

INDUSTRIAL  
COMMUNICATION  
JOURNAL



ETHERNET



WIRELESS



SECURITY



Profinet und OPC UA

# Industrielle Kommunikation schaltet mit TSN den Turbo zu

Seite 6

**SIEMENS**

Bild: Siemens AG



## TSN IN DER PRODUKTION

Einstieg ins Time  
Sensitive Networking

Seite 12

## MARKTSPIEGEL KABEL UND LEITUNGEN

Überblick derzeitiger  
Lösungen am Markt

Seite 24



## SCHWER- PUNKT

Trends Industrial  
Security

Seite 26







Kai Binder, Chefredakteur

**Einen wesentlichen Schwerpunkt dieser Ausgabe stellt das Thema Security dar und zwar Security aus Sicht der Betreiber oder Hersteller von Maschinen und Anlagen. Wer sich einen Überblick über die aktuelle Bedrohungslage verschaffen will, der findet zahlreiche aktuelle Informationen in unserem Schwerpunkt Industrial Security ab S. 26.**

## Hacken wird einfacher

Die Anfänge der Stuxnet-Entwicklungen gehen vermutlich auf das Jahr 2005 zurück, die ersten bekannten Infektionen stammen aus dem November 2007. Trotzdem werden noch heute – also mehr als zehn Jahre später – alle Angriffe auf Industriesteuerungen mit Stuxnet verglichen. Dabei haben sich die Angriffsvektoren heute weiter diversifiziert und vereinfacht. Neben Ransomware sind industrielle Rechnersysteme zunehmend auch durch sogenannte Krypto-Malware bedroht. Durch die hohen Kurse für Kryptowährungen wie Bitcoin entwickeln offensichtlich viele Malware-Autoren Krypto-Miner, mit denen sie viel Geld verdienen. Davon sind laut Microsoft und Kaspersky auch industrielle Steuerungssysteme betroffen. Der Aufwand, ein Steuerungssystem zu hacken, ist heute (verglichen mit Stuxnet :-)) längst nicht mehr so groß wie damals und steht nicht nur Insidern offen. Doch zunehmend bevorzugen Hacker einfache Angriffsmöglichkeiten wie Phishing. Nur drei Prozent der Cyber-Angriffe erfolgen heute über das Umgehen von Sicherheitsmechanismen!

Obwohl die Aufmerksamkeit für das Thema Security auch im industriellen Sektor mittlerweile sehr hoch ist, bekommen Produktionsunternehmen immer noch keine guten Zeugnisse ausgestellt, wenn

es um die Abwehr von Cyberangriffen geht. Doch woran liegt dies? Zunächst einmal ist Cybersicherheit – verglichen mit Brandschutz oder Zutrittsschutz – ein relativ neues Feld, das noch dazu ein erhebliches Maß an technischem Know-how erfordert und das ist besonders in diesem Bereich rar. Und um in dem Beispiel zu bleiben: Auch wenn jeder einen Feuerlöscher bedienen kann, so kann noch lange nicht jeder einen Cyberangriff eindämmen. Tatsächlich ist es noch schlimmer: Jeder kann einen Brand leicht erkennen, einen Cyberangriff dagegen erkennt man auch dann häufig nicht, wenn man hinschaut.

Doch ist der Kampf dann schon verloren? Im Gegenteil: Immer deutlicher wird, dass wir uns intensiv dem Thema widmen müssen. Vieles kann man schon mit einfachen Maßnahmen erreichen. Wer diese nicht ergreift, handelt heute sträflich fahrlässig: Mehr als 30 Prozent aller erfolgreichen Cyberangriffe sind heute zufälliger Beifang!

In diesem Sinne wünsche ich Ihnen viel Spaß bei der Lektüre.



Kai Binder  
kbinder@sps-magazin.de



### ■ RJ45 + M12

**Angelegene Steckverbinder & umfangreiches Sortiment an Industrial Ethernet-Leitungen**

- Umspritzter RJ45-Stecker: Kat.5 und 6<sub>A</sub>, Abgang 180°, 90°
- Umspritzter M12-Stecker + Buchse: Kat. 5/D-kodiert und 6<sub>A</sub>/X-kodiert, Abgang 180°, 90°
- Umfangreiche Kabel-Stecker-Kombinationen möglich
- UL-/CSA-approbiert
- Für Schaltschrank / Maschine / Feld

**Entwerfen Sie Ihr eigenes Produkt!**

**HELUKABEL® GmbH**  
Daten-, Netzwerk- & Bustechnik  
71282 Hemmingen, Germany  
Tel.: +49 7150 9209-181  
juergen.berger@helukabel.de

[helukabel.com](http://helukabel.com)

# Was bringt Künstliche Intelligenz für Industrie 4.0?

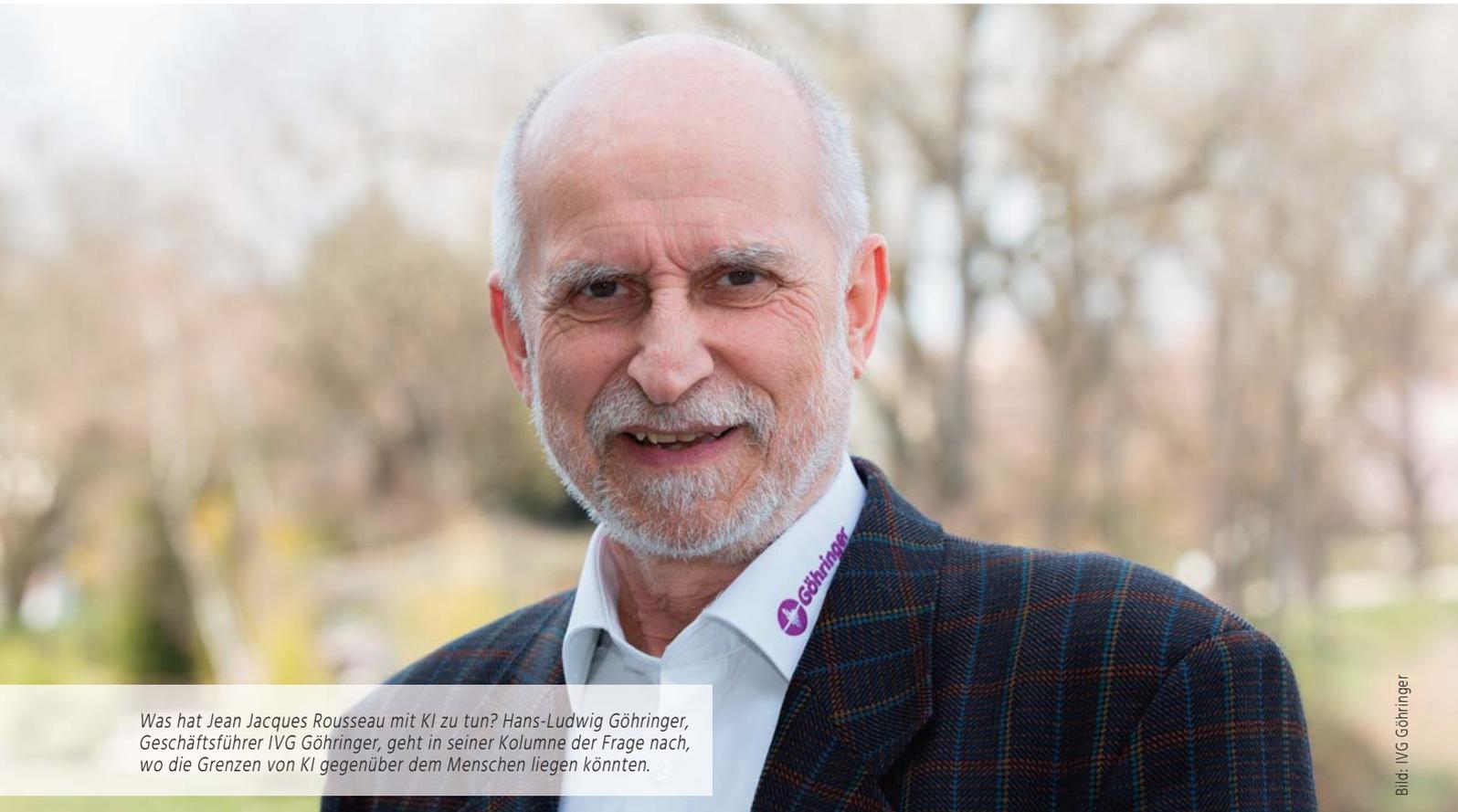


Bild: IVG Göhringer

Was hat Jean Jacques Rousseau mit KI zu tun? Hans-Ludwig Göhringer, Geschäftsführer IVG Göhringer, geht in seiner Kolumne der Frage nach, wo die Grenzen von KI gegenüber dem Menschen liegen könnten.

