SPS MAGAZIN
SONDERAUSGABE 3/2020
www.sps-magazin.de

# INDUSTRIAL COMMUNICATION JOURNAL

ETHERNET WIRELESS SECURITY


Titelbild: IBHsoftec Gesellschaft für Automatisierungstechnik mbH / ©Song_about_summer/©Nataliya Hora/©roystrmzy/stock.adobe.com

IBH Link IoT und TeamViewer

## Mehr als nur sicherer Zugriff auf die Maschine

Seite 6

TeamViewer Internet of Things

IBHsoftec

### SENSOREN IM INTERNET DER DINGE
LoRa – die komplementäre Technologie
Seite 21

### ENDLICH EINIGKEIT BEI M12 PUSH-PULL?
Interview Push-Pull-Steckverbinder M12
Seite 26

### STEUERUNGSUNABHÄNGIGE DIAGNOSE IN ETHERCAT
Herstellerübergreifende Transparenz
Seite 28

# 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

sps connect
The digital automation hub

**24. – 26.11.2020**
Virtuell

New Automation Technology **BECKHOFF**

# Der Preis der Daten

## *Vernetzte Fertigung braucht sichere Begleitung*

***Die Industriekommunikation ist ohne Zweifel im Wandel. Während in den Anfangsjahren die Steigerung der Performance oberstes Ziel war, wird diese jetzt schlichtweg vorausgesetzt. In den Fokus der produzierenden Unternehmen rücken Themen, die sich im Umfeld von Industrie 4.0 oder dem IIoT bewegen. Geschwindigkeit und Determinismus sind allenfalls im Bereich der Drahtlos-Technologien noch ein wichtiges Thema, also z.B. bei WI-FI 6 oder 5G.***

Kai Binder, Chefredakteur SPS-MAGAZIN

Viele Jahre lang haben sich Unternehmen vor Hackerangriffen sicher gefühlt. Einerseits, weil die Vernetzung der Produktion nicht sonderlich ausgeprägt war. Andererseits, weil ein gewisses Maß an Expertenwissen notwendig war, um die speziellen Technologien der Industriefertigung mit den Bordmitteln der Hacker lahmzulegen. Gegangen wäre es – manchmal auch sehr einfach. Mit der durchgängigen Vernetzung – der vertikalen und horizontalen Integration der Fertigungsunternehmen zu Smart Factory – und der Nutzung der Cloudtechnologien verlassen die Daten zunehmend das halbwegs sichere Umfeld der (proprietären) Fertigungsinseln und des eigenen Betriebsgeländes.

Mit der vermehrten Nutzung von Standard-IT-Architekturen im Produktionsumfeld, gepaart mit der Vernetzung bis in den letzten Winkel der Fertigung, steht das Thema Security ganz oben auf der Agenda der Industrie, weil sie zum attraktiven Ziel von Kriminellen geworden ist. Damit verändern sich auch die Aufgaben der Industriekommunikation und Security muss bereits im Design einer Verbindung mitgedacht werden. Man muss sich bewusst werden, dass Security kein Zustand ist, sondern ein Prozess, der dauerhaft zu unseren Aufgaben gehört. Die Implementierung dieser Prozesse ist ein erheblicher Aufwand, der sich allerdings rechnet: Um das Ausmaß der Bedrohung für Produktionsunternehmen zu beschreiben, eignet sich gut eine Pressemeldung des Bitkom aus dem vergangenen Jahr. Da heißt es: *„Durch Sabotage, Datendiebstahl oder Spionage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 102,9 Milliarden Euro (2019) – analoge und digitale Angriffe zusammengenommen. Der Schaden ist damit fast doppelt so hoch wie noch vor zwei Jahren (2016/2017: 55 Milliarden Euro p.a.). Drei Viertel der Unternehmen (75 Prozent) waren in den vergangen beiden Jahren von Angriffen betroffen, weitere 13 Prozent vermuten dies."*

Es ist also durchaus eine gute Idee, bei diesem Thema seine Hausaufgaben zu machen. Denn die Vernetzung setzt sich fort: deterministisch, wireless und sicher. Daher finden Sie auch all diese Themen in dieser Ausgabe des INDUSTRIAL COMMUNICATION JOURNALs. Ich wünsche wie immer viel Spaß beim Lesen.

Ihr Kai Binder
kbinder@tedo-verlag.de


Bild: IBHsoftec Gesellschaft für Automatisierungstechnik mbH




## Marktübersicht Security

**Seite 40**

Jetzt anmelden!


# SPS MAGAZIN TechTalks

## Ein Thema – Drei Firmen – Eine Stunde

Die SPS TechTalks präsentieren die neuesten Trends und Anwendungen der Automatisierungsbranche in mehreren einstündigen Webinaren. In ihren zwanzigminütigen Vorträgen stellen jeweils drei Unternehmen aktuelle Produkte und Lösungen zu einem Thema vor.

| Termin | Thema |
|---|---|
| **10. November,** 10:30 Uhr | Nächste Generation der Maschinensteuerung: on der SPS zum IoT-Controller |
| **10. November,** 15:30 Uhr | So geht HMI heute: Visualisierung mit Webtechnologien |
| **11. November,** 10:30 Uhr | Industrial 5G - Was die neue Drahtlostechnologie für die Automatisierung bringt |
| **11. November,** 14 Uhr | SPE- Einfache und flexible Kommunikation im Feld |
| **11. November,** 15:30 Uhr | Track-Systeme für die Next Generation - Antriebslösungen |
| **17. November,** 10:30 Uhr | Moderne Tools für die Elektrokonstruktion |
| **17. November,** 15:30 Uhr | Analytics an der Maschine |
| **17. November,** 15:30 Uhr | Aus dem IoT auf die Maschine. Remote Management – aber sicher! |
| **18. November,** 15:30 Uhr | Wartung, Analyse, Produktivität: Motoren im industriellen IoT |
| **18. November,** 15:30 Uhr | Wettbewerbsvorteil durch Digital Twin und Simulation |
| **01. Dezember,** 15:30 Uhr | Komponenten und Lösungen für smarte Verbindungstechnik |
| **01. Dezember,** 15:30 Uhr | Saftey needs Security: Ganzheitliche Sicherheit in der smarten Fabrik |

**Sprache:** Deutsch | **Moderation:** Kai Binder, Mathis Bayerdörfer

Kostenlos Anmelden unter **sps-magazin.de/techtalks**

*IBH Link IoT und TeamViewer*

# Mehr als nur sicherer Zugriff auf die Maschine

***Die Firmen IBHsoftec und TeamViewer haben in einer Kooperation eine Lösung für den Fernzugriff auf Maschinen, Anlagen und Geräte geschaffen. Der IBH Link IoT besteht aus einer IBHsoftec-Schnittstellenhardware und der TeamViewer IoT-Software und bündelt damit die Kompetenzen beider Unternehmen in einem Produkt. Wir haben uns die vorgestellte Remote-Lösung einmal genauer angeschaut.***


Remote Services für eine Maschine sind nicht nur in Pandemie-Zeiten für einen möglichst reibungslosen Produktionsablauf von großer Bedeutung. Steht eine Maschine, ist es heute einfach nicht mehr zeitgemäß, zwei Tage auf einen Servicetechniker zu warten, der dann ein Problem löst, welches er ebenso gut auch mittels Fernzugriff hätte lösen können, vielleicht mit einer helfenden Hand an der Maschine vor Ort. Beispiele für solche Situationen kennen wir alle nur zu gut. IBHsoftec und TeamViewer machen Remote-Service-Einsätze jetzt nicht nur einfach, sondern sorgen auch noch dafür, dass die helfende Hand vor Ort genau sieht, was sie tun soll. Doch dazu später mehr ...

## Sicheren Zugriff einfach machen

Fest steht: Ein einfacher, sicherer und zuverlässiger Zugriff auf die Maschinensteuerung ist gar nicht so einfach zu etablieren und über Jahre hinweg zu pflegen. Dafür hat IBHsoftec gemeinsam mit TeamViewer nun eine Lösung entwickelt, die mit nahezu allen ethernetfähigen Steuerungen z.B. der Hersteller Siemens, Rockwell, Mitsubishi, Beckhoff, B&R, Bosch Rexroth usw. funktioniert. So wie die Anforderungen der Anwender nach Einfachheit, Sicherheit und Zuverlässigkeit ist auch dieser Fachartikel aufgebaut und behandelt die Aspekte in entsprechender Reihenfolge.

## Expertenwissen ‘out of the Box’

Das Modul IBH Link IoT ermöglicht zusammen mit TeamViewer IoT den einfachen und sicheren Zugriff auf Steuerungen und deren Programmierung. Das gesamte Expertenwissen, das notwendig ist, um eine sichere Fernwartung zu ermöglichen, steckt in dieser Kombi-Lösung. Im Kern ist dies ein kompaktes Gerät zur Hutschienenmontage mit vier Ethernet-Ports und einer 24V-Stromversorgung, das als Gateway für alle ethernetfähigen Steuerungen über die Protokolle TCP und UDP dient. Die vorinstallierte TeamViewer Software und das dazugehörige Management-Portal sorgen dafür, dass man sicher und einfach aus der Ferne auf das Gateway zugreifen kann. Die Implementierung ist dabei denkbar unkompliziert: Ein vom Maschinenhersteller vorkonfigurierter IBH Link IoT wird in die Maschine integriert, indem eine Schnittstelle an die SPS, die andere an das Firmennetzwerk angeschlossen wird – fertig. So muss selbst für die Implementierung der Fernwartungsfunktion kein Techniker des Maschinenherstellers zum Endanwender fahren. Auch die Konfigurationsaufgaben auf Seiten des Service-Anbieters sind schnell und einfach zu erledigen. Zu ihnen gehört beispielsweise die Eingabe eines Assignment-Keys in die Managementkonsole, der für die eindeutige Identifikation des Gerätes bei der Kommunikation notwendig ist.

Bild: IBHsoftec Gesellschaft für Automatisierungstechnik mbH

Nur mit dem korrekten Assignment-Key ist der Aufbau der Remote-Verbindung überhaupt möglich. Auch Benutzergruppen und Rollen mit entsprechenden Berechtigungen können in der Managementkonsole konfiguriert werden. Für den Verbindungsaufbau bedarf es keinerlei Anpassung von Firewallregeln oder Portfreigaben, denn durch die TeamViewer-Technologie wird der Datentunnel aus dem Zielnetzwerk heraus geöffnet und das Zielgerät lässt die Verbindung nur von legitimierten Geräten und Personen zu.

## Management mit gewohnten Werkzeugen

Diese Architektur hat sowohl für den Maschinenhersteller, der die Fernwartung durchführt, als auch für den Endkunden zahlreiche Vorteile. Komplexe und aufwändige Konfigurationsarbeiten entfallen. Dadurch ist die Lösung in der Regel 'out of the Box' einsatzbereit. Anwender und Hersteller können in der für sie gewohnten Umgebung arbeiten, ohne dass an der Steuerung bzw. dem Maschinenprogramm irgendwelche Konfigurationsanpassungen durchgeführt werden müssen. So bleiben auch die IP-Adressen der SPSen im Original-Zustand. Die Verbindung auf die Steuerung erfolgt in gleicher Weise, als wäre der Service-Mitarbeiter vor Ort.

## Performance auch bei kleinen Bandbreiten

'Wie vor Ort' bezieht sich im Übrigen auch auf die Performance. Hier macht sich die ausgereifte TeamViewer-Technologie bemerkbar. Das Tool bevorzugt UDP-Verbindungen, was den Kommunikationsoverhead deutlich reduziert. TeamViewer ist außerdem eine Punkt-zu-Punkt-Verbindung, wodurch die Performance die volle Bandbreite der Verbindung nutzen kann. Das macht TeamViewer sehr schnell. Bei der Fernwartung von SPSen macht sich positiv bemerkbar, dass keinerlei Bildschirmdaten übertragen werden, weil die Anwendung, also das SPS-Management-Tool, beim Serviceanbieter läuft. Das macht die Lösung von IBHsoftec und TeamViewer so performant, dass sie auch bei geringen Bandbreiten zuverlässig funktioniert.

## Einfache Nachrüstung auch für Altanlagen

Da die Lösung von IBHsoftec keinerlei Änderung an der bestehenden Automatisierungslösung erfordert, ist die Nachrüstung von bestehenden Anlagen problemlos möglich. Tatsächlich ist genau dies eine Spezialität des Unternehmens. Selbst längst abgekündigte Generationen von Steuerungen beispielsweise aus der S5-Reihe können durch die verschiedenen Geräte von IBHsoftec bei Bedarf in die OPC-UA-Kommunikation integriert werden (mittels IBH Link UA). Gerade weil ältere Steuerungen überhaupt nicht auf die Sicherheitsrisiken der modernen Cyber-Welt vorbereitet sind, ist eine Einbindung in Fernwartungslösungen überhaupt

## *Liste kompatibler Steuerungen*

- ✔ *Simatic S5, S7-200, S7-300, S7-400, S7-1200, S7-1500,*
- ✔ *Siemens Logo!*
- ✔ *Sinumerik-CNC 840D*
- ✔ *Rockwell Controllogix und Compactlogix*
- ✔ *Mitsubishi Melsec IQR, FX5, QnA und L Serie*
- ✔ *Mitsubishi- Roboter*
- ✔ *Bosch Rexroth*
- ✔ *Beckhoff*
- ✔ *B&R*

*sowie alle ethernetfähigen Steuerungen, die über die Protokolle TCP und UDP erreichbar sind.*

# *VDMA mahnt mehr Cyberschutz für Produktion an*

***Mehr als die Hälfte der deutschen Industrieunternehmen hat durch Cyberattacken finanzielle Schäden erlitten, so eine Studie des VDMA. Dass die Zahl solcher Angriffe abnimmt, ist nicht in Sicht. Daher wird es immer wichtiger, Industrial Networks und Operational Technology (OT)-Umgebungen zu schützen. Dabei helfen Ansätze, die auch beim Schutz von Büronetzwerken Verwendung finden.***

*Auf rund 103 Milliarden Euro schätzt der Digitalverband Bitkom die Schäden, die deutsche Unternehmen durch Cyberangriffe im letzten Jahr verzeichneten. Mehr als ein Fünftel der Firmen war von Datenspionage betroffen. In 17 Prozent der Unternehmen sabotierten Angreifer Produktionsanlagen und Informationssysteme. Zu vergleichbaren Ergebnissen kommt der VDMA in der Studie Cyberrisiken im Maschinen- und Anlagenbau von 2019. Demnach führten bei der Hälfte der Unternehmen Cyberattacken zu finanziellen Schäden. Als Ursache dafür werden zum einen Produktionsausfälle angeführt, zum anderen waren bei fast einem Drittel der Unternehmen Hackerangriffe dafür verantwortlich. Mithilfe von Erpressersoftware (Ransomware) die Daten auf IT- und OT-Systemen zu verschlüsseln und erst nach Zahlung eines Lösegelds wieder freizugeben – oder auch nicht.*

nur dann verantwortbar, wenn solide Sicherheitsmechanismen in der Fernwartungslösung vorhanden sind. Hier kommt eine der Kernkompetenzen von TeamViewer, ihre Anwendung robust und resilient gegen die Angriffe von Cyberkriminellen zu halten, zum Tragen (siehe auch Kasten).

## Kostenlose Updates für IBH Link UA

Viele Anwender kennen bereits die oben schon erwähnte IBH-Lösung zur Einbindung älterer Steuerungen in die OPC-UA-Kommunikation IBH Link UA. Für Besitzer dieser Geräte steht eine neue Firmware mit der TeamViewer-Funktion kostenfrei zur Verfügung. Es wird lediglich eine Lizenz von TeamViewer benötigt. So können auch sie ihre Anwendung einfach per TeamViewer fernwarten.

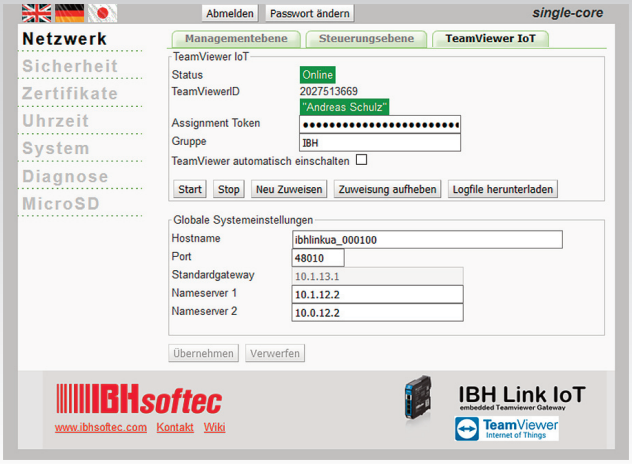
## Sicherheit ist kein Zustand, sondern ein Prozess

Jeder weiß, dass Sicherheit kein Zustand ist, sondern ein Prozess. Wer eine sichere Fernwartungslösung entwickeln möchte, benötigt tiefe Kenntnis und langjährige Erfahrung, um den Machenschaften der Cyberkriminellen möglichst keine Angriffsfläche zu bieten. Als Maschinenbauer muss man sich an dieser Stelle daher auf Unternehmen verlassen, die diese Kenntnis mitbringen. TeamViewer-Verbindungen laufen über komplett gesicherte Datenkanäle, die mit einem RSA Public/Private Key Exchange aufgebaut und mit 256-Bit-AES verschlüsselt sind. Diese Technik wird in vergleichbarer Form auch bei https/SSL eingesetzt und entspricht dem neuesten Stand der Technik. Da der Private Key niemals den Client – in diesem Fall das IBH Link IoT – verlässt, ist durch dieses Verfahren technisch sichergestellt, dass Dritte den Datenstrom nicht entschlüsseln können. Das gilt somit auch für die TeamViewer Routingserver. Nicht einmal TeamViewer als Betreiber der Routingserver könnte den verschlüsselten Datenverkehr lesen.

## *Ziele von Remote Service*

- ✔ *Reisekosten vermeiden*
- ✔ *Responsezeiten verkürzen*
- ✔ *Produktionsausfälle reduzieren*
- ✔ *Durchschnittliche Zeit für Reparaturen reduzieren*
- ✔ *Qualitätssicherungsprozess von Produkten steigern*
- ✔ *Equipment-as-a-Service-Angebote*
- ✔ *Produktionsausschuss reduzieren*
- ✔ *Produktivität der Mitarbeiter steigern*






Konfiguration über Web-Interface

## Ein Bild sagt mehr …

Der Blick in das SPS-Programm verrät viel, manchmal muss man sich allerdings auch – im wahrsten Sinne des Wortes – ein Bild von der Maschine machen. Passend dazu gibt es das Produkt TeamViewer Pilot, das nicht nur eine Video-Übertragung von der Maschine zum Service-Manager ermöglicht, sondern das auch einen Rückkanal bietet, durch den der Servicetechniker mittels Augmented Reality entsprechende Anweisungen direkt in das Live-Bild der Anlage auf dem Bildschirm eines Mobilgeräts einblenden kann. Dies erfolgt beispielsweise durch Pfeile oder einfache Freihandzeichnungen. So kann der Anwender einen Echtzeit-Videostream an den Service-Profi übertragen und gleichzeitig durch grafische 3D-Symbole erklärt bekommen, wie er die notwendigen und richtigen Handgriffe an der Maschine ausführen muss, damit alles wieder läuft. Dadurch ist TeamViewer Pilot die perfekte Ergänzung für die Fernwartungslösung von Maschinen- und Anlagenbauern und ein modernes Werkzeug für Service und Maintenance.

## Fazit

Sowohl IBHsoftec als auch TeamViewer sind ausgewiesene Experten auf ihrem Gebiet mit jahrzehntelanger Erfahrung. Durch die Kombination dieses Knowhows in einer Lösung ist mit dem IBH Link IoT für Anwender ein Produkt entstanden, das einen einfachen, sicheren und robusten Fernzugriff auf Maschinen und Anlagen zulässt. Remote Services sind nicht nur in Pandemie-Zeiten von größter Bedeutung. Sie reduzieren die Kosten und erhöhen die Produktivität. Wer eine technische Plattform für seine Remote-Services sucht, der sollte sich daher die Lösung der beiden Partner genauer ansehen. ■



IBHsoftec GmbH
www.ibhsoftec.com

TeamViewer Germany GmbH
www.teamviewer.com

Bild: IBHsoftec Gesellschaft für Automatisierungstechnik mbH

# Neues Konzept für das Anlagen- und Geräte-Monitoring

Das neue Konzept der Namur Open Architecture (NOA) hat das Ziel, Produktionsdaten einfach und sicher für die Anlage- und Geräteüberwachung (Monitoring) sowie Optimierungen nutzbar zu machen. Smarte Sensoren, Feldgeräte, mobile Geräte und die allgegenwärtige Nutzung von IT-Geräten generieren immer mehr Daten, die innerhalb der klassischen Namur-Automatisierungspyramide für den Nutzer kaum zugänglich sind. NOA will das ändern, ohne die breit akzeptierten Vorteile traditioneller Automatisierungsstrukturen zu beeinflussen, indem die Daten auf einem zweiten Kanal rückwirkungsfrei übertragen werden. Das Konzept eignet sich somit für bestehende Anlagen (Brownfield). Außerdem ist NOA mit aktuellen Weiterentwicklungen in der Automatisierung, wie z.B. dem Advanced Physical Layer (APL) oder dem modularen Ansatz (MTP), kompatibel, wodurch es sich auch für Neuinstallationen (Greenfield) zukunftssicher einsetzen lässt. NOA nutzt die traditionellen Prozessautomatisierungssysteme und definiert eine neue Monitoring- und Optimierungsdomäne. Die Architektur setzt sich dabei aus den folgenden Bausteinen zusammen: ein standardisiertes Informationsmodell (NOA-IM) basierend auf OPC UA, die NOA-Diode, die NOA-Verification-of-Request-Komponente und das Konzept des NOA Aggregating Servers.

