteht aus möglichst wenigen, aber effektiven Elementen der Softwareschichten. Innerhalb der Boot-Zeit von weniger als 10s werden hier Kernel-Daten, Systemlayer (Debian) sowie das In.core-Framework und abschließend die Steuerfläche In.core Appliance geladen.

In.hub GmbH
www.inhub.de

Das Gateway HUB-GM100 von in.hub ermgölicht auch komplexe sicherheitsrelevante Auftgaben, wie Maschinendiagnostik, Predictive-Maintenance sowie Prozessoptimierung.

Kolumne von Hans-Ludwig Göhringer

Industrial Ethernet wird um TSN erweitert


Bild: I-V-G Göhringer

Fast unscheinbar ging die Meldung zu Time-Sensitive Networking (TSN) schon im Frühjahr 2017 durch die Fachpresse. Ich vermute, das ist vielen Anwendern erst mal entgangen oder zumindest war die Tragweite nicht bewusst. Um den Hintergrund zu verstehen, muss man die Geschichte von Ethernet und die der Feldbusse etwas näher durchleuchten.

Was hat IP-basierte Kommunikation über Ethernet so weit nach vorne gebracht und was macht dessen Erfolg aus? Ganz einfach: Schon früh hat sich die Ethernet-Welt von der Applikation abgekoppelt und dafür gesorgt, dass sich das Ethernet-System kontinuierlich weiter entwickelt, speziell unter dem Gesichtspunkt des olympischen Gedanken: schneller – höher – weiter. Andere Feldbus- und Netzwerk-Technologien waren in der Applikation gefangen. Sie hatten zum Teil keine Chance, sich weiter zu entwickeln und werden damit langfristig wieder vom Markt verschwinden. Mit der Entscheidung, TSN in Profinet zu integrieren, hat sich die PNO vermutlich schwer getan – zumal das praktisch einer Abkündigung der IRT-Konzepte gleich kommt.

Den großen Vorteil sehe ich darin, dass bei der IEEE-Technologie, auf der TSN basiert, eine kontinuierliche Weiterentwicklung praktisch garantiert ist. Auf der vergangenen Messen wurden in ersten konkreten Umsetzungen bereits gezeigt, wie sich TSN in Ethernet-basierende Netze integrieren lässt – man konnte schon erkennen, dass je nach System sich unterschiedliche Vorteile herauskristalisieren. Auf der kommenden SPS-Messe kann man sicher noch mehr erkennen. ■

Hans-Ludwig Göhringer
IVG Göhringer
www.i-v-g.de

Neues Framework für OPC UA

Entwicklungs- und Betriebskosten sparen

Das Unternehmen Talsen Team hat mit der ersten Version von APPIO ab Mitte Juni 2019 ein neues Framework für OPC UA vorgestellt. Die Open-Source-Anwendung vereinfacht und automatisiert laut Hersteller die Konfiguration, den Betrieb und die Wartung von OPC-UA-Netzwerken. Dabei stellt das Framework eine Erweiterung des Standards dar, um Mechanismen zur Steigerung der Wandlungsfähigkeit von OPC-UA-Netze zu ergänzen, ohne ihn dabei zu verändern. Es verwendet open62541 als bevorzugten OPC-UA-Referenz-Stack und ist von seiner Architektur betriebssystemneutral. Die Implementierung des Frameworks wird derzeit vorrangig für Linux-Systeme vorangetrieben. Als Open Source unterliegt es der Mozilla License und ist vollständig über die Kommandozeile steuer- sowie automatisierbar. Mit ihm soll Plug&Produce greifbar werden. Die Deployment-Services arbeiten zustandslos und stellen definierte Einsprungspunkte im Deployment-Workflow für manuelle Ergänzungen bereit, wie generate, build, validate und deploy. Außerdem orchestrieren die Management-Services die einzelnen Server/Publisher- und Client/Subscriber-Instanzen mittels einer zentralen Laufzeitinstanz, z.B. create, start, stop, supervise, update sowie delete. Das Framework wird testgetrieben entwickelt und die Entwickler suchen noch Kooperationspartner, die sich an der Weiterentwicklung beteiligen. Derzeit arbeitet das talsen team in Kooperation mit dem Maschinenbauer Zuwa-Zumpe gemeinsam an einem realitätsnahen Anwendungsfall. Bei diesem wird APPIO eingesetzt um intelligente Pumpen flexibel zu vernetzen und zu steuern. ■

Sebastian Sessler,
Head of Business Development,
Talsen Team GmbH
www.talsen.team

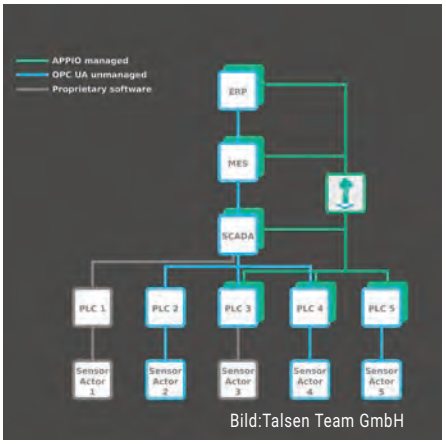
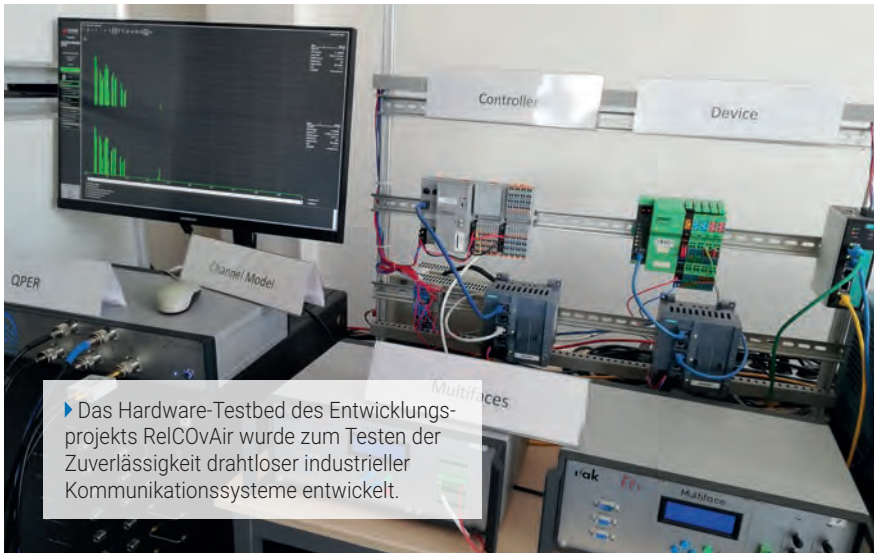


Bild:Talsen Team GmbH

Über das neue Framework sollen OPC-UA-Netzwerke wandelbar und anpassungsfähig gemacht werden.

Soft- und Hardware-Testbed

Testsystem für die drahtlose Industrie-kommunikation



Das Hardware-Testbed des Entwicklungsprojekts RelCOvAir wurde zum Testen der Zuverlässigkeit drahtloser industrieller Kommunikationssysteme entwickelt.

Im Celtic-Plus-Projekt 'Reliable Industrial Communication Over the Air (RelCOvAir)' wurde unter Leitung des Fraunhofer IIS ein neues Testsystem für drahtlose Industriekommunikationssysteme entwickelt. Es setzt sich aus einem soft- und einem hardwarebasierten Testbed zusammen. Dabei handelt es sich um prototypische Lösungen zur Kontrolle der Leistungsfähigkeit von Übertragungssystemen.

Im ersten Schritt hat das Projektteam tatsächliche Kanaleigenschaften und störende Funksignale im typischen Industrieeinsatz untersucht. Die Ergebnisse sind in ein realitätsnahes Funkausbreitungsmodell eingeflossen. Der Anwender kann mit dem Software-Testbed spezifische Kanalcharakteristiken zunächst auf simulierte Computermodelle drahtloser Kommunikationssysteme anwenden. Über die Hardware-Testumgebung mit dazugehörigem Kanalsimulator kann dann echte Hardware getestet werden.

Realistische Bewertung

Mit dem Testsystem kann das Verhalten drahtloser Systeme in industriellen Umgebungen von Anfang an realistisch bewertet werden. Zudem soll das System Unternehmen dabei unterstützen, durch standardisierte Systeme und Kriterien mit geeigneten Testbeds ein Übertragungssystem passend für ihren Einsatzbereich auszuwählen. ■

Dipl.-Ing. Thomas Heyn, Gruppenleiter Connectivity, Fraunhofer IIS
www.iis.fraunhofer.de

Bild: ©Andrea Dieguez

Die großen Vorteile von Time-Sensitive Networking

Viel mehr als nur Geschwindigkeit

TSN stellt für industrielle Netzwerke eine deutliche Steigerung der Performance in Aussicht. Doch die Erweiterung des Ethernet-Standards ausschließlich auf neue Eigenschaften bei Geschwindigkeit und Durchsatz zu reduzieren, ist viel zu kurz gegriffen. Davon ist Dr. Thomas Holm überzeugt. Der Innovations-Chef bei Wago zeigt im INDUSTRIAL COMMUNICATION JOURNAL auf, wo weitaus schwerer wiegende Vorteile von Time-Sensitve Networking liegen.

Die aktuellen Erweiterungen des Ethernet-Standards, die gemeinhin als TSN bekannt sind, sind sehr vielseitig und bieten der Automatisierung große Vorteile. Sie haben sogar das Zeug, einen echten Paradigmenwechsel in der industriellen Kommunikation einzuleiten. Dennoch wird regelmäßig und öffentlichkeitswirksam vor allem die steigende Übertragungsgeschwindigkeit und Leistung in den Vordergrund gestellt. Welche entscheidenden Vorteile TSN darüber hinaus für die Industrie bereit hält, kommt in der Diskussion und Berichterstattung meines Erachtens oft zu kurz.

Der Blick auf das Ganze

Viele namhafte Player der Automatisierung konzentrieren sich zu stark auf die Performance-Zuwächse. Stattdessen muss man das Konzept der Ethernet-Erweiterung und die Vision dahinter ganzheitlich betrachten. Dann merkt man schnell, welche grundliegenden Veränderungen TSN für die Kommunikationstechnik mitbringt. Erst wenn es möglich ist, dass Geräte über Standard-Ethernet mit TSN-basierten Produktionsstrukturen kommunizieren, lässt sich auch wirklich die klassische Automatisierungspyramide mit ihren auf die Ebenen gekapselten Technologien auflösen. Ein Ansinnen, dass ja seit einigen Jahren immer im gleichen Atemzug mit Industrie 4.0 genannt wird. TSN bietet also die Basis, damit aus der Feldebene heraus direkt an jedes Gerät auf anderen Ebenen kommuniziert werden kann, ohne wie bisher auf Gateways zugreifen zu müssen oder die Kommunikationstechnologien komplett zu verändern. Natürlich bringt die Durchgängigkeit einer solchen Netzwerkinfrastruktur auch neue Herausforderungen mit sich, z.B. in Bezug auf IT-Security oder funktionale Sicherheit. Aber sie ist im Endeffekt eine der Schlüsselfertigkeiten von TSN – und als Mehrwert deutlich höher anzusetzen, als irgendwelche Performance-Zuwächse, die die überwiegende Mehrheit der Applikationen heute wie in Zukunft überhaupt nicht benötigt.

Thomas Holm, Wago

> *TSN an und für sich ist richtig und gut – wirklich mächtig wird es aber erst im Zusammenspiel mit OPC UA.*

Die Macht des Zusammenspiels

Ein weiterer essenzieller Punkt beim Thema TSN: Die Erweiterung von Ethernet an und für sich ist richtig und gut – wirklich mächtig wird sie aber erst im Zusammenspiel mit OPC UA. Weil Wago neben der bereits angesprochenen Offenheit der Fertigungsnetze vor allem die Kombination mit OPC UA – als dem semantischen Counterpart von TSN – als besonders wertvoll und zielführend betrachtet, sind wir auch in der FLC-Arbeitsgruppe (Field Level Communication) der OPC-Foundation sehr aktiv. Denn schlussendlich findet sich im Zusammenspiel von deterministischer Kommunikation und einheitlicher Semantik der Missing Link für viele Zukunftsfragen der Automatisierung. Es ist u.a. der Enabler dafür, dass sich Geräte, Maschinen und Anlagenteile künftig selbst beschreiben, untereinander verstehen und automatisch passend konfigurieren. Das wiederum ist eine Voraussetzung dafür, dass der modulare Ansatz im Maschinen- und Anlagenbau in der Praxis tatsächlich zum Fliegen kommen kann.

Die Standards der Anderen

Trotz aller Offenheit, die TSN zugeschrieben wird, sprechen die Nutzerorganisationen und die dahinter stehenden Automatisierungsanbieter der Verzichtbarkeit ihrer proprietären Standards überwiegend ab. In wie weit Ethernet-ba-

Bild: Wago Kontakttechnik GmbH & Co. KG

sierte Kommunikationsstandards wie Profinet oder Ethercat weiterhin ihre Daseinsberechtigung behalten, ist aus heutiger Sicht schwer einzuschätzen. Sicherlich werden sie aber noch auf absehbare Zeit weiterbestehen. Schließlich sind an der Entwicklung von TSN und deren Adaption auf die Automatisierung sehr viele Stakeholder beteiligt, auch die Vertreter der heute etablierten Industrial-Ethernet-Derivate. Alle Parteien versuchen dabei, den TSN-Standard entsprechend zu prägen, um ihn mit den eigenen bestehenden Strukturen bestmöglich zu kombinieren. Und so geht es in den entsprechenden Spezifizierungsgremien manchmal leider weniger um technologische Fragen als um solche der Auslegung und Kompatibilität – sprich um herstellerspezifische Interessen.

Die Profile der Automatisierung

In jedem Fall bin ich überzeugt, dass TSN in der Industrie sehr umfangreich zur Anwendung kommen wird. Wie genau, das steht ein Stück weit noch in den Sternen. Einen großen Teil zur Aufklärung beitragen wird die IEC60802, die auf Basis von Anwendungsszenarien in der Industrie TSN-Profile für die Automatisierungstechnik beschreiben soll. Sie wird definieren, was TSN für die einzelnen Ebenen eigentlich bedeutet und auch, welche Mechanismen und Standards die Automatisierungshersteller bei ihren künftigen Lösungen einhalten müssen. Damit entscheidet die Norm letztendlich auch, wie einfach oder kompliziert die Einbindung von Standard-Ethernet-Geräten und -Strukturen aus anderen Unternehmensbereichen in die Produktion umsetzbar wird. In der IEC60802 liegt also in gewisser Weise die Gretchenfrage in Sachen Kompatibilität. Ebenso wird sie zum Schlüssel, der die automatisierungsrelevanten Bestandteile im Technologiebaukasten von TSN hervorhebt und den Nutzern an die Hand gibt. Denn die Industrieanwender werden mitnichten alle Möglichkeiten der Ethernet-Erweiterung durch TSN brauchen können.

> *Für Maschinenbauer und Fertigungsunternehmen ist es jetzt an der Zeit, sich mit dem Thema TSN ernsthaft auseinanderzusetzen.*

Nächste Schritte zur Marktreife

Für Maschinenbauer und Fertigungsunternehmen ist es jetzt an der Zeit, sich mit dem Thema TSN ernsthaft auseinanderzusetzen. Auch wenn die Marktdurchdringung in nächster Zeit nicht sprunghaft ansteigt ist es wichtig, die Möglichkeiten bzw. Vorteile von TSN und dessen Potenzial für die eigene Fertigung zu kennen. Aktuell besteht zudem auch noch die große Chance, sich in die Spezifizierung der Technologie einzubringen. Sehr spannend wird es in Bezug auf TSN sicherlich auch auf der SPS-Messe im November – vor allem was die Demonstratoren angeht. Wago stellt an seinem Stand die nächste Stufe einer solchen Messeapplikation aus und präsentiert, wie sich die Integration von I/O-Signalen auf TSN-Basis ohne Zeitverlust für hochsynchrone Automatsierungsnetze realisieren lässt. Die Messe bietet für uns gleichzeitig eine gute Gelegenheit, um das Anforderungsprofil der zukünftigen Wago-Controllern zu schärfen. In diesem Sinne bieten wir uns dem Maschinen- und Anlagenbau auch als Partner an, um die Technologie hinter TSN frühzeitig zu verstehen und zu beherrschen. Kurzum, man kommt heute an TSN nicht mehr vorbei – weder als Anbieter, noch als Anwender. Und um den Bogen wieder zu schließen: Natürlich werden wir auf der SPS auch die mögliche Performance-Steigerung von TSN beleuchten. Ich freue mich auf anregende Diskussionen am Wago-Messestand. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/11044

Autor: Dr. Thomas Holm,
Innovations-Chef,
Wago Kontakttechnik GmbH & Co. KG
www.wago.com

OPC UA als Standard für die industrielle Kommunikation

Sicherung der Innovationsführerschaft oder Zeitverschwendung?

Im Maschinen- und Anlagenbau fällt das Schlagwort OPC UA immer häufiger. Doch um was geht es dabei genau und welche Bedeutung hat der Kommunikationsstandard für die Branche? Aller Voraussicht nach eine sehr hohe, sind sich alle Experten einig. Stand heute bedarf es aber noch eine Menge Aufklärungsarbeit – nicht nur im Maschinenbau, sondern vor allem auch bei den Endanwendern .

Hans Egermeier (l.) und Ulrich Viethen beschäftigen sich intensiv mit OPC UA und leisten Aufklärungsarbeit in Maschinenbau und Endanwenderschaft.

Was ist OPC UA eigentlich? Das Kürzel steht für Open Platform Communications Unified Architecture und versteht sich als industrielles M2M-Protokoll, dessen Basis durch die Norm IEC62541 standardisiert ist. Dahinter stehen inzwischen 14 einzelne Basisspitzspezifikationen, jeweils mit einem ordentlichen Umfang. Wenn man berücksichtigt, dass alleine im VDMA momentan rund 40 aktive Arbeitskreise auf OPC UA aufbauende Spezifikationen definieren, wird deutlich welche Bedeutung die Branche dem Standard zuschreibt.