**Das Thema KI (Künstliche Intelligenz) ist im Prinzip so alt wie die Computertechnik selbst. In der Forschung gab es, zumindest in der Theorie, erste Erfolge. Doch beim Versuch der praktischen Umsetzung stellte sich schnell heraus, dass die Hardware nicht leistungsfähig genug war. Entsprechend verlor die KI-Forschung an Bedeutung.**

**F**ast 50 Jahre galt, ab 1965 gerechnet, das Mooresche Gesetz. Das besagte eine Verdoppelung der Transistoren je Flächeneinheit alle zwei Jahre. Unabhängig davon, dass sich die Halbleiterindustrie zwischenzeitlich den physikalischen Grenzen nähert, haben wir heute eine Technologie mit enormer Leistungsfähigkeit. Die KI-Forschung ist längst wieder im Gange und mit künstlichen neuronalen Netzen gab es auch Fortschritte. Gesichter werden erkannt, Strategiespiele wie Schach oder Go werden von Rechnern gewonnen. Ganz aktuell ist das Thema Sprachsteuerung, das sich gerade enorm verbreitet. Allerdings scheint es, dass die Technik dort aufhört, wo der gesunde Menschenverstand anfängt. Da sehe ich auch die Grenzen von KI. Seit dem 17. Jahrhundert streiten wir Menschen über die richtige Methode des Lernens. Schaut man unsere heutige Ausbildung an, so ist das ein typischer Konditionierungsvorgang – wie bei neuronalen Netzen. So wie man einen 100m Läufer trainiert, damit er immer besser

wird. Ich denke, für schnelles Lernen ist das ok. Aber wir sollten auch das andere Lernen nicht vergessen, wie es durch Jean Jacques Rousseau im 17ten und modifiziert durch Maria Montessori im 18ten Jahrhundert beschrieben wurde – dass wir zum Lernen alle Sinne benutzen. Jean Jacques Rousseau beschreibt, wie ein Kind lernt, sich in einem stockdunklen Haus sicher zu bewegen. Im übertragenen Sinne spielen plötzlich andere Sensoren eine Rolle. Hat man an diese bei BigData und Cloud nicht gedacht, lässt sich der Fehler in der Maschine nicht diagnostizieren. Allein die richtige Auswahl und Platzierung der Sensoren entscheidet über den Lernerfolg. Damit ist klar, dass KI heute das Lernen als Konditionierungsvorgang übernehmen kann – jedoch nur, wenn alle notwendigen Daten vor Ort vollständig erfasst werden. ■

IVG Göhringer  
www.i-v-g.de

## TITELSTORY

**Profinet und OPC UA: Industrielle Kommunikation schaltet mit TSN den Turbo zu**

Die Digitalisierung der Produktion stellt auch die industrielle Kommunikation vor neue Anforderungen wie höhere Bandbreiten, größere Robustheit und garantierten Quality of Service (QoS). Immer häufiger erfordern komplexe Prozesse Echtzeitfähigkeit auch über die Maschine hinaus. Siemens setzt dabei weiter auf Industrial Ethernet als zukunftssicheren Netzwerkstandard, der gleich zwei etablierte Protokolle in einem Netzwerk kombiniert: Während OPC UA seine Vorteile auf der Daten- und Managementebene ausspielen kann, punktet Profinet mit seiner Deterministik, 'harten' Echtzeitfähigkeit und standardisierten Profilen vor allem auf der Steuerung- und Feldebene. Mit Time-Sensitive Networking – TSN – werden beide Protokolle zudem künftig den 'Turbo' zuschalten können.



Titelanzeige: Siemens AG



6

Bild: Siemens AG

**Markt-Trends-Technik**

- 4 Kolumne: Was bringt Künstliche Intelligenz für Industrie 4.0?
- 10 Aktuelles aus der Branche

**TSN-Faktencheck**

- 12 Einstieg ins Time Sensitive Networking leicht gemacht
- 13 Neuheiten und Produktvorstellungen

**Wireless und Remote**

- 15 Vernetzte Clouds im Produktionsumfeld
- 16 Mehr als 20Mio. Profinet-Geräte im Markt
- 18 Messdaten mit 5G kabellos in Echtzeit übertragen
- 20 Remote-Lösung für Neuanlagen und Retrofit

**Komponenten und Lösungen**

- 24 Marktübersicht: Kabel und Leitungen
- 36 CC-Link in der Anwendung
- 38 Lichtwellenleiter auch für die härtesten Umgebungen
- 41 Produktübersicht: Ethercat-Komponenten

**Sicherheit****Schwerpunkt Trends Industrial Security**

- 26 Cyberangriffe gegen Industrierechner
- 28 Hacker bevorzugen einfache Angriffsmöglichkeiten wie Phishing
- 29 Produktionsrechner und -anlagen sind Sicherheitsrisiko
- 30 Neue Umfrage zeigt den Stand aktueller Cybersicherheit
- 31 Industrieanlagenschutz mit Firewalls
- 32 Ransomware bedroht zunehmend industrielles Steuerungssystem
- 34 Wie können Industrieunternehmen ihre IT-Angriffsfläche verringern?
- 35 Produktübersicht: IT- und Netzwerksicherheit

**Service**

- 3 Editorial
- 42 Vorschau, Inserenten, Impressum

**Warum 5G die Welt der Industrie 4.0 verändert**

Bild: ZVEI e.V.

Den neuen Mobilfunkstandard industriegerecht mitgestalten, darum geht es bei der 5G-Acía-Initiative, die der ZVEI auf der Hannover Messe vorgestellt hat. **Seite 11**

**Mehr als eine Cloud managen**

Bild: SmartFactory-KL/A. Sell

Wie Daten in der Cloud ausgewertet werden können, wenn verschiedene Cloudlösungen innerhalb einer Produktionsanlage eingesetzt werden. **Seite 15**

**Fernwirken und Fernwarten**

Bild: Heimholz GmbH & Co. KG

Durchgängige Remote-Lösung für Neuanlagen und Retrofit **Seite 20**



Bild: Siemens AG

Profinet und OPC UA:

# Industrielle Kommunikation schaltet mit TSN den Turbo zu

***Auch auf der Hannover Messe 2018 war die industrielle Kommunikation als Schlüssel zum digitalen Unternehmen ein Besuchermagnet – verbunden mit der Frage: Wohin geht die Reise? Die Anforderungen an Transparenz, nahtlose Vernetzung und Durchgängigkeit sind die Grundlage moderner Kommunikationskonzepte. Gleichzeitig verlangt die Digitalisierung aber auch weiter steigende Reaktionsschnelligkeit und Flexibilität: Möchten Unternehmen flexibel auf die Anfragen aus dem Markt eingehen und somit die individuelle Massenproduktion umsetzen, so muss die Produktion hochgradig agil sein. Was ist der Preis dafür? Ein radikaler Umbau der Kommunikationslandschaft?***

**G**anz im Gegenteil, so die Überzeugung von Stephan Schott, Marketing Manager bei der Siemens AG „Industrial Ethernet ist und bleibt das zukunftssichere Netzwerk, auf das unsere Kunden auch weiterhin bauen können. Erstens bietet es langfristige Planungs- und Investitionssicherheit. Zweitens kombiniert es mit Profinet und OPC UA zwei führende

Standards in einem Netzwerk, die jeweils ihre spezifischen Stärken ausspielen können – und nahtlos miteinander harmonieren. Und drittens profitieren Anwender von der Offenheit für neue Entwicklungen, die den notwendigen Technologieschub für die weitere Digitalisierung bringen. Aktuell betrifft dies vor allem Time-Sensitive Networking (TSN), das durch die Vereinigung



TSN – der Turbo für Profinet und OPC UA

mehrerer existierender Standards das Ethernet weiterentwickelt. Sowohl Profinet als auch OPC UA werden diese wichtige Basistechnologie in den kommenden Jahren als 'Turbo' zuschalten können. Was charakterisiert also Industrial Ethernet-Netzwerke mit Profinet (sogenannte Profinet-Netzwerke) heute, und welche zusätzlichen Eigenschaften werden sie mit TSN gewinnen?

### Zwei, die miteinander können – Profinet und OPC UA

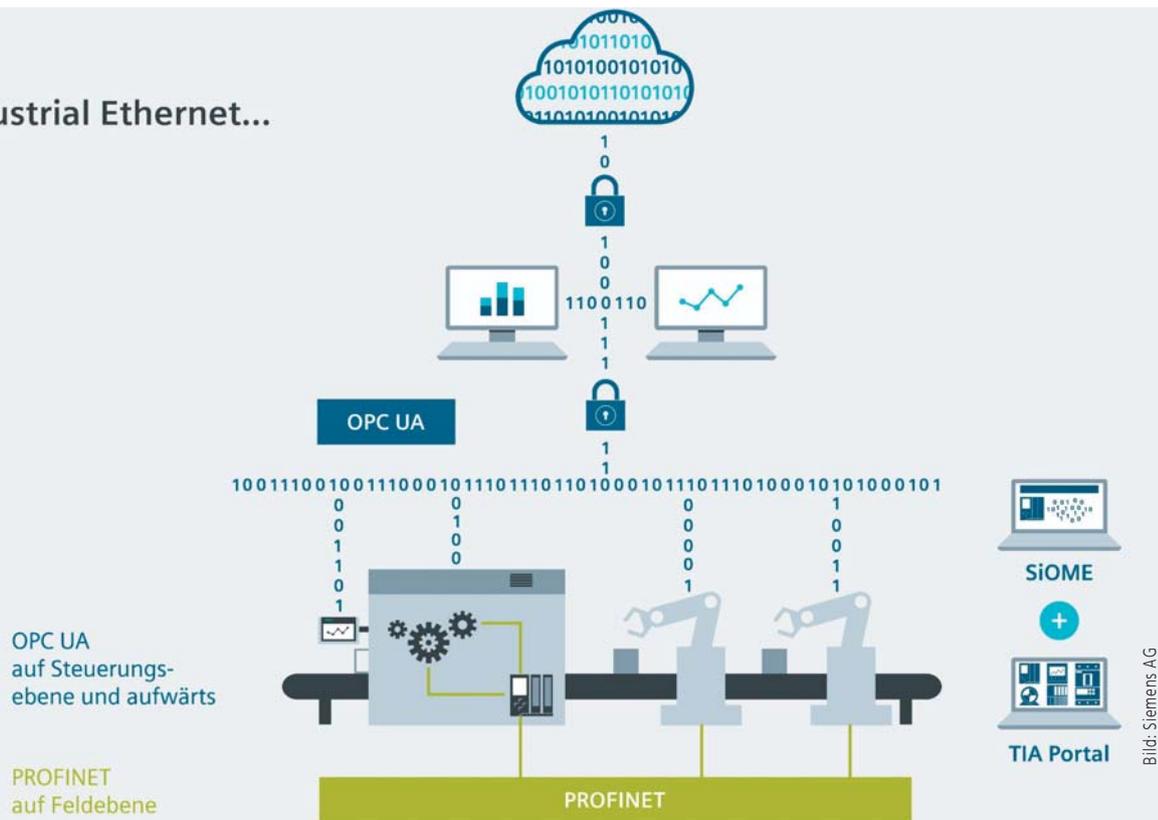
Profinet ist mit einer installierten Basis von mehr als 20 Millionen Knoten (Stand 2017) das am weitesten verbreitete Netzwerk im Shopfloor. Stephan Schott fasst die wesentlichen Fähigkeiten zusammen: „Dank harter Echtzeit und Deterministik bietet Profinet die benötigte Performanz für alle Applikationen in der Feldebene. Darüber hinaus stellt es ausreichend Bandbreite sogar für Videos oder HD-Bilder, die beispielsweise für die Produkthaftung und