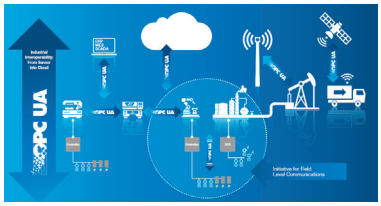
Namur - Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.
**www.namur.net**

# PNO wählt neuen Vorstand

Die diesjährige Mitgliederversammlung der Profibus Nutzerorganisation fand aufgrund von Covid-19 erstmals virtuell statt. Im Rahmen der turnusmäßigen Vorstandswahl wurden als Vorsitzender Karsten Schneider von Siemens und als Stellvertreter Prof. Dr. Frithjof Klasen von der TH Köln sowie Dr. Jörg Hähniche von Endress + Hauser Process Solutions wiedergewählt. Neu in den Vorstand gewählt wurde Frank Moritz von Sick. Die Mitgliederversammlung bestätigte ferner die Beiräte Klaus Erni von Emerson, Marco Henkel von Wago, Andreas Hennecke von Pepperl+Fuchs, Dr. Hans Krattenmacher von SEW-Eurodrive, Martin Müller von Phoenix Contact, Matthias Prinzen von Festo und Frank Welzel von Harting.

Profibus Nutzerorganisation
**de.profibus.com**

# Vorstellung der FLC-Spezifikation für Oktober geplant

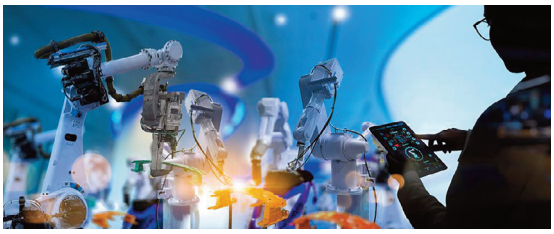



Seit dem Start der FLC-Initiative auf der SPS 2018 sind mehr als 60 Mitgliedsunternehmen in den sieben FLC-Working-Groups der OPC Foundation tätig. Die daraus hervorgehenden Spezifikationen sollen das OPC UA Framework um spezifische Funktionen für Automatisierungskomponenten auf der Feldebene erweitern. Aktuell gehen die Planungen davon aus, einen ersten Release Candidate Ende Oktober vorstellen zu können. Darin wird es vor allem um die Anbindung von Steuerungen untereinander gehen.

OPC Foundation Europe
**www.opcfoundation.org**

## Forschungsprojekt für dynamisches Netzwerkmanagement in der Industrie

Im Projekt 'Kitos – Künstliche Intelligenz für TSN zur Optimierung und Störungserkennung' arbeiten Wissenschaftler und Ingenieure gemeinsam an Lösungen für ein dynamisches Netzwerkmanagement in der Industrie. Hier sollen Konzepte für das Management TSN-basierter Netzwerke unterstützt durch künstliche Intelligenz entwickelt werden. Die Konsortialpartner arbeiten an KI-Algorithmen, die Netzwerken die notwendige Dynamik und Zuverlässigkeit für Industrie-4.0-Szenarien geben und es den Anwendern erlauben, diese einfach und ohne tiefere Netzwerk- oder KI-Kenntnisse einzusetzen. Intelligente Werkzeuge unterstützen bei der Entscheidungsfindung, erlauben eine effizientere Ressourcennutzung und ermöglichen performantere Konfigurationen. Dabei sollen selbstlernende Verfahren, die sich stetig weiterentwickeln, genutzt und zur Konfiguration und Verbesserung eines modernen Kommunikationsnetzes eingesetzt werden. So soll z.B. ein besserer Schutz gegen Ausfälle erreicht oder auftretende Probleme bei Überlastungen gelöst werden.



Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI)
**www.dfki.de**

## Internationaler Standard für Laborgerätekommunikation

Die OPC Foundation hat im Rahmen ihrer Hauptversammlung die Gründung der Joint Working Group 'LADS – Laboratory Agnostic Device Standard' verkündet, der neben der OPC-Foundation die Industrieverbände Spectaris und VDMA angehören. Das Ziel von LADS ist die Schaffung eines herstellerübergreifenden, offenen Standards für Analysen- und Laborgeräte, der umfassend die verschiedenen Kundenbranchen und ihre jeweiligen Workflows abbildet, nachhaltig anwendbar ist und auch künftigen Anforderungen der Digitalisierung und Automatisierung gerecht wird. Im Rahmen der OPC UA Working Group wird der Standard als sogenannte OPC UA Companion Specification für Analysen- und Laborgeräte erarbeitet. Das ermöglicht auch die Anbindung an die klassische industrielle Infrastruktur.

OPC Foundation Europe
**www.opcfoundation.org**

## OPC-UA-Spezifikation für Profinet veröffentlicht

Die Nutzerorganisation von Profibus und Profinet hat die erste OPC-UA-Companion-Spezifikation für Profinet veröffentlicht. Sie beschreibt ein standardisiertes OPC-UA-Objektmodel für Profinet-Geräte. Dadurch können Komponenten von unterschiedlichen Herstellern einheitlich Gerätedaten übergeben. So ist es für Tool-Hersteller einfacher, die Informationen herstellerübergreifend einzusammeln.

Profibus Nutzerorganisation e.V.
**www.profibus.com**

## Einsatz von CC-Link-Schnittstellen wächst um 12 Prozent

Die Anzahl der Geräte, die über die CC-Link-Standards kommunizieren, ist im letzten Jahr um über 12% gestiegen und hat weltweit knapp die Marke von 30Mio. erreicht. Diese Zahlen wurden von der Nutzerorganisation CLPA veröffentlicht. In den vergangenen Jahren wurde ein durchschnittliches jährliches Wachstum von über 2Mio. neuer Geräte pro Jahr verzeichnet.

CC-Link Partner Association – Europe
**eu.cc-link.org**

## Update für Spezifikation 61131-3

Die gemeinsame OPC-PLCopen-Arbeitsgruppe hat ein Update der UA für die Spezifikation 61131-3 fertiggestellt. Die aktualisierte Version (OPC 30000) ist jetzt als Release Candidate für Mitglieder verfügbar. Der Kommentierungszeitraum endet am 24. Oktober dieses Jahres. Der Überprüfungszeitraum zum Ausstieg aus Ansprüchen endet am 23. November 2020.

OPC Foundation Europe
**www.opcfoundation.org**

*Aus alt mach modern und sicher:*

# IT-Security für Smart Factorys

***102,9 Milliarden Euro – das ist die durchschnittliche Schadenssumme, die in deutschen Unternehmen durch Sabotage, Datendiebstahl oder Spionage in einem Jahr durch Cyberkriminalität entstanden ist. Das errechnete der Digitalverband Bitkom im Rahmen einer Umfrage zum Thema Wirtschaftsschutz in der digitalen Welt. Gleichzeitig wachsen IT und Produktion immer mehr zusammen.***

Bitkom stellte in der gleichen Untersuchung fest, dass die Anzahl der durch Cyber-Kriminalität, Sabotage und Spionage betroffenen Wirtschaftsunternehmen innerhalb von zwei Jahren von 53 auf 75 Prozent gestiegen ist.

## Herausforderungen durch Digitalisierung

Lange wurden die Technologien in der Fertigungsbranche getrennt voneinander behandelt: Die Fertigungstechnik (OT) funktionierte eigenständig neben der Informationstechnologie (IT). Diese Grenzen verschwimmen jedoch immer mehr durch die Digitalisierung der Produktion sowie dem IoT und der daraus resultierenden Vorteile. Im industriellen Kontext finden sich Schwachstellen in der stationären Technologie sowie im Industrial Network – lokal und in der Cloud gleichermaßen. Bei ersterem handelt es sich um die Legacy-IT: Veraltete Betriebssysteme werden nicht mehr von den Herstellern unterstützt und erhalten somit keine Sicherheits-Updates. Jahre später ist das Stopfen dieser Sicherheitslücken mit hohem Aufwand verbunden oder im schlimmsten Fall nicht mehr möglich. Zwar entsteht durch die Verschmelzung ein besserer Überblick über die Systeme, das bedeutet aber auch, dass Daten zentral gesammelt und verarbeitet werden. Viele dieser Daten lagern weiterhin in lokalen Netzwerken, doch machen immer mehr Unternehmen Gebrauch vom effizienteren und flexibleren Cloud Computing. Sensible Daten finden ihren Weg auf Server in der Cloud. Laut ihres Cloud Adoption and Risk Report schätzt McAfee, dass mehr als ein Fünftel der Daten in der Cloud sensible oder unternehmenskritische Inhalte aufweist. Diese Datenansammlung befindet sich an einem Ort und Saboteure und Cyber-Kriminelle freuen sich über die wertvolle Ausbeute.

## Whitelisting, SIEM- und DLP-Lösungen

Sicherheitsbestrebungen müssen IT und OT umfassend einbeziehen. Dafür existieren Lösungen, mit denen eine risikobehaftete Komplettumstellung der gesamten IT-Landschaft vermieden werden kann.Mithilfe von Whitelisting werden Anwendungen und Codes auf eine Autorisierungsliste gesetzt, die innerhalb des Unternehmensnetzwerks ausgeführt werden dürfen. Zusätzlichen Schutz bieten Security Information and Event Management (SIEM)- und Data Loss Prevention (DLP)-Lösungen. Diese überwachen Hard- sowie Software und machen in Echtzeit auf eine unbefugte Nutzung und Weitergabe von Daten aufmerksam, so dass mit Gegenmaßnahmen reagiert werden kann. DLP-Lösungen, die die Compliance auf dem lokalen Netzwerk sicherstellen, müssen durch Cloud Access Security Broker (CASB) erweitert werden, damit die gleichen Sicherheitsrichtlinien auf Cloud-Dienste übertragen werden können. Der Datentransfer zwischen Anwendern und Anwendungen wird ebenfalls in Echtzeit überwacht und auffällige Aktivitäten der Administration gemeldet.

## Human Machine Security

Durch die Verbreitung des (Industrial) Internet of Things ((I)IoT) ergibt sich ein weiterer Bereich, der einer ganzheitlichen Sicherheitsstrategie bedarf, um aufkommende Bedrohungen für Systeme im IoT rechtszeitig zu erkennen und zu verhindern. Die dafür unerlässliche Zusammenarbeit von Mensch und Maschine in einer Sicherheitsarchitektur nennt sich Human Machine Security Teaming (HMST). Künstliche Intelligenz (KI) nutzt maschinelle Lern- und User and Entity Behavioral Analytics (UEBA)-Prozesse, die die IT-Systeme auf Muster hin automatisiert analysiert. Durch die gewonnenen Insights können menschliche Datenanalysten potenzielle Bedrohungen identifizieren und angemessen darauf reagieren. Das Zusammenspiel von menschlicher Expertise und KI entlastet nicht nur die Mitarbeiter, sondern senkt präventiv das Gesamtrisiko in einem Unternehmen.

## Fazit

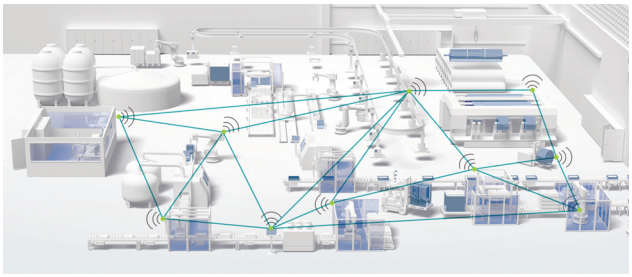
Die IT-Sicherheit im produzierendem Gewerbe muss auf einer ganzheitlichen Sicherheitsarchitektur aufgebaut werden, bestehend aus technischen Lösungen und dem Know-how sowie der Aufmerksamkeit aller Mitarbeiter. Wie jedes Bauwerk braucht auch die IT-Sicherheit ein Fundament, auf dem sie fußen kann: So wurde beispielsweise 2017 für die Automobilindustrie der Trusted Information Security Assessment Exchange, kurz TISAX, eingeführt, der u.a. das Risiko innerhalb der Supply Chain mindern soll, ein Opfer von Industriespionage zu werden. Diese Zertifizierung, die McAfee Ende 2019 erhielt, soll für ein höheres und einheitliches Sicherheitsniveau sorgen. Vielleicht ist es an der Zeit, eine solche Zertifizierung in anderen Branchen einzuführen, um von Anfang an, bevor technische Lösungen aktiv werden müssen, eine Sicherheitsgrundlage zu schaffen, von der alle Beteiligten profitieren. ■

**Der Artikel entstand nach einer Vorlage der McAfee GmbH.**
**www.mcafee.com**

Bild: ©LuckyStep/stock.adobe.com

# WLAN Mesh für Automatisierungsnetzwerke

Das Funkmodul WLAN 2100 von Phoenix Contact bietet mit der neuen Firmware 2.6 neben Access Point und Client zusätzlich die Betriebsart WLAN Mesh. Damit können sich selbst organisierende Ad-hoc-Netzwerke realisiert werden, die keine zentrale Infrastruktur wie WLAN Access Points benötigen. Einfache Planung, geringer Installations- und Erweiterungsaufwand sowie flexible Anpassungsfähigkeit an sich ändernde Rahmenbedingungen sind Eigenschaften, die ein WLAN-Mesh-Netzwerk auszeichnen. Es ist Layer-2-transparent, sodass auch industrielle Automatisierungsprotokolle wie Profinet oder Profisafe über das Netzwerk kommunizieren können. Das Mesh-Routing-Protokoll ist unabhängig vom physikalischen Übertragungsmedium. Daher können neben Funk- auch Kabelverbindungen im Mesh-Netzwerk verwendet werden. Die Kommunikation ist wie bei WLAN üblich mit WPA2 Security und AES-Verschlüsselung



gegen Manipulation und Abhören gesichert. Das Einsatzgebiet von WLAN Mesh sind Automatisierungsanwendungen, bei der die übliche Stern-Netzwerkstruktur von WLAN nicht passt.

**Phoenix Contact GmbH & Co. KG**
**www.phoenixcontact.com**

# IP67-Switche für Ethernet und Profinet

Die neue Produktlinie von Helmholz umfasst M12-Switche in Schutzart IP67 für Ethernet (unmanaged) und Profinet (managed). Die beiden Modelle verfügen über ein Kunststoffgehäuse und können in Temperaturumgebungen von –40 bis +75°C eingesetzt werden. Die Komponenten sind wasserbeständig, staubdicht und bieten eine zuverlässige Datenkommunikation sowie eine hohe Ausfallsicherheit. Durch eine optionale dezentrale Montage im Feld soll sich der Verdrahtungsaufwand zwischen Schaltschrank und einzelnen Ethernet-Komponenten zudem reduzieren. Sowohl der Ethernet-

als auch der Profinet-Switch ist für die schaltschranklose Montage geeignet. Die Switche sind mittels Plug&Play sofort betriebsbereit und sorgen so für eine schnelle, zeitsparende Installation.

**Helmholz GmbH & Co. KG**
**www.helmholz.de**

# Kompaktes Netzwerk-Analysegerät

Für Netzwerktechniker und Administratoren ist es häufig eine große Herausforderung, herauszufinden, welches Messgerät oder Werkzeug sich am besten für die bevorstehende Fehlersuche oder Fehlerbehebung in einem Netzwerk eignet. In den meisten Fällen steht das Falsche oder gar kein Mess-Tool zur Verfügung, um vor Ort Fehler zu finden und zu beheben. Das Messgerät Netool.io von NetPeppers ist sehr kompakt und passt in jede Hosentasche. IT-Experten haben damit immer das passende Messgerät für die Netzwerkanalyse- und -übersicht dabei. Denn mit dem Gerät können in Sekunden alle wichtigen Parameter eines Netzwerks ausgewertet werden. Außerdem lassen sich bei tiefer gehenden Anwendungsproblemen Pakete aufzeichnen und im .pcap-Format abspeichern. Die Auswertung erfolgt unkompliziert über eine eigene App, die auf allen bekannten Betriebssystemen wie iOS, Android oder Windows in den jeweiligen App Stores verfügbar ist.


**NetPeppers GmbH**
**www.netpeppers.com**

## IO-LINK-MASTER-MODUL MIT MULTI-PROTOKOLL-UNTERSTÜTZUNG

Bild: Contec

Das IO-Link-Master-Modul CPSL-08P1EN von Contec ist benutzerfreundlich und bietet aufgrund der Multi-Protokoll-Unterstützung die Möglichkeit, Daten mithilfe verschiedener Übertragungsprotokolle zu transferieren. Zur Verfügung stehen Ethercat, Profinet, Ethernet/IP, Modbus TCP und CC-Link IE Field Basic. Das Modul verfügt über eine integrierte Webbrowser-Funktion und kann ohne Verwendung spezieller Tools über einen Browser konfiguriert werden. Es verfügt über einen Temperaturbereich von –20 bis +60°C. Das Modul ist durch die beiliegenden Abdeckkappen auf allen Steckverbindern staub- und wasserdicht gemäß IP67. Es verfügt über LED-Statusanzeigen für jeden Kanal und bietet flexible Montagemöglichkeiten. Die Installation kann entweder im Schaltschrank oder aufgrund der Schutzart IP67 direkt vor Ort erfolgen.

**Plug-In Electronic GmbH**
**www.plug-in.de**

# Medienkonverter zum Schutz gegen elektromagnetische Störungen

Der neue Medienkonverter KGC-261-DP von KTI kommt als industrieller Kupfer/Glasfaser-Wandler dort zum Einsatz, wo Ethernet-Verbindungen im industriellen Umfeld auf Lichtwellenleiter treffen. Der Konverter ist PoE-fähig und versorgt aufgrund von High PoE++ angeschlossene Netzwerkgeräte über das Kupferkabel mit bis zu 128W. Damit kann der Konverter nicht nur Signale wandeln, wenn LWL- auf Ethernet-Verbindungen treffen, sondern auch über das Twisted-Pair-Kupferkabel angeschlossene Geräte mit Strom versorgen, die bisher aufgrund ihres höheren Leistungsbedarfs für die Speisung durch PoE nicht in Frage kamen. Das erhöht den Einsatzradius. Die ebenfalls neuen Modellvarianten KGC-261-DP-AT und KGC-261-DP-BT unterstützen die vom Institute of Electrical and Electronics Engineers genormten PoE-Standards IEEE802.3af/at (15,4/32W) bzw. IEEE802.3af/at/bt (15,4/32/90W) pro Port. Alle drei Modellversionen sind in einer G- und einer I-Variante erhältlich. Die I-Variante ist gemäß IEC61850-3 und IEEE1613 zertifiziert. Überall dort, wo große elektromagnetische Störungen auftreten, wie z.B. bei Energieversorgern in Umspannwerken, im Bereich von PV-Anlagen oder Off-Shore-Windparks, erfüllen die Switche KGC-261-DP/I die Anforderungen dieser Norm. Die Sicherheits-Features sind bei allen Ausführungen identisch: Die Funktion PoE Shutdown Protection vermeidet Störungen oder Defekte bei angeschlossenen Geräten, die nicht kompatibel sind. Ein Verpolungsschutz verhindert das falsche Anschließen der DC-Stromzufuhr. Die Stromzufuhr kann außer über die Klemme auch über ein Steckernetzteil oder den Mini-DIN-4-Anschluss erfolgen. Der Relay Output ermöglicht die Ausgabe von Alarmsignalen an externe Endgeräte. Der Automatic Laser Shutdown soll Augenverletzungen am Glasfaserport vermeiden.


Der Medienkonverter KGC-261-DP von KTI steht in verschiedenen Ausführungen zur Verfügung.

**KTI Distribution GmbH**
**www.kti.de**

*5G für die Industrie*

# Was kostet ein 5G-Campusnetz?

***Kabellose Kommunikation in der Industrie ist oft limitiert — sei es durch die endliche Anzahl der nutzbaren Geräte oder die Menge der übertragbaren Daten. Mit 5G sollen solche Probleme bald der Vergangenheit angehören. Vielerorts können private Kommunikationsnetze, sogenannte Campusnetze, eine sinnvolle Lösung sein. Doch in welchen Szenarien nutzen solche Netze und vor allem, was kosten Einrichtung und Betrieb?***

Die Möglichkeiten von 5G klingen verheißungsvoll: große Datenraten bei geringen Latenzzeiten für kabellose Echtzeitanwendungen. Dabei machen verschiedene Anwendungsprofile die Nutzung von 5G in unterschiedlichen Einsatzfällen möglich: Mit Enhanced Mobile Broadband (eMBB) werden Spitzendatenraten über 10GBit/s möglich. Ultra Reliable Low Latency Communication (URLLC) unterstützt Latenzzeiten unter einer Millisekunde und bietet eine Verfügbarkeit nahe 100 Prozent. Mit massive Machine-type Communication (mMTC) lassen sich batteriebetriebene Geräte über zehn Jahre betreiben und bis zu einer Million Geräte pro Quadratkilometer anbinden. Unternehmen können diese Vorteile sogar auf dem eigenen Gelände in privaten 5G-Netzen nutzen — die passende Lizenz vorausgesetzt.