Mächtige Kombination

Das liegt an verschiedenen Eigenschaften: Im Gegensatz zum Vorgänger OPC kann das Protokoll Maschinendaten nicht nur transportieren, sondern auch maschinenlesbar semantisch beschreiben – was als Grundlage für die automatische M2M-Kommunkation der Zukunft gilt. Eine zweite wichtige Besonderheit ist, dass das Übertragungsprotokoll serviceorientiert aufgebaut ist. „Das bedeutet: Es wurden moderne Softwaremechanismen genutzt, um das System möglichst lange Zeit skalierbar und veränderbar zu machen", erklärt Dr. Hans Egermeier, Geschäftsführer des Ingenieurbüros Lean DT und der Softwareschmiede Talsen Team, den daraus resultierenden Nutzen. Aktuell ist der Kommunikationsstandard und die dahinter stehenden Möglichkeiten aber noch nicht überall angekommen. „Die Selbstverständlichkeit, mit der Anbieter von Automatisierungslösungen über OPC UA reden, gibt es bei den meisten Anwendern und Produktionsunternehmen noch nicht", betont Dr. Ulrich Viethen, Unternehmensberater und ehemaliger Geschäftsführer des Antriebsherstellers AMK. „Vielfach ist OPC UA dort noch überhaupt kein Begriff. Fragt man heute die Maschinenbauer, wer bereits große Erfolge mit OPC UA errungen hat, oder wen der Standard OPC UA schon zum Innovationsführerschaft gemacht hat, dann sind die Stimmen noch verhaltener."

Wie offen ist OPC UA?

OPC UA wird von der dahinter stehenden Organisation, der OPC Foundation, als komplett offener Standard propagiert. Aber was heißt das eigentlich genau? Offiziell lautet die Definition: Ein offener Standard bezieht sich auf ein Format oder Protokoll, das:

- einer vollständig öffentlichen Bewertung und Nutzung ohne Hemmnisse auf eine für alle Beteiligten gleichermaßen zugänglichen Weise unterliegt,
- ohne jegliche Komponenten oder Erweiterungen ist, die von Formaten oder Protokollen abhängen, die selbst nicht der Definition eines offenen Standards entsprechen,
- frei ist von juristischen oder technischen Klauseln, die seine Verwendung von jeglicher Seite oder jeglichem Geschäftsmodell einschränken,
- unabhängig von einem einzelnen Anbieter geleitet und weiterentwickelt wird in einem Prozess, der einer gleichberechtigten Teilnahme von Wettbewerbern und Dritten offen steht,
- verfügbar ist in verschiedenen vollständigen Implementierungen von verschiedenen Anbietern oder als vollständige Implementierung gleichermaßen für alle Beteiligten.

Roundtable Mensch und Mechatronik

Dieser Artikel geht auf einen Vortrag beim letzten Expertenkreis Mensch und Mechatronik zurück. Die Veranstaltung fand bei Phoenix Contact und Trumpf statt und beschäftigte sich mit verschiedenen aktuellen Kommunikationsthemen. Neben OPC UA wurden auch IO-Link sowie Cloud-Konzepte für den Maschinenbau besprochen. Die Roundtable-Runde – teils Automatisierer, teils Maschinenbauer, teils Berater – wurde von ITQ initiiert und trifft sich bereits seit über zehn Jahren regelmäßig zur Diskussion aktueller Trends in der industriellen Fertigung.

Insgesamt gibt es wohl nur wenige existierende Beispiele, die diesen Anforderungen vollständigen genügen. Die meisten so genannten offenen Standards rangieren in einer gewissen Grauzone – und sind dennoch als solche erfolgreich. Im Gegensatz zu vielen bereits in der Automatisierung vorhandenen und als offen bezeichneten Standards kann OPC UA den aufgeführten Kritierien gerecht werden – zumindest im Wesentlichen. Natürlich hat OPC Foundation gewisse Zugangsbeschränkungen für OPC UA definiert, und auch im Rahmen der aktuell entstehenden Spezifikationen kann nicht jeder tun und lassen was er will. Es werden schon einige Regeln vorgegeben. Ganz frei von technischen Klauseln sind entsprechende Lizenzen im Umfeld von OPC UA auch nicht. In jedem Fall hat OPC UA das Zeug dazu – im Vergleich zu den bisherigen Feldbus- und Industrial-Ethernet-Standards – ein neues Level der Offenheit in die industrielle Kommunikation zu tragen. „Ob OPC UA in Sachen Offenheit schon der Weisheit letzter Schluss ist, lässt sich aus heutiger Sicht schwer sagen", sagt Viethen. „Aber es ist ein sehr großer Schritt in die richtige Richtung." Egermeier ergänzt: „Ein Standard kann ja überhaupt nur dann wirklich offen sein, wenn Unternehmen, die im harten Wettbewerb stehen, gleichermaßen in ihn investieren." Das scheine bei OPC UA aktuell der Fall und gleichzeitig die Voraussetzung für dessen Erfolg in der Automatisierung.

OPC UA als dynamisches System

Konzeptionell handelt es sich bei OPC UA um ein dynamisches System, das sich stetig weiterentwickeln und ergänzen lässt. „Eine Software, die nicht laufend weiterentwickelt wird, ist aus technischer Sicht tot", bringt es Egermeier auf den Punkt. „Aber man hat in der IT längst Mechanismen gefunden, um trotzdem für die praktische Anwendung eine hohe Schnittstellenstabilität zu garantieren." So sei OPC UA in Hinsicht auf möglichst geringe Versionsabhängigkeit sehr clever aufgebaut. Doch die hohe Flexibilität birgt nicht nur Vorteile. Denn OPC UA ist nicht immer gleich OPC UA – es handelt sich ja letztlich um eine Sammlung verschiedener Features. Es ist also nicht pauschal sichergestellt, dass ein OPC-UA-fähiges Gerät auch alle Dienste eines anderes nutzen oder verstehen kann bzw. der Datenaustausch reibungslos klappt. „Hier handelt es sich in der Tat um ein verbreitetes Missverständnis", führt Egermeier aus. „Um die gesamte Bandbreite der industriellen Kommunikation abzudecken, kann der Standard in Gänze ungemein viel." Aus diesem Block werde von den jeweiligen Geräteherstellern aber oft nur der benötigte Teil an Services implementiert. Diese Tatsache kann dann in der Praxis gegebenenfalls zu Kompatibilitätsproblemen führen.

Fünf Thesen für OPC UA

Ulrich Viethen und Hans Egermeier haben zum künftigen Stellenwert von OPC UA die folgenden fünf Thesen formuliert. Sie werden in den nächsten Ausgaben des SPS-MAGAZINs auch nochmals einzeln behandelt.

- **These 1:** Offene Standards sind von strategischer Bedeutung im Wettbewerb zur Erzeugung der notwendigen Produktflexibilität für den Maschinenanwender und damit gleichermaßen für den Maschinenbauer.
- **These 2:** Für die Rationalisierung und Wartbarkeit werden große Softwaresysteme architekturell in Fraktale zerlegt. Die Standardisierung ist für die Wirtschaftlichkeit komplexer werdenden Produktionsanlagen entscheidend.
- **These 3:** Durch die Cloud wird die Marktrelevanz des Maschinenbauers zukünftig entschieden. Die industrielle M2M-Kommunikation bis hinunter zu Sensor und Aktor wird in der Cloud Kundenmehrwert erzeugen.
- **These 4:** OPC UA ist der derzeit umfassendste Wandlungsbefähiger im Sinne der industriellen, herstellerunabhängigen M2M-Kommunikation. Derzeit ist keine vergleichbare Alternative zu OPC UA für den Maschinenbau absehbar.
- **These 5:** OPC UA wird auf der IT-Seite die Bedeutung der DIN933 (Gewindeschraube) für die Automatisierungstechnik erlangen. Ein technischer Vendor Lock-in kann in Zukunft nicht mehr akzeptiert werden. *(mby)* ■

Ingenieurbüro Lean-Digital-Transformation
www.lean-dt.com

Echtzeit-Kommunikation mit Varan für Stickereimaschinen

Stich für Stich

Edle Stickereien verleihen Stoffen und Kleidungsstücken ein exklusives und individuelles Aussehen. In diesem Sinne entwickelt und produziert das Schweizer Unternehmen Lässer seit 1982 Stickmaschinen. Für die Systemkommunikation in harter Echtzeit setzt das Unternehmen auf das Echtzeit-Ethernet-Bussystem Varan.

Bei den Stickmaschinen von Lässer sorgt ein durchgängiges Steuerungs- und Antriebskonzept mit Echtzeitkommunikation über Varan für hohe Qualität.

Erfunden haben die Schweizer die Stickerei zwar nicht – das waren die Ägypter und Chinesen schon rund 5.000 v. Chr – aber die erste automatische Stickmaschine kam aus der Schweiz, die sogenannte Schifflimaschine. Sie wurde im Zuge der ersten industriellen Revolution Mitte des 19. Jahrhunderts von Isaak Groebli entwickelt. Deren Prinzip ähnelt dem einer klassischen Nähmaschine und ist bis heute praktisch unverändert, der Begriff Schiffli wird in der Branche längst weltweit verwendet. Das Portfolio von Lässer reicht von kleinen Stickmaschinen bis zu großen Anlagen mit vielen Extraoptionen. Dabei setzt Lässer durchgängig auf ein modulares Automatisierungssystem von Sigmatek mit schneller und sicherer Systemkommunikation über den Echtzeit-Ethernet-Bus Varan.

Hohe Performance

Für die bis zu 30m lange Hochleistungsstickmaschine MVD71 Multidrive wird als Hauptrechner ein PC-341-L von Sigmatek eingesetzt. Mit Dual-Core-Prozessor verfügt er über die hohe Performance, die für den aufwändigen Stickprozess benötigt wird. Die Steuerung beinhaltet zwei Varan-Echtzeit-Ethernet-Manager. Einerseits für die Kommunikation mit den dezentralen I/Os und anderseits für das Antriebssystem. Speziell bei solch dynamischen Anwendungen kann das Protokoll seine Vorteile ausspielen. Mit Varan ist es möglich, Drives mit je 16 Byte Ist- und Soll-Werten mit einem einzigen Schreib/Lese-Befehl in 5µs zu aktualisieren. Eine MVD71-Stickmaschine erledigt bis zu 720 Stiche pro Minute. Auf die Zykluszeit gerechnet bedeutet dies, dass der Stickprozess gerade mal 80ms dauert. In den ersten 40ms wird der schwere Stickrahmen positioniert, auf dem der Stoff aufgespannt ist. In der zweiten Hälfte des Zyklus wird der Stich ausgeführt. Dazu müssen sich Nadel und das Schiffli synchron bewegen. Die Positionierung muss exakt erfolgen. Ungenauigkeiten würde man im Stickmuster mit bloßem Auge erkennen. Der Hauptantrieb, der ebenfalls mehrere Servoachsen umfasst, bewegt Nadeln und Schiffli. Weiter werden der Stoffdrücker, die Fadenwalze und der Bohrer von einem oder mehreren Drives angetrieben. Zudem sind zwei Antriebe für das Aufwellen des Stoffes im Einsatz. Bei einer Maschine mit zusätzlichen Optionen kommen weitere Antriebe dazu. Je nach Maschinenlänge und Konfiguration spielen bis zu 16 Drives zusammen, die über Varan präzise angesteuert und synchronisiert werden.

Sicherer Datenaustausch

Mit Varan erfolgt der Datenaustausch nicht nur schnell sondern auch sicher. Jedes vom Manager gesendete Datenpaket wird unmittelbar vom Client rückbestätigt. Antwortet dieser innerhalb der vereinbarten Timeout-Zeit nicht, oder ist die Antwort fehlerhaft, wiederholt der Manager bis zum Erhalt einer gültigen Rückbestätigung den Befehl, ohne den Nachrichtenzähler zu erhöhen. Dadurch erkennt der Client den Befehl als Wiederholung. Diese Vorgangsweise stellt sicher, dass am Ende des Buszyklus alle Prozessdaten konsistent sind. Die permanente Überprüfung der Datengültigkeit wird durch die kleinen Daten-Frames möglich – selbst bei Zykluszeiten unter 100µs.

Schnelle Reaktion

Damit die MVD71 von Lässer ihre Stickmission einwandfrei erfüllt, sind bis zu 1200 I/Os im Einsatz. Jeder Faden wird überwacht. Bei Fadenbruch stoppt die Maschine augenblicklich. Anhand der Fehlermeldung und einer LED, die den Zustand jedes Fadens farblich darstellt, erkennt die Bedienperson sofort, welcher Faden gerissen ist. Für die Überwachung der Fäden ist eine von Sigmatek für Lässer entwickelte Platine mit eigenem Controller zuständig. Auf dieser werden jeweils mehrere Stickstellen zu einer Einheit zusammengefasst und überwacht.

Nahtlose Integration

Die für den Betrieb einer modernen Stickmaschine geforderte Funktionalität ist sehr vielfältig. „Bei der Sigmatek-Lösung sind alle für die Applikation nötigen Funktionen nahtlos integriert“, erklärt Reto

Bilder der Doppelseite: Sigmatek GmbH & Co KG

Durch Industrial Ethernet Varan werden Präzision, Verfügbarkeit und Effizienz der Flachbett-Stickmaschinen deutlich erhöht.

Spirig, Entwicklungsleiter Steuerungssystem bei Lässer. „Diese Durchgängigkeit von Steuerung, Visualisierung, Motion Control, Safety, Engineering und Echtzeitkommunikation über Varan vereinfacht und verkürzt die Realisierung des Maschinenkonzeptes." Mit Einsatz des Bussystems kann auf aufwändige, diskrete Verkabelungen für Sicherheitskreise verzichtet werden. Die sicherheitsrelevanten Signale werden zeitgleich mit den Prozessdaten übertragen. Das Varan-Protokoll dient dabei als Container für die Safety-Telegramme und arbeitet nach dem Black-Channel-Prinzip. Das Bussystem ist bei den Sicherheitsbetrachtungen ausgeschlossen, wodurch die Weiterleitung der Safety-Daten über die Rückverdrahtung oder andere Transportmedien uneingeschränkt möglich ist.

Flexibel und offen

Bustopologien lassen sich mit Varan einfach und flexibel in Baum-, Stern- und Linienstruktur aufbauen. Es ist möglich, mehrere Systeme durch einen übergeordneten Manager zu einem synchronen Gesamtnetz zu kaskadieren. Dadurch entsteht eine Multi-Manager-Struktur. Die Synchronisation der Teilnetze erfolgt vollautomatisch mit einem Jitter <100ns. Einzelne Systeme können während des laufenden Betriebs an- und abgekoppelt werden. Netzwerk-Splitter bieten die Möglichkeit, das Varan-System mit Firmennetzen oder anderen Ethernet-Systemen zu verbinden. Der Manager stellt Prozess- und Servicedaten zur Verfügung, die netzübergreifend ausgetauscht und über OPC UA auch an höhere Ebenen oder in die Cloud transportiert werden können. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/9635

David Eisl,
Technologie-Berater VNO,
Varan-Bus-Nutzerorganisation
www.varan-bus.net

Feldbusemulation in der kompletten Anlage

Simulation und Kommunikation

Im Maschinenbau und in der industriellen Automatisierungstechnik spielt die Time-to-Market eine Schlüsselrolle für den Unternehmenserfolg. Diejenigen, die es schaffen, den für die Entwicklung erforderlichen Zeitaufwand zu reduzieren, ohne Kompromisse bei der Qualität einzugehen, sind gegenüber Wettbewerbern klar im Vorteil. Wichtig sind besonders eine einfache Implementierung und ein intensiver Test verteilter Automatisierungslösungen – und deren Kommunikation.

Machineering bietet mit der Simulationssoftware IndustrialPhysics die Möglichkeit, eine virtuelle Inbetriebnahme zur Absicherung von Automatisierungssystemen durchzuführen. Zudem steht mit der Field Box 1 Herstellern und Anlagenbetreibern eine Emulation für Profinet, Ethernet/IP und Ethercat zur Verfügung. In dieser Feldbusemulation werden Nachrichten von nicht vorhandenen Geräten nachgebildet. Damit kann die Echtzeitkommunikation im kompletten System getestet werden, ohne dass das Feldbusnetz werden muss.

Prozessbegleitende Simulationssoftware

Mit der Simulationssoftware IndustrialPhysics lassen sich komplexe, mechatronische Anlagen und Roboter über den gesamten Prozess von der Planung bis zum Servicefall einfach, schnell und realistisch simulieren. Testläufe der erstellten SPS-Programme können zudem genau überprüft werden. Änderungen des dynamischen Verhaltens der Anlage sind aufgrund der physikbasierten Simulation sofort sichtbar. Die dadurch mögliche virtuelle Absicherung verringert Standzeiten, ermöglicht Variationen am Modell und spart so Zeit und Geld. Auch nach der Fertigstellung der Anlage können im laufenden Betrieb Anpassungen im Vorfeld simuliert werden bevor diese auf die reale Maschine übertragen werden.

Echtzeitfähigkeit via Plug&Play

Die Field Box kann entweder direkt auf dem Schreibtisch oder auch im Test Rack für die Anbindung an eine reale Steuerung eingesetzt werden. Angebunden an die Simulationssoftware wird sie lediglich via

Weil die Feldbusemulation immer wichtiger wird, bietet Machineering mit der Ultimate-Variante seiner Simulationssoftware IndustrialPhysics die Field Box standardmäßig im Bundle an.

Plug&Play mit dem Rechner bzw. der Steuerung verbunden und ist sofort einsatzbereit. Dabei kann es sich um reale oder auch virtuelle Steuerungen handeln. So können in frühen Phasen unterschiedliche Steuerungen getestet werden – erst später muss sich der Anwender wirklich entscheiden. Der große Vorteil gegenüber der klassischen virtuellen Inbetriebnahme ist dabei, dass die Feldbusemulation keine Ressourcen des Simulationsrechners nutzt. Sie findet vielmehr komplett extern in der Field Box statt. Somit entfallen Änderungen an der SPS, die bisher zusätzlich den sogenannten ComTCP-Client implementieren musste.