Qualitätssicherung wichtige Medien sind sicher. Anwender können praktisch jede Art von Netzwerktopologie realisieren, ob kabelgebunden oder kabellos. Und nicht zuletzt setzen viele Industrieunternehmen auf standardisierte Profile wie Profisafe, Profienergy und Profidrive: Sicherheitsgerichtete Anwendungen, Energietransparenz und -effizienz sowie standardisierte Kommunikation in der Antriebstechnik – all das läuft über ein Kabel. Ab der Steuerungsebene übernimmt dann in vielen Industrial Ethernet-Netzwerken ein weiterer Standard die Kommunikation: OPC UA – nach dem Motto „Jeder dort, wo er am stärksten ist“. OPC UA hat sich in der vertikalen Kommunikation etabliert und ist mittlerweile häufig auch in der Maschine-zu-Maschine-Kommunikation anzutreffen. Dazu trägt maßgeblich bei, dass es auf allen Ebenen eine sichere, einfache und herstellerübergreifende Geräteanbindung erlaubt – bei höchsten Security-Standards. Das zugrundeliegende Informationsmodell sowie international standardisierte Schnittstellen (Companion Specifications) bilden die Grundlage für den einfachen Datenaustausch und Vorteile bei der Integration in Automatisierungsnetzwerke. Für Siemens ergibt die Aufgabenteilung zwischen den beiden Standards Sinn: „Profinet und OPC UA laufen nicht nur über eine und dieselbe Standard Ethernet-Leitung. Beide sind auch vollständig in unserem Totally Integrated Automation (TIA)-Portfolio integriert. Das TIA Portal hält dabei eine wichtige Neuerung parat: Zusammen mit dem Siemens OPC UA Modeling Editor – kurz SiOME – machen wir es unseren Anwendern leicht, die Daten aus dem TIA Portal Variablenhaushalt auf Companion Specifications abzubilden“, erläutert Stephan Schott. Solche Spezifikationen haben hohe Bedeutung für die weitere Standardisierung. Beispiel Verpackungsmaschinen: Hier sichert eine Companion Specification allen Maschinen, die den 'PackML'-Standard erfüllen, eine identische Schnittstelle für die Kommunikation nach außen – egal von welchem Hersteller sie gebaut wurden. 'Mission accomplished' also mit Profinet und OPC UA? Angesichts der rasanten Entwicklungen von Digitalisierung und der Anforderungen an das Internet der Dinge (IoT) steigt die Notwendigkeit höherer Bandbreiten, größerer Robustheit und einem garantierten Quality of Service (QoS). Komplexe Prozesse mit Echtzeitanforderungen werden auch außerhalb der Maschine neue Herausforderungen an die Kommunikation schaffen.

### Profinet bleibt Maß der Dinge

Bei der Lösung dieser Zukunftsaufgaben fällt die Offenheit von Profinet-Netzwerken als entscheidender Vorteil ins Gewicht. „Wir werden unsere heutige Strategie eines leistungsstarken Profinet-Netzwerkes mit TSN weiterführen“, bezieht Stephan Schott in dieser Frage auch klar Stellung. TSN – Time-Sensitive Networking – ist durch Weiterentwicklung des Ethernet-Standards in der IEEE802.1 entstanden. Es wertet die bestehenden Ethernet-Mechanismen um die Qualitäten auf, die künftig gefragt sein werden: erweiterte Quality of Service (QoS) Mechanismen, Zeitsynchronisation, geringe Übertragungslatenz und stoßfreie Redundanz. Nicht zuletzt basiert TSN auf geschützten Streams, die es ermöglichen, mehrere echtzeitfähige Protokolle wie Profinet und OPC UA PubSub parallel in einem Netzwerk zu betreiben – die Verwirklichung der geforderten Netzwerk-Konvergenz im Standard, die von Profinet heute schon im Feld bekannt ist. Welchen Technologie-Push dies ermöglichen wird, hat

## Industrial Ethernet...



Industrial Ethernet: ein gemeinsames Netzwerk für OPC UA und Profinet

...ein Netzwerk für alles!

Siemens auf der Hannover Messe 2018 schon angedeutet – mit einem erstmals vorgestellten Modell zur M2M-Kommunikation, basierend auf OPC UA PubSub mit TSN. Wie im wirklichen Leben, war dabei eine Simatic S7-1500 Station über einen Kommunikationsprozessor an ein TSN-Netzwerk angebunden, das vollständig mit Netzwerkkomponenten aus der Scalance-Familie aufgebaut war. Wie es sich für zwei exzellent harmonisierende Spieler gehört, wird aber nicht nur OPC UA von TSN profitieren: Die Profibus & Profinet International (PI) arbeitet derzeit an der Spezifizierung von Profinet auf TSN. So soll es möglich werden, Profinet mittelfristig ebenfalls auf die TSN-Mechanismen abzubilden und dessen Vorteile auch in der Feldebene nutzbar zu machen. Neben einer höheren Bandbreite für den immer stärker werdenden Traffic bieten vor allem die bei TSN entstehenden Standard Bausteine den Geräteherstellern künftig vielfältige Realisierungsmöglichkeiten für die Profinet Feldebusschnittstelle. Dass mit all dem erst der Anfang einer vielversprechenden Entwicklung gemacht ist, liegt auf der Hand. Auch deshalb beteiligt sich Siemens aktiv an der weiteren Erprobung von TSN im Testbed des Labs Network Industrie 4.0. Unter LNI4.0 werden Testumgebungen und -installationen in Deutschland für Industrie 4.0 miteinander vernetzt. Siemens gehört zu den Gründungsmitgliedern von LNI 4.0. Gemeinsam mit verschiedensten Industrieunternehmen setzt Siemens hier nun alles daran, um die Interoperabilität auf TSN-Basis zwischen verschiedenen Herstellern zu testen und im Testbed das Potenzial von TSN für die M2M-Kommunikation und die Vernetzung von Maschinen bis hin zur Cloud zu erforschen.

### Investitionssicherheit und Dynamik auf einem Kabel

Als Fazit lässt sich festhalten, dass Siemens in der industriellen Kommunikation vor allem auf eins setzt – Kontinuität. „Während OPC UA seine Vorteile auf der M2M-, Daten- und Managementebene ausspielen kann, bietet Profinet mit seiner Deterministik, ‚harten‘ Echtzeitfähigkeit und seinen standardisierten Profilen vor allem Stärken auf der Feldebene. Die Kombination aus beidem und die durchgängige Vernetzung werden auch in Zukunft mit TSN der Maßstab in der Automatisierung sein“, betont Stephan Schott. Für Anwender ist dies zweifellos eine gute Nachricht. Dahinter steht die Tatsache, dass Siemens auf beide Standards setzt, beide komplementär miteinander im uneingeschränkten Parallelbetrieb anbietet und sich als Gründungsmitglied in beiden Organisationen - der PI und der OPC Foundation - einsetzt. Gemeinsam mit Siemens engagieren sich mehrere Dutzend namhafter globaler Unternehmen für die Weiterentwicklung des Ethernet-Standards. Die Aussichten, mit Profinet und OPC UA auf Basis von TSN nachhaltigen Investitionsschutz und hohe Dynamik in der Welt der Digitalisierung zu verbinden, stehen also sehr gut. ■

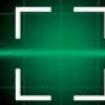
**Autor:** **Stephan Schott,**  
Marketing Manager in der Division Digital Factory  
Siemens AG  
[www.siemens.de/tsn](http://www.siemens.de/tsn), [www.siemens.com/tsn](http://www.siemens.com/tsn)

Direkt zur Marktübersicht [i-need.de](http://i-need.de)

[www.i-need.de/?f9595](http://www.i-need.de/?f9595)

# Highend-Messtechnik

Äußerst präzise, schnell und robust.



< 1  $\mu$ s zeitsynchron  
100 ppm  
24 Bit  
bis 50.000 Samples/s

## [www.beckhoff.de/messtechnik](http://www.beckhoff.de/messtechnik)

Mit den EtherCAT-Messtechnikmodulen der Serie ELM wird die hochpräzise, schnelle und robuste Messtechnik integraler Bestandteil der PC-basierten Steuerung von Beckhoff. Direkt integrierbar in das modulare EtherCAT-Klemmensystem lassen sich die ELM-Module mit dem umfassenden Portfolio von über 500 EtherCAT-Klemmen kombinieren.

- schnell: Abtastraten bis zu 50.000 Samples/s
- zeitpräzise: exakte Synchronisierung < 1  $\mu$ s
- wertpräzise: Messgenauigkeit von 100 ppm
- proaktiv: integrierte Anschluss- und Funktionsdiagnose in den einzelnen Modulen
- flexibles Stecker-Frontend: LEMO, BNC, Push-in
- Eingangsbeschaltungen: Spannung 20 mV ... 60 V, Strom 20 mA, IEPE, DMS, RTD/TC

 **automatica**

Halle B6, Stand 320



Durchgängige Messkette: von der Datenerfassung bis zur Analyse in der Cloud.