## Welche Kosten anfallen

Seit November 2019 können Frequenzen für lokale Anwendungen bei der Bundesnetzagentur beantragt werden. Die Investitionen setzten sich im Wesentlichen zusammen aus den einmaligen Kosten für die Frequenzzuteilung, laufenden Frequenznutzungsbeiträgen, der Planung und dem Aufbau der Kommunikationsinfrastruktur sowie den Kosten, die für Instandhaltung und Betrieb des 5G-Netzes entstehen. Die laufenden Frequenznutzungsgebühren bestehen aus Frequenznutzungsbeiträgen gemäß §143 Abs. 1 TKG (Telekommunikationsgesetz) sowie Beiträgen gemäß §31 EMVG (Gesetz über elektromagnetische Verträglichkeit) und §35 FUAG (Gesetz über Bereitstellung von Funkanlagen auf dem Markt). Diese Gebühren werden rückwirkend auf ein Jahr erhoben und die Höhe wird nach den jeweils geltenden Frequenzschutzbeitragsverordnung bestimmt. Die Kosten für Planung, Anschaffung und die Implementierung der eigenen Kommunikationsinfrastruktur werden im wesentlichen von der Campusgröße sowie der jeweiligen Anwendung bestimmt. Zudem kommen Kosten für Instandhaltung hinzu.

Einsatzbereiche von 5G reichen von der Fabrikautomation über die Landwirtschaft und Hafenanwendungen bis hin zur Prozessindustrie.

## Nicht nur für die Industrie

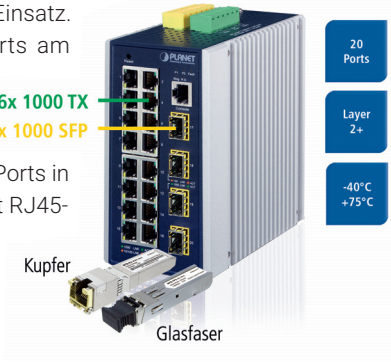
Als 5G-Anwendungsszenarien wird klassischerweise die Fabrikautomation genannt mit modularen, flexiblen Arbeitszellen oder fahrerlosen Transportsystemen. Doch auch andere Bereiche können von der 5G-Technologie profitieren. Z.B. lassen sich im Ackerbau mit Precision Farming jede Menge Informationen bei Aussaat und Ernte ermitteln, die Optimierungen für den weiteren Anbau ermöglichen. Weitere Einsatzgebiete finden sich in Containerhäfen. Dort werden große Warenmengen umgeschlagen und es entstehen große Datenmengen, die die Kapazität bisheriger kabelloser Kommunikationsnetze übersteigen können. Mit 5G wird eine zuverlässige, sichere, kabellose Kommunikation zwischen Kränen, Containern, Fahrzeugen und Mitarbeitern möglich. Ähnliches gilt für Flughäfen und die dort eingesetzten Vorfeldfahrzeuge. Und auch für die Prozessindustrie bieten sich unterschiedliche Einsatzgebiete. 5G ermöglicht z.B. durchgängige Kommunikation auf dem Betriebsgelände von Ölraffinerien oder Chemieparks. Grundsätzlich eignet sich die Technologie überall dort, wo Sensoren Datenmengen liefern, die bislang nicht kabellos übertragen werden konnten. ■



HMS Industrial Networks GmbH
www.hms-networks.com

# 20-Port-Ethernet-Switch

Der Ethernet Switch IGS-20040MT von Spectra bietet mit seinen 16x 10/100/1000TX Ports und 4x 100/1000FX (SFP) Ports eine hohe Konnektivität bei geringen Abmessungen. Zu seinen Leistungsmerkmalen zählen eine Netzwerkredundanz durch ERPS-Ringfunktion, eine redundante Spannungsversorgung von 9 bis 48VDC, ein Fehler-Alarm-per-Relais-Ausgang und je ein digitaler Ein-/Ausgang sowie ein Betriebstemperaturbereich von –40 bis +75°C. Die Einstellungen der Netzwerk-Management-Funktionen sind über Web, Telnet oder SNMP möglich und für die Datensicherheit kommen SSH, TLS und SNMPv3 zum Einsatz. Sind alle 16 Kupfer-Ports am Switch belegt, können mit Hilfe des SFP-Moduls MGB-GT nicht benötigte SFP-Ports in weitere Kupfer-Ports mit RJ45-Anschluss gewandelt werden.




**Spectra GmbH & Co. KG**
**www.spectra.de**

# Industrie-router mit zwei LTE-Cat6-Modems


Unitronic hat einen neuen Industrierouter von Teltonika Networks vorgestellt. Der RUTX12 wurde für unternehmenskritische Anwendungen entwickelt und verfügt über zwei gleichzeitig einsatzbereite LTE-Cat6-Modems. Dadurch können Geschwindigkeiten bis 600MBit/s erreicht werden. Der Router ermöglicht eine nahtlose Umschaltung des LTE-Dienstes und des Lastausgleichs. Durch das robuste Aluminiumgehäuse ist er für verschiedene Industrieeinsätze geeignet. Ein breit definierter Eingangsspannungsbereich von 9 bis 50VDC mit Verpolungs- sowie Überspannungsschutz und Einsatztemperaturen von –40 bis 75°C lassen den Router auch in rauen Umgebungen sicher arbeiten. Das Produkt verfügt über fünf GBit-Ethernet-Ports und zwei SIM-Karten-Slots. DualBand 802.11ac WiFi mit 2,4GHz und 5GHz AC ist ebenso integriert wie eine GNSS-Schnittstelle, ein USB2.0-Interface und Bluetooth LE 4.0. Der Router ist mit dem Teltonika-Remote-Management-System kompatibel, das die Ferneinrichtung, -konfiguration und -verwaltung ermöglicht.

**Unitronic GmbH**
**www.unitronic.de**

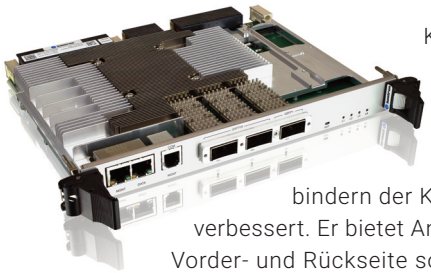
# M2M-SIM-Karten für LTE-Industrieanwendungen mit bedarfsangepassten Tarifen

Das Unternehmen Wireless Netcontrol bietet M2M-SIM-Karten mit bedarfsangepassten Tarifen. Der früher einheitliche Markt der SIM-Kartenverträge hat schon seit einigen Jahren den Markt der M2M-SIM-Karten hervorgebracht. Und es lohnt sich für Anwender in Industrie und Anlagentechnik ausschließlich solche SIM-Karten einzusetzen. Denn M2M-Karten bieten moderate Datenraten, weil hier niemand Netflix-Videodaten abruft, sondern technische Daten, Messwerte und Befehlsketten fließen – und das uplink wie downlink, also in beide Richtungen. M2M-Karten bieten in der Regel landesweites, europaweites – gegebenenfalls auch weltweites – Roaming. So haben diese Karten sogar im Inland unabhängig vom Provider an jedem Standort Kontakt in das lokal stärkste Netz. Garantiert oder bei Bedarf auch zusätzlich buchbar sind wichtige M2M-Spezialdienste, zuverlässig beförderte SMS und Datenvolumen im Pool aller SIM-Karten. Die üblichen Monatsgebühren betragen nur wenige Euro,


meist ein Bruchteil dessen, was für einen herkömmlichen Kartenvertrag fällig ist.

**Wireless Netcontrol GmbH**
**www.wireless-netcontrol.de**

# Non-blocking-Ethernet-Switch



Kontron bietet ab sofort mit dem VX6940 einen 6HE-VPX-Switch an. Die Signalintegrität wird durch die Verwendung von VPX-Steckverbindern der Klasse RT3 über die Backplane verbessert. Er bietet Anschlussmöglichkeiten auf der Vorder- und Rückseite sowie luftgekühlte und robuste Versionen. Der non-blocking-L2/L3-Switch basiert auf dem Broadcom-BCM56760-Switch mit 72x 10GbE-Ports und hoher Dichte. Er verfügt über eine 100G-Uplink-Fähigkeit und bietet eine I/O-Bandbreite von 720Gb. Die BCM56760-Lanes sind mit einer 12x 40G-Backplane-Datenebene, 8x oder 12x 10G-Steuerebene, 2x Front-QSFP28 40G/100G sowie 1x Front-QSFP+ 40G verbunden, die für Conduction-Cooled-Anwendungen auf der Backplane abgebildet werden können.

**Kontron S&T AG**
**www.kontron.de**

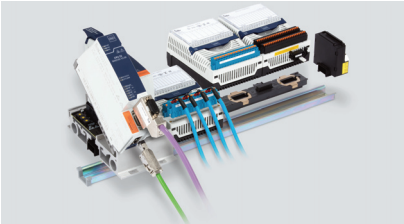
# Kompakte Gigabit-Ethernet-Switche

Plug-In Electronic hat die neuen Ethernet-Switche von Brainboxes vorgestellt. Die kompakten Geräte verfügen über fünf Unmanaged-Ethernet-Ports, eine Verbindungsüberwachung und einen weiten Betriebstemperaturbereich. Die Plug&Play-Funktion sorgt für eine einfache Installation. Die GBit-Ethernet-Switche gibt es in drei Ausführungen: eine OEM-Variante ohne Gehäuse (SW-115), eine DIN-Rail-Standardvariante (SW-515) und ein Modell, das sich für ein raues Umfeld eignet (SW-715). Die Switche können von +5 bis +30VDC mit Strom versorgt werden und haben einen Betriebstemperaturbereich von –40 bis +80°C.


**Plug-In Electronic GmbH**
**www.plug-in.de**

# Remote-I/O-System jetzt Profinet-zertifiziert

Das Remote-I/O-System IS1+ für explosionsgefährdete Bereiche von R. Stahl ist



jetzt auch Profinet zertifiziert und erfüllt dabei die Kriterien eines Conformance-Class-B-Gerätes. Durch die Unterstützung von MRP-Ringen und S2-Systemredundanz eignet sich das System für den Einsatz in Anwendungen mit hohen Anforderungen an die Verfügbarkeit. Mit der Profinet-Funktion Dynamic Reconfiguration sind Änderungen an der Konfiguration, z.B. das Hinzufügen oder Tauschen von I/O-Modulen, online ohne Unterbrechung der Kommunikation möglich. Auch beim Austausch der CPU-Baugruppe ist kein erneutes Konfigurieren oder Parametrieren erforderlich. Als Shared Device arbeitet das System mit mehreren Controllern simultan zusammen.

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

# Industrial Ethernet in der Messtechnik

***Wenn es um die Universalität einer Technologie geht, dann ist Ethernet kaum zu schlagen. Es ist über Generationen hinweg nun schon abwärtskompatibel, vor allem aber ist es extrem schnell. Das kann man sich in der Fertigung und in der industriellen Messtechnik zu Nutze machen – macht man auch …***

Unzählige Daten werden heute in Apparaten, Maschinen oder Anlagen erhoben, einige werden berechnet aber viele davon müssen gemessen werden. Vor allem aber müssen sie übertragen werden. Gerade für Messdaten, die im laufenden Prozess erhoben werden, ist Ethernet mit seinen industriellen Ausprägungen eine gute Wahl, denn es ist sehr schnell. Aber nicht nur in puncto Geschwindigkeit überzeugt die Technologie: Es ist einfach zu installieren, zuverlässig im Betrieb und flexibel in der Handhabung. Für nahezu jede Problemstellung gibt es eine passende Lösung. Vor allem ist Ethernet aber skalierbar in Performance und Sicherheit. Alles in allem eine überzeugende Technologie, die sich zu Recht die Fertigungswelt erobert hat. *(kbn)* ■

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


*www.i-need.de ist das Infoportal, das wir passgenau für die Belange der Automatisierungsbranche entwickelt haben. Eine intelligente Suche hilft beim Finden der passenden Komponenten.*

Die Komplexität industrieller WLAN-Anwendungen wird weiter wachsen. WLAN-Komponenten nach neuem Standard machen die drahtlose Kommunikation flexibler und effizienter.

*Bessere Nutzung der Frequenzen machts möglich:*

# Wi-Fi 6 bringt Effizienzschub für industrielle Anwendungen

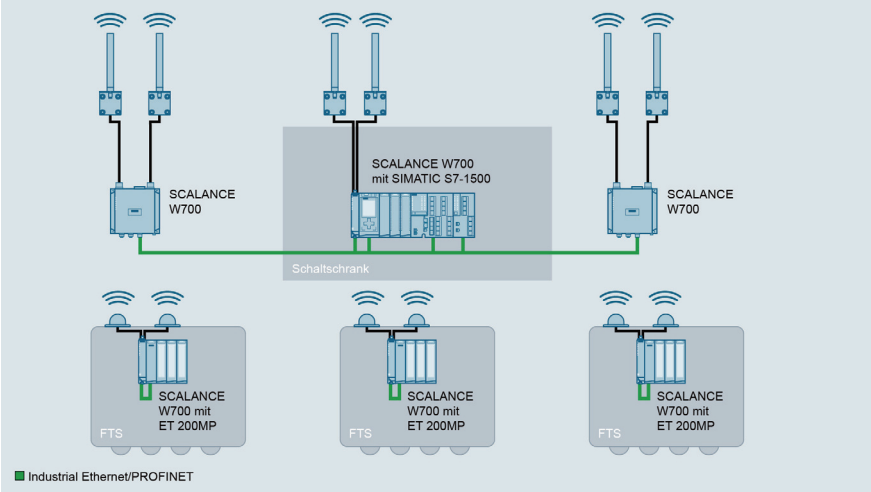
***Die Frage ist nicht ob, sondern wie IEEE802.11ax (alias Wi-Fi 6) und 5G die drahtlose mobile Kommunikation im Industrieumfeld vorantreiben. Siemens unterstützt beide Technologien, um für unterschiedlichste Anforderungen optimale Lösungen zu bieten. Speziell Wi-Fi 6 setzt als erster WLAN-Standard nicht mehr vorrangig auf mehr Bandbreite, sondern auf effizientere Nutzung der Frequenzen durch jeden einzelnen Client bei einer wachsenden Teilnehmerzahl. Der Standard bietet dafür Funktionen, die es in industrietaugliche Komponenten umzusetzen gilt.***

Wireless LAN ist im industriellen Umfeld längst viel mehr als die bloße drahtlose Verbindung weniger stationärer Teilnehmer. Mit proprietären industriellen Zusatzfunktionen, den sogenannten iFeatures – wie der industrial Point Coordination Function (iPCF) – hat Siemens schon frühere WLAN-Standards um Echtzeitfähigkeit erweitert und fit für anspruchsvolle industrielle Anwendungen gemacht. Applikationen mit mobilen Teilnehmern wie Krankatzen, fahrerlose Transport- und Shuttle-Systeme, Hochregallager/Regalbediengeräte, Einschienenhängebahnen und in zunehmendem Maß mobile Roboter in modularen Produktionsumgebungen sind heute weltweit etabliert. Die Technologie ist aus der Automatisierungswelt nicht mehr wegzudenken. Noch weniger aus der durchgängig digitalen Fabrik mit immer mehr IIoT-Geräten sowie mobilen Virtual-/Augmented-Reality-Devices zur Visualisierung von Daten und Prozessen, z.B. für Assisted Work. Die Zahl der Teilnehmer in den Funknetzwerken steigt weiter und damit der Bedarf an noch flexiblerer, effizienterer Kommunikation. Dabei müssen Handhabung und Koordination, Service und Wartung für den Anwender einfach beherrschbar bleiben. Der jüngste WLAN-Standard IEEE802.11ax, die sechste, von der Wi-Fi Alliance prägnant Wi-Fi 6 getaufte Generation, bringt dafür eine Reihe an leistungs- und ausbaufähigen Funktionen mit.

## Häppchenweise effizienter kommunizieren

Einen großen Schritt zu höherer Effizienz ermöglicht die Funktion OFDMA (Orthogonal Frequency-Division Multiple Access/Mehrfachzugang durch orthogonale Frequenzteilung), eine im Mobilfunk bereits etablierte, für WLAN aber neue Art der Datenübertragung. Bislang nutzt WLAN das Verfahren Orthogonal Frequency-Division Multiplexing (OFDM). Dabei kann immer nur jeweils ein Client zu einem bestimmten Zeitpunkt mit dem Access Point kommunizieren und belegt den Kommunikationskanal exklusiv für

Bilder der Doppelseite: Siemens AG




Dank kürzerer Latenzzeiten lassen sich beispielsweise fahrerlose Transportsysteme in größerer Teilnehmerzahl auch bei höherer Geschwindigkeit sicher betreiben.

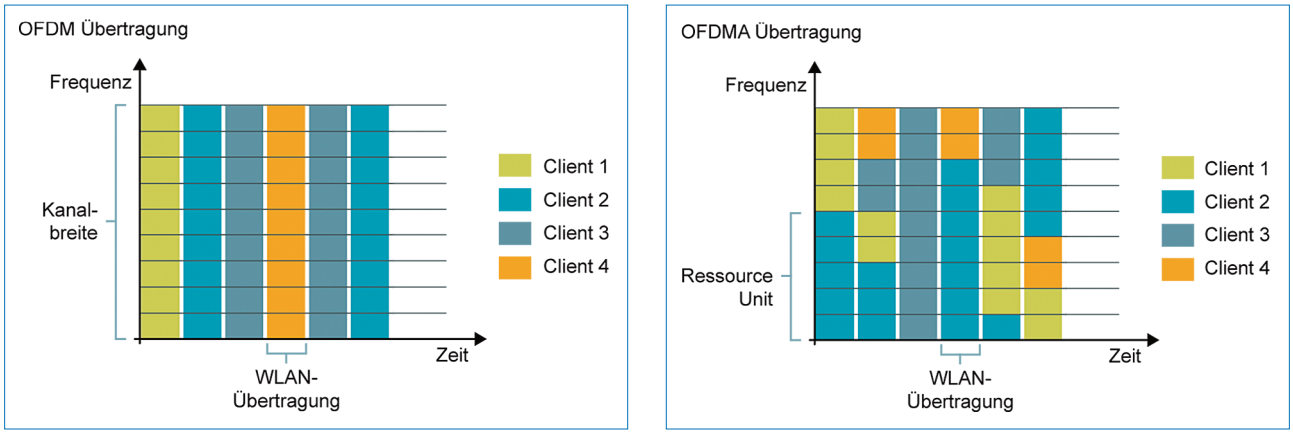
die Datenübertragung. Mit OFDMA wird der Kommunikationskanal in mehrere Unterkanäle, sogenannte Ressource Units (RU), aufgeteilt. Diese Unterkanäle lassen sich variabel bündeln und von verschiedenen Clients nutzen. So können Daten gleichzeitig, ergo in kürzeren Abständen übertragen werden. Das kann zu geringeren Latenzzeiten, gerade für kleine Pakete wie Profinet Telegramme, führen und damit letztendlich zu kürzeren Zyklus- und Reaktionszeiten der Automatisierungslösungen. In einem WLAN mit durchgängig OFDMA-fähigen Access Points und Clients resultieren daraus verschiedene Vorteile. So können in kürzerer Zeit mehr Teilnehmer als bisher kommunizieren oder bei gleicher Anzahl mehr Daten im bisherigen Zeitfenster übertragen werden. Damit kann z.B. ein fahrerloses Transportsystem (FTS) oder ein Schubplattenfördersystem schneller auf unvorhergesehene Ereignisse reagieren, etwa auf Personen im Fahrbereich. Es lässt sich folglich mit einer höheren Geschwindigkeit betreiben, ohne die Gefährdung zu erhöhen. In einem Hochregallager bedeutet dies deutlich höhere Umschlagraten. Damit ist die Basis geschaffen, um die immer häufiger auftretenden Anforderungen nach zuverlässiger Echtzeit für Automatisierungskomponenten und datenintensive Applikationen wie Kameraübertragungen parallel zu bewältigen.

## Energieverbrauch und Funklast reduzieren

Eine weitere neue Funktion von Wi-Fi 6 ermöglicht es, eine definierte Target Wake Time (TWT) für jeden Teilnehmer zu vereinbaren um Clients nur bei Bedarf anzusprechen und ‘aufwecken’ zu können. Diese verbrauchen somit weniger Energie, was mitunter zu längeren Laufzeiten und Wartungszyklen batteriebetriebener WLAN-Geräte führt. In komplexen Systemen viel wichtiger ist aber der Aspekt, dass ‘schlafende’ Teilnehmer nicht funken und damit den Kommunikationskanal nicht belegen. Das wiederum erleichtert die Planung und Koordination sehr vieler Teilnehmer und führt leichter zu stabiler, störungsfreier Kommunikation. Drei verschiedene TWT-Modi machen diesen Teil des Standards sehr flexibel.