Emulation wird immer wichtiger

Weil gerade die Feldbusemulation für Unternehmen immer wichtiger wird, bietet Machineering mit der Ultimate-Variante seiner Simulationssoftware die Field Box standardmäßig im Bundle an. Mit einer Systemzykluszeit von 100µs werden Reaktionszeiten unter 1ms bei wenigen Geräten, z.B. in einer Werkzeugmaschine, bis hin zu mehreren ms bei einem großen Automatisierungsnetzwerk bspw. einer Fördertechnikanlage erreicht. Mit der Field Box 1 kann ein Maschinenmodell, das direkt auf den mechanischen CAD-Daten basiert und das Maschinenverhalten mit Prozessgut realistisch nachbildet, ganz einfach um die Echtzeitkommunikation auf Feldbusebene erweitert werden. Mittlerweile ist es sogar möglich, auch Antriebe nachzubilden und damit deren realistisches Verhalten gegenüber der SPS darzustellen. Neben Profinet sind auch Ethernet/IP sowie Ethercat per Konfiguration in der Field Box 1 aktivierbar und damit eine synchrone bzw. auch asynchrone Kommunikation möglich.

Antriebsbibliothek und Echtzeitfähigkeit

Wie bereits für die Roboterbibliothek umgesetzt, entwickelt Machineering parallel eine Bibliothek für diverse Antriebssysteme. Mit den Standardimplementierungen von Antriebsmodellen, wird dem Maschinenbauer die Arbeit abgenommen, realistische Modelle mühsam selbst nachzubilden. Die Bibliothek enthält gängige Antriebe, weitere können auf Anfrage integriert werden. Zudem haben fortgeschrittene Anwender die Möglichkeit, über einen Plugin-Mechanismus eigene Antriebsbibliotheken zu realisieren und so auch Spezialanpassungen abzubilden. Besonders die Echtzeitfähigkeit wird immer entscheidender für die Unternehmen. Deshalb können Anwender eine Ultimate-Lizenz von IndustrialPhysics mit der Field Box zur Erstellung der kompletten Simulationsmodelle nutzen. Zusätzlich kann der Anwender mehrere separate Field Boxes mit der Runtime RT einsetzen. So entstehen SPS-Teststände, an denen fertige Maschinenmodelle zusammen mit Steuerungen oder eben Antrieben während der Programmierung und auch im Dauerlauf getestet werden können. So erstellt z.B. Anwender mittels der Vollversion jeweils projektbezogen neue Maschinenmodelle und gibt diese an die SPS-Teststände mit IndustrialPhyiscs Runtime RT weiter. Hier kann – quasi auf dem Trockendock – die SPS-Software angepasst oder fertig entwickelt und getestet werden, ohne dass der Entwickler das Haus verlassen muss.

Mittler zwischen SPS und Feldgeräten

Die Field Box vermittelt also in Echtzeit zwischen dem I/O-Abbild des gesamten Maschinenmodels in einer SPS und den verteilten Einzel-I/O-Abbildern aller Feldgeräte. Die SPS – egal ob real oder nur virtuell – kann so z.B. mit 30 optionalen Geräten kommunizieren, diese abfragen und testen. Ein normales Simulationsmodell läuft mit einer Abtastrate von 5 bis 10ms für die meisten mechanische Vorgänge. Feldbussysteme wie Profinet, Ethernet/IP oder Ethercat dagegen haben Reaktionszeiten im ms-Bereich und weit darunter. Mit dem erforderlichen Rechenaufwand, der für diese Auflösung erforderlich ist, sind herkömmliche Rechner schnell überfordert und mit ihrer Mehrkernarchitektur gleichzeitig überdimensioniert. Da die Feldbusemulation vollständig von der Field Box 1 übernommen wird, kann diese Funktion einem Simulationsmodell einfach mit dem Gerät hinzugefügt werden. Die Modelle werden so auf einer normalen Workstation oder einem Laptop erstellt und dann mit der Field Box auf die Feldbusebene erweitert. IndustrialPhysics weiß, wie die Field Box parametriert werden soll. Viele der notwendigen Informationen sind standardmäßig bereits integriert. So sind die komplette Hardwarekonfiguration sowie umfassende Importfilter aus den Steuerungsumgebungen bereits enthalten. ■

Dr. Georg Wünsch,
CEO von Machineering,
Machineering GmbH & Co. KG
www.machineering.de

Bild: Machineering GmbH & Co. KG

4G-Kommunikation sichert Trinkwasserversorgung

Retrofit für mehr Zuverlässigkeit

In kritischen Anwendungen spielt eine zuverlässige Datenübertragung eine enorm wichtige Rolle, umso mehr als wenn wegen weiter Distanz Funklösungen unvermeidbar sind. Kommt die Infrastruktur in die Jahre, ist die Sicherheit aber oft nicht mehr gegeben, wie das folgende Beispiel aus der Trinkwasserversorgung zeigt. Modernisierungsmaßnahmen und die Kombination aus altbewährter Struktur und neuer Technik schaffen dann Abhilfe.

Die Firma Quantum ist auf Engineering-und Automatisierungsservices für die industrielle und gewerbliche Fertigung spezialisiert. Das Angebot richtet sich auch an viele Industriezweige mit geographischen Außenstandorten wie Bergbau, Energieerzeugung oder Abwasser. Unabhängig von der Entfernung sind diese Branchen auf ständige Kommunikation angewiesen. Deswegen bietet Quantum seit vielen Jahren Lösungen, um drahtlose Funkgeräte ohne Lizenz entweder seriell oder über Ethernet zu verbinden.

Verzögerung im Datenverkehr

Mit dem Aufkommen von Ethernet-verbundenen Geräten können bestimmte Frequenzen, einschließlich der 900MHz-Funkkommunikation, keinen schnellen Ethernet-Verkehr mit hoher Bandbreite mehr unterstützen. Diese Geräte erreichen nur eine maximale Datenrate von 1024kBit/s, was im Vergleich zu Wi-Fi (802.11) und 4G/LTE-Datenraten sehr langsam ist. Das kann zu einer verzögerten Übermittlung dringend benötigter Daten führen, z.B. Alarme oder Überwachungsbefehle. Die Herausforderung vergrößert sich zudem durch Funk-Repeater, ineffiziente SPS-Messaging-Schemata, flache Netzwerke oder übermäßige Abfrageraten. Eine Situation, die für kritische Anwendungen natürlich nicht tragbar ist. Deswegen müssen solche Missstände in vielen Fällen durch den Übergang zu 4G/LTE- oder WLAN-Netzen und die daraus entstehenden robusten drahtlosen Kommunikationsinfrastruktur behoben werden.

Pipeline sichert Wasserversorgung

In einem konkreten Projekt ging es um die kilometerlange Pipeline einer Gemeinde, die zwei weitere Städte durchquert, um Wasser an eine Aufbereitungsanlage zu liefern. Entlang der Versorgungslinie befinden sich vier Schranken für Pumpstationen, die den Wasserfluss steuern und überwachen. Für die Kommunikation innerhalb der 18km waren sechs 900MHz-Funkgeräte im Einsatz, damit die einzelnen Steuerungen und die Aufbereitungsanlage in Kontakt bleiben. Seit Einführung der ursprünglichen Lösung hatte das städtische Wachstum die Leistung des Mobilfunkanbieters zunehmend beeinträchtigt. Es gab auch zusätzliche Hindernisse, einschließlich eines Höhenunterschieds von 650° zwischen der ersten Steuerung und der Aufbereitungsanlage. Eine inkonsistente und unzuverlässige Kommunikation machte es nahezu unmöglich, die vier Pumpstationen fernzusteuern. Die Probleme waren so dringlich, dass sie ein erhebliches Risiko für die Wassererzeugung und -lieferung darstellten. Das Unternehmen Quantum hat die Stadt bei dem Retrofit-Projekt beraten und empfohlen, zur Kommunikation auf ein 4G LTE- Mobilfunknetz umzusteigen.

Kombination aus alt und neu

Um die Probleme zu lösen und das neue Kommunikationssystem zu ermöglichen, war es nötig, die vorhandene Infrastruktur mit moderner Technik zu kombinieren. Dies erforderte nicht nur die 4G/LTE-Ausrüstung, sondern auch Multi-Carrier-Mobilfunk-RTUs mit GPS und Steuerung. Diese lieferte Red Lion mit dem Modell RAM 6000, das für die erweiterte Steuerung und Kommunikation zur Überwachung von Remote-Assets entwickelt wurde. Die RTUs bieten bis zu fünf Ethernet-Ports und einen seriellen RS232-Port. Sie verfügen zudem über eine webbasierte Event-Engine, die integrierte I/O-Vorgänge auslösen oder SMS-Nachrichten basierend auf Echtzeitdaten senden. Seit der Implementierung des neuen Netzwerks, muss sich die Stadt bezüglich einer ineffizienten Funkinfrastruktur keine Sorgen mehr machen. Sie verfügt jetzt stattdessen über ein zuverlässiges Kommunikationssystem, mit dem sich jede RTU-Schranke aus der Ferne nahtlos überwachen lässt. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/F/37013

Laetitia Donovan,
Director Global Marketing Communication,
Red Lion Controls
www.redlion.net

Dauerhaft fit für Industrie 4.0

Sicherer Zugriff auf Daten und Maschinen

Im Zuge der Digitalisierung wollen Unternehmen aus Zeit- und Kostengründen ihre Prozesse immer weiter vernetzen. Die Smart Machinery Gateways von Insys icom sollen diese Vernetzung sicher und kosteneffizient ermöglichen und Maschinen und Anlagen dauerhaft fit für Industrie 4.0 machen. Dabei integrieren sie Industriestandards und -protokolle wie OPC UA oder Siemens S7/S5.

Die Lösung von Insys icom besteht aus IoT-Gateways zur Datenanbindung von Maschinen. Sie gewähren laut Hersteller unterschiedlichen Benutzern einen kontrollierten, sicheren Zugriff auf die Maschinen und deren Daten. Anwender können so über den gesamten Lebenszyklus ihrer Anlagen wichtige Kennzahlen generieren und weiterverarbeiten.

Wenig Programmieraufwand

Die icom Smart Machinery Gateways binden Steuerungen und Maschinen lokal z. B. über OPC UA, Siemens S7/S5, Modbus und Codesys an und tauschen deren Daten mit MES-, ERP- und Scada-Systemen aus. Auch Bestandsanlagen lassen sich so ohne Programmieraufwand aufrüsten. Bei der Ab- und Inbetriebnahme einer Maschine können die Unternehmen mit Hilfe des Fernzugriffs Zeit sparen. Denn das Team vor Ort kann die Live-Daten einfach mit den Arbeitern im Werk teilen und die notwendigen Anpassungen direkt vornehmen.

Daten auslesen und anbinden

Im laufenden Betrieb einer Maschine werden Daten ausgelesen und Kennzahlen, wie z.B. OEE, generiert. Sie sollen Anbietern und Betreibern bei der Verbesserung ihrer Produkte und Dienstleistungen helfen. Die aktuellen Werte lassen sich selektiv an verschiedene Parteien übermitteln. Dadurch sieht jeder nur das, was er sehen darf. Auch im Bereich Wartung und Service spielt die Datenanbindung von Anlagen eine Rolle. Durch Predictive Maintenance werden Serviceeinsätze zustandsabhängig erledigt und Ausfälle vermieden. Im Falle einer Störung werden Serviceteams direkt alarmiert, um durch schnelle und zielgerichtete Fehlerbehebung die Stillstandszeiten zu reduzieren. Dabei ist ein transparenter und sicherer Fernwartungszugriff für die Service- und Diagnoseeinsätze notwendig.

Datenerfassung sowie professionelle Fernwartung

Die Komplettlösung besteht aus mehreren Komponenten. Mit diesen lassen sich verschiedene Anwendungsfälle vom Datenerfassen über Edge Computing bis zu professioneller Fernwartung umsetzen. Als Basiselement fungiert ein VPN-Router der Serien MRX, MRO, SCR und ECR. Die Gateways verfügen über das IoT-Betriebssystem Icom OS, die integrierte Rechenleistung für eigene Applikationen Icom SmartBox und die skalierbare Software zur Vernetzung und Verarbeitung von Datenpunkten Icom Data Suite. Letztere ermöglicht dem Gateway nicht nur Edge Computing, sondern macht es auch zu einem intelligenten Protokollwandler: Der Router vernetzt Maschinen

Highlights der icom Smart Machinery Gateways:

- OPC UA, Siemens S7/S5, Modbus, Codesys, MQTT
- ERP, MES, Scada, Cloudanbindung
- Condition Monitoring und Alarmierung direkt auf dem Gateway (Edge Computing)
- industrielle IT-Sicherheitsstandards
- gesicherte Fernwartung über VPN
- konfigurieren statt programmieren

Bild: Insys Microelectronics GmbH

Die zentrale Vernetzung von Maschinen und Anlagen spielt eine immer wichtiger werdende Rolle und soll z.B. über die Gateways von Insys icom ermöglicht werden.

über etablierte Industrieprotokolle wie OPC UA, Siemens S7/S5, Modbus und Codesys, verbindet diese mit MES, ERP- und Scada-Systemen oder liefert deren Daten an Clouds. Insys bietet zusätzlich die Device-Management-Lösung Icom OAM (Operations, Administration & Maintenance) an. Sie soll die Inbetriebnahme- und Rollout-Prozesse sowie den Betrieb der Gateways einfach, schnell und sicher gestalten.

Leichter Betrieb und einfache Verwaltung

Der Managed Service erleichtert beim Einsatz mehrerer Geräte den Betrieb, die Verwaltung und die Wartung. Die Web-Plattform des icom OAM liegt in einer eigenen sicheren Cloudumgebung. Sie befindet sich in einem deutschen, ISO27001-zertifizierten Rechenzentrum. Die manuelle Ausführung der Tätigkeiten würde einen hohen administrativen und personellen Aufwand bedeuten. Das kann die Produktivität und Wettbewerbsfähigkeit schwächen. Mit dem Icom OAM lassen sich hingegen Automatismen nutzen, die Fehler vermeiden sowie einen termingerechten Rollout und reibungslosen Betrieb sichern. Der Managed Service ist auf die Router und Gateways von Insys Icom ausgelegt und ermöglicht es, Updates effizient auszurollen. Das icom OAM unterstützt die Administratoren von Icom Smart Devices und soll deren Arbeit erleichtern. Je mehr Router verwaltet werden müssen, desto hilfreicher ist das icom OAM. Auch bei kleinen Anwendungen bietet es Vorteile wie Übersichtlichkeit und Effizienz sowie IT-Sicherheit. Das System überwacht die Verwaltungsvorgänge und protokolliert über ein Activity Log alle updaterelevanten Ereignisse der Geräte, z.B. die Ausführung eines Auto-Updates oder Profilaktivierung. Administratoren können Gerätedaten, wie die Seriennummer, Details zu Updates oder Firmware-Version, und die Aktivität des Routers einsehen. Neue Firmware-Updates, Zertifikate sowie Sicherheitseinstellungen und Konfigurationen lassen sich mit dem Icom OAM über mehrere Router hinweg vornehmen. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/5875

Katrin Geier,
Marketing Specialist Corporate Communication & PR
Insys icom | Eine Marke der Insys Microelectronics GmbH
www.insys-icom.com

Impressum

VERLAG/POSTANSCHRIFT:
Technik-Dokumentations-Verlag
TeDo Verlag GmbH®
Postfach 2140, 35009 Marburg

Tel.: 06421/3086-0, Fax: -380
E-Mail: info@sps-magazin.de

Internet: www.sps-magazin.de

LIEFERANSCHRIFT:
TeDo Verlag GmbH
Zu den Sandbeeten 2
35043 Marburg

VERLEGER & HERAUSGEBER:
Dipl.-Ing. Jamil Al-Badri †
Dipl.-Statist. B. Al-Scheikly (V.i.S.d.P.)

REDAKTION:
Kai Binder (Chefredakteur, kbn),
Mathis Bayerdörfer (Chefredakteur, mby),
Georg Hildebrand (ghl)

WEITERE MITARBEITER:
Bastian Fitz, Tamara Gerlach, Pascal Jenke, Christina Jilg, Theresa Klingelhöfer, Lena Krieger, Kristine Meier, Melanie Novak, Kristina Sirjanow, Florian Streitenberger, Natalie Weigel, Sabrina Werking

ANZEIGEN:
Sina Debus, Heiko Hartmann, Daniel Katzer, Markus Lehnert, Thomas Möller

ANZEIGENDISPOSITION:
Michaela Preiß
Tel. 06421/3086-0
Es gilt die Preisliste der Mediadaten 2019.

GRAFIK & SATZ:
Tobias Götze, Julia Marie Dietrich, Stefanie Hartmannshenn, Fabienne Heßler, Melissa Hoffmann, Kathrin Hoß, Ronja Kaledat, Patrick Kraicker, Ann-Christin Lölkes, Cara Richter, Nadin Rühl

DRUCK:
Offset vierfarbig
Dierichs Druck+Media GmbH & Co. KG
Frankfurter Straße 168, 34121 Kassel

BANKVERBINDUNG:
Sparkasse Marburg/Biedenkopf
BLZ: 53350000 Konto: 1037305320
IBAN: DE 83 5335 0000 1037 3053 20
SWIFT-BIC: HELADEF1MAR

GESCHÄFTSZEITEN:
Mo.-Do. von 8.00 bis 18.00 Uhr
Fr. von 8.00 bis 16.00 Uhr

ISSN 0935-0187
Vertriebskennzeichen G30449

- Anzeigen -

Ethernet in der Antriebstechnik

In der Antriebstechnik spielt die Möglichkeit zur einfachen Anbindung von oder in andere Systeme eine zentrale Rolle. Dazu werden bevorzugt Standards wie Feldbusse oder Ethernet genutzt. Auf ihrer Basis entstehen hochperformante, dezentrale Antriebslösungen.