New Automation Technology

**BECKHOFF**

## TÜV Nord prüft und zertifiziert nach IEC62443-2-4

TÜV Nord prüft und zertifiziert künftig nach IEC62443-2-4. Die Norm IEC62443 (Industrial Communication Networks – Networks and System Security) hat sich als international anerkannter Standard zum Konformitätsnachweis im Umfeld von Industrial Security der Prozess- und Automatisierungsindustrie etabliert. Die voranschreitende Digitalisierung und die Interaktion von Produkten und Systemen führen aber auch hier dazu, dass neben klassischen Konformitätsbewertungen in Safety, Performance und Energieeffizienz das Thema Cyber Security in den Vordergrund rückt. Mit Hilfe der Normenreihe IEC62443 lässt sich nachweisen, dass Betreiber, Integratoren und Hersteller zeitgemäße Cyber-Security-Standards für industrielle Automa-

tisierungssysteme nutzen. „TÜV Nord hat die Erarbeitung und Umsetzung des IEC-Regelwerks von Beginn an mit vorangetrieben. Umso mehr freuen wir uns, dass wir weltweit unter den ersten drei Prüforganisationen sind, die diese Zertifizierung im IEC62443-Schema anbieten dürfen“, sagte Sandra Gerhartz, Geschäftsführerin TÜV Nord CERT. Die Anerkennung ist nur für IEC62443-akzeptierte Prüforganisationen möglich. Mit der IEC62443-2-4 hat das Unternehmen seinen IEC62443-Scope erweitert.

TÜV Nord AG  
[www.tuev-nord.de](http://www.tuev-nord.de)

## Huawei und Telefónica Deutschland starten NB-IoT-Projekt

Im Rahmen der Hannover Messe haben Huawei, Telefónica Deutschland und der IoT-Anbieter Q-loud gemeinsam ein auf NarrowBand-Internet of Things (NB-IoT) basierendes Smart-Metering-Pilotprojekt für den Flughafen in München gestartet. Unzureichende Funksignale in Gebäuden und Untergeschossen schränken die Anwendung von Sensoren in vielen Einsatzgebieten am Flughafen ein. Daher ist eine Alternative zur analogen und manuellen Ablesung von Zählerwerten von Strom, Wasser und Gas erforderlich. Mit der testweisen Implementierung von NB-IoT eröffnen sich perspektivisch ganz neue Einsatzfelder von Sensoren am Flughafen München. Dieser hat gemeinsam mit Huawei und Telefónica Deutschland eine Lösung erarbeitet, die auf NB-IoT basiert und mit der ältere, analoge Systeme in die digitale Welt gebracht werden können. Die EnergyCam, ein Kamerasystem, das der IoT-Anbieter Q-loud entwickelt hat, kann den Zählerstand eines klassischen Rollenzählers erfassen, analysiert das Bild und erkennt den angezeigten Zählerstand durch eine integrierte Software und überträgt diesen digitalisiert per Narrow-Band-IoT im Telefónica-Netz an die Huawei-IoT-Plattform OceanConnect. Diese Lösung ermöglicht der Flughafen-IT, schnell auf die Messdaten zuzugreifen und diese zur Analyse zu nutzen. Die Wahl der passenden technologischen Infrastruktur erfordert von Organisationen wie dem Flughafen München die Berücksichtigung vieler Faktoren: Die erforderliche Vernetzungstechnik soll im Idealfall auf der gesamten Fläche des 1.575ha großen Areals – das entspricht rund 2.200 Fußballfeldern – verfügbar sein. Sie darf z.B. Systeme der Flugsicherung auf gar keinen Fall stören. Johann Götz, am Flughafen München verantwortlich für die Software- und Infrastrukturentwicklung, sagt: „Für die jetzt anstehende digitale Weiterentwicklung des Flughafens ist damit schon eine wichtige Voraussetzung geschaffen: Die Bereiche IT und Technik müssen ihre Kompetenzen gleichermaßen



Jörg Diederichs, CTO/VP New Business (IoT/I4.0) bei Huawei Technologies in Düsseldorf



Jürgen Pollich, Leiter M2M und Connected Services bei Telefónica in Deutschland

Bilder: Huawei Technologies Deutschland GmbH

einbringen, wenn die physische Welt auf dem Gelände ihren Anschluss ans Internet bekommt und so Teil des Internet of Things werden soll.“ Alexander Rupprecht, Director B2B Business Brand P&L bei Telefónica in Deutschland sagt: „Wir haben für dieses Pilotprojekt erstmals im Bereich des Flughafens München mit NarrowBand-IoT einen neuen Mobilfunkstandard für den Erprobungszeitraum implementiert, der speziell für das Internet der Dinge gedacht ist. Damit wird energiesparende Datenübertragung von entsprechenden IoT-Devices erst sinnvoll möglich.“

Huawei Technologies Co., Ltd.  
[www.huawei.com/de](http://www.huawei.com/de)

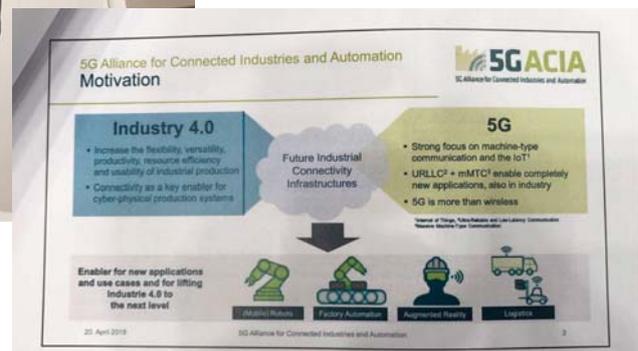
# „Warum 5G die Welt der Industrie 4.0 verändern wird“

**Für die Industrie ist die kommende Mobilfunkgeneration 5G von großer Bedeutung. Die Anfang April im ZVEI gegründete Arbeitsgemeinschaft '5G Alliance for Connected Industries and Automation' (5G-Acia) hat sich zum Ziel gesetzt, 5G erfolgreich in der industriellen Produktion zu etablieren und von vornherein industriefähig zu gestalten.**



Dr. Andreas Müller, Vorsitzender der 5G-Acia, hat die Initiative öffentlich auf der diesjährigen Hannover Messe gestartet.

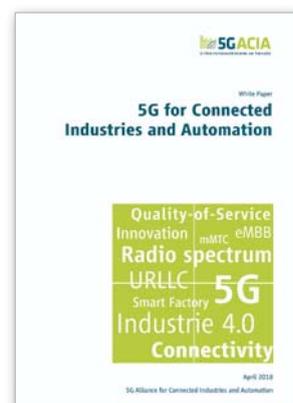
Mit 5G ist es möglich, Industrie 4.0 noch schneller umzusetzen und auf die nächste Entwicklungsstufe zu heben. Mit der Technologie lässt sich ein bisher ungekanntes Maß an Flexibilität, Wandelbarkeit und Mobilität in der industriellen Produktion realisieren. Denn 5G bietet viele Vorteile, u.a. eine sehr leistungsfähige drahtlose Vernetzungstechnologie, die selbst für kritische industrielle Anwendungen geeignet ist. 5G-Acia bringt sich aktiv in die Standardisierung und Regulierung von 5G mit ein. Gleichzeitig identifiziert und analysiert sie mögliche Anwendungsfälle und die damit einhergehenden Anforderungen seitens der Industrie. „5G wird das zentrale Nervensystem der Fabrik der Zukunft werden und sich disruptiv auf die industrielle Fertigung auswirken“, sagt Dr. Andreas Müller (Bosch), Vorsitzender der 5G-ACIA. „In der 5G-Acia bringen wir erstmalig alle wichtigen Akteure weltweit zusammen. Dadurch sind wir in der Lage, konzertiert und zielgerichtet daran zu arbeiten, dass die Belange der Industrie entsprechend berücksichtigt werden.“ In der Initiative haben sich sowohl Vertreter der klassischen Automatisierungs- und Fertigungsindustrie als auch führende Organisationen aus dem Bereich der IKT-Industrie zusammengeschlossen. Zu den derzeit 26 Mitgliedern zählen: Beckhoff, Bosch, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), Deutsche Telekom, Endress+Hauser, Ericsson, Festo, Fraunhofer Gesellschaft, Harting, Hirsch-



Bilder: ZVEI e.V.

mann Automation & Control, Huawei, Infineon, Institut für industrielle Informationstechnik (iIT), Institut für Automation und Kommunikation e.V. (ifak), Intel, Mitsubishi, Nokia, NXP, Pepperl+Fuchs, Phoenix Contact, R3 – Reliable Realtime Radio Communications, Siemens, Trumpf, Vodafone, Weidmüller und Yokogawa. Im Whitepaper '5G for Connected Industries and Automation' gibt die Initiative einen ersten Überblick über das Thema und stellt ihre Ziele vor. ■

QR-Code  
scannen  
und das  
Whitepaper  
kostenlos lesen.