## Kanäle räumlich näher wiederverwenden

Ziel der neuen Standard-Funktion Spatial Reuse mit Basic Service Set (BSS) Coloring ist es, Kanäle räumlich näher beieinanderliegend wiederverwenden zu können. Auch dann, wenn diese räumlich so nah sind, dass normalerweise starke Beeinträchtigungen zu erwarten sind. Dazu wird jedem BSS, bestehend aus einem Access Point und zugehörigen Clients, eine ‘Farbe’ (das heißt eine Zahl) zugeordnet und eine dynamische Kanal-Freigabeschwelle definiert. Dadurch können die Teilnehmer auch dann zuverlässig kommunizieren, wenn der Kanal eigentlich durch Teilnehmer einer anderen Farbe belegt wäre, diese aber mit geringerer Leistung senden. Damit entfallen die bisherigen Wartezeiten auf einen freien Kanal und die Kanäle können effizienter wieder




Wi-Fi 6 führt die gleichzeitige Nutzung eines WLAN-Kanals für bis zu neun Teilnehmer ein (OFDMA, rechtes Bild). Das kann die Latenzzeiten deutlich verkürzen. Bis Wi-Fi 5 kann immer nur ein Teilnehmer zu einem bestimmten Zeitpunkt kommunizieren (OFDM, linkes Bild).

genutzt werden. Spatial Reuse ermöglicht so eine deutlich effizientere Nutzung des Frequenzspektrums und neue Paradigmen bei der Planung von Anlagen. Es vereinfacht durch die räumlich nähere Wiederverwendbarkeit der Kanäle beispielsweise die Abstimmung unter mehreren Anlagenlieferanten in einer Fabrik. In industriellen IoT-Umgebungen ist eine bessere Verteilung vieler Clients auf verschiedene Access Points und damit eine höhere Störfestigkeit (Übertragungsqualität) auf engem Raum erreichbar.

## Mehr Effizienz auch für industrielle Anwendungen?

Der Standard mit seinen Verbesserungen allein kann noch nicht alle Anforderungen für Automatisierungslösungen in den verschiedenen Industrien abbilden. Um OFDMA echtzeitfähig nutzen zu können, muss beispielsweise das richtige Scheduling (Kommunikations-Planung bzw. -Steuerung durch die Access Points) implementiert werden. Der kritische Punkt bei drahtloser Kommunikation, nämlich der Übergang eines Clients von einem Access Point zu einem anderen, wurde im Standard weder betrachtet, noch verbessert. Hier bedarf es industrieller Anpassungen im Stil der bereits bekannten industriellen Zusatzfunktion iPCF für deterministische Echtzeitkommunikation.

## Fazit

Der Trend in der Automatisierung geht dahin, dass Automatisierungsprotokolle mit harten Echtzeitanforderungen parallel zu datenintensiven Applikationen wie Kameras betrieben werden. Um alle Applikationen problemlos über eine drahtlose Verbindung betreiben zu können, bedarf es Erweiterungen der bereits im Standard vorhandenen Mechanismen. Nicht nur die Möglichkeiten des neuen Standards zu nutzen, sondern darüber hinauszugehen und bezüglich Echtzeit und Zuverlässigkeit echte Mehrwerte in der Automatisierung zu schaffen, ist exakt der Anspruch, den Siemens mit Industrial Wireless LAN bereits umsetzt und auch mit Wi-Fi 6 umsetzen wird. ■

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

**Kilian Löser, Produktmanager für Industrial Wireless LAN, Siemens AG**
**www.siemens.de**

# *Professional Services: Umfassende Unterstützung in allen Belangen industrieller Kommunikationsnetzwerke*

*Um die ständig zunehmenden Möglichkeiten industrieller Kommunikation voll ausschöpfen und nutzen zu können, bietet Siemens gemeinsam mit branchen- und IT-erfahrenen Solution-Partnern aufeinander abgestimmte Industrial Networks Professional Services für bestehende wie neue industrielle Kommunikationsnetzwerke. Das Team wurde eigens dafür etabliert, Hersteller wie Betreiber von Maschinen und Anlagen mit Netzwerktechnik von Siemens und anderen Ausrüstern in jeder Lebenszyklusphase zu unterstützen, von der Planung bis zum Service. Auf Wunsch beraten erfahrene Spezialisten bei der Auslegung industriegerechter LAN- sowie WLAN-Netzwerkinfrastrukturen und -mechanismen und übernehmen auch die Inbetriebnahme sowie die Optimierung vor Ort. Darüber hinaus vermitteln verschiedene Standard- und kundenindividuelle Schulungen fundiertes Produkt- und Netzwerkfachwissen.*

Bilder: Siemens AG

Bild: iStock.com/Irina_Strelnikova; Herman Vasyliev / Tedo-Verlag GmbH

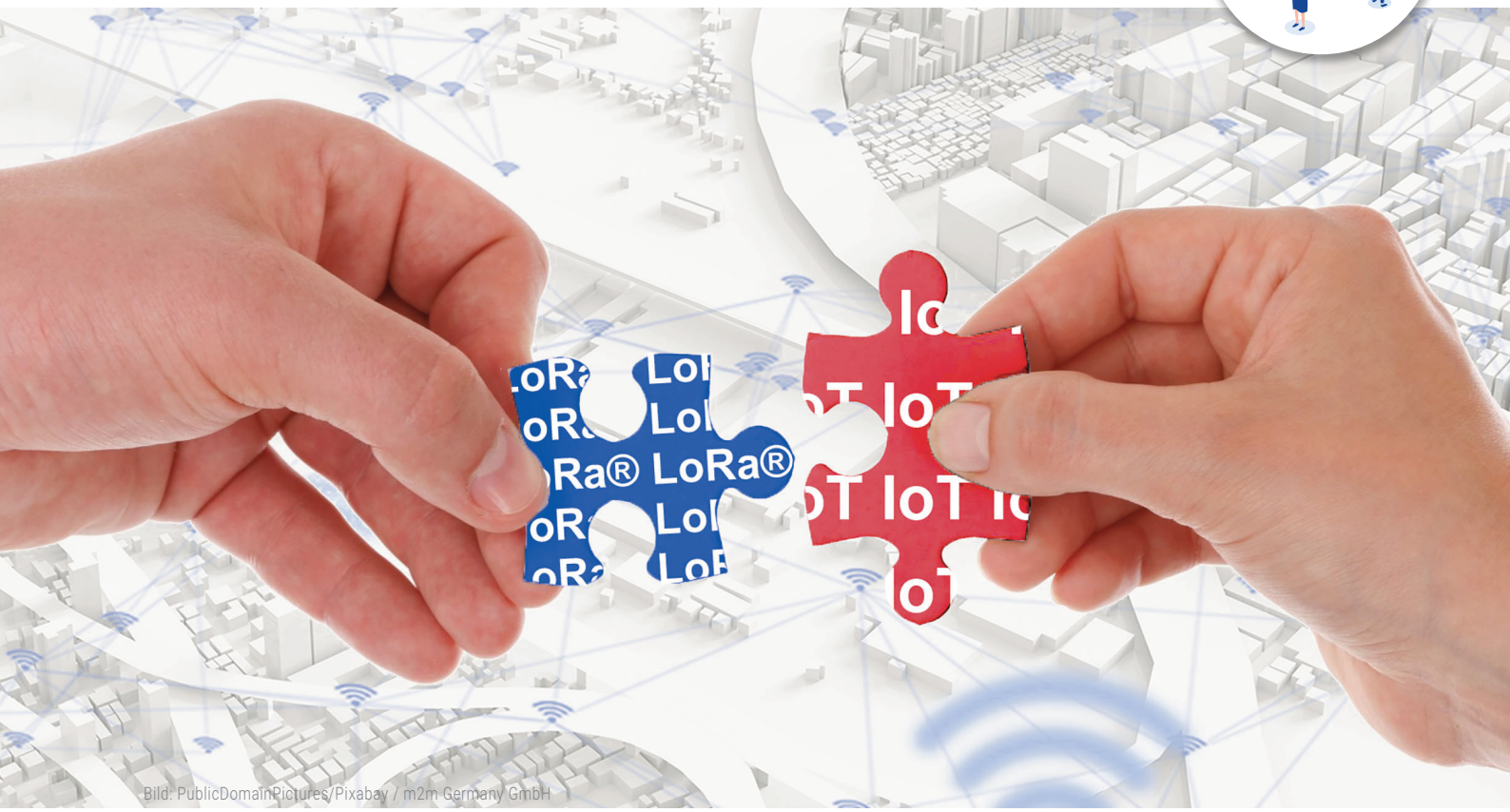



Bild: PublicDomainPictures/Pixabay / m2m Germany GmbH

*LoRa – die komplementäre Technologie*

# Sensoren im Internet der Dinge

***Das Thema IoT hat an greifbarer Relevanz gewonnen und wird immer interessanter, auch für bestehende Systeme und Bestandsanlagen. Sensoren sind dabei die wichtigsten Datengeneratoren des IoT. Sie sind Enabler für neue Prozesse und moderne Businessmodelle – durch sie entsteht eine neue, digital vernetzte Welt. Sensoren registrieren Position, Feuchtigkeit, Temperatur, Helligkeit, Dichte, Bewegung, Beschleunigung, Lautstärke, Abstände, Farben, Muster etc. Doch erst die passende Kommunikationstechnologie ertüchtigt die Sensoren für das IoT. Wir zeigen, welchen Beitrag LoRa dazu leisten kann.***

Die Methoden der einzelnen Sensoren sind vielfältig und durch die Integration von Funk in bereits bestehende Messverfahren, eröffnen sich ungeahnte Möglichkeiten. Zentrale Herausforderungen dabei sind die zuverlässige Verbindung und Kommunikation unterschiedlichster Dinge miteinander, ohne das Sicherheitsaspekte vernachlässigt werden, die Kosten im Rahmen bleiben und energiesparende Technologien zum Einsatz kommen. All das gewährleisten auf LoRa basierende Funksensoren und bieten eine klare Alternative für einen Einstieg ins IoT – eine entsprechende Infrastruktur vorausgesetzt.

## Die Basis für das Internet of Things

Für die vernetzten Dinge von morgen wird eine passende Infrastruktur benötigt, die die unzähligen Geräte- und Sensordaten handhaben kann. Bewährte Funkstandards wie WLAN, 3G/4G, Bluetooth sind dafür nur bedingt geeignet, da die Geräte – für sich und im Verbund – zu viel Energie verbrauchen, die Reichweite zu gering ist und eine tatsächliche Vernetzung zu aufwändig ist. Der Funkstandard LoRa ist hier eine reelle Alternative. LoRa ist speziell für kleine, batteriebetriebene Geräte entwickelt worden, um von diesen Daten über Gateways

Bild: iStock.com/Irina_Strelnikova; Herman Vasyliev / TeDo Verlag GmbH

Bild: Sensing Labs


LoRa-Gateway mit Modbus-Schnittstelle

in das Internet zu senden. LoRa offeriert eine verlässliche Kommunikation bei Reichweiten von bis zu 15km im unlizenzierten Frequenzband von 868MHz. Es ist eine hoch skalierbare Technologie – nahezu unbegrenzt ist die Anzahl der Endgeräte die eingebunden werden können und LoRa/LoRaWAN ist ein weltweiter Standard. LoRaWAN ist die Schnittstelle zwischen dem IoT-Gerät und einer Cloud. Das LoRaWAN Netz ist in seiner Topologie sternförmig – der Deckungsbereich ist nach allen Seiten offen und verknüpfbar. Grundsätzlich funktioniert LoRaWAN ähnlich wie ein herkömmlicher W-LAN Access Point: Daten werden von IoT-Geräten via Gateway empfangen und über das Internet an eine Cloud gesendet. In der Cloud stehen die Daten dann dem Anwender zur Verfügung. Im Gegensatz zu Wi-Fi oder GSM bzw. LTE wird für LoRa keine SIM-Karte oder ein Authentifizierungsschlüssel wie bei W-LAN benötigt.

## Weniger ist mehr

Die einzige Einschränkung bei LoRa ist die sehr niedrige Datenrate (<50kbps), das bedeutet, die Anwendungen dürfen nicht nach hohen Datenraten verlangen. Handelt es sich jedoch um kurze Statusmeldungen, Steuerbefehle, GPS Standortdaten und aktualisierte Sensordaten, dann ist LoRa die perfekte Wahl. LoRa ist nicht die Lösung für das Senden von Dauersignalen, aber ideal für den Intervallversand von kleinen Datenpaketen. Und genau das ist oft relevant bei IoT-Anwendungen, im Besonderen bei der Mess- & Regeltechnik geht es doch meist um Ereignis gestütztes Melden oder Status Benachrichtigungen.

Sicherheitsabstand einhalten dank LoRa-Tracker

Bild: Abeeway

## Komplementäre Sensoren

Im Zeitalter von Industrie 4.0 und IoT sind die Anforderungen für Sensoren enorm gestiegen. Durch Funkintegration in bereits bewährte Sensoren, lassen sich komplett neue Szenarien abbilden und Sensor2Cloud Lösungen realisieren. Implementiert man beispielsweise den Funkstandard LoRa in einen Ultraschallsensor werden neue Anwendungen ermöglicht. In der industriellen Anwendung zeichnen sich Ultraschallsensoren neben ihrer Zuverlässigkeit besonders durch ihre enorme Vielseitigkeit aus. Sie lösen auch besonders komplexe Aufgaben beim Erfassen von Objekten oder Füllständen, weil ihr Messprinzip unter fast allen Umständen zuverlässig funktioniert.

## Vielseitig einsetzbar

Kein anderes Messverfahren lässt sich so breit und in so vielen unterschiedlichen Anwendungen erfolgreich einsetzen. Ultraschallsensoren senden hochfrequente, für den Menschen nicht hörbare Schallimpulse zur Messung aus. Diese breiten sich in der Luft keulenförmig aus und werden reflektiert, sobald sie auf eine Oberfläche treffen. Die Sensoren arbeiten nach dem Prinzip der Puls-Laufzeit-Messung. Dabei messen sie die Zeit zwischen dem Aussenden der Schallwellen bis zum Empfang des vom Objekt reflektierten Echos. Auf diese Weise können sowohl Objekte detektiert als auch ihr Abstand zum Sensor (beispielsweise Silo-Füllstände) ermittelt werden. Bislang wurden solche Sensoren kabelgebunden verbaut, um mit Strom versorgt zu werden und die erfassten Messdaten zu übermitteln. An einen komplett drahtlosen Einsatz war somit nicht zu denken. Durch die Implementierung von LoRa kann dies wiederum ermöglicht werden. Somit können Füll- und Pegelstände bestimmt werden bei Containern, Tanks und Silos, aber auch Pegelstände von Flüssen und Seen, können aus der Ferne überwacht werden. Darüber hinaus kann bei zusätzlicher Implementierung von GPS auch die Geoposition eines Behälters via LoRaWAN Verbindung ermittelt werden. Interessant ist dabei, dass LoRa-Sensoren sowohl in einem privaten, als auch in einem öffentlichen betriebenen LowPower-Funknetz betrieben werden können. In zusätzlicher Kombination mit Bluetooth, kann dann auch via App, auf alle gesammelten und im Netz bereitgestellten Sensordaten, jederzeit zugegriffen werden. Überhaupt gilt für die batteriebetriebenen, auf LoRa-basierenden Funksensoren, dass mit ihnen, in Kombination mit entsprechenden LoRa-Gateways, eine einfache Nachrüstung für Bestandsanlagen

Bild: m2m Germany GmbH

Ultraschallsensor mit integrierter Lora-Funktechnologie, OEM-Entwicklung von m2m Germany

Bild: Éolane

▸ Smarter Wartungs-Assistant: LoRa-Sensor mit eingebetteter KI

und Gebäude umgesetzt werden kann. Es gibt LoRa-fähige Gateways die über Modbus Schnittstellen verfügen und via TCP/IP an Scada-Systeme eingebunden werden können, womit Retrofit für Bestandsanlagen und Gebäude im Handumdrehen realisiert werden kann. Ventile regeln oder das Schalten von Prozessen generell, kann via LoRa-Sensorik schnell auf IIoT-Level gebracht werden.

## Noch mehr Potenzial – LoRa Sensorik und KI

LoRa Sensorik kann aber noch viel mehr, im Besonderen dann, wenn embedded KI -Edge Computing mit ins Spiel kommt. Dann kann sogar ein Wartungs-Assistent für industrielle Instandhaltung – für eine vorbeugende 'industrial maintenance', ermöglicht werden. Besonders geeignet dafür sind Schwingungsanalysen und Vibrationsmessungen. Sie sind nachweislich ein sehr guter Frühindikator für Maschinenausfälle und Wartungsbedarfe. Daher liegt es nah, auch Schwingungssensoren mit LoRa auszustatten. Es gibt bereits einen solchen LoRa-Schwingungs-Sensor, der eine Plug&Play-Lösung ohne großen Implementierungsaufwand zur Verfügung stellt. Er verfügt über einen 6-Achsen Beschleunigungsmesser, der Schwingungsmessungen im 1 bis 6.4kHz-Bereich, in einstellbaren periodischen Abtastungen, erfasst. Darüber hinaus registriert der Sensor Temperaturwerte mit einer Genauigkeit von ±1°C. Es ist ein batteriebetriebener Sensor, der sofort einsatzbereit ist; die Stromversorgung erfolgt durch eine AA Batterie 2.000mA mit einer Nennbetriebszeit von 2 bis 4 Jahren. Der Sensor erkennt und analysiert die Schwingungen der Maschine/Anlage, die es zu überwachen gilt. Dabei lernt er sich selbstständig auf die Maschine ein (embedded KI) und reagiert nach der Einlern-Phase bei Abweichungen vom Normalzustand mit dem Absetzen von Alarm-Benachrichtigungen. Der persönliche Wartungs-Assistent weist auf Unregelmäßigkeiten hin und erlaubt frühzeitig auf einen möglichen Ausfall zu reagieren. Stillstände und kostspielige Instandhaltungsarbeiten können reduziert werden.

## Kein Ende der Möglichkeiten in Sicht

LoRa steht noch am Anfang seiner Möglichkeiten. Noch wird der Schwerpunkt von LoRa eher im IoT-Industriebereich angesiedelt. Doch das Interesse steigt. Immer mehr Städte errichten ihr eigenes LoRaWAN Netz, um vielfältige Szenarien umzusetzen. Von Smart Parking Konzepten, über Monitoring der Fernwärmeleitungen bis hin zu Straßenbeleuchtungskonzepten und Smart Farming Anwendungen. Die Facility-Branche signalisiert ebenfalls ihr Interesse an der kostengünstigen Lösung, lassen sich doch via LoRa-Sensorik sämtliche Verbräuche innerhalb eines Gebäudes monitoren und regeln. Darüber hinaus können Passage-Sensoren helfen, Reinigungspersonal effizienter einzusetzen – so dass dem Nutzungsgrad entsprechend Reinigungsintervalle angepasst werden können. Waste-Management ist auch ein spannender Punkt – sowohl für das Facility-Management, als auch für kommunale Entsorgungsbetriebe. Das Feld für LoRa-Sensoren ist noch bei Weitem nicht ausgeschöpft – allein die Tatsache, dass es aktuell LoRa basierende Lösungen für das Einhalten von Sicherheitsabständen während der Covid-19 Pandemie gibt, zeigt wie flexible diese komplementäre Technologie eingesetzt werden kann. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/37593

Karin Reinke-Denker M.A.,
Marketing & PR,
m2m Germany GmbH
www.m2mgermany.de

# Inserentenverzeichnis

*Forschungsprojekt prüft Rahmenbedingungen für neuen Kommunikationsstandard*

# Bosch startet 5G-Tests im Halbleiterwerk Reutlingen

***Bosch ist einer der Vorreiter beim Thema Industrie 4.0 und setzt auf 5G als wichtigen Baustein für die Digitalisierung und Vernetzung in der Produktion und Logistik. Das Unternehmen beginnt jetzt mit Verträglichkeitstests und Kanalmessungen für den Aufbau eines 5G-Netzes im Halbleiterwerk in Reutlingen.***

Dr. Michael Bolle, Bosch-Geschäftsführer und CDO/CTO erklärt: „Bei Bosch haben wir uns frühzeitig mit 5G in Forschung und Entwicklung beschäftigt und sind überzeugt, dass der neue Mobilfunkstandard für einen Schub bei Industrie 4.0 sorgt." Das Unternehmen beteiligt sich daher aktiv am internationalen Forschungsprojekt 5G-Smart mit dem Ziel, das Potenzial des neuen Kommunikationsstandards in realen Produktionsumgebungen zu erproben, zu demonstrieren und zu bewerten. Im Rahmen von 5G-Smart werden im Bosch-Halbleiterwerk, am Ericsson-Standort in Kista in Schweden sowie auf dem 5G-Industry Campus Europe des Fraunhofer IPT in Aachen 5G-Anwendungen für die Fertigung getestet.