Längst gehören industrielle Antriebslösungen auf Basis von Ethernet zum Standard in den Produktionshallen – und sie werden in Zukunft in der Anbindung von Antrieben immer wichtiger. Im Vergleich mit klassischen Feldbussen erreichen sie Kommunikationsraten, die häufig um Faktor 10 höher liegen. Die hervorragenden Echtzeiteigenschaften sowie die Verarbeitung großer Datenmengen erlauben schnellere Regelungen und damit verbunden nicht nur eine höhere Ausbringung einer Maschine oder Anlage sondern auch eine höhere Produktqualität – beides Faktoren, die bekanntermaßen immer sehr gefragt sind. Von Bedeutung ist aber auch die Tatsache, dass durch die schnelle Kommunikation die Umsetzung schneller dezentraler Antriebskonzepte erst möglich wird. *(kbn)* ■

Unsere Produktübersichten finden Sie auch online unter:
www.sps-magazin.de/pues

Automatisiert geprüft

I/O-System deckt vielseitige Anforderungen ab

Auf der Suche nach der passenden Automatisierung für Prüfanlagen liegt eine Herausforderung darin, dass keine Maschine wie die andere ist. Unterschiedliche Produkte müssen auf verschiedene Qualitätsmerkmale und Funktionen überprüft werden, weswegen die Maschinen sehr flexibel sein müssen. Das wiederum setzt auch ein agiles Verbindungs- bzw. Verdrahtungskonzept voraus.

Jeder Steckplatz kann als Ein- oder als Ausgang genutzt werden, was maßgeschneiderte Modullösungen erlaubt.

In den Produktionsstätten des Elektroanbieters Hager werden breit gefächerte Vorgaben für die dortigen Prüfanlagen gemacht. Nur wenige Bereiche der Anlagenteile können nach wiederkehrenden Mustern gestaltet werden. Nicht einfacher wird die Aufgabe dadurch, dass die I/O-Dichte stets sehr hoch ist, der Platz aber knapp. Wichtig ist außerdem, dass die Maschinen in kurzer Zeit fertiggestellt werden, da die Zyklen für die Einführung von neuen Produkten eng getaktet und verbindlich sind. Weil das Verdrahtungskonzept also besonders flexibel sein muss, hat sich das Unternehmen für das modulare, dezentrale und kompakte Feldbusssystem Cube67 von Murrelektronik entschieden.

Hohe Flexibilität der I/O-Module

Ein Vorteil besteht darin, dass Hager beim Cube67-System auf viele unterschiedliche I/O-Module zurückgreifen kann. Je nach Bedarf werden Komponenten mit vier oder acht Steckplätzen in die Installation eingebunden. In manchen Maschinen kommen Module für M12-Stecker zum Einsatz. Häufig greift das Unternehmen aber auch auf die M8-Module zurück. Das spart Platz und ermöglicht es, viele I/O-Punkte auf wenig Raum zu verbinden. Die Module werden direkt neben der Sensorik und Aktorik angebracht, z.B. auf pneumatisch betriebenen Einheiten oder Greifern. So lassen sich die Sensoren und Aktoren mit kurzen Leitungen anbinden, was den Aufwand für die Verlegung reduziert und Kosten spart. Ein weiterer Vorteil ist die hohe Funktionalität der Ports. Der Anwender kann für jeden Steckplatz entscheiden, ob er ihn als Ein- oder Ausgang nutzt. Damit lassen sich aus Standardmodulen maßgeschneiderte Lösungen generieren, mit denen die Sensorik und Aktorik im nahen Umfeld eines Moduls integriert wird. Durch diesen Ansatz kann die Anzahl der vorzuhaltenden Modulvarianten ebenso wie die Gesamtzahl der benötigten Module reduziert werden. Dabei entstehen Kosten-, Platz- und Installationsvorteile. Außerdem lassen sich mit Cube67 und dem Multipolstecker auch Ventile direkt ansteuern.

Eine Leitung für Daten und Energie

Ein weiterer Vorteil für Hager ist, dass die Module des Systems von Murrelektronik über eine Systemleitung verbunden werden. Der Aufbau erfolgt in Stern- oder Linientopologie und bietet damit hohe Flexibilität. Die Leitung überträgt sowohl die Daten als auch die Energie für Sensorik und Aktorik. Es sind also nicht zwei getrennten Leitungen nötig. Die Systemleitung bekommt Hager genau in den erforderlichen Längen sowie vorkonfektioniert geliefert. Dadurch spart das Unternehmen Zeit und kann viele Fehlerquellen ausschließen. Denn die Funktionalität der vorkonfektionierten Leitungen prüft Murrelektronik schon im Fertigungsprozess.

Hohe Verfügbarkeit durch Diagnose

Für Hager ist eine hohe Anlagenverfügbarkeit von großer Bedeutung. Aus diesem Grund gilt es, eventuelle Fehler schnell zu detektieren und zu beheben. Dazu nutzen die Konstrukteure des Unternehmens die Diagnosemöglichkeiten des Cube67-Systems. So kann selbst der Anwender die Ursache eines Problems unkompliziert finden und beseitigen. Bei größeren Störungen können sich die Mitarbeiter von Hager per Fernzugriff über das Internet aufschalten. Durch das breite Modulangebot von Cube67 ist es möglich, einfach den Busknoten auszutauschen und die Anlagen damit für den Einsatz in einem übergeordneten Profinet oder Ethernet/IP-System fit zu machen. Unterhalb des Busknotens kann die Struktur unverändert bleiben. Der Aufwand für Dokumentation und Programmierung, aber auch für interne Prozesse wie Einkauf oder Vorratshaltung, wird damit reduziert. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/p/22675

Alexander Hornauer,
Corporate Marketing,
Murrelektronik GmbH
www.murrelektronik.com/de

Bild: Murrelektronik GmbH

Produktionsprozesse durch die Analyse von Daten verbessern

Betriebsparameter mit künstlicher Intelligenz ermitteln

Künstliche Intelligenz wird in der Industrie vermehrt eingesetzt. Sie dient z.B. dazu, einem Maschinenbediener bei der Interpretation von Daten für Steuerungsumgebungen zu helfen. Mithilfe von Prognosemodellen auf KI-Basis können jedoch auch Betriebsparameter ermittelt und dadurch Ausschussquoten verringert werden.

Die Umsetzung von Industrie-4.0-Anwendungen in einer Anlage oder Fabrik entwickelt sich immer weiter. Es werden fortwährend neue Ideen integriert und Wendungen erwartet. Jedes Unternehmen befindet sich dabei in einer anderen Phase. Jedoch haben alle Firmen etwas gemeinsam: Sie sichten die Daten ihrer Fertigungslinien, sortieren und analysieren diese. In einer Prozesssteuerungsumgebung wird eine hohe Datenmenge generiert, die nicht von einer Person allein interpretiert werden kann. Bediener können von der Informationsflut überwältigt werden und somit Möglichkeiten der Prozess- und Qualitätsverbesserung ungenutzt bleiben.

Maßnahmen durch KI vorhersagen

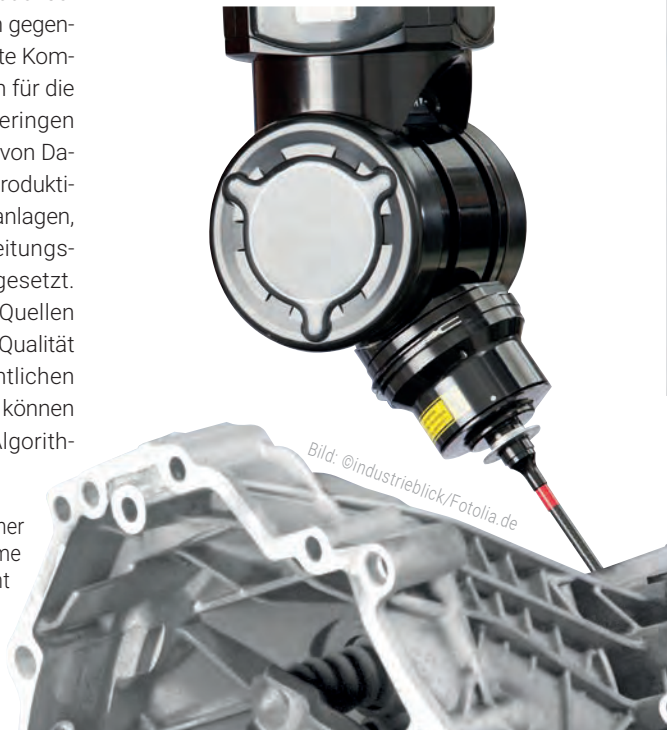
Daher sollte die menschliche Expertise durch künstliche Intelligenz erhöht werden. KI soll nicht nur zu Analysezwecken genutzt werden, sondern auch, um Maßnahmen vorherzusagen und einzuleiten. Eine korrekte Vorhersage der nächsten Schritte in einer bestimmten Situation und die Ergreifung von präventiven Korrekturmaßnahmen können nützlich sein. So z.B. wenn die Vorhersage und die Maßnahmen auf kostengünstige Weise, im angemessenen Umfang und früh genug erfolgen, damit Ergebnisse sinnvoll verändert und so z.B. Auschuss vermieden werden kann. Das Ziel künstlicher Intelligenz besteht darin, die Kosten von Qualitätsmängeln durch den Nutzen großer Datenmengen zu senken. Das kann durch die richtige Vorgabe der Parametereinstellung erfolgen. Wenn künftige Ereignisse in vollem Umfang standardmäßig vorhergesagt werden, könnten dadurch verschiedene Disziplinen verbessert werden. Passende Beispiele dafür sind Google, Facebook und Amazon. Dort wurde die Anwendbarkeit und Effizienz von Plattformen und Massenwerbung durch KI verbessert.

Künstliche Intelligenz in der Produktion

Zu Fertigungslinien z.B. in Schwerindustriezweigen gehören immer mehrere Prozessabläufe. Diese laufen parallel oder sequenziell, beeinflussen sich jedoch gegenseitig. Sie erfordern eine bestimmte Kombination aus Produktionsvariablen für die passende Effizienz und einen geringen Verlust. KI-Lösungen wie Inspect von DataProphet werden in komplexen Produktionsumgebungen wie in Montageanlagen, Gießereien sowie Mineralaufbereitungs- und Langstahlwalzwerken eingesetzt. Dort werden aus verschiedenen Quellen Verlaufsdaten zu Produktion und Qualität gesammelt und in einer übersichtlichen Ansicht dargestellt. Anschließend können die Daten in Echtzeit mittels KI-Algorithmen verarbeitet werden, um potenziellen Qualitätsproblemen bei nachgelagerten Prozessen vorzugreifen. Darüber hinaus können proaktiv Korrekturmaßnahmen zur Vermeidung von Qualitätsabweichungen vorgegeben werden. Inzwischen kann der Anwender mithilfe von überwachten oder unbeaufsichtigten maschinellen Lernmethoden digitale Kopien von Anlagen erstellen. So kann er die passende Betriebsweise von komplexen Prozessen in der Industrie ermitteln.

Steuerungen über KI-Abläufe einstellen

Bei herkömmlichen statistischen Methoden stellen die Menge, die Rate und die Diversität der Daten in umfangreichen Herstellungsprozessen ein Problem dar. Unbeabsichtigte Konsequenzen treten oft in großen, komplexen Fertigungslinien auf und können häufig nicht durch statistische Prozesssteuerungen bewältigt



Durch den Einsatz von künstlicher Intelligenz können Qualitätsprobleme in der Industrie frühzeitig erkannt und behoben werden.

werden. Dafür können KI-Algorithmen Kaskadeneffekte analysieren und erfolgreich Vorhersagen treffen. Vorgeschlagene Betriebsparameter sollen unbeabsichtigte Konsequenzen verhindern und die Qualität verbessern. Die Feinabstimmung von Produktionsparametern erfolgt bisher unabhängig von vor- oder nachgelagerten Variablen auf Zell- oder Maschinenebene. Deshalb konnten die Auswirkungen von Änderungen bei vorgelagerten Prozessen nur schwierig ermittelt und weitere Probleme verhindert werden. Durch KI-Abläufe können Steuerungen abhängig von den relativen Auswirkungen der einzelnen Zellen oder Maschinen innerhalb der gesamten Fertigungslinien eingestellt werden. Durch die gleichzeitige Nutzung von Daten aus verschiedenen Quellen einer Produktionsanlage erhält der Anwender ein umfassendes Bild. Aufgrunddessen kann er anschließend die richtigen Produktionsparameter einstellen. Dabei soll der beste Betriebsstatus der Fertigungslinie erreicht und mögliche Defekte an den einzelnen Stationen des Produktionsprozesses effektiv verringert werden. Das Unternehmen DataProphet arbeitet mit einer Gießerei für Motorblöcke zusammen. Hohe Ausschuss- und Nacharbeitsquoten haben zu Problemen geführt, die sich auch negativ auf die Kosten ausgewirkt haben.

Ausschussquote verringern

Gelöst wurde das Problem, indem Produktionsdaten unterschiedlicher Formate wie Excel-Dateien und Access-Datenbankdaten aus allen Teilen des Unternehmens gesammelt wurden. Anschließend hat das Unternehmen mit dem Prognosemodell Inspect die passenden Betriebsparameter ermittelt und Motorblöcke mit möglichen Defekten identifiziert. So wurde die Ausschussquote im ersten Betriebsmonat um 50 Prozent verringert und die externe Ausschussquote innerhalb der ersten drei Monate vollständig reduziert. Dadurch wurden durch den Einsatz von Inspect kein einziges defektes Gussstück mehr produziert und Kosten eingespart. Die Funktionen von solchen Lösungen sollen es den Benutzern ermöglichen, den gesamten Produktionsprozess durch die Analyse von Verlaufsdaten aus unterschiedlichen Quellen und von Echtzeitproduktionsdaten aufzuzeichnen. Damit erhalten die Bediener ein genaues Bild der Produktions- und Qualitätsdaten jedes hergestellten Teils. Anschließend können die Benutzer Berichte mit Vorgaben für die richtigen Parameteränderungen einsehen. Dadurch können sie die Effizienz aktueller mit früheren Betriebsparametern vergleichen. Die Lösung soll Qualitätsabweichungen, Betriebsausfälle und Verluste verringern und dadurch den Produktionszustand konstant halten. ■

Frans Cronje,
CEO & Mitbegründer,
Data Prophet
www.dataprophet.com

Kabel und Verbindungstechnik

Kabel und Leitungen werden oft als Lebensadern einer Maschine bezeichnet. Sie ermöglichen die Energieversorgung und Datenübertragung. Daher kommt ihnen in der Automatisierung auch eine entsprechend hohe Bedeutung zu.

Als Fortsetzung aus der vorhergehenden Ausgabe des INDUSTRIAL COMMUNICATION JOURNALs (2/2019) vermittelt der folgende Marktspiegel einen Eindruck vom Angebot an industriellen Leitungen und deren Anbietern. Das Spektrum beginnt mit Standardkabeln zur Energieversorgung, die fest und geschützt vor Umgebungseinflüssen in den Maschinen und Anlagen verlegt werden. Kommen Leitungen hingegen in beweglichen Bereichen der Applikation zum Einsatz, steigen die Anforderungen schnell – hier sind spezielle Ausführungen gefragt. Weil das Kabel dann enge Biegeradien oder hohe Biegezyklen bewältigen muss. Oder weil es harten bzw. aggressiven Umwelteinflüssen ausgesetzt ist. In beiden Fällen sind besondere Materialien und Verseilkonzepte gefragt. Weiter geht es mit Leitungen, die nur für bestimmte Kommunikationsprotokolle, z.B. Profinet oder besondere Datenraten ausgelegt sind. Den kompletten Überblick aller Anbieter auf dem Markt gibt natürlich auch die Online-Plattform i-need.de. *(mby)* ■