ZVEI e.V.  
www.zvei.org

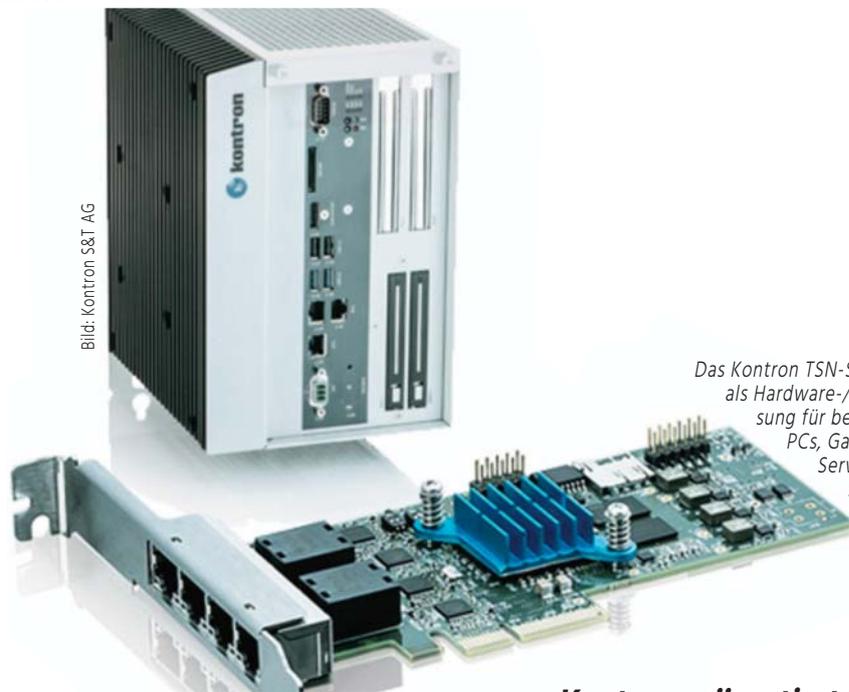


Bild: Kontron S&amp;T AG

Das Kontron TSN-Starterkit ermöglicht als Hardware-/Software-Upgrade-Lösung für bestehende SPSen, Box PCs, Gateways und Industrial Server den einfachen Einstieg ins Time Sensitive Networking.

### Kontron präsentiert TSN-Starterkit

# Einstieg ins Time Sensitive Networking leicht gemacht

**Kontron stellte erstmals auf der embedded world eine Erweiterungslösung für Time Sensitive Networking (TSN) für Fog Computing vor. Das Herzstück des Starterkits ist der wartungsfreie Industriecomputer KBox C-102-2, der eine TSN-Netzwerkkarte bereits mit Software und Real Time Linux Betriebssystem vorintegriert hat.**

Die TSN-Spezifikationen sorgen dafür, dass Datenpakete garantiert zeitgerecht und hoch verfügbar zugestellt werden. Kontrons Industriecomputer der KBox-Serie werden u.a. für die Steuerung von Maschinen oder die Visualisierung und Inspektion des Fertigungsprozesses eingesetzt. Die KBox C-102-2 des Starterkits ist mit einem leistungsstarken CPU der Intel Core i5 Prozessorreihe der sechsten Generation und Linux Betriebssystem mit Echtzeiterweiterungen ausgestattet. Ihr wartungsfreies Systemdesign verfügt über einen lüfter- und batterielosen Aufbau und sorgt so für eine lange Lebensdauer und eine hohe Systemverfügbarkeit. Durch die modulare Bauweise der standardisierten COM Express-Technologie sind die Systeme flexibel und skalierbar. Die KBox C-102-2 des Starterkits verfügt über zwei PCI-Slots. Einer der PCI-Slots ist mit der TSN-Netzwerkkarte belegt. Damit stehen vier zusätzliche TSN switched Ethernet Ports mit 10/100/1000MBit/s zur Verfügung.

#### Zukunftssicher durch Software- bzw. FPGA-Update

Die TSN-Netzwerkkarte von Kontron umfasst einen integrierten Switch für redundante Netzwerke mit vier GBit-Ethernet-Ports. Sie erfüllt die Spezifikationen gemäß IEEE 802.1 TSN für Timing und Synchronisation, Traffic Scheduling, Frame Preemption, Stream Reservation Protokolle. Weitere Funktionen können ggf. per SW- oder FPGA-Update nachgeladen werden. Mit der Standard-PCI-Express-Netzwerkkarte einschließlich der dazugehörigen Netzwerk- und Switch-Treiber für Linux können Industriecomputer mit einem redundanten Ring-, Linien-, Daisy-Chain- oder stern-

förmigen TSN-Netzwerk verbunden werden. Die Kontron TSN-Netzwerkkarte ist speziell für raue Industrieumgebungen geeignet und kann im industriellen Temperaturbereich von -40 bis +85° Celsius betrieben werden. Zum Software-Umfang gehören Beispielapplikationen zum Versenden von TSN-Paketen, sowie eine Network-Analyzer-Applikation, die TSN-Performance-Parameter ermittelt und anzeigt. Außerdem kann die Zeitsynchronisation über PTP IEEE 802.1AS über ein einfaches SW-Tool und einen 1-pps Sync Ausgang evaluiert werden.

#### Fazit

Das Kontron Starterkit ermöglicht als Hardware-/Software-Upgrade-Lösung für bestehende SPSen, Box PCs, Gateways und Industrial Server den einfachen Einstieg ins Time Sensitive Networking. Zudem erleichtert es die einfache Integration von Endgeräten in das TSN-Netzwerk. Als Teil der Kontron Security Solution Reihe unterstützt die KBox C-102-2 des Starterkits auch die Kontron Appprotect Security Lösung. Diese sorgt durch einen Hardware-seitig integrierten Security-Chip von Wibu-Systems in Verbindung mit einem passenden Softwareframework für den Schutz von IP-Rechten sowie einen Kopier- und Reverse-Engineering-Schutz. ■

Autor: Kontron S&T AG  
www.kontron.de

Direkt zur Marktübersicht [i-need.de](http://i-need.de)

[www.i-need.de/?f68808](http://www.i-need.de/?f68808)

## Ethercat-Ansatz von führenden TSN-Switch-Herstellern unterstützt

Im November 2017 hat die Ethercat Technology Group (ETG) ein TSN-Profil veröffentlicht, welches spezifiziert, wie Ethercat die TSN-Technologien nutzen wird. Da Ethercat TSN-Streams für deterministische Kommunikation in einer heterogenen Netzwerkumgebung nutzt, werden sie dort verwendet, wo es am sinnvollsten ist: oberhalb der Ethercat-Segmente. Das bedeutet, dass alle der hochperformanten Charakteristiken dieser Technologie beibehalten werden, und Ethercat-Geräte für TSN nicht angepasst werden müssen. Die TSN-Stream-Adaptation, welche die Ethercat-Segmente mit dem TSN-Netzwerk verbindet, kann sowohl im TSN-Switch, als auch im ersten Ethercat-Gerät integriert werden. TSN-Technologieanbieter, darunter Moxa, Hirschmann, Hilscher und Xilinx, kündigen nun ihre Unterstützung für diesen Ansatz an. Für den Executive Director der ETG, Martin Rostan, zeigt dies, dass die ETG mit ihrem Ansatz zur TSN-Integration auf dem richtigen Weg ist: „Obwohl TSN noch nicht in der Praxis eingesetzt werden kann, haben sich führende Technologieanbieter bereits dem Ethercat-Ansatz verschrieben.“ Die Ethercat Technology Group koordiniert, die sich auf TSN beziehenden Ethercat-Spezifikationen, durch eine Liaison mit der IEEE 802.1 Working Group. So kann die ETG Technical Working Group auf Entwürfe der IEEE 802.1-Spezifi-



Bild: Ethercat Technology Group

Vertreter der TSN-Switch-Hersteller, die künftig den Ethercat-Ansatz unterstützen wollen

kationen zugreifen und somit sicherstellen, dass das Ethercat-TSN-Profil den neusten Entwicklungen folgt. Die Stream-Adaptation im Profil beschreibt die Nutzung von Standard-TSN-Funktionalitäten und nimmt weder Änderungen an TSN vor, noch verlangt es irgendwelche Anpassungen an den handelsüblichen Ethercat-Geräten.

Ethercat Technology Group  
www.ethercat.org

Anzeige

# IBHsoftec

## Der kompakte OPC UA Server für S5- und S7-Steuerungen

### IBH Link UA

OPC UA Server mit integrierter Firewall

- OPC UA Server für die einfache Anbindung an MES-, ERP- und SAP-Systeme sowie Visualisierungen
- OPC UA Client zur Kommunikation mit anderen OPC Servern
- 4 Ethernet Ports mit Firewall für eine saubere Trennung der Prozess- und Leitebene
- Skalierbare Sicherheitsstufen durch Austausch digital signierter Zertifikate
- S7-kompatible SoftSPS zur Datenvorverarbeitung integriert
- S7-Steuerungen über S7 TCP/IP oder IBH Link S7++ ansprechbar
- S5-Steuerungen schnell und günstig über IBH Link S5++ ansprechbar
- Komfortable Konfiguration mit dem kostenlosen IBH OPC Editor, Siemens STEP7 oder dem TIA Portal
- Administration per Webbrowser
- Historische Daten
- Alarms & Conditions
- MQTT-Anbindung



OPC UA

## Profinet zeigt erste Umsetzung auf TSN

Wie bei allen neuen Technologien stehen bei Profibus & Profinet International (PI) immer zuerst der Anwendungsfall und die damit verbundenen Anforderungen im Vordergrund. Erst, wenn diese Grundlagen soweit erarbeitet sind, geht es in die konkrete Umsetzung. Bei TSN (Time Sensitive Networking) ist dies nun der Fall. PI zeigte auf der Hannover Messe anhand einer Demoapplikation, wie sich TSN in Profinet integrieren lässt. Die Organisation weist damit den Weg für die weiteren Spezifikations- und Standardisierungsarbeiten. Die Live-Demo besteht aus einem TSN-Netz, bei dem sich die Topologie zur Laufzeit ändern lässt, ohne das Netz neu konfigurieren zu müssen. Ein sichtbarer Vorteil gegenüber der heutigen IRT-Welt, bzw. einer statischen TSN-Konfiguration. Auch wurde gezeigt, wie sich bestehende Profinet-Netze und Geräte integrieren lassen. Dies ist für einen einfachen und fließenden Umstieg auf TSN unerlässlich. Vor über zwei Jahren startete PI die Industrie 4.0 Working Group mit der Aufgabe, die Anforderungen von Industrie 4.0 und dem IIoT (Industrial Internet of Things) an Profinet zu erarbeiten. Unter Mitwirkung zahlreicher, führender Unternehmen wurden die Anwendungsfälle beschrieben und die Anforderungen an fünf essentiellen Technologien (TSN, OPC UA, Security, Semantik und IPv6) erarbeitet. Gerade bei TSN zeigt sich, dass die zugrundeliegenden IEEE-Standards sehr viel Freiraum für die Nutzung erlauben. Daher war es wichtig, die industriellen Randbedingungen genau zu definieren. Für Profinet bedeutet dies, dass vor allem die Anwendersicht, also wie die Nutzer die Technologie erleben, sich möglichst nicht von der heutigen Welt unterscheiden soll. Ferner ist es notwendig, dass TSN auch Verbesserungen bringt, wie z.B. ein Plug & Work-Verhalten. Im nächsten Schritt will die Profibus Nutzerorganisation nun die Spezifikationsarbeit hinsichtlich der Integration von TSN in Profinet weiter vorantreiben, die bis zur Hannover Messe im nächsten Jahr vorliegen soll.