## 5G-Netzaufbau im Bosch-Halbleiterwerk

Die industrielle Fertigung befindet sich in einem digitalen Wandel: Manuelle Prozesse werden reduziert, technische Assistenzsysteme halten Einzug, Sensoren senden eine Vielzahl von Daten, der Grad der Vernetzung zwischen Menschen, Ma-


Habeiterwerk Reutlingen

Bilder der Doppelseite: Robert Bosch GmbH

schinen und Anlagen steigt. 5G gilt als Schlüsselfaktor. „Eine schnelle, zuverlässige und sichere Datenübertragung ist Basis für Industrie 4.0. In Kombination mit 5G werden wir die Produktion in den Fabriken weiter steigern und verbessern", erklärt Bolle. Im Halbleiterwerk in Reutlingen startet Bosch jetzt zusammen mit Ericsson mit Verträglichkeitstests, die Aufschluss darüber geben sollen, inwieweit 5G die Produktion beeinflusst. „Die Halbleiterfertigung ist äußerst komplex und sensitiv. Über 1.000 Tests durchlaufen Wafer, ehe die mikroskopisch kleinen Elemente in unterschiedlichen Produkten zum Einsatz kommen, z.B. in Airbags, Smartphones oder eBikes. Elektromagnetische Wellen können bei der Fertigung Störquellen sein. Wir testen, wie sich 5G auf die Produktion auswirkt", sagt Andreas Müller, Bosch-Forscher und Vorsitzender der internationalen Initiative 5G-ACIA (5G Alliance for Connected Industries and Automation). Zudem werden Kanalmessungen durchgeführt. Sie sollen Erkenntnisse liefern, wie sich eine optimale Netzabdeckung gewährleisten lässt, wo und wie engmaschig z.B. Sendeantennen im Werk platziert werden müssen. Auf Basis der Ergebnisse plant Bosch, ein 5G-Testnetz bis Herbst in der Halbleiterfertigung in Reutlingen zu errichten und erste 5G-Anwendungen umzusetzen. Dabei prüfen Ingenieure, inwiefern sich Maschinen und Anlagen anstelle von WLAN oder einer Verkabelung noch effizienter und besser über 5G realisieren und anbinden lassen. Einsatzfelder sind unter anderem autonome Transportsysteme, die über eine lokale Cloud gesteuert werden oder der Fernzugriff auf Maschinen und die Kommunikation von industriellen Anlagen untereinander.

## Waferfab in Dresden: Weltweit erste 5G-fähige Halbleiterfabrik von Bosch

Die Erkenntnisse aus dem Forschungsprojekt in Reutlingen lassen sich künftig auch bei den Planungen von 5G-Netzen nutzen, beispielsweise im neuen Halbleiterwerk in Dresden. „Wir bauen in Dresden die weltweit erste 5G-fähige Halbleiterfabrik von Bosch. Von Tag eins an wird das Werk 5G-ready sein", sagt Bolle. In die neue Waferfab investiert Bosch rund eine Milliarde Euro – die größte Einzelinvestition der Firmengeschichte. Ende 2021 soll die Produktion anlaufen. Die Mikroelektronik ist Wegbereiter für Industrie 4.0 – und das auf unterschiedlichen Ebenen. Zum einen ist Industrie 4.0 ohne intelligente Sensorik undenkbar, zum anderen zählt die Halbleiterfertigung selbst zu den Vorreitern einer vernetzten Produktion. Sie ist nahezu vollautomatisiert und setzt auf künstliche Intelligenz, um Fertigungsprozesse in Echtzeit zu optimieren.

## EU-Forschungsprojekt ermittelt Bedingungen für 5G in der Fertigung

Beim Projekt 5G-SMART kombiniert ein multidisziplinäres Team, bestehend aus Telekommunikationsunternehmen, Netz- und Fabrikbetreibern, Anlagen- und Maschinenbauern sowie Universitäten, 5G mit Industrie-4.0-Lösungen. Darüber hinaus untersuchen die Projektpartner im Bosch-Halbleiterwerk in Reutlingen die Elektromagnetische Verträglichkeit (EMV), sie führen Kanalmessungen durch und


Halbleiter aus Siliziumkarbid in der Bosch Waferfab in Reutlingen

Waferfertigung in der Bosch-Halbleiterfabrik

prüfen, wie sich der Einsatz von 5G in realen Produktionsumgebungen verhält. Zudem sollen neue 5G-Geschäftsmodelle identifiziert werden. Das von der Europäischen Union geförderte Projekt ist auf insgesamt zweieinhalb Jahre angesetzt und endet im November 2021. ■

**Dennis Christmann**
**Sprecher Internet der Dinge (Industrial), Industrie 4.0, Künstliche Intelligenz (Industrie), 5G**
**Robert Bosch GmbH**
**www.bosch.de**


Bild: Phoenix Contact GmbH & Co.KG

*Interview Push-Pull-Steckverbinder M12*

# Endlich Einigkeit bei M12 Push-Pull?

***Nachdem Steckverbinder-Hersteller bei M12 Push-Pull-Verriegelungen lange verschiedene Ansätze verfolgt haben, bringt die IEC61076-2-010 endlich ein branchenweit einheitliches System. Diese Meinung vertreten Dirk Peter Post, Head of Global Product Management Circular Interface Connectors bei Harting Electronics, und Jürgen Sahm, Senior Specialist Product Marketing Circular Connector bei Phoenix Contact, im Interview. In einer Presseerklärung im Frühsommer hatten Phoenix Contact, Harting, Molex, Murrelektronik, Binder, Conec, Escha und Weidmüller bereits bekannt gegeben, einen neuen Standard für die Push-Pull-Verriegelung von M12-Steckverbindern am Markt etablieren zu wollen. Das Ziel der herstellerübergreifenden Kompatibilität soll mit der 2020 veröffentlichten Norm schon bald umgesetzt werden.***

**Es wird derzeit viel über neue Schnellverriegelungssysteme gesprochen. Welche Neuigkeiten gibt es für Rundsteckverbinder M12?**

Jürgen Sahm: Dieses Thema wird seit Jahren im Markt diskutiert. Verschiedene proprietäre Lösungen haben dabei punktuell zu Erfolgen geführt, ein Marktstandard konnte in der Vergangenheit jedoch nicht erzielt werden. Der Wunsch nach einem einheitlichen, standardisierten System ist aber nie verstummt und heute aktueller denn je. Der neue Ansatz M12-Steckverbinder mit Push-Pull-Schnellverriegelung bietet jetzt das Potenzial für einen herstellerübergreifenden Marktstandard. Die Reichweite einer einheitlichen Technologie ist immens und bedeutend für viele Zweige der Industrie.

**Welche Vorteile bietet eine Push-Pull-Verriegelung beim M12-Steckverbinder?**

Dirk Peter Post: Die Verriegelung mittels Push-Pull bringt eine hohe Zeitersparnis von circa 80 Prozent beim Anschließen der Automatisierungskomponenten, da ein Verschrauben nicht mehr erforderlich ist. Auf das Jahr hochgerechnet lassen sich so enorme Einsparpotenziale in der Montage realisieren. Durch das verbesserte Handling können Geräteports zudem kompakter angeordnet werden, was dem Wunsch nach Miniaturisierung und wirtschaftlicher Verkabelung entspricht. Neben der Zeitersparnis entfällt die Überprüfung des korrekten Anzugsmoment der Verriegelung mittels Drehmomentschlüssel. Der Anwender erhält ein akustisches Feedback, das die korrekte Verriegelung anzeigt. Somit haben wir eine einfache, schnelle und sichere Verriegelung.

**Sie haben den Wunsch des Markts nach einem standardisierten System angespro-**

Bild: Harting Deutschland GmbH & Co. KG

**chen. Wie sieht es mit einem normierten Standard für M12 mit Push-Pull aus?**
Sahm: Es gibt eine Norm, die sämtliche Ausführungsformen für einen M12-Push-Pull-Standard beschreibt. Die IEC61076-2-010 beschreibt sowohl eine Innen- als auch eine Außenverriegelung mittels Push-Pull. Sie enthält damit alle Varianten, die für eine durchgängige Systemlösung im Umfeld der Automatisierungstechnik Anwendung finden. Somit kann die IEC61076-2-010 als Erweiterung des M12-Standards mit Schraubverriegelung gesehen werden, wie er in der Basisnorm IEC61076-2-101 beschrieben wird. Der Clou ist, dass die einzige Änderung zum etablierten M12 darin besteht, dass das M12-Gewinde um einen Einstich ergänzt wird und gleichzeitig die bewährten Eigenschaften des M12-Vollgewindes beibehalten werden. Dadurch können die Geräte mittels eines sogenannten M12-Duo-Ports universal ausgerüstet werden und sind zukünftig wahlweise mit Push-Pull oder mit den am Markt weit verbreiteten M12-Schraubsteckverbindern anschließbar, also beide Anschlüsse sind möglich. Sogar Leitungsverlängerungen durch fliegende Push-Pull-Kupplungen können mit marktüblichen Standardkomponenten umgesetzt werden.

**Gibt es weitere Konzepte und Normen zum Thema M12-Push-Pull?**
Post: Neben der IEC61076-2-010 gibt es auch noch die IEC61076-2-012, die eine Push-Pull-Innenverriegelung beschreibt. Die 012 entstand aus Konzepten vorhandener, nicht genormter PP-Industriesteckverbinder, die in das M12-Format hinein konstruiert wurden. Deshalb gibt es keine homogene Integration in die M12-Welt.

**Wie unterscheiden sich diese Normen im weiteren Vergleich?**
Sahm: Obwohl beide Normen dem gleichen Zweck der Schnellverriegelung dienen, sind sie doch sehr verschieden. Während die IEC61076-2-010 auf dem Vollgewinde aus der Ursprungsnorm IEC61076-2-101 basiert und somit den Weltstandard für Automatisierungskomponenten in seiner bekannten Form unangetastet lässt, wurde bei der IEC61076-2-012 das Gewinde durch drei Segmente unterbrochen. Die Gewindeunterbrechungen sind notwendig, damit die drei Rasthaken des Kabelsteckers durch das Gewinde in die Rastposition eintauchen können. Solche Systeme erfordern, dass die Winkelzuordnung zwischen Push-Pull-Mechanismus und Kontaktträger bei der Geräteintegration sehr genau eingehalten wird, da sonst der Push-Pull-Steckverbinder blockiert und nicht mehr in den Port steckbar ist. Bei der Lösung auf Basis der IEC61076-2-010 ist keine Gewindeunterbrechung erforderlich, da die Rastkontur an den Anfang des M12-Gewindes gelegt wurde und als Einstich auf einfache Art bei der Gewindeherstellung im Standardprozess realisiert werden kann. Das macht das Design-in für den Gerätehersteller besonders einfach. Die Gerätesteckverbinder sind genauso wie beim bewährten M12-Standard rotationssymmetrisch ausgelegt, wodurch die Push-Pull-Mechanik des Geräteports nicht zur Kodierung des M12-Kontaktträgers ausgerichtet werden muss. Dies gibt dem Gerätehersteller einen hohen Freiheitsgrad, die Kabelabgänge der Ports einfach und vor allem wirtschaftlich zu gestalten. Die M12-Basisnorm -101 und die Push-Pull-Norm -010 sind auch bezüglich der Design-in-Anforderungen konsistent, sie arbeiten sozusagen im Gleichschritt. Das geht soweit, dass ein herkömmlicher M12-Port mit Standardgewinde – ohne konstruktiven Eingriff in die Gerätekonstruktion – durch einen kompatiblen Duo-Port mit Push-Pull ausgetauscht werden kann und das sogar nachträglich bei bestehenden Gerätekonzepten. Hinzu kommen noch weitere Vorteile, beispielsweise dass die Push-Pull-Verriegelungselemente in Kunststoff oder Metall ausgeführt werden können. Dadurch sind kostengünstige Push-Pull-Steckverbinder aus Kunststoff herstellbar, die in erweiterten Applikationsbereichen wie Agrar- oder Chemieindustrie einsetzbar sind.

**Gibt es eine Tendenz, welche Norm von den etablierten großen M12-Herstellern unterstützt wird und warum?**
Post: Ja, die gibt es. Die acht für M12-Steckverbinder etablierten Hersteller Weidmüller, Conec, Escha, Molex, Murrelektronik, Binder, Harting und Phoenix Contact haben sich für die Unterstützung der IEC61076-2-010 ausgesprochen. Die Hauptgründe dafür sind die herstellerübergreifende Funktionssicherheit und wirtschaftliche Herstellbarkeit durch die Nähe zur Basisnorm 101 sowie eine einfache Integration ins Gerät, ohne große Aufwände bei Design-in. Ebenfalls spielen die schnelle und breite Verfügbarkeit des neuen Systems und die Investitionssicherheit durch eine breite Herstellerunterstützung eine große Rolle. Aus diesen Gründen fließt die DNA der M12-Basisnorm (-101) in die 010 unverändert ein und wird mit dem Know-how der oben genannten M12-Hersteller zu einem neuen Welt-Standard fortgeschrieben. Dadurch, dass sich die Hersteller nicht nur normativ, sondern auch in der Praxis einer abgesicherten herstellerübergreifenden Austauschbarkeit des Push-Pull-Systems verschrieben haben, kann sich der Anwender eines wie vom M12-Standard gewohnten breiten, technisch ausgereiften Produktportfolios mit allen Vorzügen des Multi-Sourcing bedienen.

**Kann man auf Grund der herstellerübergreifenden Kompatibilität bereits sagen, dass sich die IEC61076-2-010 zum Marktstandard entwickeln wird?**
Sahm: Proprietäre Lösungen mit erhöhtem Aufwand beim Design-in haben heutzutage keine Chance in der Industrie. Einfache, standardisierte Lösungen, die einer durchgängigen Systemtopologie folgen, sind das Gebot der Stunde. Diesem übergreifenden Gedanken haben sich die acht Hersteller verschrieben. Die Botschaft ist, dass sich die M12-Standardnorm und die Push-Pull-Norm in weiten Teilen decken und alle in der industriellen Verdrahtung mit M12 erforderlichen Varianten enthalten. Durch den einfachen Einstich muss der Design-in-Prozess nicht geändert werden – so einfach ist der Schritt zum Push-Pull. ■



Harting Deutschland
GmbH & Co. KG
www.harting.com

*Herstellerübergreifende Transparenz in Ethercat*

# Steuerungsunabhängige Diagnoseschnittstelle

***Diagnoseeigenschaften sind für den Erfolg einer Feldbustechnologie von zentraler Bedeutung. Um die Diagnose in Ethercat-Netzwerken noch besser zu machen, hat die Ethercat Technology Group (ETG) mit der Spezifikation ETG.1510 'Profile for Master Diagnosis Interface' eine herstellerunabhängige Diagnoseschnittstelle definiert, die es der Ethercat-Steuerung auf nutzerfreundliche und standardisierte Weise ermöglicht, detaillierte Informationen zur Netzwerkdiagnose sowie zum Systemzustand für Tools von Drittanbietern zur Verfügung zu stellen.***

Alessandro Figini, Ethercat-Technology-Experte, ETG

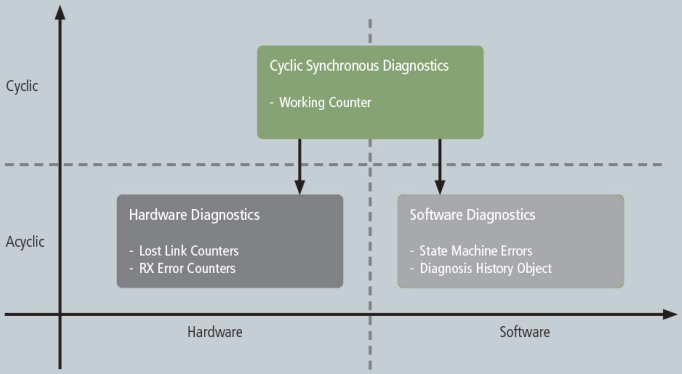
In der heutigen Industrie gehört die durchgängige Verfügbarkeit von Maschinen und Anlagen zu den wichtigsten Faktoren in Bezug auf Effizienz und Wettbewerbsfähigkeit. Ethercat hat sich hier nicht zuletzt aufgrund seiner robusten Kommunikationsinfrastruktur als zuverlässige Technologie bewährt. Nichtsdestotrotz können industrielle Umgebungen selbst für die zuverlässigsten Kommunikationstechnologien wie Ethercat herausfordernd sein. Sich permanent bewegende Maschinenteile oder kontinuierliche Vibrationen können vorübergehende Leitungsverluste oder langfristig sogar Kabelbrüche verursachen, während EMV-Störungen sich gerade auf dem Kommunikationspfad befindende Signale verfälschen können. In all diesen Fällen sind es die Diagnosefähigkeiten des Feldbusses, die Fehler erkennen, lokalisieren und deren mögliche Ursachen ergründen müssen. Je besser sie funktionieren, desto kürzer sind die Ausfallzeiten einer Maschine.



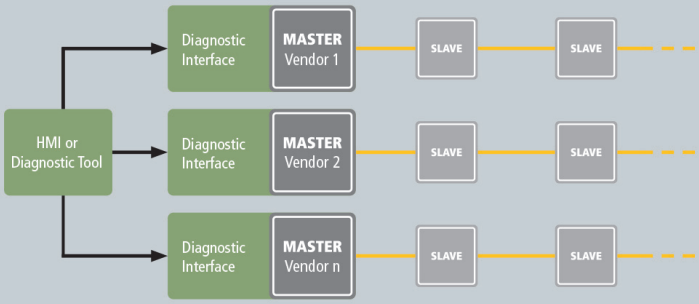
## Mehr als herkömmliches Ethernet

Die Ethercat-Technologie verfügt über ganz besondere Diagnoseeigenschaften, die über die entsprechenden Fähigkeiten des herkömmlichen Ethernet weit hinausgehen. Dabei werden die nötigen Informationen entweder über die Ethercat-Kommunikationschips (ESC) direkt in Hardware oder aber mittels Software-Funktionalitäten zur Verfügung gestellt. Auf Geräteseite sind daher keine speziellen Erweiterungen erforderlich. Jedes Ethercat-Datenpaket endet mit einem 16-Bit-Working-Counter-Feld, das von allen vom Datagramm selbst adressierten Geräten inkrementiert wird. Unstimmigkeit zwischen dem erwarteten und dem tatsächlich erhaltenen Wert des Working Counter bedeutet, dass nicht alle gekoppelte Geräte das Datagramm erfolgreich verarbeitet haben und daher nicht mit konsistenten Daten im aktuellen Zyklus arbeiten. Dies kann eine direkte Fehlerreaktion in der Steuerung anstoßen. Ist das der Fall, werden Eingangsdaten, die das Datagramm transportiert, verworfen. Die Steuerung kann azyklisch zusätzliche Informationen abrufen und ermöglicht so die Lokalisierung sowie die Erkennung etwaiger Gründe für das Kommunikationsproblem. Auf der Hardware-Seite über-

Bilder der Doppelseite: Ethercat Technology Group




Übersicht der Diagnosefunktionalitäten von EtherCAT




Prinzip der Master-unabhängigen EtherCAT-Diagnoseschnittstelle

Übersicht der Diagnosefunktionalitäten von Ethercat (links) und Prinzip der steuerungsunabhängigen Ethercat-Diagnoseschnittstelle (rechts)

wacht und erkennt jeder Ethercat Slave Controller einen Leitungsverlust genauso wie eine Signalunterbrechung auf jedem Port und inkrementiert entsprechend den korrespondierenden Link Lost Counter oder RX Error Counter. Auf der Software-Seite hingegen können Kommunikationsfehler wie z.B. ein abgelaufener Watchdog auf den zyklischen Daten oder ein Synchronisationsverlust innerhalb des Netzwerks einen unerwarteten Zustandsübergang in der Ethercat State Machine auslösen. Diese Fehler werden vom AL Status Code angezeigt, der vom Software Stack zurückgegeben wird, wann immer ein unerwarteter Zustandsübergang eintritt.

## Diagnose unabhängig von der Zykluszeit

Der Steuerung in allen Ethercat-Netzwerken stehen somit alle notwendigen Diagnoseinformationen zur Verfügung, um den Netzwerkstatus zu überwachen sowie Fehler erkennen und lokalisieren zu können. Zur Auswertung und Nutzung müssen diese 'rohen' Daten an Diagnose-Tools sowie Anwender weitergegeben werden. Mit der Spezifikation ETG.1510 'Profile for Master Diagnosis Interface' hat die Ethercat Technology Group eine Lösung definiert, die es externen Tools ermöglicht, unabhängig vom Steuerungshersteller sowie der Software-Implementierung auf die vom Ethercat-Netzwerk zur Verfügung gestellten Diagnoseinformationen zuzugreifen. Die ETG.1510 erweitert die Spezifikation ETG.1500 'Ethercat Master Classes'. Die Diagnoseinformation wird in das Ethercat-Objektverzeichnis abgebildet, das in der ETG.1500 definiert und zu diesem Zweck ergänzt wurde. Dies bedeutet insbesondere, dass Objekte im Indexbereich 0x8000 die Netzwerkstruktur wie von der Steuerung erwartet basierend auf der Offline-Konfiguration beschreiben, während Objekte im Bereich 0x9nnn die aktuelle Netzwerktopologie anzeigen, wie sie mittels eines Online-Scans festgestellt wurde. Die Diagnoseinformation selbst ist im Indexbereich 0xAnnn in Form von konsistenten, kumulativen Zählern abgebildet, die den Netzwerkstatus vom Systemstart bis zum gegenwärtigen Zeitpunkt zusammenfassen. So kann mit einer Frequenz auf die Diagnoseschnittstelle zugegriffen werden, die unabhängig von der Zykluszeit des Ethercat-Netzwerks ist, und externe Tools müssen keine Echtzeitleistung erbringen. Der Zugriff auf die Diagnoseinformationen erfolgt über das bewährte 'CAN application protocol over Ethercat' (CoE). Die CoE-Dienste werden in der Steuerung mithilfe der Standard-Mailbox-Gateway-Funktionalität über das Objektverzeichnis der Steuerung geroutet, das in der Spezifikation ETG.8400 beschrieben ist. Basierend auf bereits existierenden und vollständig standardisierten Protokollen und Funktionalitäten kann die Diagnoseschnittstelle damit einfach als schlanke Software-Erweiterung zusätzlich zu jeder Standard-Steuerungsimplementierung realisiert werden. Die benötigten Ressourcen einer solchen Software-Erweiterung sind sehr gering, weshalb sich die Diagnoseschnittstelle für alle Steuerungslösungen inklusive einfacher und kompakter Embedded-Systeme eignet.