Anbieter	Internet-Adresse	Feldbusleitungen	Sensor-/Aktor-Leitung	ASI-Sensor-/Aktor-Leitung	CAN / Devicenet	Devicenet für Energieführungsketten	Interbus	Profibus	Profibus PA
Laser 2000 GmbH	www.laser2000.de								
Leoni Fiber Optics GmbH	www.leoni-fiber-optics.com						•	•	•
Leoni Kerpen GmbH	www.leoni-industrial-projects.com				•			•	•
Leoni Special Cables GmbH	www.leoni-industrial-solutions.com		•	•	•	•	•	•	•
Letronic e.K.	www.letronic.de		•	•	•	•	•	•	•
Lindy-Elektronik GmbH	www.lindy.de								
Lumberg Automation, (Belden)	www.lumberg-automation.com		•	•	•		•	•	
MC Technologies GmbH	www.mc-technologies.net								
Meilhaus Electronic GmbH	www.meilhaus.de								
Metz Connect GmbH	www.metz-connect.com								
MIL-Kabel-Systems GmbH	www.mil-kabel-systems.com								
MKU Metrofunk Kabel-Union GmbH	www.metrofunk.de							•	
Muckenhaupt & Nusselt GmbH & Co. KG	www.munu-kabel.de								
Murrelektronik GmbH	www.murrelektronik.com		•	•	•		•	•	
Mütron Müller GmbH & Co.KG	www.muetron.de		•	•	•	•	•	•	•
Nexans Deutschland GmbH	www.nexans.de		•	•	•	•	•	•	•
Norres Schlauchtechnik GmbH & Co. KG	www.norres.com								
Omerin	www.groupe-omerin.com								
Pepperl+Fuchs GmbH	www.pepperl-fuchs.com		•	•	•	•	•	•	•
Pflitsch GmbH & Co. KG	www.pflitsch.de								
Phoenix Contact Deutschland GmbH	www.phoenixcontact.com		•		•		•	•	•
Plastro Mayer GmbH	www.plastromayer.de								
Preising GmbH & Co. KG	www.preising.net								
Prysmian Kabel und Systeme GmbH	de.prysmiangroup.com								
Reichle & De-Massari GmbH	www.rdm.com								
Reiku GmbH	www.reiku.de								
SAB Bröckskes GmbH & Co. KG	www.sab-kabel.de		•		•	•	•	•	•
Schaltag AG	www.schaltag.ch								
Secomp GmbH	www.secomp.de								
Siemens AG	www.siemens.com			•				•	•
Signum Computer GmbH	www.signum-vision.com								
Sommer Cable GmbH	www.sommercable.com							•	
Stecker Express GmbH	www.stecker-express.de		•	•			•	•	
Straschu Elektro-Vertriebs-GmbH	www.straschu.de								
TE Connectivity	www.te.com		•	•	•	•	•	•	•
Telegärtner Karl Gärtner GmbH	www.telegaertner.com								
Telemeter Electronic GmbH	www.telemeter.info								
Thorsten Beulecke Kabelvertrieb	www.beulecke.de		•	•	•	•	•	•	•
TKD Kabel GmbH	www.tkd-kabel.de			•	•	•	•	•	•
Tsubaki Kabelschlepp GmbH	www.kabelschlepp.de		•		•	•	•	•	•
ⓘ Hans Turck GmbH & Co. KG	www.turck.com		•	•	•	•		•	•
ⓘ U.I. Lapp GmbH	www.lappkabel.de		•	•	•	•	•	•	•
UBF EDV Handel und Beratung	www.ubf.de								
Vogtländisches Kabelwerk GmbH	www.voka.de		•		•		•	•	•
W.L. Gore & Associates, Inc.	www.gore.com				•			•	
W+P Products GmbH	www.wppro.com								
Wago Kontakttechnik GmbH & Co. KG	www.wago.com		•		•			•	
ⓘ Weidmüller GmbH & Co. KG	www.weidmueller.de		•	•	•	•		•	•
Wieland Electric GmbH	www.wieland-electric.com		•	•				•	
WireMasters GmbH & Co	www.wiremasters.de								
Wisi Communications GmbH & Co.KG	www.wisi.de								
Woertz Systemhaus MBA AG	www.woertzonline.de								
XBK-Kabel Xaver Bechthold GmbH	www.xbk-kabel.de								
Yamaichi Electronics Deutschland GmbH	www.yamaichi.de								

Profibus für Energieführungsketten	Profibus außen- und erdverlegbar	Industrielles Fast-Ethernet-Kabel	Industrial Ethernet für Energieführungsketten	Hybridleitung (Cu + Lichtwellenleiter) PVC	Hybridleitung (Cu + Lichtwellenleiter) PUR	Energie- + Datenleitung in einem Cu-Kabel	Leitungen nach Desina-Norm	Leitungen für Sicherheitsbus	Leitungen für andere Bussysteme	**Lichtwellenleiter**	Lichtwellenleiter simplex POF	Lichtwellenleiter duplex POF	Lichtwellenleiter Glasfaser	Lichtwellenleiter für Energieführungsketten	**Serviceleistungen und Zusätze**	Kabelkonfektionierung	Konfektionierungswerkzeuge	Konfekt. von Energieführungsketten	Konstruktion und Entwkl. von Leitungen, Kabeln	Kundenspezifische Kabelbedruckung	Vorverdrahtete Frontstecker für Simatic	Kabelschutzsysteme
				•	•						•	•	•	•			•					
•	•	•	•	•	•		•				•	•	•	•		•	•			•		
•	•	•	•	•	•	•		•	•		•	•	•	•		•	•		•	•		
•	•	•	•	•	•	•	•	•	•							•		•	•	•		
•	•	•	•			•	•	•											•	•		
																•						
		•														•				•		
																•			•			
									•								•					
													•			•	•			•		
																•			•	•		
											•	•				•			•			
																			•	•		
•		•	•	•	•	•	•		•							•			•	•	•	•
•	•	•	•	•	•	•	•	•			•	•	•	•		•	•	•	•	•		•
•	•	•	•	•	•	•	•	•					•			•			•	•		
																						•
																			•			•
•		•	•			•		•	•							•				•		•
																						•
•	•	•	•			•					•	•	•	•		•	•			•		•
																•			•			
																•	•	•				
																			•			
																	•					
																						•
•	•	•	•	•	•	•	•									•		•	•	•		
																•			•	•		
																•			•			
•	•	•	•	•	•	•	•		•		•	•	•	•		•	•		•	•	•	
																•			•			
		•	•	•	•	•					•	•	•	•		•	•		•	•		•
																•	•	•				•
																•			•			•
•	•	•	•	•	•	•	•	•			•	•	•	•		•	•	•	•	•		•
																•						•
																			•			
•	•	•	•	•	•	•	•	•			•	•	•	•		•			•	•	•	•
•	•	•	•	•	•	•		•	•		•	•	•			•	•	•	•	•	•	•
•		•	•	•	•	•	•		•		•	•	•	•		•		•	•	•		
•		•	•			•					•					•	•			•		
•	•	•	•	•	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•
									•		•	•	•	•		•						
	•	•				•		•	•										•	•		
				•	•	•																
				•	•						•	•	•	•		•	•		•	•		•
		•							•								•					
•		•	•				•		•		•	•	•	•		•	•		•	•	•	•
						•			•							•	•		•			
					•	•							•	•		•	•		•	•		•
																•						
																•			•			
																•			•	•		
		•	•			•			•							•	•			•		

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand:17.07.2019

Erste Produktionsnetze auf Basis des neuen Standards:

Autarkes 5G-Netz für die Produktion

Die 5G-Technologie soll ab März 2020 in Deutschland ausgebaut werden. E.GO Mobile, Ericsson, Vodafone und SEW-Eurodrive wollen die Technologie für ein autarkes Produktionsnetz nutzen. Die Unternehmen arbeiten derzeit an einer Umsetzung, bei der es um die Fertigung von Elektroautos mithilfe eines mobilen Assistenzsystems geht.

Der Hersteller von Elektrofahrzeugen e.GO Mobile geht in vielen Dingen neue Wege. So setzt er in seiner modernen Fertigung und Montage im Werk 1 ganz auf neue Konzepte. SEW-Eurodrive war hier bereits in der Konzeptionsphase eingebunden. Dazu rüstet SEW-Eurodrive ein erstes mobiles Assistenzsystem für die Fertigung bei e.GO Mobile auf 5G-Technologien um.

Geringe Latenzzeit durch Network Slicing

Auch in der Vernetzung und dem damit verbundenen Datenaustausch der mobilen Assistenzsysteme untereinander sowie mit anderen Produktionsschritten geht e.GO Mobile neue Wege. Das Mobilfunknetz soll vollständig vom öffentlichen Funknetz isoliert sein. Dazu nutzen die Unternehmen die Standards und Protokolle der 5G-Technologie. SEW-Eurodrive rüstet in diesem Zuge ein mobiles Assistenzsystem auf die modernen Mobilfunkstandards um, weitere könnten im Anschluss folgen. Damit kommen in der Automobilproduktion in einem autarken 5G-Netz die Technologien Mobile Edge Computing und Network Slicing zum Einsatz. Mobile Assistenzsysteme, Maschinen und Werkzeuge tauschen so nahezu in Echtzeit Informationen über den aktuellen Standort, zum momentanen Batteriezustand oder zur geplanten Fahrroute aus. Vodafone stellt die moderne Mobilfunktechnologie Network Slicing speziell und virtuell für das e.GO-Werk 1 bereit. Sie verringert die Latenzzeit auf weniger als 10ms. Die mobilen Assistenzsysteme sind mit Sensoren ausgestattet und erfassen eigenständig Umgebungsinformationen. Somit schafft die Technologie für e.GO ein autarkes Netz nach Maß für die Anforderungen der Serienproduktion von Elektroautos.

Datenauswertung via Mobile Edge Computing

Beim Mobile Edge Computing werden die erfassten Daten direkt in der Produktionshalle ausgewertet und gelangen per Mobilfunk in Echtzeit zurück zum Fahrzeug. Basierend auf den Daten passt das Fahrzeug die Fahrtrichtung und Geschwindigkeit an. Im Nahfeld kann ein mobiles Assistenzsystem mit der eingebauten, referenzlosen Navigation oder einem anderen Ortungsverfahren autonom navigieren. Insgesamt 36 kleine Mobilfunkantennen sorgen in der Produktionshalle für Bandbreiten im Gigabit-Bereich. Die Kommunikation zwischen den Maschinen untereinander soll so schneller, die digitale Durchdringung der Produktionsprozesse höher und Arbeitsabläufe effizienter werden. Damit lösen die beteiligten Unternehmen die WLAN-Kommunikation ab und sammeln Erfahrungen in der Nutzung zellfunkbasierter Kommunikation. Mit dem Einsatz der 5G-Technologien kommen damit schon heute erste Technologien von morgen produktiv zum Einsatz. ■

5G für die Industrie

Zehn Jahre nach dem Release von 4G (LTE) wird mit 5G der nächste Performancesprung in der Mobilfunktechnologie vollzogen. Während 3G und 4G im industriellen Bereich eher in Nischen eingesetzt werden, könnte 5G bald in sehr vielen Produktionsnetzen Einzug halten. Es ist nicht nur sehr viel schneller – im Gegensatz zu seinem Vorgänger LTE (300MBit/s bis 1GBit/s) soll 5G Datenraten bis 10GBit/s ermöglichen, hohe Sicherheit und Verfügbarkeit gewährleisten sowie Latenzen bis zu 1ms bieten. Auch die Tatsache, dass für industrielle Anwendungen durch die Frequenzvergabe der Aufbau autarker, privater Netze vorgesehen ist, wird die Verbreitung der Mobilfunktechnologie im industriellen Bereich deutlich vergrößern.

Vodafone GmbH
www.vodafone.de

Bild: Vodafone GmbH

Konfigurationsdaten werden an die Maschine geschickt, während Informationen zu Output oder Störungen an das Betriebsdaten-Erfassungssystem von Wieland zurückkommen.

Bild: Wieland Electric GmbH

LiFi-Einsatz in der Produktion

Licht als drahtlose Alternative zu Funk

Aktuell halten verschiedene neue Technologien Einzug in die Fabrik. LiFi ist eine davon: Sie nutzt das Spektrum des Lichts, um Daten zu übermitteln und kann damit eine Alternative zu WLAN und Bluetooth darstellen. Denn im Vergleich zu Funk ist sie vor elektromagnetischen Störungen sicher und im Mikrosekundenbereich bei Datenraten bis 1GBit/s echtzeitfähig.

Wie die Vorteile von LiFi im industriellen Umfeld genutzt werden können, wird derzeit von Wieland Electric getestet. Das mittelständische Unternehmen setzt den Datenübertragungsstandard bereits in der eigenen Produktion ein. Konkret kommt die optische Datenübertragung an einer Fertigungslinie für Elektronikbauteile zum Einsatz. Dabei werden Daten zu Steuerung der Anlage sowie zur Betriebsdatenerfassung zwischen LiFi-Sender und -Empfänger übertragen. Konfigurationsdaten gehen an die Maschine, während Informationen zu Produktivität oder Störungen an das Betriebsdaten-Erfassungssystem von Wieland zurückkommen. Die Anbindung an das Datennetz erfolgt über die optische Kommunikationslösung Trulifi 6013 von Signify, die eine sichere Punkt-zu-Punkt-Verbindung herstellt und Übertragungsraten von 250MBit/s unidirektional und 2x250MBit/s bidirektional ermöglicht.

Störungsfreie Übertragung

Nicht nur die hohe Datenrate spricht für den Einsatz im industriellen Umfeld. Auch die störungsfreie und unkomplizierte Übertragung, die mit LiFi überall dort möglich ist, wo die Raumsituation Funkwellen oder Kabel schwierig macht, ist wichtig. Vor allem im stationären Einsatz bietet LiFi hohe Flexibilität. Schließlich sind in modernen Produktionshallen die Fertigungseinheiten und Arbeitsplätze immer häufiger mobil und modular aufgebaut, sodass sie je nach Anforderung neu gruppiert werden müssen. Werden sie einfach unter der datenübertragenden Lichtquelle neu positioniert, so ist die 1:1-Verbindung zwischen Access Point und Client schnell aufgebaut und die Einheit wieder vernetzt. Mühsame Verkabelungen entfallen dadurch und der Produktionsausfall lässt sich reduzieren. Beim Einsatz von LiFi genügt schon eine einfache räumliche Trennung, um die Datenübertragung sicher zu machen, da die Licht nutzende Technologie keine Wände durchdringen kann und immer Sichtkontakt braucht. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/11386

Dipl.-Ing. Stephan Lauer,
Business Development Manager Licht + Gebäude,
Wieland Electric GmbH
www.wieland-electric.com

Die Roboter fahren in der Nokia-Fabrik selbständig ohne feste Routen.

Drahtlose Kommunikation für automatisierte Logistik

LTE ganz privat

Nicht nur die Produktion, sondern auch die Logistik automatisiert Nokia in seiner Fabrik im Norden Finnlands. Selbstfahrende Roboter transportieren Waren selbständig und ohne feste Routen. Sie sind dabei weder über WiFi noch Bluetooth verbunden – ein privates LTE-Netz ermöglicht, dass die Roboter einen zuverlässigen Dienst verrichten.

Der kleine Roboter rollt über den Hallenboden. Er transportiert Elektronikbauteile vom Lager zur Produktion. Auf seinen Wegen ist er aber nicht auf einer festen Route unterwegs: Wenn immer ein Hindernis auftaucht, bremst er ab und umfährt es. Auch Veränderungen der Umgebung bereiten keine Probleme, wenn z.B. Regale woanders stehen. Die intelligente Maschine arbeitet autonom. Sie kommuniziert mit anderen Maschinen sowie Sensoren und erfasst selbständig, wenn Nachschub gebraucht wird – und liefert ihn an.

LTE statt WiFi

Der Roboter der Firma Omron ist nicht allein. Eine ganze Reihe seiner Kollegen fährt durch Nokias Fabrik und liefert Teile aus. Die Firma baut und testet dort Basisstationen für Telekommunikationsdienste sowie 5G-Geräte. Die Produktion läuft weitgehend automatisch. Zudem hat Nokia zusätzlich die Logistik automatisiert. Die Roboter, sogenannte Autonomous Guided Vehicles (AGV), sind über ein Netzwerk untereinander sowie mit einer Steuereinheit verbunden. Früher nutzte die Fabrik dafür Ethernet-Kabelverbindungen, später WiFi. Aber beides hatte Nachteile: Veränderte sich das Gelände, mussten für neue Verbindungen weitere Kabel verlegt werden. Zwar war das bei WiFi nicht nötig, dafür tauchten andere Probleme auf, z.B. dass Metallregale das Funksignal störten. Hatten die Roboter keine Verbindung mehr, blieben sie einfach stehen. WiFi-Netze haben zudem nur eine begrenzte Reichweite und die Roboter konnten außerhalb nicht agieren. Mitarbeiter mussten sie erneut manuell mit dem Netzwerk verbinden. In Folge war die Logistikkette häufig unterbrochen und wichtige Teile nicht an ihrem Standort. Diese Probleme haben sich erledigt, seitdem die autonomen Fahrzeuge über ein privates LTE-Netz verbunden sind. Sie rollen nun uneingeschränkt überall auf dem Fabrikgelände umher. Verbindungen müssen nicht neu konfiguriert werden, wenn sie in einer anderen Halle eingesetzt werden. Metall stört den Funkkontakt nicht und das transportierte Material ist demzufolge immer genau dort, wo es gerade benötigt wird. Seit dem Einsatz steigerte sich die Effektivität der Logistikprozesse um 30 Prozent. Zugleich wurden Wartungsarbeiten für die Roboter um 98 Prozent gesenkt.

Vorteile von LTE-Netzen

Die Bandbreite bei einem privaten LTE-Netz wird nicht wie in einem öffentlichen Netz mit anderen Nutzern geteilt. Der Frequenzbereich von 3,7GHz ist allein für Industrieanwendungen vorgesehen. Das ist auch sicherer, weil alle Daten innerhalb des eigenen Netzwerks bleiben und die einzelnen Geräte sich über SIM-Karten im Netzwerk identifizieren müssen. Ein solches Netz hat verschiedene Vorteile gegenüber anderen Verbindungsarten: LTE erreicht Orte, an denen

Bild: ©Petri Kekkonen / Nokia GmbH

WiFi nicht funktioniert. Es müssen auch keine Kabel für die Kommunikation verlegt werden. Darüber hinaus sind Verbindungen zuverlässig und die Netze robust. Anders als WiFi ist LTE für groß angelegte Implementierungen gemacht und kann besser skaliert werden. Es können deutlich mehr Geräte darin funken, wodurch mehr parallele und dynamische Prozesse möglich sind. Gleichzeitig müssen weniger Zugangspunkte geschaffen werden, da schon zwei Basisstationen ausreichen, um eine komplette Fabrikhalle auszuleuchten.Ein privates LTE-Netz funktioniert schon sehr gut mit 4G wie das Beispiel der Nokia-Fabrik zeigt. Die Industrie muss also nicht auf 5G warten, um ihre Fabriken zu vernetzen. Weil das Netzwerk aber mit beiden Standards umgehen kann, können Unternehmen auf Wunsch nach und nach von 4G auf 5G umstellen.

Weitere Dienste im privaten Netz

Auf ein privates LTE-Netz können weitere Dienste aufgesetzt werden. Mit der Plattform Nokia Digital Automation Cloud wird auf Wunsch z.B. High Accuracy Indoor Positioning möglich: Damit können Assets bis auf eine Entfernung von weniger als einem halben Meter getrackt werden. Über sogenannte Asset Tags an den Gegenständen spürt ein Locator sie auf. So lassen sich Logistikpfade nachvollziehen, z. B. bei den autonomen Robotern: Auf welchen Wegen waren sie in der Halle unterwegs und wo sind sie am häufigsten zu finden? Über die Cloud kann außerdem ein Kommunikationsdienst für Mitarbeiter implementiert werden. Sie nutzen dazu mobile Geräte wie Tablets oder Smartphones. ■

Bild: ©Petri Kekkonen / Nokia GmbH

Mithilfe von Tablets können Mitarbeiter direkt über das private LTE-Netz mit Kollegen kommunizieren.