Profibus Nutzerorganisation e.V.  
www.profinet.com

## NI kooperiert mit Huawei im Bereich TSN

NI hat im Rahmen der Hannover Messe gemeinsam mit anderen Branchenführern das Testbed 'Time-Sensitive Networking (TSN) + OPC Unified Architecture (OPC UA)' vorgestellt, das sechs wichtige Anwendungsfälle aus der Industrie abdeckt. Das auf der Veranstaltung ausgestellte Testbed dient der Demonstration verschiedener realitätsgetreuer Simulationen und Bedingungen aus dem Bereich Smart Manufacturing, um den hohen Determinismus und die geringe Latenz von TSN aufzuzeigen. Der vom IEEE entwickelte Kommunikationsstandard TSN bildet eine der Grundlagen für das industrielle Internet der Dinge (IIoT). Im Gegensatz zu Standard-Ethernet spielt bei TSN, wie der Name bereits sagt, die Zeit eine wichtige Rolle. Mit zunehmender Größe des IIoT und der steigenden Anzahl an vernetzten Dingen und Systemen werden Timing und Priorisierung im Netzwerk immer wichtiger, weshalb ein Standard wie TSN dringend benötigt wird. NI arbeitet mit seinen Branchenpartnern

intensiv an der Weiterentwicklung von TSN-Technologie, wozu auch die Einführung von Testbeds gehört, die den Weg für echte IIoT-Bereitstellungen ebnen sollen.

National Instruments Germany GmbH  
www.ni.com

## Gemeinsames TSN + OPC UA Testbed für Smart Manufacturing



Bild: Huawei Technologies Deutschland GmbH

All, Avnu Alliance, ECC, Fraunhofer FOKUS, Huawei, Schneider Electric und zahlreiche weitere Stakeholder kündigten gemeinsam das TSN + OPC UA Testbed für Smart Manufacturing an

Auf der Hannover Messe haben mehr als 20 internationale Organisationen und führende Industrieanbieter gemeinsam das 'Time-Sensitive Networking (TSN) + OPC Unified Architecture (OPC UA) Smart Manufacturing Testbed' für sechs große Industrial-Internet-Szenarien angekündigt. Zu den an dem Testbed beteiligten Akteuren gehören neben Huawei auch die Alliance of Industrial Internet (AII), die Avnu Alliance, das Edge Computing Consortium (ECC), Fraunhofer Fokus, Schneider Electric, HollySys, National Instruments Corporation (NI), B&R Automation, TTTech und Spirent Communications. Das Testbed wurde auf der Industriemesse vorgestellt. Zu diesem Zweck wurden verschiedene reale Smart-Manufacturing-Bedingungen simuliert, um TSN + OPC UA vorzuführen. Es soll Industrieunternehmen dabei helfen, ihre Effizienz zu steigern, indem Ausfallzeiten reduziert, die Gesamtgeräteeffizienz (OEE) verbessert und die Gesamtbetriebskosten (TCO) gesenkt werden. Das Testbed entspricht den OPC-UA-Standards und stellt sicher, dass mehrere Geräte unterschiedlicher Hersteller problemlos in einem System zusammenarbeiten können. Es integriert Software-Defined Networking (SDN)-Technologie, um den Datenverkehr auf der Grundlage eines präzisen Timings zu priorisieren und sowohl Echtzeit- als auch Nicht-Echtzeitdaten über ein einziges Netzwerk zu übermitteln. Dies ermöglicht Konnektivität und Interoperabilität für Maschinen, Personen und Dinge im gesamten Netzwerk und überbrückt die letzte Meile auf dem Weg zum Industrial Internet.

Huawei Technologies Deutschland GmbH  
www.huawei.com



Die Daten der SmartFactory-KL-Industrie-4.0-Anlage werden durch eine übergeordnete SmartFactory-KL-Cloud gesamthaft ausgewertet und interpretiert.

## Vernetzte Clouds im Produktionsumfeld

# Mehr als eine Cloud managen

**Wie können Daten in der Cloud gesamthaft ausgewertet und interpretiert werden, wenn verschiedene Cloud-Lösungen innerhalb von einer Produktionsanlage zum Einsatz kommen? Das Partnerkonsortium der SmartFactory-KL-Industrie-4.0-Produktionsanlage führte auf der Hannover Messe ihre Lösung vor: Eine übergeordnete Cloud-Plattform, die alle eingesetzten Cloud-Lösungen aggregiert.**

Produzierende Unternehmen nutzen datengetriebene Anwendungen, um verlässliche Voraussagen über Zustände ihrer Produktionsanlagen zu erhalten. Für die dafür notwendige Datenauswertung und Interpretation stehen verschiedene Cloud-Lösungen am Markt zur Verfügung. Jede dieser Lösungen stellt Expertenwissen bereit, das für eine verlässliche Dateninterpretation bei der konkreten Anwendung notwendig ist. Diese Clouds stellen zunächst jeweils herstellerbezogene Einzelösungen dar. Erst wenn sie durch eine übergeordnete Cloud-Plattform vernetzt werden, können die verschiedenen Daten der Produktionsanlage herstellerübergreifend zusammengeführt und in einem Gesamtbild der Anlage bereitgestellt werden.

### Use Case SmartFactory-KL-Cloud

Eine solche Cloud-Plattform, die das gesamte Expertenwissen aller Cloud-Lösungen aggregiert, demonstrierte die SmartFactory-KL, gemeinsam mit ihren Partnern auf der Hannover Messe an Hand ihrer Produktionsanlage. In der SmartFactory-KL-Anlage kommen verschiedene Cloud-Lösungen zum Einsatz, die an die zugehörigen Edge Devices in den Fertigungsmodulen angebunden sind. Das Qualitätssicherungsmodul nutzt beispielsweise für Predictive Maintenance eine andere Cloud als das Fertigungsmodul. Die SmartFactory-KL-Cloud führt nun als übergeordnete Cloud-Plattform die Daten der einzelnen Hersteller-Clouds zusammen, prüft sie und verteilt sie zielgerichtet weiter. So kann die SmartFactory-KL-Cloud beispielsweise Rückschlüsse aus fehlerhaften oder abweichenden Daten ziehen und dem Produktionsmitarbeiter über ein smartes Gerät

wie eine Datenbrille eine entsprechende Wartungsanweisung kommunizieren. Auf den Anwender zugeschnittene Services wird es auch in Zukunft nur vom Experten, also den Anbietern einzelner Cloud-Lösungen, geben. Das bedeutet, dass eine Firma auf mehrere Clouds mit unterschiedlichen Informationen zurückgreifen muss. Für eine sinnvolle Nutzung in der Produktion wird deshalb eine Cloud-Plattform benötigt, mit der sich die verschiedenen Clouds vernetzen können.

### Weiterer Use Case: Service-Provider-Cloud per 5G-Technologie

Ferner ist die Service-Provider-Cloud per 5G-Technologie direkt an das flexible Transportsystem angebunden und führt mit den Daten aus der optischen Erfassung des Werkstücks die eigentliche Qualitätskontrolle durch. „Wir sehen einen Trend, dass Clouds wie Maschinen als Dienste betrachtet werden können, die modular kombinierbar sind. Auch das Pay-per-Use-Bezahlsystem ist ein Indikator dafür, denn der Nutzer bezahlt bei vielen Anbietern nur die abgerufenen Leistungen. Ein weiterer Vorteil für die Nutzung von Cloud-Plattformen liegt in ihrer relativ einfachen Bedienbarkeit. So können beispielsweise auch Automatisierer diese einsetzen, ohne selbst IT-Experte zu sein“, so das Fazit von Prof. Dr. Detlef Zühlke, Vorstandsvorsitzender der SmartFactory-KL. ■

**Autorin:** Dr. Haike Frank  
Leitung PR & Marketing  
Technologie-Initiative SmartFactoryKL e.V.  
[www.smartfactory-kl.de](http://www.smartfactory-kl.de)

# Mehr als 20Mio. Profinet-Geräte im Markt

**Die Zahl der installierten Geräte für IO-Link, Profinet und Profibus ist im vergangenen Jahr gestiegen. Das hat die Organisation Profibus & Profinet International (PI) notariell erfasst.**