## Fazit

Dank der Ethercat-Diagnoseschnittstelle, die mit der Spezifikation ETG.1510 eingeführt wurde, können Anbieter von Maschinen- und Netzwerkdiagnose-Tools eine universelle Schnittstelle zum Sammeln von Diagnosedaten aus Ethercat-Netzwerken nutzen. Sie können diese Informationen anwenderfreundlich und grafisch intuitiv an Techniker und Ingenieure weitergeben, ohne dabei jedes Mal herstellerspezifisch die Steuerung berücksichtigen oder das Zugriffsprotokoll für jede unterschiedliche Steuerungsimplementierung anpassen zu müssen. ■

**Alessandro Figini,**
**Ethercat-Technology-Experte,**
**Ethercat Technology Group**
**www.ethercat.org**


*Terz Spark-XS mit 24VDC Versorgung*

# Robuste M12-PoE-Switche

***Intelligente Produktionsverfahren erfordern immer häufiger den Austausch von Informationen mit ihrer Umgebung. Kommunizierende Montageroboter, selbstfahrende Gabelstapler und vollautomatisierte Lagersysteme benötigen umfangreiche Sensorik. Eine zuverlässige Versorgung mit Energie und Daten ist unerlässlich bei Neuinstallationen und Nachrüstungen. Aber ist noch ausreichend Platz im Schaltschrank?***

Der Terz Spark-XS mit 24VDC Versorgung ermöglicht durch PoE die Übertragung von Energie und Daten über ein Kabel.

Der modulare Anlagenbau gewinnt immer mehr an Bedeutung in der Automatisierungstechnik. Eine flexible Anpassung an neue Anforderungen und eine schnelle Adaptierung und Nachrüstung bestehender Maschinen, ist heutzutage der Standard. Dies ist jedoch nicht der einzige Trend in der Industrie. Auch die Dezentralisierung von Komponenten in kleinere Schaltschränke bis hin zu einem völlig schaltschranklosen System wird immer stärker verfolgt. In fahrerlosen Transportsystemen (FTS) ist es aufgrund der Gesamtgröße des Fahrzeugs schwierig, überhaupt alle erforderlichen Komponenten und Funktionen unterzubringen. Durch die stark wachsende Anzahl von komplexen Sensorsystemen und Kameras wird der ohnehin schon begrenzte Platz noch weiter reduziert. Insbesondere moderne 3D-Kameras und Laserscanner benötigen eine sichere und zuverlässige Stromversorgung, ebenso wie eine stabile Anbindung an die Kommunikationsinfrastruktur. Ein Ausfall oder ein unzuverlässiger Betrieb dieser Systeme würde zum sofortigen Stopp der Produktion oder der Materialzulieferung führen und einen Produktionsausfall verursachen. Wie lassen sich diese Herausforderungen unter dem Aspekt der immer weiter voranschreitenden Digitalisierung bewältigen?

## Raus aus dem Schaltschrank

Die Dezentralisierung der einzelnen Automatisierungskomponenten hat sich als eine echte Alternative zur klassischen Schaltschrankvernetzung etabliert. Zunehmend werden Komponenten mit einer hohen Schutzart IP65/67 oder höher angeboten und ermöglichen so völlig neue Anlagenkonzepte. Einen zentralen Dreh- und Angelpunkt nehmen dabei Industrial-Ethernet-Switche ein, die in modernen Anlagen das Rückgrat für die Datenkommunikation bilden. Aber nicht nur für die Übertragung von Daten sind Switche geeignet, sondern auch für die Stromversorgung der Endteilnehmer über Power over Ethernet (PoE). Die Übertragung von Daten und die gleichzeitige Versorgung mit Energie über das Ethernet-Kabel bietet viele Vorteile. Bei der Vernetzung von Kamerasystemen und diverser Sensoren, die den PoE-Standard unterstützen, können Platz und Kosten für eine zusätzliche Verkabelung und Netzteile gespart werden. Durch die Dezentralisierung werden die benötigten Kabellängen optimiert und der Installationsaufwand reduziert. Durch die kürzeren Kabel lassen sich Leitungsverluste reduzieren und die Effizienz der gesamten Anwendung steigern.

## Erhöhte Flexibilität und modulare Bauweise

Es ist zum Teil sehr schwierig, bestehende Maschinen mit neuen komplexen Funktionen nachzurüsten, die zusätzliche Komponenten und Verkabelung erfordern. Mit dem Einzug der Industrie 4.0 und der zunehmenden Informationstransparenz wird dies aber immer weiter in den Fokus



Bilder der Doppelseite: Terz Industrial Electronics GmbH

rücken. Durch die Reduzierung des Platzbedarfs für die Verkabelung und Platzierung der Switche im Feld, gestaltet sich die Modernisierung deutlich einfacher. Kompakte Ethernet-Switche mit kleiner Portzahl sammeln die Daten dezentral direkt an den Sensoren ein und versorgen diese auch mit Strom. Das nachzurüstende System lässt sich Dank der modularen Bauweise separat testen und kann später deutlich einfacher integriert und auf weitere Maschinen adaptiert werden.

## Kostenersparnis

Schaltschränke können auf das wesentliche reduziert werden und in einigen Fällen kann man sogar komplett auf sie verzichten. Auch für die Verkabelung und Stromversorgung gilt dieses Prinzip. So lassen sich nicht nur die Materialkosten durch Einsparung von Kabellänge und zusätzliche Netzteile senken, sondern auch der Aufwand für die Installation der Komponenten und Verlegung der Kabel wird reduziert.

## Funktionssicherheit für die Anlage

Entscheidend für den Einsatz in industriellen Applikationen ist nicht nur die Widerstandsfähigkeit gegenüber Schock- und Vibrationen, sondern auch die elektrischen Eigenschaften, die unter allen auftretenden klimatischen Umweltbedingungen eingehalten werden müssen. Dies gilt umso mehr bei Verzicht auf einen schützenden Schaltschrank. Der neue Spark-XS PoE-Switch mit vibrationssicherer M12-Anschlusstechnik auf fünf Ports, wurde speziell für den Einsatz in rauen industriellen Umgebungen außerhalb des Schaltschranks mit einem erweiterten Temperaturbereich von -40 bis +70°C designt und entwickelt. Der Spark versorgt bis zu vier Teilnehmer mit Energie und Daten über D-kodierte M12-Steckverbinder. Die Daten werden über einen X-kodierten M12-Uplink-Anschluss mit Gigabitgeschwindigkeit weitergeleitet. Durch die hohe Bandbreite auf dem Uplink-Port besteht ausreichend Reserve für moderne Kameras und Sensoren. Das robuste IP65/67-Metallgehäuse ist staubdicht, schützt gegen das Eindringen von Wasser und sogar gegen kurzzeitiges Untertauchen. In vielen Applikationen ist das Hochfahren ein kritischer Moment. Durch die unter Umständen auftretenden hohen Stromimpulse während des Einschaltvorgangs der angeschlossenen Komponenten, kann die Belastung der Energieversorgung zu Fehlerfällen führen. Alle Terz-Switche verfügen über eine Einschaltstrombegrenzung und reduzieren somit die Last auf die Versorgungsspannung, um ein sicheres Hochfahren der Anlage zu gewährleisten. Die vier PSE (Power Sourcing Equipment)-Ports arbeiten nach dem IEEE-Standard 802.3at Typ 1. Ein integrierter DC/DC-Wandler erzeugt die für PoE nötigen 48V Spannung aus den in der Industrie üblichen 24VDC. Somit können bereits vorhandene Netzteile für die Versorgung des Switches eingesetzt werden. Terz setzt bei seinen PoE-Switche auf eine doppelte Absicherung der Ports, um auch im Fehlerfall die Anlagensicherheit zu gewährleisten. Neben der üblichen internen Schmelzsicherung pro Port wird bei den Terz PoE-Switche, im Gegensatz zu marktüblichen Lösungen, der spannungsführende Pfad der PoE-Ports geschaltet und überwacht. Im Fehlerfall fließt maximal der durch die Einzelsicherungen limitierte Strom. Das Risiko eines Kabelbrands für den Fall, dass es zu einer Abscherung oder einer anderen Beschädigung des Kabels kommt, wird hierdurch reduziert. Die Lebensdauer der Maschinen und Anlagen in der Industrie erstreckt sich über mehrere Jahre, diese gilt demzufolge auch für alle Komponenten, die außerhalb des Schaltschranks installiert werden. Um auch bei Vibrationen zuverlässig zu funktionieren, erfolgt die Befestigung der Switche direkt auf der Montagewand mittels M6-Schrauben. Falls diese nicht elektrisch leitfähig und nicht geerdet ist, wird die Funktionserde über einen separaten Kabelschuh angeschlossen. Der mechanische und elektrische Anschluss kann so unabhängig voneinander durchgeführt werden. Um den steigenden Anforderungen gerecht zu werden, sind bereits weitere PoE-Switche als Portfolioergänzung in Planung. Neben Varianten mit größeren Portzahlen in hoher Schutzart, wird es auch kompakte RJ45-Varianten für kleine Schaltschränke geben.

## Fazit

Flexible Produktion und die wandelbare Fabrik werden in den kommenden Jahren weiter in den Fokus der Hersteller rücken. Die Philosophie einer nahezu schaltschranklosen Installation unterstützt dieses Konzept und bietet in Zukunft die Möglichkeit für völlig neue Ansätze bei der Entwicklung. Hier können kompakte und robuste schaltschranklose Komponenten ihre Stärke ausspielen und bieten maximale Flexibilität bei der Entwicklung dieser Systeme. ■



TERZ Industrial Electronics GmbH
www.terz-ie.com


Geprüft und entwickelt für die Industrie nach dem internationalen IEEE-Standard 802.3at, auch für die Systemintegration als RJ45 Variante.

Join now!

Bild: ©MicroOne/stock.adobe.com

# SPS MAGAZIN Webinare im TeDo Verlag

***Das SPS-MAGAZIN startet ab Oktober mit den TechTalks eine eigene Webinar-Serie, bei der verschiedene Themen aus der Automatisierung in einer Stunde von je drei Firmen in drei 20-minütigen Vorträgen näher beleuchtet werden. Einige Themen möchten wir Ihnen hier vorstellen. Der Link zur kostenfreien Anmeldung für die TechTalks finden Sie hier: www.webinare.i-need.de.***

Bild: ©Sikov/stock.adobe.com

## Nächste Generation der Maschinensteuerung: Von der SPS zum IoT-Controller

Wie Maschinenbauer und Betreiber das Internet gewinnbringend nutzen können und welche Art von Steuerungsplattform für das IIoT-Zeitalter besonders gut passt erläutert unser Webinar am Beispiel von drei unterschiedlichen Steuerungsfamilien.

Bild: ©metamorworks/stock.adobe.com

## Industrial 5G – Was die neue Drahtlostechnologie für die Automatisierung bringt

Mit Industrial 5G kommt eine neue Wireless-Technologie. Nur wer sich rechtzeitig auf den Wandel einstellt, schöpft das volle Potenzial aus.

Bild: ©Xantaro/Fotolia.com

## SPE - Einfache und flexible Kommunikation im Feld

Single Pair Ethernet (SPE) bietet im Zeitalter des Industriellen Internets der Dinge eine einfache, platzsparende und leistungsfähige Möglichkeit der Verbindungstechnik bis in die Feldebene.

Bild: ©ipopba/Fotolia.com

## Aus dem IoT auf die Maschine: Remote Management, aber sicher!

Nicht erst seit Corona erwarten Betreiber von Maschinen und Anlagen sichere, robuste aber auch umfangreiche Servicemöglichkeiten an ihren Assets. Wir zeigen, wie diese Anforderungen kostengünstig umgesetzt werden können.

# WLAN für die Industrie

***Die Anforderungen an Industrie-WLAN sind hoch. Sowohl an die Zuverlässigkeit als auch an die Latenzzeiten stellen industrielle Anwendungen höhere Anforderungen als die typische Heim- oder Büroanwendung.***

Komponenten für die Produktion werden auf Robustheit und Zuverlässigkeit hin entwickelt. Beim industriellen WLAN gilt das nicht nur für die entsprechende 'Verpackung' sondern auch und gerade für die hochverfügbare Verbindung der Netzwerkteilnehmer. Industrial WLAN hat seine Praxistauglichkeit in vielen Anwendungen bewiesen und sich seinen festen Platz in der Fabrikhalle erobert. Die folgende Herstellerübersicht zeigt Anbieter in diesem Marktsegment. Deren Produkte samt Eigenschaften und Leistungsdaten listet ergänzend die Produktsuchplattform i-need.de online auf. (*kbn*) ■

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.
**14597**
Hilden
02103/ 97885-0
www.advantech.de
EKI-6340

Artila Electronics Co., Ltd.
**26276**
Düsseldorf
0211/ 938898-0
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/ 654-0
www.dold.com
Funk-Sicherheitsmodul UH 6900

HMS Industrial Networks GmbH
**35212**
Karlsruhe
0721/ 989777-410
www.hms-networks.de
Anybus Wireless Bridge II

Insys Microelectronics GmbH
**20771**
Regensburg
0941/ 58692-0
www.insys-icom.de
EBW-W100

IPC2U GmbH
**23270**
Langenhagen
0511/ 807259-0
www.ipc2u.de
RS930W Wireless Switch



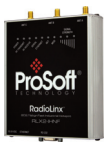
Lucom GmbH
**14253**
Fürth
0911/ 957606-00
www.lucom.de
GhostBridge - High Perf. Wireless Eth. Bridge

MC Technologies GmbH
**34000**
Hannover
0511/ 676999-187
www.mc-technologies.net
Wifi LTE Antenne (MC0114531-A)

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


Primation Systemtechnik GmbH & Co. KG
**1722**
Grasbrunn
089/ 46260-0
www.primation.de
702-W

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




ProSoft Technology
**24501**
Frankfurt
+33/ 5343687-20
www.prosoft-technology.com
RLX2-IHNF-E

Siemens AG, Industrial Communication
**1758**
Nürnberg
0911/ 895-0
www.siemens.de
Scalance W788/748 RJ45

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

Wachendorff Prozesstechnik GmbH & Co. KG
**14349**
Geisenheim
06722/ 9965-20
www.wachendorff-prozesstechnik.de
WLAN Access Point/Client WLANAPCC

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/ 9324-0
www.wieland-electric.com
Wienet AP-ETH-A

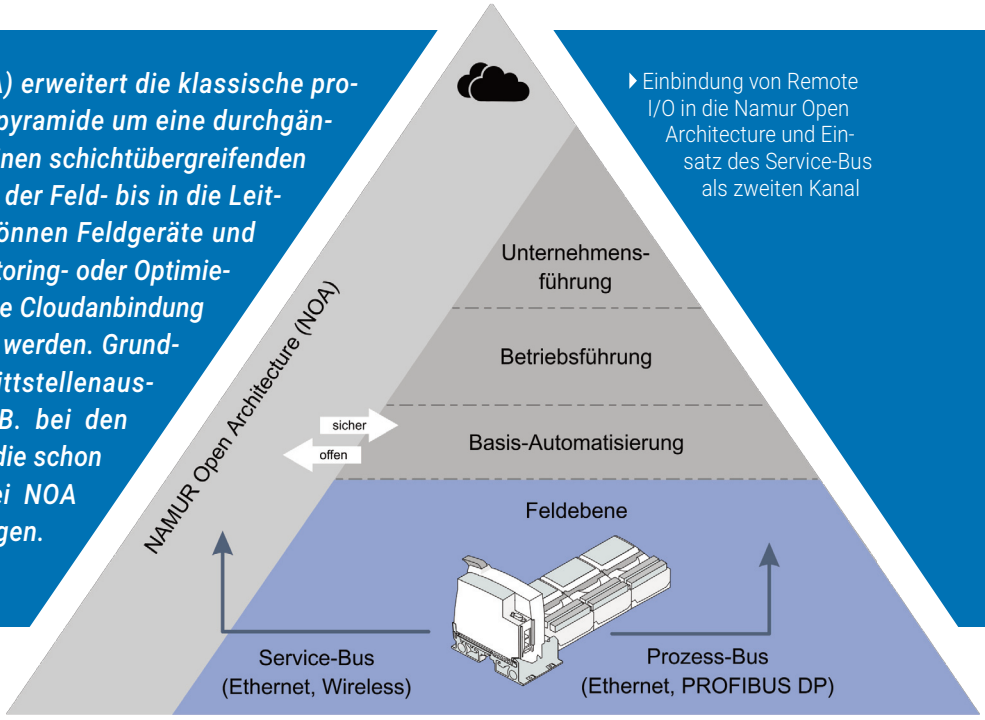
Wiesemann & Theis GmbH
**24425**
Wuppertal
0202/ 2680-110
www.WuT.de
WLAN Client Bridge

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 08.09.2020

*Offene Kommunikationsstrukturen für die Prozessindustrie*

# Remote I/O-System IS1+ und Namur Open Architecture

***Die Namur Open Architecture (NOA) erweitert die klassische prozessindustrielle Automatisierungspyramide um eine durchgängige Kommunikationsstruktur, die einen schichtübergreifenden transparenten Datenaustausch von der Feld- bis in die Leitebene vorsieht. Auf diese Weise können Feldgeräte und Steuerungen in übergeordnete Monitoring- oder Optimierungskonzepte eingebunden und eine Cloudanbindung im Sinne der Industrie 4.0 realisiert werden. Grundlage dafür ist eine passende Schnittstellenausstattung der Feldgeräte – wie z.B. bei den Remote I/O-Systemen von R. Stahl, die schon länger über einen ähnlich wie bei NOA beschriebenen zweiten Kanal verfügen.***




Einbindung von Remote I/O in die Namur Open Architecture und Einsatz des Service-Bus als zweiten Kanal

Schon seit mehr als 30 Jahren hat der Explosionsschutz-Spezialist R. Stahl Remote I/O-Lösungen für explosionsgefährdete Bereiche im Programm. Obwohl sich die neueste System-Generation IS1+ gegenüber ihren Vorgängern durch zahlreiche Innovationen auszeichnet, besteht ihr zentraler Vorteil in einem langjährig bewährten, auf offenen Systemschnittstellen basierenden Grundkonzept. Es gestattet den Betrieb der Geräte mit nahezu jedem Automatisierungssystem, bietet umfangreiche Diagnosefunktionen mit hohem Mehrwert für Plant-Asset-Management-Anwendungen und ermöglicht über eine Service-Bus-Schnittstelle die parallele Übertragung von Diagnosedaten und HART-Informationen angeschlossener Feldgeräte. Speziell mit dem Service-Bus und der vollständigen Transparenz für das HART-Protokoll empfiehlt sich das Remote I/O-System IS1+ für moderne Anlagenkonzepte im Sinne der Namur Open Architecture.

## Zweiter Kanal für parallele Datenkommunikation

Der Service-Bus, im Umfeld der NOA auch als 'zweiter Kanal' bezeichnet, ist keine neue Erfindung. Schon die ersten Remote I/O-Systeme, die R. Stahl bereits in den achtziger Jahren entwickelt hatte, verfügten über eine eigene Diagnose- und Konfigurationsschnittstelle bis in die Zone 1. Bei IS1+ wurde diese zunächst für die Gerätekonfiguration über Modbus RTU genutzt oder diente in Profibus DP-Umgebungen als separater Zugang für erweiterte Diagnostik und HART-Informationen. Seit 2003 lassen sich das Remote I/O-System und angeschlossene HART-Feldgeräte mittels DTM-Treibern wahlweise über den Service-Bus oder den Prozess-Bus in Field-Device-Tool-Applikationen (FDT) des Plant Asset Managements (PAM) einbinden. Während bei Profibus DP der zweite Kanal vorwiegend als separates physikalisches Netzwerk realisiert wird, da das Tunneln eines zusätzlichen Protokolls bei diesem Feldbus relativ aufwändig ist und von Automatisierungssystemen nur bedingt unterstützt wird, eröffnete die Ethernet-Ausstattung von IS1+ die Möglichkeit, Profinet-, Ethernet/IP- oder Modbus TCP-Netzwerke mit integriertem Service-Bus bis in die Zone 1 auszudehnen.