Alexander Kirchner, Head of Business Development Digital Automation, Nokia
www.dac.nokia.com/de_int/

Kabellose Kommunikation auf der Steuerungsebene

Schon gefunkt?

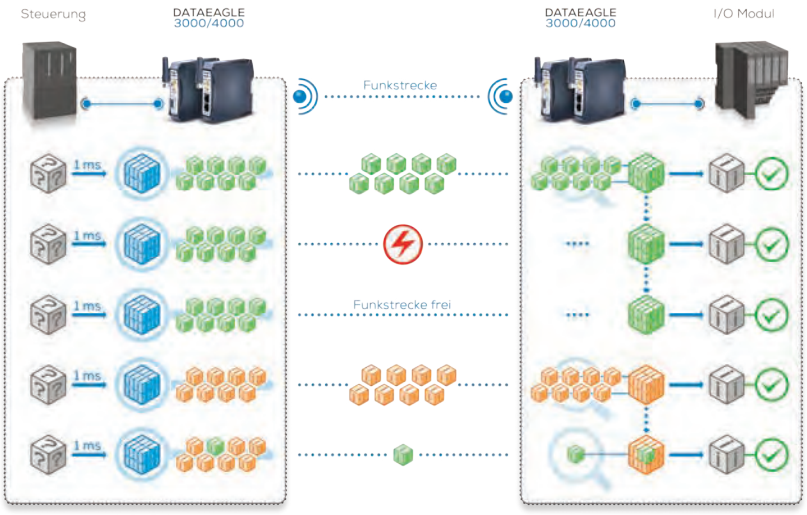
Kabellose Kommunikationslösungen sind fester Bestandteil in der Automatisierung. Sie werden meist mit Feldbussen verbunden und bieten einen hohen Nutzen für industrielle Anwendungen. Auch auf der Steuerungsebene bieten Funktechniken Vorteile gegenüber der klassischen Vernetzung.

Im Zusammenhang mit den Diskussionen über Industrie 4.0 ist auch das Ende der üblichen Automatisierungspyramide ein Thema. Die Pyramide mit ihren streng getrennten Ebenen verwandelt sich in ein Netzwerk mit vielfältigen Kommunika-

Die verschiedenen Modulserien von Schildknecht sind auf unterschiedliche Anforderungen je nach Bedarf ausgelegt.

Bild: Schildknecht AG

tionsbeziehungen zwischen den Komponenten einer Anlage. Das betrifft auch die klassische Steuerungsebene. Die Kommunikationsstrecken sind heute meist durch Feldbusse einschließlich ethernetbasierter Systeme wie Profinet realisiert. Derzeit entwickelt sich ein erheblicher Anstieg für WLAN als Kommunikationslösung in der Industrie. Zum Aufbau flexibler Produktionsprozesse werden Daten von vielen Sensoren benötigt. Sie werden dort per Kabel an die Steuerung kommuniziert. Dabei sind die Maschinen und Anlagen oft schwer zugänglich. Dagegen bieten Funktechnologien wie WLAN und Bluetooth eine Lösung. Beide sind in der IEEE standardisiert und daher weltweit nutzbar. Während sich WLAN für sehr hohe Datenraten eignet, ist Bluetooth auf hohe Reichweiten bis zu 1km ausgelegt.



Die Datenvorbereitung der Dataeagle-Funkmodule 3000 und 4000 ermöglicht eine stabile Funkübertragung.

Feldbusse übernehmen Kommunikationsaufgaben

Nach anfänglicher Skepsis bei der Einführung der Funktechnik in die Automatisierungsbranche stieg die Akzeptanz kontinuierlich an. Im Zentrum eines solchen Systems steht die Steuerung. Sie enthält relevante Daten von Sensoren und Geräten aller Art und gibt die resultierenden Ergebnisse bzw. Informationen an den Empfänger weiter. Solche Kommunikationsaufgaben übernehmen heute überwiegend Feldbussysteme wie Profibus, Profinet, CAN und Powerlink. Für kabellose Strecken müssen die Module auf die Sprache des jeweiligen Bussystems ausgelegt sein. Die Modulserie Dataeagle von Schildknecht stellt passende Funkmodule und Lösungen für unterschiedliche Anforderungen bereit.

Stabile Funkübertragung

Die Funkmodule der Serien 3000 und 4000 unterstützen neben Profibus und Profinet auch Profisafe. Dabei ermöglicht das zweite Modul auch OpenSafety über UDP. Dadurch sollen Sicherheitsanforderungen erfüllt und die Akzeptanz von Wireless-Lösungen gesteigert werden. Die Module ermöglichen eine stabile Funkübertragung von Daten aus Bussystemen mittels einer patentierten Datenvorverarbeitung. Die enthaltenden Funktionsblöcke sollen die Netzbelastung reduzieren und die Übertragungsqualität dauerhaft aufrechterhalten. Dafür werden die Datenpakete durch verschiedene Algorithmen auf Redundanz, Zeitstempel und Telegramminhalt analysiert und zwischengespeichert. Die Datenaktualisierungszeit von 1ms an der Steuerung bleibt dabei bestehen. Über eine ähnliche Funktion verfügt auch die Serie Dataeagle 6000. Dabei ist die Übertragung der CAN-Messages durch Parametrierung auf wichtige Punkte begrenzt. Anwendungen der Geräte sind z.B. in Anlagen der Kran- und Bühnentechnik, in Verzinkereien und selbstfahrenden Transportfahrzeugen.

Die Modelle der Serie Dataeagle stehen in verschiedenen Gehäuseausführungen und als OEM-Baugruppe bereit.

Erforderliche Variantenvielfalt

In vielen Fällen befinden sich die Steuerung und ihre Kommunikationspartner nicht in einer übersichtlichen Ebene, sondern in einem eingeengten Umfeld mit beweglichen Komponenten und eingeschränkter Zugänglichkeit. Dadurch werden kabellose Kommunikationsstrecken sowie eine hohe Flexibilität der konstruktiven Ausführung der Funkmodule und Antennen benötigt. Daher stehen die Module in unterschiedlichen Gehäuseausführungen sowie auch als OEM-Baugruppe zur Verfügung.

Aus der Steuerungsebene in die Cloud

Sind die Maschinen in der Industrie weltweit installiert und soll die Überwachung zentral erfolgen, wird zur Kommunikation eine globale Konnektivität benötigt. Diese bietet die Modulserie Dataeagle 7000. Sie enthält eine eSIM-Karte für etwa 400 Mobilfunk-Provider. Darüber können die Zustandsdaten einer Anlage mittels Unsteered Roaming an eine Cloud oder das Dataegale-Portal übertragen werden. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/9280

Thomas Schildknecht, Vorstand
Schildknecht AG
www.schildknecht.ag

Bilder: Schildknecht AG

WLAN für die Industrie

Das Dogma, dass Wireless für den Einsatz in der Fabrik nicht zuverlässig genug wäre, geht immer weiter zurück. So ist z.B. WLAN als drahtlose Technologie mittlerweile auch in industriellen Anwendungen gut vertreten.

WLAN ist aus dem Büro- und Consumer-Umfeld sehr bekannt. Die Hardware ist durch ihre Verbreitung im Massenmarkt zudem praxiserprobt und preiswert. Deswegen gehört WLAN zu den bevorzugten Standards, wenn Wireless-Lösungen in der Automatisierung umgesetzt werden müssen. Die folgende Herstellerübersicht zeigt die Anbieter in diesem Marktsegment. Deren Produkte samt Eigenschaften und Leistungsdaten listet ergänzend die Produktsuchplattform i-need.de online auf. *(mby)* ■

Direkt zur Marktübersicht auf
i-need.de
PRODUCT FINDER
www.i-need.de/106

Acal BFi Germany GmbH
26233
Gröbenzell
08142/ 6520-0
www.acalbfi.de
Lantronix PremierWave 2050

Advantech Europe B.V.
14598
Hilden
02103/ 97885-0
www.advantech.de
EKI-135x

Artila Electronics Co., Ltd.
26276
Düsseldorf
0211/ 93889-80
www.artila.com
Matrix-513

Bressner Technology GmbH
17137
Gröbenzell
08142/ 47284-70
www.bressner.de
B&B Ghostbridge2-EU

E. Dold & Söhne KG
31316
Furtwangen
07723/ 6540
www.dold.com
Funk-Sicherheitsmodul UH 6900

Hirschmann Automation and Control GmbH
1743
Neckartenzlingen
07127/ 14-0
www.beldensolutions.com
BAT54-F

Insys Microelectronics GmbH
20775
Regensburg
0941/ 58692-0
www.insys-icom.de
EBW-WH100

IPC2U GmbH
23270
Langenhagen
0511/ 807-259-0
www.rumoco.de
RS930W Wireless Switch

Lucom GmbH
14253
Fürth
0911/ 957606-00
www.lucom.de
GhostBridge - High Perf. Wireless Eth. Bridge

MC Technologies GmbH
34000
Hannover
0511/ 676999-187
www.mc-technologies.net
WIFI LTE Antenne (MC1213531-A)

National Instruments Germany GmbH
1721
München
089/ 741313-0
www.ni.com

Pericom AG
1725
Gailingen
07734/ 4870-343
www.pericom.biz
245U-E

Phoenix Contact Deutschland GmbH
14738
Blomberg
05235/ 3-12000
www.phoenixcontact.com
FL BT EPA

Primation Systemtechnik GmbH & Co. KG
1723
Grasbrunn
089/ 46260-0
www.primation.de
702M12-W

Pro-face Deutschland GmbH
23707
Solingen
0212/ 25826-0
www.pro-face.de
SP5660TP

ProSoft Technology
24501
Frankfurt
+33/ 534368720
www.prosoft-technology.com
RLX2-IHNF-E

Siemens AG, Industrial Communication
1759
Nürnberg
0800/ 5090-100
www.siemens.de/iwlan
Scalance W788/748 M12

Sphinx Computer Vertriebs GmbH
1732
Laudenbach
06201/ 75437
www.sphinxcomputer.de
AWK-5222

Wachendorff Prozesstechnik GmbH & Co. KG
16794
Geisenheim
06722/ 9965-538
www.wachendorff.de
eWON Flexy

Wago Kontakttechnik GmbH & Co. KG
21092
Minden
0571/ 887-679
www.wago.com
WLAN Ethernet Gateway

Weidmüller GmbH & Co. KG
1762
Detmold
05231/ 1428-259
www.weidmueller.de
IE-WL-AP-BR-CL-ABG-US

Welotec GmbH
17468
Laer
02554/ 9130-00
www.welotec.com
DM500

Wieland Electric GmbH
30691
Bamberg
0951/ 9324-228
www.wieland-electric.com
Wienet AP-ETH-A

Wiesemann & Theis GmbH
24425
Wuppertal
0202/ 2680-110
www.WuT.de
WLAN Client Bridge

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 26.08.2019


Bild: Hlancom Systems GmbH

Steigende Anforderungen an die Netzinfrastruktur

Verschlüsselter Fernzugriff über VPN und SD-WAN

Mit der zunehmenden Vernetzung von Produktionsanlagen steigen die Anforderungen an die Netzinfrastruktur. In Kombination mit einer verschlüsselten VPN-Verbindung ermöglichen moderne Netzwerkkonzepte wie Software-defined Networking (SDN) einen sicheren Zugriff von außen, z.B. für Predictive Maintenance. Mithilfe von Cloudlösungen erfolgt die Konfiguration sowie das Management von Netzwerken ortsunabhängig.

In Zukunft werden herkömmliche Fertigungsstrukturen durch selbststeuernde, intelligente und miteinander vernetzte Produktionssysteme ersetzt. Das Ziel ist z.B. die Etablierung effizienter Steuerungsprozesse. Über das intelligente Monitoring der Produktionsdaten können Unternehmen in Echtzeit auf geänderte Rahmenbedingungen reagieren, über die Fertigungssteuerung eingreifen und Anpassungen vornehmen. Die Anzahl der mechanischen Komponenten in Fertigungsnetzwerken, wie Sensoren, Aktoren oder intelligente Steuerungssysteme wächst. Ihre Verfügbarkeit und Erreichbarkeit werden zunehmend geschäftskritisch. Damit steigt auch die Bedeutung der Fernwartung. Vor dem Hintergrund der Produktionseffizienz und der Betriebskosten werden heute Maschinen und komplette Industrieanlagen dauerhaft von überall remote überwacht und gewartet.

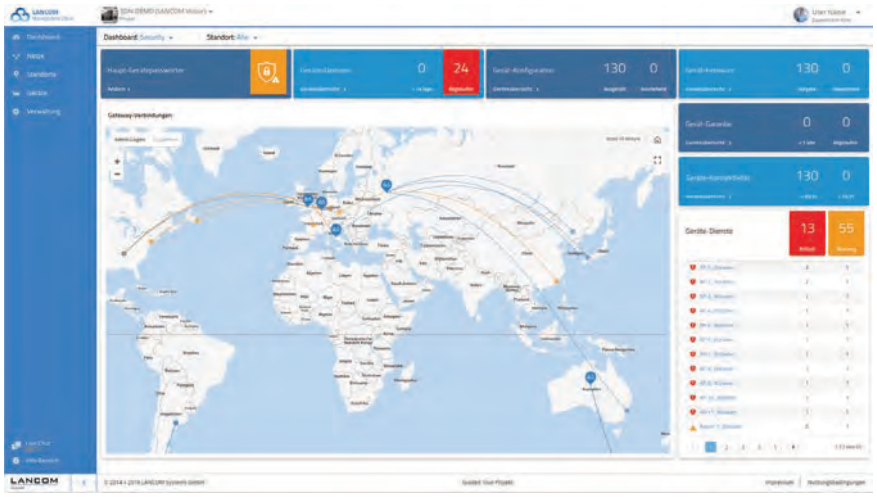
Vorausschauende Wartung

Mit der zunehmenden Vernetzung verändert sich auch das Prinzip der Fernwartung. Anstatt erst dann zu reagieren, wenn Fehler auftreten, dominiert heute die vorausschauende Instandhaltung. Bei der sogenannten Predictive Maintenance wird die Wahrscheinlichkeit für auftretende Defekte oder Ausfälle bereits im Vorfeld errechnet. Die Grundlage dafür bilden die Prozess- und Produktionsdaten von Maschinen und Geräten, die im laufenden Betrieb kontinuierlich und in Echtzeit von Sensoren erfasst werden. Mithilfe von Algorithmen und dem Einsatz künstlicher Intelligenz werden die Daten auf Fehlermuster hin untersucht und ausgewertet. Das Monitoring beschränkt sich dabei nicht mehr nur auf die reine Zustandsüberwachung der Maschinen. Auch Datenströme zwischen den Komponenten im Produktionsnetz werden überwacht, um Abweichungen von normalen Betriebszuständen zu erkennen.

Bilder der Doppelseite: Bild: Hlancom Systems GmbH

Anfälligkeit für Cyber-Attacken

Fernwartung und Predictive Maintenance sollen nicht nur die Effizienz und Lebensdauer von Maschinen steigern, sondern auch die Komplexität vernetzter Produktionsanlagen erhöhen. Dabei nimmt jedoch die Anfälligkeit für Cyber-Attacken zu. Je mehr Zweige der Aufbau der Produktionsanlagen hat, desto größer ist ihre Angriffsfläche. Jeder offene Netzzugang ist ein potenzieller Angriffspunkt von außen. Maschinen kommunizieren heute nicht nur ständig untereinander, sondern auch innerhalb der Systeme der Unternehmens-IT. Die Fabrik der Zukunft wird künftig noch mehr Verbindungen heraus aus dem Maschinennetzwerk haben als heute schon durch den Fernzugriff von Herstellern oder die Produktionsbetriebe selbst. Auch Kunden und Lieferanten werden in die vernetzte Produktionswelt eingebunden. Damit digital vernetzte Fertigungsanlagen kein Ziel für Hacker werden, sind erhöhte Sicherheitsvorkehrungen im Netzwerk nötig.



Software-Clients ermöglichen den Fernzugriff von jedem Ort.

Verschlüsselter Zugriff über VPN

Netzwerke in der Fertigung waren bisher hauptsächlich auf Ausfallsicherheit und hohe Verfügbarkeit ausgelegt. Heute spielt der sichere Fernzugriff auf das Produktionsnetzwerk, z.B. über VPNs, eine wichtige Rolle. Sie nutzen reguläre Internetverbindungen wie DSL/SuperVectoring, G.fast, Mobilfunk oder Glasfaseranschlüsse als Kommunikationsweg. Die Datenübertragung erfolgt jedoch verschlüsselt über einen VPN-Tunnel. Die individuellen Befugnisse von Mitarbeitern, Partnern und Kunden können über virtuelle Netze (VLAN) rollenbasiert vergeben werden. So wird nur Zugriff auf die jeweils relevanten Daten gewährt. Die Verschlüsselung über IPsec VPN gewährleistet hohe Sicherheit beim Remote Access auf Fertigungsanlagen über das Internet. Je nach Struktur des vorhandenen internen Netzes und abhängig vom Anlagentyp kann der Fernzugriff über dedizierte M2M-VPN-Gateways, VPN-Router oder sogar per Software-Client erfolgen. Letztere ermöglichen den mobilen, sicheren Fernzugriff von jedem Ort.