Bei Profinet wurde mit den in 2017 in den Markt gebrachten 4,5Mio. Geräten die Rekordzahl des Vorjahres um weitere 25 Prozent gesteigert. Damit haben mit Ende 2017 in Summe ca. 21Mio. Profinet-Geräte die Produktion automatisiert. Die Jahreszahl von Profibus ist nach einigen Jahren des Rückgangs mit 2,3Mio. installierten Geräten nahezu unverändert gegenüber dem Vorjahr geblieben. Die Gesamtzahl nähert sich der 60Mio.-Grenze. Der Vergleich der beiden Jahreswerte zeigt, dass in 2017 fast doppelt so viele Profinet- als Profibus-Geräte in den Markt gebracht worden sind. Die Summe der beiden Jahreswerte stellt mit 6,8Mio. ein Allzeithoch dar. Stabil zeigt sich auch die Entwicklung von Profibus in der Prozessautomatisierung. Mit dem in 2017 erzielten Jahreswert von 0,9Mio. sind nun 11,5Mio. Profibus-Geräte in prozesstechnische Anlagen eingeflossen. Die Entwicklung von Profisafe weist durch den höchsten bisher erzielten Jahreswert von nahezu 2Mio. in den Markt gebrachten Knoten weiterhin einen sehr positiven Trend auf, was einem Wachstum von 25 Prozent gegenüber dem Vorjahr entspricht. In Summe

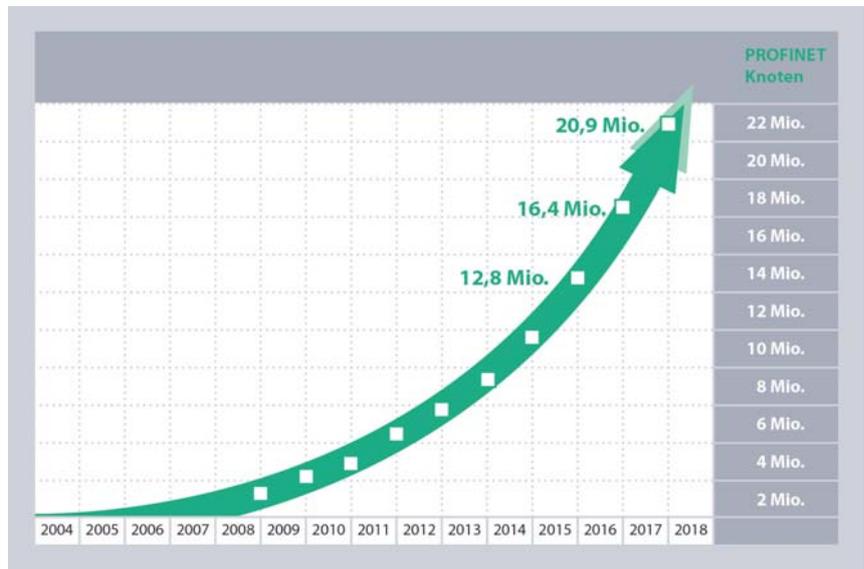
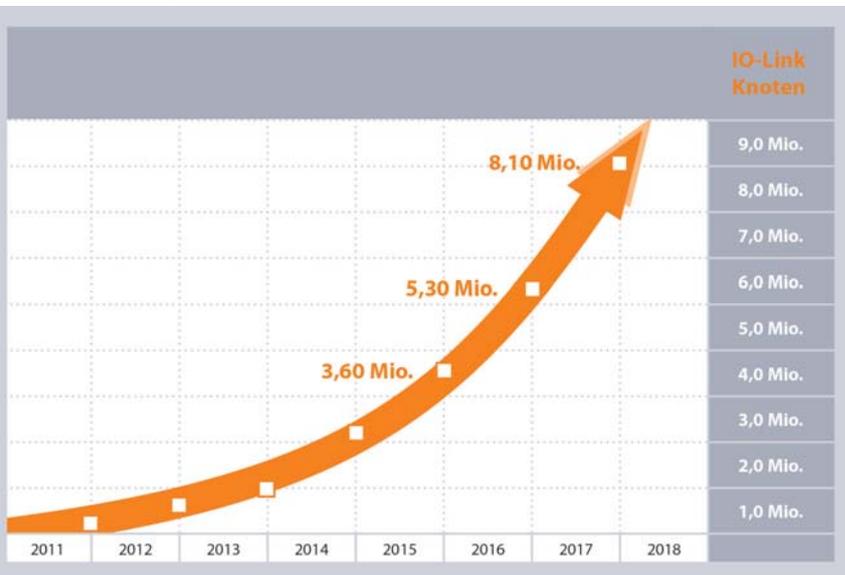


Bild: Profibus Nutzerorganisation e.V.

steuert Profisafe insgesamt auf die Zahl von 9Mio. zu. Wie in den früheren Jahren erzielte IO-Link auch in 2017 in zweierlei Hinsicht einen Rekord. Zum einen wurden 2,8Mio. IO-Link-Geräte in den Markt gebracht, und zum anderen betrug das Wachstum im Vergleich zum Vorjahr mehr als 50 Prozent. Die Gesamtzahl der installierten IO-Link-Geräte summiert sich damit auf mehr als 8Mio. Für Karsten Schneider, Vorstandsvorsitzender der PNO und Chairman von Profibus & Profinet International (PI), sind die Zahlen ein Beleg für die Richtigkeit der Entscheidungen bei PI, die in den früheren Jahren hinsichtlich Fortentwicklung der Technologien getroffen wurden. "Dies spiegelt sich letztendlich auch in unseren Mitgliedszahlen wider. Denn allein die Organisation in Deutschland kann nunmehr 400 Unternehmen zu ihren Mitgliedern zählen, was ein großer Vertrauensbeweis in unsere Organisation und unsere Innovationskraft ist. Wir arbeiten hart an der Positionierung unserer Technologien im Industrie-4.0-Umfeld," so Schneider.

Bild: Profibus Nutzerorganisation e.V.



Firma: Profibus & Profinet International (PI)  
de.profibus.com

Direkt zur Marktübersicht [i-need.de](http://i-need.de) [www.i-need.de/?f8554](http://www.i-need.de/?f8554)

## Einfache Datenintegration von Modbus-Steuerungen in IoT und Cloud



Bild: Softing Industrial Automation GmbH

Mit diesem Gateway von Softing bringt man Modbus-Steuerungen sicher in aktuelle IT-Infrastrukturen – per OPC UA oder MQTT.

Das Softing-Gateway Datafeed UAGate MB ist jetzt verfügbar. Das Produkt ermöglicht die sichere Integration von Prozess- und Maschinendaten aus Modbus-Steuerungen in IoT- und Industrie-4.0-Lösungen. Das Gateway zielt auf die Kommunikation zwischen Modbus-Steuerungen in industriellen Netzen und Anwendungen in der IT ab. Es gestattet den Zugriff auf Prozess- und Maschinendaten der Steuerungen über OPC UA oder MQTT. Dabei unterstützt es relevante IT-Security-Standards, wie SSL-Verschlüsselung und X.509-Zertifikate. Über das Gateway können auch mehrere Anwendungen parallel angebunden werden. Diese Eigenschaft unterstützt hybride Architekturen, in denen Teile der Gesamtlösung vor Ort, andere Teile in der Cloud laufen.

**Softing Industrial Automation GmbH**  
[www.industrial.softing.com](http://www.industrial.softing.com)

## VPN-Router als IoT-Gateway für Industrie und Gebäude

Mit der SCR-Serie bringt Insys Icom LTE- bzw. LAN-Router mit in einem kompakten Gehäuse auf den Markt. Die Geräte sind auch als Varianten mit I/Os erhältlich. Lokal lassen sich IP-basierte sowie serielle Geräte anbinden. Die SCR-Serie verfügt über das Betriebssystem Icom OS und die Linux-Umgebung Icom Smart-Box. In dieser virtuellen Umgebung lassen sich in sog. Containern (LXC) Skripte und Programme – auch unabhängig voneinander – auf dem Router ausführen sowie Daten speichern und verarbeiten. Der SCR ist somit nicht nur zur sicheren Fernwartung einsetzbar, sondern auch eine Lösung für Edge Computing-Anwendungen wie Condition Monitoring oder Data Analytics. U.a. lassen sich Zustände und Werte angeschlossener Geräte überwachen, sowie verschiedene Cloud-Dienste für Anwendungen wie Reporting oder Benchmarking anbinden. Für IT-Sicherheit sorgen eine Stateful Firewall sowie VPN-Funktionalität, z.B. über den VPN-Dienst Icom Connectivity Suite – VPN.



Bild: Insys Microelectronics GmbH

*Router mit optionalen I/Os von Insys Icom in kompakten Gehäusen zur flexiblen Montage. Auch für Edge Computing-Anwendungen – beispielsweise im Condition Monitoring – eignen sich die Geräte.*

**Insys Microelectronics GmbH**  
[www.insys-icom.de](http://www.insys-icom.de)

Anzeige

# Immer alles im Blick

... ganz ohne Verrenkungen.