## IP-Kommunikation bis in Ex-Bereiche

Das 100MBit/s-Ethernet ermöglicht der IP-Kommunikation den Weg bis in explosionsgefährdete Bereiche der Feldebene und kombiniert Prozess-Bus und Service-Bus effektiv mitei-

Bilder der Doppelseite: R. Stahl Schaltgeräte GmbH

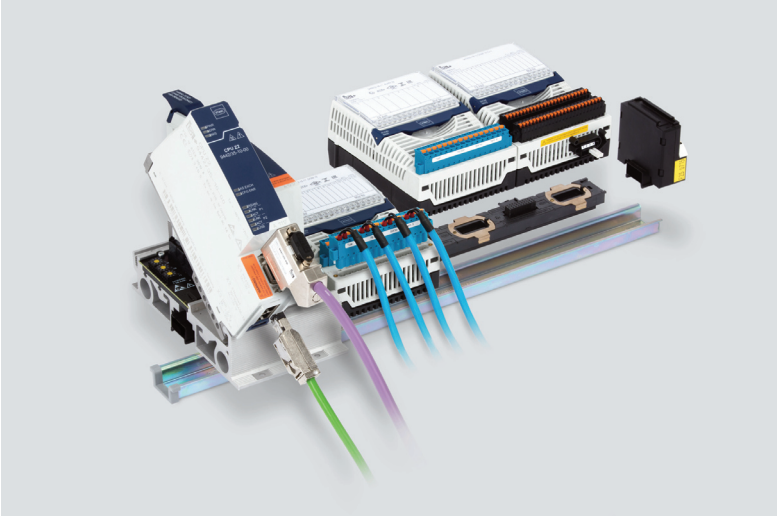
nander. Durch den integrierten Webserver eröffnen sich interessante neue Use Cases für den Remote Zugriff. So vereinfachte der IP-basierte Datenverkehr nicht nur bei Inbetriebnahmen Remote Loop Checks bis zur Feldgeräteebene, ohne dass Personal im Feld anwesend sein musste – auch Firmware-Updates am anderen Ende der Welt ließen sich unter entsprechenden Security-Vorkehrungen von nun an per Internet durchführen. Weitere Möglichkeiten bestehen im Auslesen von Versionsständen, in der Kontrolle des korrekten Anschlusses von HART-Geräten auch ohne Leit- oder PAM-System oder im Vergleich von Soll-/ Ist-Bestückung der IS1+ Systeme. Insbesondere im Kontext von NOA-Aktivitäten und -Strukturen schufen zuletzt die neuesten, 'mehrsprachigen' CPUs (Communication Processing Units) von IS1+ die Basis für eine ganze Reihe an Optionen.

## Multi-Protokoll-CPU vereinfacht Migrationskonzepte

Speziell bei Migrationsvorhaben, etwa zur Infrastrukturmodernisierung oder der Netzwerkerweiterung mit verschiedenen Übertragungsprotokollen, sorgen die Multi-Protokoll-CPUs von IS1+ für deutliche Vereinfachungen. Diese integrieren sowohl die Protokollstacks für Profinet, EtherNet/IP und Modbus TCP als auch für den 'Klassiker' Profibus DP, der in eigensicherer Ausprägung als RS485-IS seit den ausgehenden neunziger Jahren häufig bei Remote I/O-Installationen auch in Ex-Bereichen eingesetzt wird. Auf diese Weise kann IS1+ in Bestandsanlagen, die migriert werden sollen, weiterhin über Profibus DP mit dem Leitsystem kommunizieren, während parallel dazu ein Ethernet-Netzwerk aufgebaut wird. Dieses lässt sich als zweiter Kanal zur Übertragung erweiterter Diagnose- oder HART-Daten nutzen. Erfolgt dann die Umrüstung auf ein Ethernet-basiertes Leitsystem z.B. mit Profinet für alle Prozess-, Diagnose- und HART-Daten, ist die erforderliche Infrastruktur bereits vorhanden und die CPU-Baugruppe braucht lediglich per Schalter auf Profinet-Kommunikation umgestellt werden. Währenddessen gewährleistet der integrierte Webserver über den zweiten Kanal weiterhin den Zugriff auf die zusätzlichen Daten. Alternativ sorgt der IS1+ DTM wie bisher üblich für die bidirektionale Übertragung von HART-Variablen und sämtlicher HART-Informationen angeschlossener Geräte, wodurch die Remote-Konfiguration oder die Funktion von Audit Trail Applikationen gewährleistet bleiben.

## Vorausschauende Eigendiagnose

Zu diesen Zwecken stellt das IS1+ System verschiedene Mechanismen bereit, mit denen sich die ordnungsgemäße Funktion von HART-Geräten kontrollieren, Drahtbrüche in Verbindungen oder Kurzschlüsse bei einfacheren Geräten wie Näherungssensoren, Kontakten oder Magnetventilen detektieren lassen. Eine gänzlich neue Funktionalität des IS1+ betrifft die vorausschauende Diagnose, bei der die einzelnen Systemkomponenten auf Basis präziser interner Messungen der Umgebungs- und Betriebsbedingungen die eigene altersbedingte Ausfallwahrscheinlichkeit ermitteln. Die errechnete Ausfallwahrscheinlichkeit wird zwölf Monate vor dem prognostizierten Ereignis gemeldet, um eine ausreichende Zeitspanne für den Ersatz zu gewährleisten. Neben der Meldung, die an das Leitsystem und Plant-Asset-Management-System gesendet wird, signalisiert eine blaue LED gemäß Namur NE107 am Gehäuse dem technischen Personal vor Ort den bestehenden Wartungsbedarf.

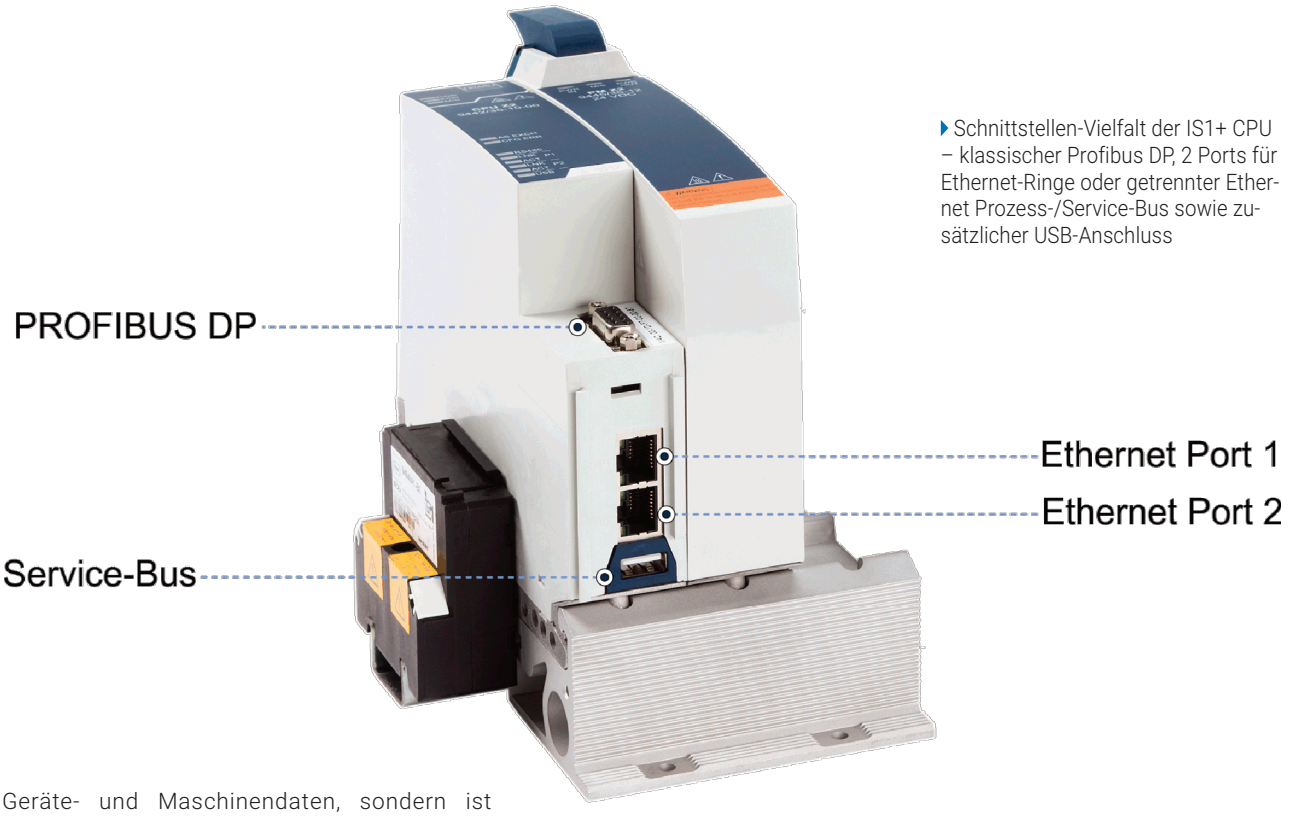


Multi-Protokoll-Talent: Die CPU von IS1+ integriert Protokollstacks für Profinet, EtherNet/IP, Modbus TCP und Profibus DP.


Feldinstallation eines IS1+ Remote I/O-Systems mit Anbindung über Ethernet und Profinet-Protokoll – optional auch mit S2 Redundanz

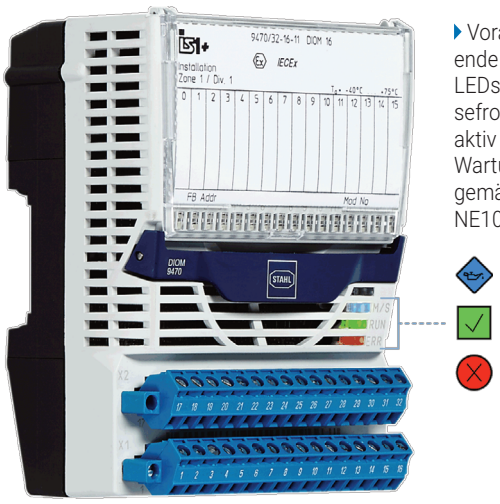
## Ertüchtigung von IS1+ für OPC UA

Im Rahmen der Entwicklungsarbeiten an der Namur Open Architecture werden auch künftige Use Cases für Remote I/O-Systeme diskutiert. Während es bei der etablierten Prozesssteuerung und ihrer Einbindung in Prozessleitsysteme außer der optionalen Ethernet-Kommunikation zu keinen grundlegenden Änderungen kommt, gewinnt der zweite Kanal für Automatisierungsnetzwerke erheblich an Bedeutung. Für den Ausbau des transparenten Parallel-Datenaustausches erweist sich der plattformunabhängige Standard OPC UA (Unified Architecture) als vorteilhaft. Denn OPC UA übermittelt nicht nur




Schnittstellen-Vielfalt der IS1+ CPU – klassischer Profibus DP, 2 Ports für Ethernet-Ringe oder getrennter Ethernet Prozess-/Service-Bus sowie zusätzlicher USB-Anschluss

Geräte- und Maschinendaten, sondern ist zudem in der Lage, diese Daten in einer maschinenlesbaren Semantik abzubilden. Als standardisiertes Informationsmodell dient die OPC UA Companion Specification, in der Geräteklassen und ihre für die Maschinenkommunikation relevanten Funktionen bzw. Speicheradressen einheitlich und herstellerunabhängig hinterlegt werden. Auf dieser Grundlage können die Informationsmodelle vollständig von Computern ausgewertet und weiterverarbeitet werden. Anders als z.B. im Robotikbereich haben sich die Companion Specifications in der Prozessautomatisierung noch nicht etabliert. Deshalb begann die FieldComm Group (FCG) im Jahr 2017 zusammen mit der OPC Foundation, später auch mit Unterstützung von Profibus/Profinet International, ein Process Automation Device Information Model, kurz: PA-DIM, zu spezifizieren. Das PA-DIM orientiert sich zu großen Teilen an den Anforderungen der Namur Open Architecture sowie den Namur Empfehlung NE107 'Selbstüberwachung und Diagnose von Feldgeräten' und NE131 'Namur-Standardgerät – Feldgeräte für Standardanwendungen'. Im Juni 2020 wurde die Version 1.0 der PA-DIM veröffentlicht. Ein halbes Jahr zuvor hatte R. Stahl an einem Use Case für Remote I/Os auf Basis von PA-DIM gezeigt, wie sich Bestandsanlagen mit Profibus DP-Protokoll ohne große Umbauten und unter Weiterverwendung der installierten HART Feldgeräte in die neue NOA Welt überführen lassen. Zu diesem Zweck hatte der Hersteller einen OPC UA Server in der CPU-Baugruppe des IS1+ Systems implementiert, der über den zweiten Kanal HART-Informationen angeschlossener Feldgeräte mit Edge Gateways oder Cloud-Systemen mittels PA-DIM austauscht.



Vorausschauende Diagnose: LEDs in der Gehäusefront zeigen proaktiv künftigen Wartungsbedarf gemäß Namur NE107 an.

## Ausblicke

Bis zum Praxiseinsatz dieser Lösung wird noch Zeit vergehen, da im ersten Release der PA-DIM bzw. in den OPC UA Companion Specifications weder das standardisierte, herstellerunabhängige Mapping der HART-Daten noch Remote I/O-Systeme berücksichtigt sind. Dennoch erweitert die OPC UA-Funktionalität in IS1+ bereits heute die vielfältigen Einsatzmöglichkeiten für die IP-Kommunikation im Feld. Im Umfeld unterschiedlicher Digitalisierungsprojekte wie NOA, Modulare Automation oder Open Process Automation (OPA), aber auch bei den Themen 'Ethernet in the Field' bzw. Ethernet-APL zeigt sich die wichtige Bedeutung der Remote-I/O-Technik. R. Stahl arbeitet mit und in diesen Arbeitsgruppen kontinuierlich an anwendungsorientierten Lösungen und Erweiterungen. ■



**André Fritsch, Senior Product Manager Remote I/O,**
**R. Stahl Schaltgeräte GmbH**
**www.stahl.de**

Bilder: R. Stahl Schaltgeräte GmbH

# Von A bis Z:
## Gefahren für die IT-Sicherheit im Home Office

*Immer noch arbeitet eine große Zahl der deutschen Angestellten von zuhause aus. Das Home Office wird dabei zunehmend zu einem Sicherheitsrisiko für die Unternehmens-IT. Rohde & Schwarz Cybersecurity hat einige zentrale Risiken im Home Office gesammelt – von A wie 'Arbeitsplatz' bis Z wie 'Zero-Day-Exploit' – und Lösungswege aufgeführt.*

### Arbeitsplatz

Im Home Office arbeiten Mitarbeiter an Küchen- und Esstischen, in Schlafräumen oder sogar in Kinderzimmern. Denn der Platz ist begrenzt und das WLAN-Signal nicht überall gleich stark. Ein solcher Arbeitsplatz bringt allerdings etliche Gefahren für die Unternehmens-IT mit sich – insbesondere

Bild: Rohde & Schwarz Cybersecurity GmbH

dann, wenn die ganze Familie zu Hause ist. Notebooks oder iPads können durch Kleinkinder beschädigt werden, ältere Kinder versuchen sich gerne aus Neugierde an den Geräten der Eltern, löschen womöglich wichtige Daten oder drucken sie versehentlich aus. Auf Küchen- und Esstischen abgestellte Getränke sind ebenfalls ein Risikofaktor – vor allem dann, wenn man sich den Tisch mit zwei Schulkindern teilt. Mitarbeiter müssen zu Hause daher besondere Vorkehrungen treffen. Ideal ist ein eigener – abschließbarer – Arbeitsraum. Mit einem WLAN-Verstärker lässt sich bei Bedarf das Verbindungssignal optimieren. Wer in der Küche oder im Wohnzimmer arbeitet, sollte zumindest beim Verlassen des Arbeitsplatzes, den Bildschirm sperren und das Notebook nach Feierabend in einen abschließbaren Schreibtisch oder Schrank einschließen.

## Bring your own device

Der Einsatz privater Endgeräte im Job war schon vor Corona ein Trend. Im Home Office heißt es jetzt in vielen Unternehmen 'Use your own device'. Doch wenn private Endgeräte genutzt werden, verlieren Unternehmen die Kontrolle über den Schutz ihrer Daten. Veraltete Rechner mit Update-Lücken und fehlenden Virenscannern bieten Hackern leichten Zugriff auf sensible Daten. Unternehmen müssen dafür sorgen, dass die Daten sicher sind und die EU-DSGVO nicht verletzt wird und ihre Mitarbeiter zu diversen Schutzmaßnahmen verpflichten.

## Cloud

Für das dezentrale Arbeiten von zu Hause sind Cloud-Anwendungen und Collaboration-Dienste sehr nützlich. Doch die Schutzmechanismen der Cloud-Anbieter entsprechen nicht den Sicherheitsanforderungen der meisten Unternehmen. Hinzu kommt: Die Mehrzahl der Cloud-Anbieter sitzt im Ausland. Viele dort geltende Regelungen – wie beispielsweise der 'Clarifying Lawful Overseas Use of Data Act' – sind nicht mit der EU-DSGVO vereinbar. Es drohen Datenspionage und Compliance-Verletzungen. Die Lösung ist ein datenzentrischer Schutz: Dabei werden Platzhalter in die Cloud eingestellt, die nur Metadaten enthalten. Die Nutzdaten werden fragmentiert im Unternehmensnetzwerk oder an einem anderen Ort abgelegt. Selbst bei einem Angriff auf die Cloud, bleiben die vertraulichen Inhalte für nicht befugte Personen unlesbar.

## Email-Anwendungen

Email-Anwendungen auf mobilen Endgeräten erleichtern die Arbeit von zu Hause ungemein. Allerdings gibt es immer wieder Sicherheitslücken, die es Hackern ermöglichen, solche Anwendungen zu knacken. Aktuell ist die Email-Anwendung von Apple betroffen. Die Angriffe verlaufen meist völlig unbemerkt. Unter dem Update iOS 13 kann die Schad-Email, ohne dass sie gelesen werden muss, den Schadcode auf das iPhone aufbringen. Haben Hacker das Gerät gekapert, kön-


Bild: Rohde & Schwarz Cybersecurity GmbH

Bilder der Doppelseite: Rohde & Schwarz Cybersecurity GmbH

nen sie diese Email wieder löschen und ihre Spuren verwischen.

## Festplatte

Vor allem Organisationen mit hohen Sicherheitsanforderungen sollten die Notebooks ihrer Mitarbeiter mit einer Festplattenverschlüsselung ausstatten. Nur berechtigte Nutzer können dann per Multi-Faktor-Authentifizierung ihre Daten und das Betriebssystem nutzen. Geht das Gerät verloren oder wird es gestohlen, ist es für Dritte nicht möglich, auf die Daten zuzugreifen.

## Hacker

Hacker nutzen die Corona-Krise aus. Mit einer Flut an Phishing-E-Mails, neu entwickelter Malware und gefälschten Informationen versuchen sie, aus der Krise Kapital zu schlagen. Für Unternehmen kann sich dadurch die bereits angespannte wirtschaftliche Lage weiter verschärfen. Ein umfassender Schutz der IT ist für jedes Unternehmen daher jetzt wichtiger denn je.

## Internet

Bereits vor der Corona-Krise galt: 70 Prozent der Hackerangriffe kommen aus dem Internet. Der aktuelle Informationsbedarf verschärft diese Gefahr noch weiter. Über gefälschte Webseiten, Emails oder Grafiken, die aus scheinbar vertrauensvollen Quellen stammen, wird Malware auf Rechner geschleust. Der beste Schutz vor Angriffen aus dem Internet ist ein virtueller Browser, wie der R&S-Browser in the Box. Kommt dieser zum Einsatz, haben Cyberkriminelle keine Chance.

## Mitarbeiter

Ein Sicherheitskonzept kann noch so ausgeklügelt sein: Als Schwachpunkt bleibt der Mensch. Mitarbeiter öffnen Phishing-Mails und laden gefährliche Anhänge herunter, sie verraten nichts ahnend ihre Zugangspasswörter an Unbefugte, die sich am Telefon als IT-Dienstleister ausgeben, und sie verbummeln wichtige Sicherheits-Updates. Im Home Office – wenn der IT-Administrator weit weg ist – ist die Verantwortung jedes Einzelnen besonders groß. Neben der richtigen IT-Sicherheitstechnik ist eine Schulung und Sensibilisierung der Mitarbeiter daher ausschlaggebend für die IT-Sicherheit im Unternehmen.

## Passwörter

Passwörter schützen Anwendungen vor unberechtigtem Zugriff. Doch Standardpasswörter sind einfach zu knacken. Und '1234' oder 'Password' bieten gar keinen Schutz vor Hackern. Gute Passwörter sind Passphrasen, wie 'Wir verschlüsseln Datenträger!' oder 'keine-Zellen-in-Excel-verbinden'. Solche Sätze sind leicht zu merken und zu tippen, aber schwierig zu knacken. Ergänzt werden sollten sie um Symbole, Zahlen oder Großbuchstaben. Um nicht den Überblick zu verlieren, ist es hilfreich, einen Passwort-Manager zu nutzen.