Software-defined Networking

Allerdings stoßen herkömmliche Netzarchitekturen in der Smart Factory mitunter schnell an ihre Grenzen. Durch die Vernetzung von immer mehr Geräten, Standorten und Services entstehen immer mehr Endpunkte. Sie erzeugen, sammeln, verarbeiten und verteilen die Daten. Diese Vernetzung findet nicht nur intern statt, sondern bindet in vielen Fällen Lieferanten und Abnehmer mit ein und muss somit völlig unterschiedliche Befugnisse abbilden. Spätestens damit steigt die Komplexität der Netzarchitektur. Unternehmen verbinden auch ihre Produktionsstätten und Anlagen mit traditionellen Wide Area Networks (WAN). Diese sind schnell überfordert. Die manuelle Einrichtung, Konfiguration und Wartung dieser Netzwerke kann für Systemadministratoren zur großen Herausforderung werden. Abhilfe bieten sogenannte Software-defined Wide Area Networks (SD-WAN). Das Prinzip stammt ursprünglich aus dem Datacenter- und Carrier-Bereich. SDN macht Netze unabhängig von der Hardware und damit agil und schnell. Im besten Fall werden alle Segmente eines Netzwerks – vom WAN über das LAN bis zu WLAN und Security – über eine einzige, zentrale Steuerungskonsole automatisiert aufgesetzt. Entsprechend integrierte Lösungen sind ein wichtiges Tool, das bisher manuelle Konfigurations- und Wartungsprozesse überflüssig machen soll. Dabei sorgt es gleichzeitig für erhöhte Transparenz und die unternehmensweite Einhaltung von Compliance- und Sicherheitsvorgaben.

VPN-Verbindungen automatisiert einrichten

Über ein SD-WAN werden VPN-Verbindungen automatisiert aufgebaut und selbst komplexe Multi-Service-Netzwerke mit reduziertem Aufwand realisiert. Ein typisches Beispiel ist die automatische und dynamische Einrichtung sicherer IPSec-VPN-Tunnel zwischen Produktionsstandorten. Die Tunnel lassen sich einfach auch bei anspruchsvollen Visualisierungsszenarien aktivieren. Die vormals zeitintensive Einzelkonfiguration entfällt. Das SD-WAN ermöglicht auch die aufwändige Integration neuer Maschinen und zusätzlicher Geräte mit Internetzugang oder die Einrichtung von Netzwerkzugängen für die Fernwartung. Selbst M2M-VPN-Gateways lassen sich bei entsprechender Unterstützung über ein SD-WAN komplett automatisiert in Betrieb nehmen. Damit ist für die physische Installation kein tiefes Netzwerkwissen erforderlich und typische Einrichtungsfehler werden effektiv vermieden. Einige zentrale Netzwerkfunktionen können heute virtuell zur Verfügung gestellt werden, wie der virtuelle VPN-Router, WLAN- Controller oder Gateways. Damit entfällt jede physische Installation vor Ort und die Einbindung neuer Standorte erfolgt im besten Fall einfach per Software-Aktivierung. Cloudlösungen sorgen dafür, dass die Konfiguration, das Management und Monitoring des Netzwerks einfach, zentral und ortsunabhängig erfolgen können. ■

Dr. Tarik Erdemir, Vice President Router & VPN-Gateways
Lancom Systems GmbH
www.lancom-systems.de

In Logistikapplikationen und Lieferketten der Automobilfertigung werden bereits 0G-Funknetze genutzt. Auch für Maschinen und Anlagen sowie weitere Assets im laufenden Betrieb bietet sich das Netz von Sigfox an. Die Sensor-to-Cloud-Kommunikation ist z.B. gut für Predictive Maintenance geeignet.

Über das neue 0G-Netz von Sigfox kann der Anlagenbetreiber effizient und kostengünstig den Zustand seiner Geräte, Maschinen und Anlagen überwachen und unerwartete Ausfälle vermeiden.

0G-Funknetz für Maschinen und Anlagen

Kleine Daten, großer Nutzen

Das zentrale Monitoring von Geräten, Maschinen und Anlagen ist bislang mit hohen Kosten verbunden. Durch die Kombination aus hoher Sicherheit bei geringen Kosten und geringem Energieverbrauch eignet sich das 0G-Netz z.B. für die Einführung von Asset Monitoring und Predictive Maintenance Services, wenn Benutzungs- und Zustandsdaten von Geräten, Maschinen und Anlagen zentral gesammelt werden müssen.

Kleine Daten, geringer Energieverbrauch

Das Netz ist sowohl in der Anschaffung als auch in der Nutzung mit niedrigen Kosten verbunden, da der Geräteherstellers schon beim Kauf der Device-Lizenz die Verbindungsentgelte zahlt. Neben den geringeren Kosten wird auch der Energieverbrauch im Sigfox-Netz gering, da die Geräteverbindung im Idle-Modus nicht existiert und weil der Verbindungsaufbau kein Handshake mit einer Basisstation erfordert. Ein adaptives oder eingebettetes Gerät sendet seine Daten und die Basisstationen hören mit, nehmen die Signale auf und übermitteln sie dann an die zentrale Device-Cloud. Im Netz gibt es in Bezug auf die Daten eine eingebaute Beschränkung, da im lizenzfreien Frequenzbereich die Datenübertragung pro Device regulatorisch begrenzt ist. Konkret bedeutet das für die Übermittlung von Daten an die Maintenance-Cloud, dass bis zu 140 Nachrichten mit je 12Byte Nutzdaten pro Tag versandt und bis zu vier Nachrichten pro Tag empfangen werden können. Über das 0G-Netz können Alarm-, Zustands- und/oder Betriebsdaten als Default Setting gesendet werden. Wird es erforderlich, dass große Datenmengen ausgetauscht werden müssen, lässt sich eine komplementäre LTE- oder GSM-Verbindung aufgebauen.

Hohe Sicherheit im Netz

Die Netzverbindung von Sigfox greift nicht in bestehende Kommunikationsinfrastrukturen eines Unternehmens ein, sondern ergänzt sie. Werden zudem nur Daten gesendet, kann auch kein Zugriff auf Devices erfolgen. Bei bidirektionalem Datenaustausch kann die Kunden-Cloud bei Bedarf zudem nur über die Sigfox-Device-Cloud mit den Geräten kommunizieren, wodurch die Verbindung resistent gegen Hacker-Angriffe wird. Durch die Abschottung eines Geräts vom Internet können Maschinen über die Verbindung auch nicht angegriffen werden. Zusammen mit einer Device- und Nachrichten-Authentifizierung, AES-Verschlüsselung der Nachrichten und optionaler Payload-Verschlüsselung, Anti-Replay-Schutz für Nachrichten sowie der hohen Störfestigkeit des Signals bietet Sigfox eine zuverlässige und sichere IoT-Connectivity.

Eingebaute Geolokalisierung

Eine Zusatzfunktion ist die Geolokalisierung, z.B. für eine effiziente Ersatzteilbereitstellung. Die Ortung kann vom Betreiber außerdem zum Asset Management genutzt werden, um den Betriebsmitteleinsatz zu verbessern oder einfach nur das Vorhandensein eines Gegenstands konstant zu überwachen. Auch lassen sich Warenströme bei Just-in-Time- oder Just-in-Sequence-Lieferungen verbessern. Ohne zusätzliche Sensorik ist das Netz rund 500 bis 1500m genau. Mit einer zusätzlichen WLAN-Sensorik kann sie bis zu 30m genau und mit GPS-Logik metergenau bestimmt werden. Setzt man zudem alternativ und/oder ergänzend Sigfox-Bubble als Beacon-Technologie ein, kann man über Geofencing auch Zonen definieren. ■

Aurelius Wosylus, Chief Sales Officer, Sigfox Germany
www.sigfox.de

Bild: Sigfox Germany GmbH

Bild: Stormshield SAS

Mit SNi40 stellt Stormshield eine Firewall für die Produktionsumgebung zur Verfügung.

Bild: ©PopTika/www.shutterstock.com

Tipps zur Absicherung der Produktion

Veraltete Steuerungssysteme vs. Digitalisierung

Industrielle Steuerungs- und Kontrollsysteme kommen in jeder Produktionsstätte zum Einsatz. Sie werden aufgrund unzureichender Sicherheitsmechanismen für Cyberkriminelle zunehmend attraktiver. Dabei lässt sich mit den nachfolgenden Tipps schon ein gutes Schutz- und Sicherheitslevel erzielen.

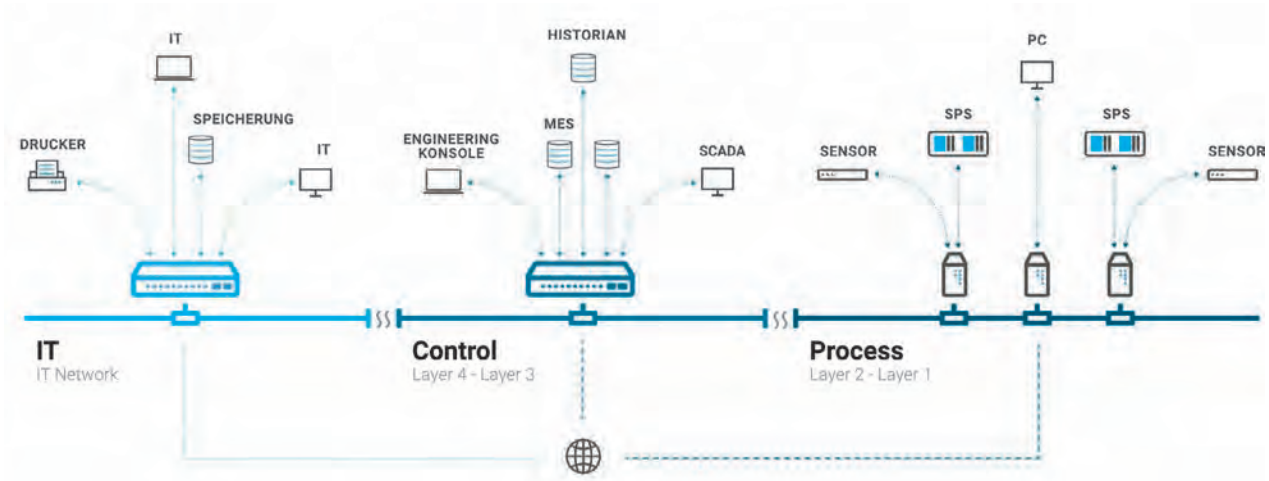
Produktionsanlagen, die auf jahrzehntealten Maschinen und Systemen basieren, in vernetzte Infrastrukturen zu integrieren, kann eine echte Herausforderung sein. Als Scada-Systeme vor über 20 Jahren entwickelt wurden, war deren Einsatz für geschlossene Umgebungen vorgesehen. Heute findet aber die Interaktion zwischen Menschen und Maschinen oft über Rechner mit obsoleten Betriebssystemen statt oder über mobile Geräte wie Smartphones, Tablets oder Notebooks. Sie waren ursprünglich nicht dafür vorgesehen, Maschinen Befehle zu erteilen. Aufgrund der zunehmenden Digitalisierung zur Steigerung von Produktivität und Wettbewerbsfähigkeit, scheinen viele Unternehmen dem IT/OT-Konvergenzrausch verfallen zu sein und vergessen dabei allzu oft die damit verbundenen Risiken.

Steigende Zahl an Cyberangriffen

Dass immer mehr industrielle Steuerungssysteme mit dem Internet verbunden sind, entspricht den Anforderungen der digitalen Wirtschaft an dynamischen Automatisierungsprozessen. Die oft mittels SPS und Scada-Protokollen gesteuerten Industriekomponenten sind jedoch für Angriffe anfällig." Der Einzug neuer Technologien zur Fernsteuerung und -überwachung erfolgt schneller als die Überwachung neuer Sicherheitslücken", so Uwe Gries, Country Manager DACH bei Stormshield. Die Folge: Cyberangriffe haben die deutsche Industrie zwischen 2017 und 2018 etwa 43 Milliarden Euro gekostet. Sieben von zehn Industrieunternehmen seien laut Bitkom solchen Attacken zum Opfer gefallen, Tendenz steigend. Kein Wunder: Über Online-Tools wie Shodan kann jeder unter mehreren Tausend allein in Deutschland über das Internet erreichbaren Industriesystemen das gewünschte Ziel identifizieren und dediziert attackieren.

Schutz für isolierte Produktionskomponenten

Wenn selbst ein mit dem Internet verbundener Industriekühlschrank der Produktionsstätte zum Verhängnis werden kann, dann nimmt die den Cyberkriminellen gebotene Angriffsfläche ein stark erhöhtes Ausmaß an. „Cyberkriminelle profitieren vom mittlerweile überholten Klischee, dass Produktionskomponenten isoliert seien und daher keinen Schutz benötigen", fügt Gries an. Eine Annahme, die dazu führt, dass Industrieunternehmen nur zögernd Authentifizierungsverfahren einsetzen, Zugriffssteuerung betreiben oder die Filterung der den Produktionssystemen erteilten Befehle vornehmen, bevor sie an die Maschinen gelangen. Erschwerend kommt die Tat-



Die Absicherung des Industrienetzwerks über eine Firewall-Lösung soll Schutz vor Cyberangriffen bieten.

sache hinzu, dass häufig Sicherheitslösungen zu sehr unterschiedlichen Zeiten in die Infrastruktur integriert wurden und daher völlig getrennt voneinander agieren. Entsprechend hoch erweist sich der Aufwand für Administratoren, eine halbwegs effiziente Überwachung des IT/OT-Informationsaustausches zu bewerkstelligen. „Gerade das Fehlen einer gezielten Überprüfung der industriellen Kommunikation ermöglicht es, Angreifern, mittels Advanced Persistant Threats IT/OT-Infrastrukturen, nach Schwachstellen zu durchsuchen und anzugreifen", betont Gries. Daher sind Maßnahmen zum Schutz kritischer Infrastrukturen angebracht.

Netzwerksegmentierung, Authentifizierung und Zugriffskontrolle

Fabriknetze werden immer komplexer. Oft sind sie mit der Zeit horizontal gewachsen, ohne Segmentierung und Trennung der kritischen Anlagen, z.B. der Server, die Produktionsdaten mit dem ERP austauschen. Daher ist es empfehlenswert, das Netz in Bereiche zu unterteilen, die entweder gar nicht oder nur teilweise miteinander verknüpft sind. Das schafft Kontrollknoten, die bei der Lokalisierung eines Angriffs hilfreich sein können und es Hackern erschweren, sich horizontal durch das Netzwerk zu bewegen. Der Einsatz von Zugriffsmechanismen erweist sich ebenfalls als sehr nützlich. Wartungstechniker oder Lieferanten greifen heute sowohl vor Ort als auch über das Internet auf Industriesysteme und -ressourcen zu. Mehrfaktorenauthentifizierung sollte hier die Regel sein. Mit Zugriffsmanagement und geeigneten Verfahren zur Identitätsprüfung können Systemadministratoren festlegen, wer zu welchem Zweck auf welche Geräte und Daten zugreifen kann und zeitgerechte Wartungsfenster definieren. Zugriff durch Unbefugte sowie außerhalb der festgelegten Zeiten wird demnach ein Riegel vorgeschoben. Zu guter Letzt sollte der Fernzugang ausschließlich über VPN erfolgen.

Abriegelung der Endpoints

Bei vielen für die Produktion relevanten Industrie-PCs werden weder Antivirus-Updates installiert noch die Betriebssysteme aktualisiert, weil Konfigurationsänderungen möglicherweise die Kompatibilität mit den darauf laufenden Industrieanwendungen gefährdet oder einfach weil ein System-Reboot bei fortlaufender Produktion unerwünscht ist. Folglich sind solche IPCs vielen Bedrohung ausgesetzt – sogar ohne Internet. Es kann, wie im prominenten Fall Stuxnet, selbst der USB-Port oder der Wartungsanschluss auf der Maschine für Angriffe genutzt werden. Bei Rechnern, die im OT-Bereich eingesetzt werden, sollte man deshalb ein Whitelisting der Anwendungen vornehmen und nur die Ausführung der Applikationen zulassen, die explizit freigegeben sind. Ebenfalls empfehlenswert ist, alle Funktionen und Softwarekomponenten zu entfernen, die nicht unmittelbar der Erledigung der vorgesehenen Aufgaben dienen, da sie ein - leicht zu vermeidendes - Sicherheitsrisiko darstellen. Eine tiefgreifende Analyse des Systemverhaltens, die keiner Signatur und keines Updates bedarf, kann zudem den Missbrauch von Schwachstellen der Anwendungen unterbinden.

IPS, DPI und IDS

Wenn man das Fabriknetzwerk mit einer IPS-Firewall (Intrusion Prevention System) oder einem DPI-System (Deep Protocol Inspection) ausstattet, können Angriffe proaktiv erkannt und abgewehrt werden. Die Lösungen dürfen allerdings nicht ausschließlich auf Signaturen basieren: Vielmehr müssen sie in der Lage sein, industrielle Protokolle wie Modbus, Profinet oder OPC UA bis auf Ebene 7 zu rekonstruieren. Herkömmliche, nur auf typische IT-Sicherheitsbedrohungen in Unternehmensnetzen spezialisierte Firewalls sind nicht in der Lage, Industrieprotokolle zu verstehen und den darüber fließenden, möglicherweise schädlichen Datenverkehr zu unterbinden. Die Fähigkeit von Industrie-Firewalls selbst Scada-Protokolle tiefgreifend zu analysieren, ermöglicht auch die Abwehr von Zero-Day-Angriffen, für die es noch keine Signatur gibt. Im Allgemeinen gilt es zudem, Attacken so schnell wie möglich zu erkennen und aufzuhalten. Zu diesem Zweck ist es nützlich, Industrie-Firewalls mit IDS-Funktion (Intrusion Detection System) einzusetzen, die kritische Segmente im Netzwerk ständig überwachen.

Notfallplan

Ein Notfallplan ist in jedem Fall unerlässlich. Er muss Verantwortlichkeiten, Meldewege und Eskalationsstufen festlegen, um für einen Angriff gerüstet zu sein. Sollte für ein internes Notfallteam nicht genügend Personal zur Verfügung stehen, empfiehlt es sich, auf externe Dienstleister zurückzugreifen. ■

Uwe Gries,
Country Manager DACH,
Stormshield SAS
www.stormshield.com/de/

Bild: Stormshield SAS

Maßnahmen gegen zunehmende Cybervorfälle

Risiken eindämmen

Auch auf Schiffen steigen die Vorfälle im Bereich Cybersecurity. Die klassischen Kaskoversicherungen für Schiffe decken derartige Angriffe jedoch in der Regel nicht ab. Deshalb haben Phoenix Contact und die Versicherung Lampe & Schwartze eine Lösung auf Basis der Security-Router FL mGuard des Herstellers entwickelt.

Auf Schiffen wird eine zunehmende Anzahl von Maschinen und Anlagen via Ethernet miteinander vernetzt. Ohne entsprechende Schutzmaßnahmen breiten sich Störungen oder Ausfälle daher sehr schnell über das Schiffsnetzwerk aus. Auslöser für die Beeinträchtigungen können sowohl Cyberangriffe als auch die Unwissenheit der eigenen Mitarbeiter sein. Um Schäden auf den Schiffen, Stillstandzeiten und hohe Kosten zu vermeiden, ist eine Absicherung der Schiffe adäquat. Eine Lösung dafür ist der Security-Router der Produktfamilie FL mGuard von Phoenix Contact. Er wird in die abrufbaren Frühwarnsysteme eingebunden und verkürzt damit die Alarmreaktionszeit.

Meist Ausschlussklausel für Cyberangriffe

Es gibt verschiedene Herausforderungen in Bezug auf Cybersecurity. Zum einen fürchten Reeder den Kontrollverlust des auf See befindlichen Schiffs. Zum anderen möchten sie Unterbrechungen der Betriebskontinuität an der Hafenmauer verhindern. Das Be- und Entladen der Schiffe soll nicht gestört werden. Doch viele Reeder bedenken dabei nicht, dass die Mehrheit der Kaskoversicherungen für Schiffe die Ausschlussklausel CL380 10/03 für Cyberangriffe beinhalten. Die internationale Seeschifffahrtsorganisation IMO hat Leitlinien für den Aufbau eines IT-Sicherheitsstandards herausgegeben. Als erheblich zeigte sich z.B. der Security-Vorfall bei Maersk. Hier war das komplette IT-System des Unternehmens betroffen, sodass die Schiffe weder be- noch entladen werden konnten. Zur Verkürzung der Betriebsunterbrechungszeiten tauschte Maersk die meisten seiner Server und Router aus. In Summe entstand ein hoher Schaden, der im wesentlichen versicherbar gewesen wäre. Über Schäden an der Schiffs-IT wurde nichts bekannt. Für den Reeder ist es wichtig zu wissen, dass das Ship-IT- und das Onshore-IT-System als ein einziges IT-System mit allen spezifischen Belangen betrachtet und versichert werden muss.

Schnelle Ausbreitung in flachen Netzwerkstrukturen

Private Laptops der Besatzungsmitglieder verursachen Störungen, die sich z. B direkt in das Schiffsnetz übertragen. Bei gro-

Bild: ©Ivan Cholakov/Shutterstock.com / Phoenix Contact Deutschland GmbH

▸ Die industriellen Security-Router von Phoenix Contact sollen die Schiffsnetzwerke vor Cyberangriffen schützen.

Eine Schadsoftware kann über verbundene Smartphones oder Smart Devices in das Netzwerk des Schiffs gelangen.

Mit der zentralen Managementsoftware können Security-Updates schnell, sicher und global auf alle Schiffe aufgespielt werden.

ßen, flachen Netzwerkstrukturen können sich die Störungen im gesamten Netz ausbreiten. Oder ein Mitarbeiter führt aus der Ferne versehentlich Änderungen am falschen System durch. Denkbar ist ebenfalls, dass Daten über eine ungeschützte internetbasierte Satellitenverbindung kopiert oder so Einstellungen am Schiffssystem verändert werden. Ferner könnte Schadsoftware über infizierte Hardware wie USB-Sticks oder Laptops in das Netz gelangen. Gleiches gilt für infizierte Smartphones oder Smart Devices, die sich über die WLAN-Schnittstellen mit dem Schiffsnetz verbinden. An Bord werden zudem in der Regel identische oder nur leicht modifizierte Passwörter vergeben. Verlässt die Besatzung das Schiff dauerhaft, findet keine Änderung dieser oder der Zugriffsrechte statt. Ein wahrscheinlicher Cybersecurity-Vorfall kann zu großen Schäden und hohen Kosten führen.

Maßnahmen gegen Cybersecurity-Vorfälle

Die Wahrscheinlichkeit und Auswirkungen von Cybersecurity-Vorfällen sollten also grundsätzlich reduziert werden. Maßnahmen, wie unbefugten Personen keinen Zugang gewähren, sensible Bereiche stets abschließen und große Schiffsnetzwerke in kleine Einheiten aufteilen, können Abhilfe schaffen. Außerdem sollten ungenutzte Schnittstellen deaktiviert oder blockiert, Lese- und Schreibrechte einschränkt und Fernzugriffe mit Hilfe eines Schlüsselschalters kontrolliert werden. Darüber hinaus ist es hilfreich, wichtige Informationen und die externe Kommunikation zu verschlüsseln und Notfallpläne für Cybersecurity zu erstellen und anzuwenden.

Abhilfe durch Security-Router

Im ersten Schritt kann ein industrieller Security-Router mit maritimer Schiffszulassung die Absicherung unterstützen. Phoenix Contact bietet entsprechende Geräte an, die derzeit über Zulassungen von DNV GL, LR, ABS und BV verfügen. Die industrietauglichen, lüfterlos konzipierten Security-Router FL mGuard bieten zuverlässige Sicherheit und Leistung in einem kompakten, hutschienenmontablen Metallgehäuse. Neben dem zugriffssicheren Aufbau von VPN-Tunneln umfassen die Geräte verschiedene industriespezifische Firewall-Funktionen. Dazu gehören z.B. eine User Firewall sowie eine Conditional Firewall zur Aktivierung definierter Firewall-Regeln. Außerdem verfügen die Geräte über eine Deep Packet Inspection für die Durchleuchtung jedes via OPC Classic oder Modbus TCP übertragenen Datenpakets. Auf diese Weise lässt sich das Defense-in-Depth-Konzept in den Anwendungen realisieren. Durch den sogenannten Stealth-Mode sind die Security-Router FL mGuard im Netzwerk unsichtbar. Werden die Geräte in bestehende Schiffsnetzwerke eingebaut, müssen die IP-Adressen der anderen Netzwerkkomponenten nicht angepasst werden. Der Installations- und Dokumentationsaufwand erweist sich somit als einfach und gering.

Frühzeitige Warnung vor regionalen Angriffen

Die Produktfamilie FL mGuard erweitert die Ship-IT systematisch und macht die Schiffe ausreichend versicherbar bzw. die Versicherungslösung erschwinglich. Ein wesentlicher Teil der Versicherungslösung beruht auf der Online-Überwachung der verbauten Steuerungen. Über das durchgeführte Monitoring werden die IT-Systeme in ein Frühwarnsystem eingebunden, das jedes Schiff individuell vor systemspezifischen oder regionalen Angriffen warnen kann. Bei einem Bruch kann der Dienstleister Phoenix Contact zur Schadensregulierung beauftragen. Die Kosten eines versicherten Schadens übernimmt die Versicherung. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/36483

Gerrit Boysen, Manager Product Marketing Security, Phoenix Contact Electronics GmbH
www.phoenixconntact.de

Achim Fischer-Erdsiek, Managing Partner, Lampe & Schwartze-Gruppe

Bild: Phoenix Contact Deutschland GmbH

Hohe Cyber-Sicherheit durch Thin Clients

Thin Clients der Serie Exicom 500 von R. Stahl HMI Systems erhalten mit dem Firmware Release v5.50 hohe Flexibilität für viele intelligente Funktionen. Die Firmware auf Basis von Windows 10 IoT Enterprise LTSB ist ein geschützter Kiosk Modus, in dem die Rechte des Benutzers eingeschränkt sind und einen Zugriff auf die Betriebssystemebene abriegelt. Zum Sicherheitskonzept gehört zudem ein Filter, mit dem sich der USB-Anschluss auf definierte Speichermedien und andere Geräte beschränken lässt. Zugriff erhalten Nutzer lediglich auf normale Einstellungen sowie für sie eingerichtete Apps wie Citrix-Clients, ERP- oder CCTV-Systeme. Ganz neu ist in der aktuellsten Firmware die gleichzeitige Darstellung unterschiedlicher Sessions.

R. Stahl Schaltgeräte GmbH
www.r-stahl.com

Industrieanlagen absichern

Bild: obs/DXC Technology/Monty Rakusen

Die gemeinsame Lösung von DXC und CyberX basiert auf einer integrierten Leitstelle, um die digitale Transformation abzusichern. Die Kommunikation zwischen Anlagen und Maschinen wird produktionsnah erfasst und schrittweise auf Sicherheitsbedrohungen in Echtzeit analysiert und bewertet. Die CyberX-Plattform soll einen schnellen Überblick über OT Assets, Schwachstellen und Bedrohungen bieten, die derzeit in der Produktion und Kontrolle der Kunden vorhanden sind. Dazu trägt der nicht-invasive Ansatz, die patentierte IoT/ICS-fähige Verhaltensanalyse und das maschinelle Lernen bei.

DXC Technology
www.dxc.technology

GATEWAY MIT FIREWALL- UND IT-SECURITY-FUNKTIONEN

Um bestehende S7-Anwendungen technisch und wirtschaftlich an OPC-UA-Clients anzubinden, bietet Insevis ein S7-IIoT-Gateway inklusive Firewall- und IT-Security-Funktionen an. Auf der LAN-Seite scannt das Gateway bis zu 2.000 Datenpunkte von bis zu 100 Partnern über aktive S7-Kommunikation (Put/Get) ein. Damit sind keine Änderungen und Freigabeprozeduren an den CPUs nötig. Auch über Modbus-TCP können Datenpunkte ausgelesen werden. Auf der WAN-Seite erfolgt die Kommunikation über OPC UA. Ein frei definierbarer Namespace erlaubt die genaue Abbildung der Kundenanlagen, alternativ können die Namespaces der S7-1500 verwendet werden. Der Anwender kann sie über einen integrierten und komfortabel zu bedienenden Web-Konfigurator mit Zugangsbeschränkung und einer umfangreichen Benutzerverwaltung konfigurieren. Dadurch muss er keine eigene Software mehr installieren. Das integrierte NodeRed bietet viele konfigurierbare Verbindungen, z.B. zu MQTT-Brokern, als SMTP-Client, Java-Skripte, Twitter-Meldungen und Sprachausgaben.

Insevis GmbH
www.insevis.de

Werkzeugmaschinen vor Cyberattacken schützen

Balluff hat ein Expertenteam etabliert, um Kunden eine ganzheitliche Beratung anzubieten. Einige der hauseigenen Geräte verfügen mittlerweile zudem über Hardware-Verschlüsselung mittels Trusted Platform Modul. Bei der digitalen Serviceunterstützung setzt das Unternehmen auf eine sichere und workflowbasierte Punkt-zu-Punkt-Verbindung. Ein weiterer Aspekt ist der Ort der Datenspeicherung. Drei von zehn Unternehmen (29%) nutzen eine Cloud-Lösung, die in ein zertifiziertes Rechenzentrum ausgelagert ist. Weitere 10% planen dies und 28% diskutieren darüber. Das zeigt der Digital Office Index 2018 des Digitalverbands Bitkom. Betrachtet man die unterschiedlichen Branchen, ist der Maschinen- und Anlagenbau Vorreiter. Bereits fast jedes zweite Unternehmen aus dieser Branche greift auf externe Clouddienstleister zurück. Vorteile einer Public Cloud sind z.B. eine einfache Skalierbarkeit, ein hohes Maß an Sicherheit, die Nutzung neuester Technologien, die Servicekontinuität und Verschlüsselung. Damit ist das Funktionieren der Lösungen auch beim Eintreten negativer Szenarien garantiert. Symmedia aus Bielefeld dagegen bietet den Kunden hybride Lösungen an, wodurch diese Flexibilität, einhergehend mit außerordentlicher Sicherheit, erhalten sollen.

Balluff GmbH
www.balluff.com

Datenexplosion und Wachstumschancen

Zwei Studien brachten es kürzlich an den Tag: Die von den Unternehmen weltweit produzierte Datenmenge wächst ins Unermessliche. Und wenn es gelänge, diese Daten flächendeckend für den Einsatz künstlicher Intelligenz in der Wirtschaft zu verwenden, hätte dies einen enormen Wachstumseffekt zur Folge. Aber unstrittig ist auch: Deutsche KMU nutzen das Wertschöpfungspotenzial von Daten – bis hin zu völlig neuartigen KI-Anwendungen – bislang kaum. Das Hamburger Unternehmen Cybus zeigt auf einfache und kostengünstige Weise, wie gerade KMU von bisher ungeahnten Möglichkeiten profitieren können. Aus der Schule ist noch bekannt, dass die erfolgreiche Verbreitung der Dampfmaschine die Produktionsbedingungen der damaligen Welt völlig auf den Kopf stellten. Nach einer Studie des McKinsey Global Institute ist das aber noch nichts im Vergleich dazu, was die Einführung von KI zukünftig vermag. Die Grundlage dafür – genügend Daten als 'Rohstoff' für die Algorithmen – schafft die Wirtschaft bereits heute. So soll das weltweite Datenvolumen bis 2025 auf 175ZB (eine Zahl mit 21 Nullen) anwachsen (2017: 23ZB). Für einen erfolgreichen Weg ins IIoT müssen die selbst produzierten Daten zunächst organisiert und analysiert werden. Aber schon hier schrecken viele KMU mit ihrem oftmals heterogenen Maschinenpark und zumeist nur kleinen IT-Abteilungen zurück.


Bild: ©metamorworks/Fotolia.com

Cybus GmbH
www.cybus.io

Überwachungssystem für Industrienetze

Insys und Rhebo präsentieren eine gemeinsame Lösung für eine sichere und stabile Kommunikation, Datenerfassung und Datenverarbeitung in Industrienetzen. Der Industrial Protector von Rhebo ist ein passives, rückwirkungsfreies Überwachungssystem für die Kommunikation in der industriellen Steuerungstechnik sowie in Leitsystemen und läuft direkt auf den Routern von Insys. Dessen Linux-Container bieten einen hohen Virtualisierungsgrad. Betreiber von Steuerungsnetzen können so direkt über den Router den Datenverkehr aufzeichnen, der hinter dem Router stattfindet. Die Daten werden dann stark komprimiert an die Anomalieerkennung geschickt, um Cyberangriffe oder technische Fehlerzustände zu identifizieren. Das Überwachungssystem analysiert fortlaufend die Kommunikation in der Steuerungstechnik und wertet sie in Echtzeit aus.

Insys Microelectronics GmbH
www.insys-tec.de

SOFTWARE FÜR SICHERE ANDROID-ANWENDUNGEN

Datalogic kündigt die neue Sicherheitssoftware Shield an. Die Lösung wurde entwickelt, um Kunden, die mobile Computer mit Android einsetzen, einen verlängerten Produktlebenszyklus zu bieten und somit deren Investition zu schützen. Mit Shield können Kunden ihre Standardsicherheitsprogramme, die häufig eine Laufzeit von zwei bis drei Jahren aufweisen, auf mehr als fünf Jahre verlängern. Im Paket enthalten sind außerdem regelmäßige Firmware Updates, die sowohl Sicherheitspatches von Google als auch vom Prozessorhersteller enthalten und Datalogic Fehlerbehebungen und Verbesserungen abbilden. Damit Kunden die neuesten Funktionen der Android Plattform umfassend nutzen können, bietet Shield auch Upgrades auf die aktuellsten Android-Hauptversionen. Damit in solchen Fällen ein reibungsloser Übergang stattfinden kann, gibt es eine zwölfmonatige Übergangsunterstützung für die vorhergehende Android-Version. Über neue Updates werden Anwender automatisch informiert, indem sie sich für eine individuelle Benachrichtigung per E-Mail registrieren. Shield ist für die folgenden Mobilcomputer von Datalogic verfügbar: Joya Touch A6, Memor 1, Memor 10 sowie alle zukünftige Mobilcomputer von Datalogic, die auf Android basieren. Mit der Verfügbarkeit von Shield gibt es außerdem eine neue Datalogic Programmier-Site, auf der Anwender alle Software-Tools für mobile Geräte finden.


Bild: ©Nmedia/Fotolia.com

Datalogic S.r.l.
www.datalogic.com

DIE APP ZUM SPS-MAGAZIN

ALLE WICHTIGEN AUTOMATISIERUNGS-NEWS VON A BIS Z SOFORT ERFAHREN!

Mit der kostenlosen App erfahren Sie alle relevanten Themen aus der Automatisierungstechnik sofort. Features wie die Vorlesefunktion, Push-Nachrichten, Bookmark-Listen und die einfache Navigation machen das Lesen zu einem neuen Erlebnis.

JETZT KOSTENLOS DOWNLOADEN!

Laden im App Store

JETZT BEI Google Play

NEWS ARENA

powered by: SPS MAGAZIN

SYSTEMSICHERHEIT

HÄNGT NICHT NUR AM SEIL!

Wie sicher ist Ihr Netzwerk?

WALL IE – INDUSTRIAL NAT GATEWAY / FIREWALL

Sichere Kommunikation und einfache Adressierung

Mit dem Siegeszug der Ethernet-Vernetzung spielt auch Cybersecurity eine ganz zentrale Rolle. **WALL IE** schützt ihr Automatisierungsnetzwerk sicher vor unbefugten Zugriffen. Durch die individuelle Konfiguration kann die Firewall ganz leicht an Ihre Anforderungen angepasst werden.

- Zugriffsbeschränkung durch Paketfilter
- Geringer Aufwand zur IP-Integration in übergeordnete Netzwerke (NAT)
- Hohe Netzwerksicherheit
- Schnelle und einfache Konfiguration durch ein responsives Webinterface
- Integration von Serienmaschinen mit gleichen IP Adressen

www.helmholz.de

Helmholz®
COMPATIBLE WITH YOU