## USB-Stick

USB-Speichergeräte sind praktisch, wenn es um die Weitergabe von großen Datenmengen geht. Auch beim dezentralen Arbeiten im Home Office ist der USB-Stick beliebt. Häufig kommen allerdings Sticks zum Einsatz, deren Ursprung niemand mehr kennt. Auf diese Weise kann Malware auf die Firmenrechner gelangen. Mitarbeiter sollten daher grundsätzlich keine USB-Speichergeräte an Firmenrechner anschließen.

## Videokonferenzen

Videokonferenzen boomen in der Corona-Krise. Sie bieten Hackern allerdings häufig ein Einfallstor in die Unternehmens-IT. Beispiel Zoom: Der Zugang zu einer Zoom-Konferenz ist für Unbefugte relativ einfach. Eindringlinge können auf diese Weise nicht nur Zugriff auf sensible Informationen erhalten; über die Chatfunktionen können sie auch Links weiterleiten, um Malware auf die Geräte zu schleusen. Unternehmen sollten stattdessen auf Konferenzsysteme setzen, die über den Browser geöffnet werden. Angreifer lassen sich dann mit Hilfe eines virtuellen Browsers isolieren.

## WLAN

Eine WLAN-Verbindung erleichtert die Arbeit im Home Office ungemein. Sie ist allerdings auch ein Sicherheitsrisiko. Denn WLAN-Netzwerke bieten Hackern die Möglichkeit, auf Daten zuzugreifen. Hacker können zudem Computerviren und Trojaner über schlecht oder nicht gesicherte WLANs in ein System einspeisen. Wichtigste Sicherheitsmaßnahmen: Zum einen sollte das Standard-Administrator-Passwort durch ein neues, starkes Passwort ersetzt und zum anderen die WPA2-Verschlüsselung aktiviert werden.

## Zero-Day-Exploits

Ein wichtiger Schutz vor Hackerangriffen sind Patches und Updates. Diese stehen allerdings erst bereit, wenn die Sicherheitslücke bereits vom Hersteller erkannt wurde. Die größte Gefahr stellen daher Angriffe dar, die eine Sicherheitslücke ausnutzen, noch bevor sie entdeckt und geschlossen wurde. Einen solchen 'Zero-Day-Exploit' kann Antiviren-Software nicht aufhalten. Der einzige mögliche Schutz bietet eine Isolierung der eingeschleusten Malware in einem virtuellen Browser. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/40681

**Dr. Falk Herrmann, CEO, Rohde & Schwarz Cybersecurity GmbH**
**www.rohde-schwarz.com/-cybersecurity**

# Security

***Wer das wirtschaftliche Potenzial von Vernetzung, Analytics und den eigenen Daten auch in der Produktion nutzen will, benötigt eine robuste Security-Architektur mit entsprechenden Geräten aber auch Prozessen.***

Die gute Nachricht vorweg: Angriffe auf Unternehmen über deren Produktionssysteme oder Fernwartungszugänge liegen erst auf Platz 7 und 8 der häufigsten Angriffsvektoren, wie das BSI im aktuellen Lagebericht zur Sicherheit der IT in Deutschland berichtet. Immer noch am häufigsten sind (auf Platz 1) das Einschleusen von Schadsoftware über USB-Sticks o.ä., (auf Platz 2) Infektionen über das Internet sowie menschliches Fehlverhalten oder Sabotage (auf Platz 3). Unsere Marktübersicht zeigt 19 Security-Appliances, die für die Anwendung in der Fertigung entwickelt wurden. Weitere Infos gibt es auf www.i-need.de. Wen das Thema Security in der Industrie regelmäßig beschäftigt, für den gibt es übrigens jeden Monat neu unseren Industrial Security Report mit allem Wissenswerten aus der Branche. *(kbn)* ■

*Direkt zur Marktübersicht auf*
**i-need.de**
PRODUCT FINDER
***www.i-need.de/125***


| | | |
|---|---|---|
| Anbieter<br>Produkt-ID<br>Ort<br>Telefon<br>Internet | Ads-Tec Industrial IT GmbH<br>**15330**<br>Nürtingen<br>07022/ 2522-200<br>www.ads-tec.de | Ads-Tec Industrial IT GmbH<br>**34408**<br>Nürtingen<br>07022/ 2522-200<br>www.ads-tec.de |
| Produktname<br>Produkttyp | Industrial Router&Firewall IRF2000 Serie<br>VPN-Router mit Firewallfunktionen | Industrial Router&Firewall IRF1000 Serie<br>VPN-Router mit Firewallfunktionen |
| Einsatzgebiete | Fernwartung, dezentrale Absicherung von Produktionsanlagen | Fernwartung, dezentrale Absicherung von Produktionsanlagen |
| Firewall-Filterung: IP, MAC-Datenpaketen, VPN | ✓,✓,✓ | ✓,✓,✓ |
| DMZ-Port (Demilitarized Zone) | | |
| Bridge-Modus, Switch-Modus, Router-Modus | ✓,✓,✓ | ✓,✓,✓ |
| Network Address Translation (NAT) | ✓ | ✓ |
| DHCP-Server | ✓ | ✓ |
| Maximal unterstützte VPN-Tunnel<br>VPN-Tunnel Realisierung mit | unbegrenzt | unbegrenzt |
| Authentifzierung/ Benutzerverwaltung | ✓ | ✓ |
| Rechtemanagement | ✓ | ✓ |
| Anwendungskontrolle, Software-Freigabe | | |
| Virenscanner bzw. Content-Filter integriert | | |
| Schutz vor Spionage | ✓ | ✓ |
| Schutz vor Manipulation | ✓ | ✓ |
| Schutz DoS-Attacken und Cache Flooding | ✓ | ✓ |
| Eingesetzte Industrial-Ethernet-Protokolle prüfen | | |
| Ethernet-Schnittstellen | 2x, 6x Gigabit | 4x Gigabit |
| Gesicherte Ports | 1x USB | |
| Einzelne Ports ein-/ausschalten | ✓ | ✓ |




| | | | | | |
|---|---|---|---|---|---|
| Anbieter<br>Produkt-ID<br>Ort<br>Telefon<br>Internet | IPC2U GmbH<br>**29565**<br>Langenhagen<br>0511/ 807259-0<br>ipc2u.de | IPC2U GmbH<br>**29582**<br>Langenhagen<br>0511/ 807259-0<br>ipc2u.de | IPC2U GmbH<br>**29658**<br>Langenhagen<br>0511/ 807259-0<br>ipc2u.de | IPC2U GmbH<br>**29660**<br>Langenhagen<br>0511/ 807259-0<br>ipc2u.de | Rockwell Automation GmbH<br>**21472**<br>Düsseldorf<br>0211/ 41553-229<br>www.rockwellautomation.de |
| Produktname<br>Produkttyp | Ruggedcom-Crossbow<br>Secure Access Management Software | Ruggedcom-M969<br>Managed Ethernet Switch | Ruggedcom-M2200<br>MIL-STD Managed Ethernet Switch | Ruggedcom-MX5000RE | Stratix 5900<br>VPN-Gateway |
| Einsatzgebiete | Fernwartung, Schutz von einzelnen Automatisierungsgeräten, Schutz von vernetzten Robotern | dezentrale Absicherung von Produktionsanlagen, Schutz von einzelnen Automatisierungsgeräten, Schutz von vernetzten Robotern | Fernwartung, dezentrale Absicherung von Produktionsanlagen, Schutz von einzelnen Automatisierungsgeräten | Fernwartung, dezentrale Absicherung von Produktionsanlagen, Schutz von einzelnen Automatisierungsgeräten | Fernwartung, dezentrale Absicherung von Produktionsanlagen, Schutz von einzelnen Automatisierungsgeräten |
| Firewall-Filterung: IP, MAC-Datenpaketen, VPN | ✓,✓,✓ | ✓,✓,✓ | | | ✓, Nein, ✓ |
| DMZ-Port (Demilitarized Zone) | | | | | Nein |
| Bridge-Modus, Switch-Modus, Router-Modus | | | | | ✓,✓,✓ |
| Network Address Translation (NAT) | | | | | ✓ |
| DHCP-Server | | | | | ✓ |
| Maximal unterstützte VPN-Tunnel<br>VPN-Tunnel Realisierung mit | | | | | IPsec |
| Authentifzierung/ Benutzerverwaltung | | | | | ✓ |
| Rechtemanagement | | | | | Nein |
| Anwendungskontrolle, Software-Freigabe | | | | | ✓ |
| Virenscanner bzw. Content-Filter integriert | | | | | Nein |
| Schutz vor Spionage | | | | | Nein |
| Schutz vor Manipulation | | | | | ✓ |
| Schutz DoS-Attacken und Cache Flooding | | | | | ✓ |
| Eingesetzte Industrial-Ethernet-Protokolle prüfen | | | | | |
| Ethernet-Schnittstellen | | 8x 10/100Mbits | 9x Gigabit Ethernet, 9x 100Base-FX | 2x Gigabit Ethernet, 48x 100Base-FX | 100 Ethernet, Gigabit |
| Gesicherte Ports | | | | | |
| Einzelne Ports ein-/ausschalten | | | | | |

| | | | | | |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| Endian Srl<br>**35459**<br>Bolzano<br>+39 0471/ 631763<br>www.endian.com | Endian Srl<br>**35460**<br>Bolzano<br>+39 0471/ 631763<br>www.endian.com | Endian Srl<br>**35461**<br>39100 Bolzano<br>+39 0471/ 631763<br>www.endian.com | Genua GmbH<br>**15153**<br>Kirchheim<br>089/ 991950-169<br>www.genua.de | Helmholz GmbH & Co. KG<br>**29734**<br>Großenseebach<br>09135/ 7380-0<br>www.helmholz.de | IPC2U GmbH<br>**23324**<br>Langenhagen<br>0511/ 807259-0<br>www.rumoco.de |
| Endian 4i Edge X<br>Industrial IoT Security Gateways | Endian 4i Edge 515<br>Industrial IoT Security Gateways | Endian 4i Edge 112<br>Industrial IoT Security Gateways | Genubox<br>VPN-Gateway, Router, Security-Modul, Secure Application Platform | Wall IE<br>Industrial NAT Gateway / Firewall | RS401 Serial Device Server |
| Fernwartung, dezentrale Absicherung von Produktionsanlagen, Schutz von vernetzten Robotern, Schutz von einzelnenAutomatisierungsgeräten | Fernwartung, dezentrale Absicherung von Produktionsanlagen, Schutz von vernetzten Robotern, Schutz von einzelnenAutomatisierungsgeräten | Fernwartung, dezentrale Absicherung von Produktionsanlagen, Schutz von vernetzten Robotern, Schutz von einzelnenAutomatisierungsgeräten | Fernwartung, Absicherung, Segmentierung, Schutz Kritischer Infrastrukturen | dezentrale Absicherung von Produktionsanlagen, Schutz von einzelnen Automatisierungsgeräten, Integration von Maschinennetzen in das übergeordnete Produktionsnetz | Industrie, Kraftwerke oder Antriebssysteme |
| ✓,✓,✓ | ✓,✓,✓ | ✓,✓,✓ | ✓,✓,✓ | ✓,✓, Nein | ✓,✓, |
| ✓ | ✓ | ✓ | ✓ | Nein | |
| ✓, Nein, ✓ | ✓, Nein, ✓ | ✓, Nein, ✓ | ✓,✓,✓ | ✓,✓,✓ | ✓,✓,✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Nein | Nein | Nein | ✓ | ✓ | ✓ |
| 300.000<br>IPsec und/oder OpenVPN | IPsec und/oder OpenVPN | IPsec und/oder OpenVPN | unbegrenzt<br>IPSec, L2TP, SSH | | |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | Nein | ✓ | ✓ |
| Nein | Nein | Nein | ✓ | Nein | ✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | TCP, UDP, blockiert nicht konforme Übertragung | TCP, UDP | ✓ |
| | 5 | | 10/100/1.000 Ethernet, LWL | 1x WAN 10/100Mbit/s, 3x LAN 10/100Mbit/s usw | 4 verschlüsselte LAN Ports Kupfer o. Glasfaser |
| | | | 1x 10, 100Base-TX, TP-Kabel, RJ45-Buchse, Autocrossing, Autonegotiation, Autopolarity | RJ45-Buchse, Autonegotiation | 4 serielle Schnittstellen + Modbus-Unterstützung |
| Nein | Nein | Nein | ✓ | Nein | ✓ |

| | | | | | |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| Rockwell Automation GmbH<br>**21478**<br>Düsseldorf<br>0211/ 41553-229<br>www.rockwellautomation.de | Siemens AG<br>**15621**<br>Nürnberg<br>0911/ 895-0<br>www.siemens.de | Siemens AG<br>**35693**<br>Nürnberg<br>0911/ 895-0<br>www.siemens.de | Weidmüller GmbH & Co. KG<br>**15591**<br>Detmold<br>05231/ 1428-259<br>www.weidmueller.de | Weidmüller GmbH & Co. KG<br>**23947**<br>Detmold<br>05231/ 1428-259<br>www.weidmueller.de | Welotec GmbH<br>**21336**<br>Laer<br>02554/ 9130-00<br>www.welotec.com |
| 1756-EN2TSC - Ethernet/IP Secure Commun.<br>Security-Modul zum ControlLogix System | Scalance M876-4/M876-3/M874-3<br>Router, Mobilfunkrouter, Security-Modul, VPN-Gateway | Sinema Remote Connect<br>Fernwartungssoftware | IE-SR-2GT-LAN<br>Router, VPN Gateway | IE-SR-2GT-LAN-FN<br>Firewall/NAT-Router | LTE-Router TK800<br>LTE-Router mit VPN und Firewall |
| Fernwartung, Schutz von einzelnen Automatisierungsgeräten | Fernwartung, dezentrale Absicherung von Produktionsanlagen, Schutz von vernetzten Robotern | Fernwartung | dezentrale Absicherung von Produktionsanlagen, Fernwartung, Schutz von vernetzten Robotern, Schutz von einzelnen Automatisierungsgeräten | Netzwerktrennung, Network Adress Translation, dezentrale Absicherung von Produktionsanlagen, Schutz von vernetzten Robotern und einzelnen Automatisierungsgeräten | Fernwartung, Smart Grid |
| Nein, Nein, Nein | ✓, Nein, ✓ | ✓, , ✓ | ✓,✓,✓ | ✓,✓, Nein | ✓,✓,✓ |
| Nein | ✓ | ✓ | Nein | Nein | ✓ |
| ✓, Nein, Nein | Nein, ✓, ✓ | , ✓, ✓ | ✓, Nein, ✓ | ✓, Nein, ✓ | ✓,✓,✓ |
| Nein | ✓ | ✓ | ✓ | ✓ | ✓ |
| Nein | ✓ | | ✓ | ✓ | ✓ |
| unterstützt bis zu 8 VPN Tunnel gleichzeitig<br>IPsec | 20<br>Open VPN IPsec | 1.024<br>Open VPN IPsec | unbegrenzt<br>IPsec und openVPN (auswählbar) | | 10<br>DM VPN, GRE, OpenVPN, IPsec |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | Nein | Nein | Nein |
| Nein | Nein | | Nein | | Nein |
| | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ✓ | | ✓ | ✓ | ✓ |
| | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ethernet/IP, blockiert nicht konforme Übertragung | | | ✓, über entsprechende Firewallregeln auf Layer 2 und 3 | ✓, über entsprechende Firewallregeln auf Layer 2 und 3 | |
| 10/100 Ethernet | 10/100 Ethernet | | 2x 10/100/1.000 BaseT(x) | 10/100/1.000 BaseT(x) | 2, Gigabit |
| | SMA-Antennenbuchse (50Ohm) | | | | |
| Nein | ✓ | | ✓ | ✓ | ✓ |

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 08.09.2020

- Anzeigen -

# IoT- und Edge-Gateways

***Das Internet der Dinge ist der effiziente und einfache Weg, um die Daten von verteilten Anwendungen transparent zusammenzuführen und zu analysieren. IoT- und Edge-Gateways schaffen den sicheren Durchgriff aus der Anwendung in die Cloud.***

Ein durchgängiges Sicherheitskonzept ist eine zentrale Anforderung an IoT-und Edge-Gateways. Zudem hilft ein breites Angebot an Schnittstellen dabei, zahlreiche unterschiedliche Geräte mit einem Gateway zu integrieren. Sowohl Northbound, also in das Internet der Dinge als auch Southbound in die Anwendung gibt es viele unterschiedliche Anforderungen. Skalierbare und anpassbare, modulare Lösungen machen einem das Leben hier deutlich einfacher. Praktisch auch, wenn für die gesamte Gerätefamilie die gleiche Software zum Einsatz kommt. Denn Zeit sparen ist doch immer gut... *(kbn)* ■



# Impressum


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

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

Internet: www.industrial-communication-journal.net

**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:**
Tamara Gerlach, Lena Krieger, Lukas Liebig, Kristine Meier, Melanie Novak, Florian Streitenberger, Natalie Weigel, Sabrina Werking

**ANZEIGEN:**
Heiko Hartmann, Daniel Katzer, Markus Lehnert, Thomas Möller

**ANZEIGENDISPOSITION:**
Christina Jilg
Tel. 06421/3086-0
Es gilt die Preisliste der Mediadaten 2020.

**GRAFIK & SATZ:**
Julia Marie Dietrich, Tobias Götze, Kathrin Hoß, Torben Klein, Patrick Kraicker, Ann-Christin Lölkes, Thies-Bennet Naujoks, 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

Hinweise: Applikationsberichte, Praxisbeispiele, Schaltungen, Listings und Manuskripte werden von der Redaktion gerne angenommen. Sämtliche Veröffentlichungen im Industrial Communication Journal erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Alle im Industrial Communication Journal erschienenen Beiträge sind urheberrechtlich geschützt. Reproduktionen, gleich welcher Art, sind nur mit schriftlicher Genehmigung des TeDo Verlages erlaubt. Für unverlangt eingesandte Manuskripte u.ä. übernehmen wir keine Haftung. Namentlich nicht gekennzeichnete Beiträge sind Veröffentlichungen der Redaktion. Haftungsausschluss: Für die Richtigkeit und Brauchbarkeit der veröffentlichten Beiträge übernimmt der Verlag keine Haftung.

Bild: ©zorandim75 / stock.adobe.com

# MEDIABERATER GESUCHT

## M/W/D

**Sie sind offen und stehen gern mit anderen Menschen in Kontakt, haben Freude am Verkauf und verfügen idealerweise über eine kaufmännische Ausbildung?**

**Dann kann das Berufsbild Mediaberatung das Richtige für Sie sein.**

### ARBEITEN IM TEDO VERLAG

Der TeDo Verlag ist ein mittelständischer Betrieb in der Marburger Region, der sich auf das Verlegen von Fachmedien für Industrie, Handwerk und Gewerbe spezialisiert hat. Wir bieten ein hochprofessionelles Umfeld, gute Entwicklungsmöglichkeiten und Mitarbeit in einem überaus erfolgreichen Team in angenehmer Arbeitsatmosphäre.

Wir suchen motivierte, kommunikative und belastungsfähige Mitarbeiter, die Spaß an der Arbeit im Team und an der Konzeption und Mitgestaltung umfangreicher Projekte haben.

### AUFGABEN UND INHALTE

- Anzeigenverkauf im B2B-Bereich (telefonisch & digital)
- Konzeption und Ausarbeitung von crossmedialen Werbekampagnen über die Plattformen Online, Print Socialmedia, Videos, Webinare etc.
- Pflege bestehender Kundenbeziehungen vor Ort und auf Messen
- Abwicklung von Angeboten und Aufträgen
- enge Zusammenarbeit mit den anderen Mitgliedern des Marketing-Teams, Redaktion und Layout
- Homeoffice in Teilzeit möglich

### IHR PROFIL

- abgeschlossene Berufsausbildung
- idealerweise erste Erfahrungen im Vertrieb und Telefonverkauf
- Souveränität und sicheres Auftreten
- Teamplayer mit sehr guter strukturierter Arbeitsweise
- Sie sind kunden- und serviceorientiert
- Sie verfügen über gute MS-Office-Kenntnisse

Senden Sie uns Ihre Bewerbung per Post oder E-Mail – oder verwenden Sie einfach unser Online-Bewerbungsformular.

TeDo VERLAG

TeDo Verlag GmbH
Manuela Weigand / Personal
Zu den Sandbeeten 2
35043 Marburg
bewerbung@tedo-verlag.de


# NAHTLOSER DATENFLUSS ÜBER NETZWERKGRENZEN HINWEG

## mit dem PN/EtherNetIP Coupler von Helmholz

Der PN/EtherNetIP Coupler ermöglicht den Datenaustausch zwischen PROFINET-Controller und EtherNet/IP-SPS. Sie möchten PROFINET und EtherNet/IP einfach und unkompliziert verbinden? Testen Sie den PN/EtherNetIP Coupler unter realen Bedingungen in Ihrer Applikation.

- Simple Konfiguration sowie übersichtliches Monitoring
- Hohe Sicherheit durch galvanische Trennung
- Platzersparnis im Schaltschrank aufgrund kompakter Bauform
- MQTT-Publisher auf beiden Netzwerkseiten

www.helmholz.de

Helmholz®
COMPATIBLE WITH YOU