Optimal auf Ihren Schaltschrank zugeschnitten

- 3 industrielle Protokolle werden unterstützt
- 2 Installationsoptionen: Hutschienen- und Rackmontage für verschiedene Schaltschrank-Typen
- 1-seitiges Konfigurations-Dashboard

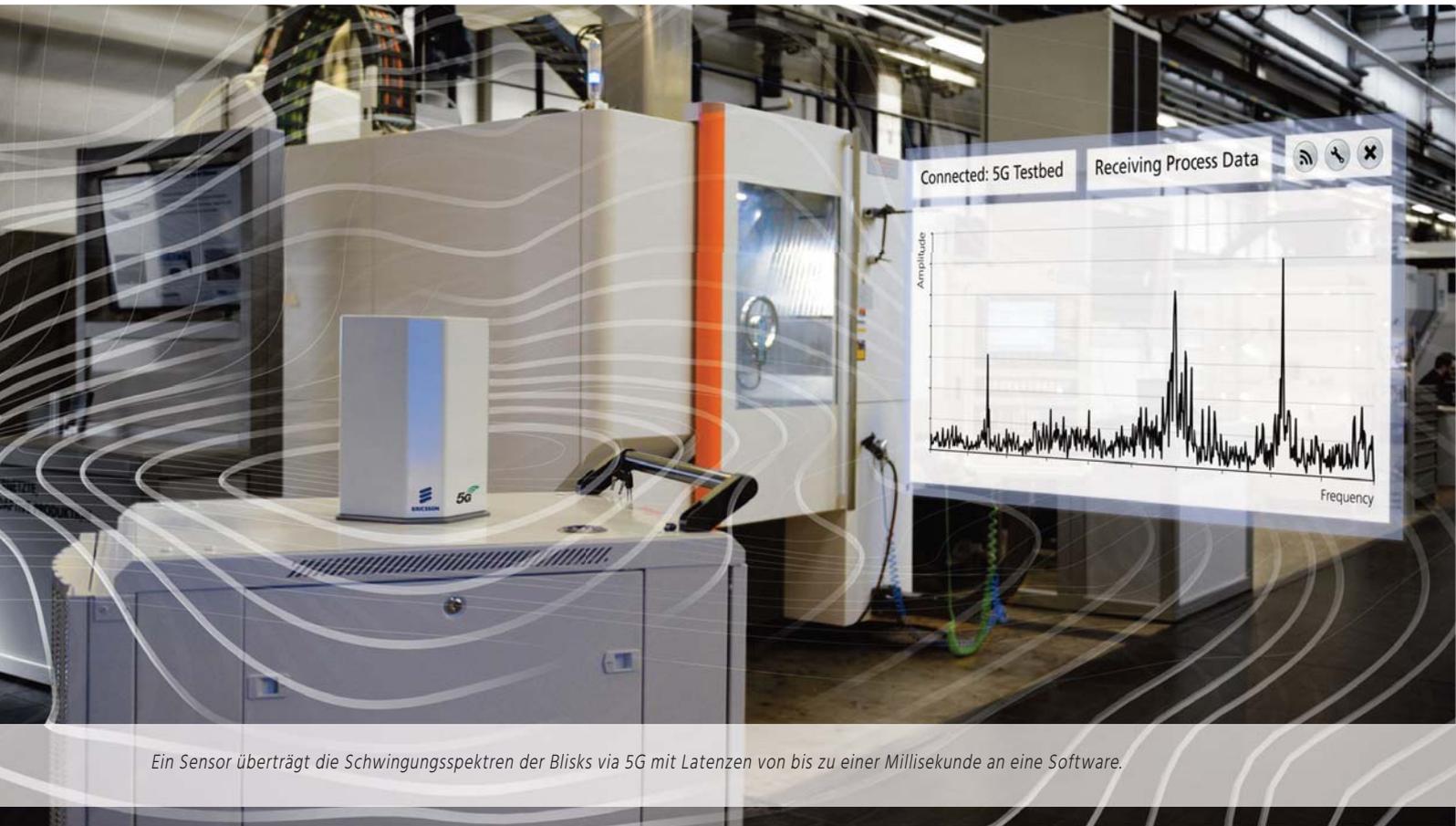
Moxa Lösungen – intelligent, einfach, sicher.



[www.moxa.com](http://www.moxa.com)



**MOXA**  
 Reliable Networks • Sincere Service



Ein Sensor überträgt die Schwingungsspektren der Blinks via 5G mit Latenzen von bis zu einer Millisekunde an eine Software.

# Messdaten mit 5G kabellos in Echtzeit übertragen

**Um Fehler in der industriellen Fertigung frühzeitig zu erkennen, messen Sensoren in Maschinen und Anlagen, ob alles einwandfrei läuft. In der Regel werden die Daten jedoch dezentral und zeitverzögert ausgewertet. Der Mobilfunkstandard 5G dagegen ermöglicht eine direkte kabellose Messung in Echtzeit. Zusammen mit Ericsson bietet Fraunhofer in Aachen eine Testumgebung für 5G-Anwendungen im industriellen Umfeld.**

Flugzeugturbinen herzustellen ist aufwändig und teuer. Alleine die Fertigung der Turbinenschaufeln – sogenannter Blinks (Blade Integrated Disks) – kann bis zu 200.000€ kosten. Höchste Sicherheits- und Qualitätsstandards müssen eingehalten, computergesteuerte Werkzeugmaschinen so programmiert werden, dass die Bauteile exakt nach den Konstruktionsplänen gefertigt werden. Sensoren an Maschinen und Anlagen überwachen permanent den Produktionsprozess. „Doch es bleibt ein Restrisiko. Denn die Qualitätsanalyse erfolgt in der Regel dezentral und zeitverzögert. Insbesondere die Eigenschwingung der Blinks während der Fertigung ist ein Problem. Dadurch kann es zu Qualitätseinbußen kommen, die aufwändig per Hand im Nachgang des Fertigungsprozesses korrigiert werden müssen“, erklärt Dr. Sascha Gierlings, Leiter der Prototypen-

fertigung am Fraunhofer-Institut für Produktionstechnologie IPT in Aachen.

## Einzige Testumgebung in Aachen

Eine Lösung für dieses Problem verspricht die Kombination aus neuester Sensortechnologie und schnellen Datenübertragungsraten, wie sie der künftige Mobilfunkstandard 5G bietet. Für den konkreten Fall der Blinkherstellung hat das Fraunhofer IPT einen speziell entwickelten Sensor direkt auf dem Bauteil angebracht. Dieser überträgt die Schwingungsspektren der Blinks via 5G mit Latenzen von bis zu einer Millisekunde an eine Software. Sie erkennt sofort, ob die Schwingungen ein zulässiges Normalmaß übersteigen bzw. kritische Frequenzen

## Isolationsüberwachungsgerät

Die Variante Iso685-D-P des Bender-Isolationsüberwachungsgerätes Isometer Iso685 kann für Systeme mit Isolationsfehlersuche eingesetzt werden. Ein integrierter Prüfstrom-Generator erzeugt bei einem aufgetretenen Isolationsfehler einen limitierten Prüfstrom gegen Erde. Dieser Prüfstrom ist variabel einstellbar. Über Isolationsfehlersuchgeräte der Serie Isoscan kann dieser Prüfstrom über Messstromwandler einem fehlerhaften Verbraucher zugeordnet werden. Das Gerät kann über einen RS-485-Sensorbus oder über einen Hutschienenbus mit den Isolationsfehlersuchgeräten EDS440 und EDS441 kommunizieren.

Bender GmbH & Co. KG • [www.bender-de.com](http://www.bender-de.com)



Bild: Bender GmbH & Co. KG

Das Isolationsüberwachungsgerät Isometer Iso685-D-P von Bender



Bild: Emka Beschlagteile GmbH & Co. KG

Der neue Vorreiber lässt sich nicht nur binnen Sekunden montieren, er ist auch mit nahezu jedem Motiv individuell gestaltbar.

## Schnellmontage-Vorreiber

Ab sofort bietet Emka seine Schnellmontage-Vorreiber mit einer frei gestaltbaren Gehäuseplatte an, um Designansprüchen besser gerecht zu werden. Sie kann in Metalloptik (z.B. gebürsteter Edelstahl), Carbon-Look oder auch mit metallischer Hochglanzoberfläche gestaltet werden, sodass sich auf dem Vorreiber beeindruckende, edle Oberflächen darstellen lassen. Die Gestaltung der Oberfläche ist grenzenlos, da der Anbieter prinzipiell jedes Design kreieren kann, das sich im Siebdruckverfahren herstellen lässt.

Emka Beschlagteile GmbH & Co. KG • [www.emka.com](http://www.emka.com)

- Anzeige -

## REDEN WIR MAL ÜBER DAS **ABDICHTEN**.

Sie haben ein Problem mit der Abdichtung gegen Späne, Staub oder Zugluft? Sie haben noch keine perfekte und zugleich kostengünstige Lösung gefunden?

Wir helfen Ihnen dabei!

Mink Leistenbürsten dichten optimal ab.

Die umfangreiche Auswahl an Standard- und Sonderprofilen sorgt für nützliche und überzeugende Resultate.

### Ihre Vorteile:

- Perfektes Abdichten, z. B. an Türen und Toren, Öffnungen oder Durchbrüchen
- Zuverlässiges Abdichten, z. B. gegen Späne, Staub oder Zugluft
- Höchste Faserqualität, dadurch extrem verschleißarm
- Optimale Beratung

Sprechen Sie uns an!



Think Mink!®

August Mink KG, D-73035 Göppingen  
Tel.: +49 (0)71 61 40 31-0 | [info@mink-buersten.de](mailto:info@mink-buersten.de)  
[www.mink-buersten.com/abdichten](http://www.mink-buersten.com/abdichten)

Wir freuen uns auf Ihren Besuch!



Halle A5 / Stand 418  
München  
19.06. - 22.06.2018



**Mink**  
Bürsten®



Bild: Helmholz GmbH &amp; Co. KG

Das Fernwartungsportal myRex24 spielt seine Vorteile beim Retrofit in Brownfield-Umgebungen genauso wie bei der Ausrüstung neuer Maschinen und Anlagen aus.

**Für Neuanlagen und Retrofit**

## Durchgängige Remote-Lösung

**Nicht nur durch die Einflüsse von Industrie 4.0 kommt der Remote-Anbindung von Maschinen und Anlagen eine wachsende Bedeutung zu. Weder Maschinenbauer noch Endanwender können heute noch großen eigenen Aufwand dafür betreiben und Spezialisten beschäftigen. Deswegen sind funktionale und bedienerfreundliche Lösungen aus einem Guss gefragt. Sie sollen nach Möglichkeit Hard- sowie Software-Seite abdecken und auch bei der Anbindung der Steuerungsebene Vorteile für die Anwendung mitbringen.**

Das Thema der Fernwartung gewinnt immer stärker an Gewicht in Maschinenbau und Industrie. „Remote-Zugriff und Alarmfunktionen sind in vielen Anwendungen längst State-of-the-Art“, bringt es Karsten Eichmüller, Geschäftsführer der Firma Helmholz, auf den Punkt. „Entsprechend werden solche Fernwartungs-Features von unseren Kunden einfach voraus gesetzt.“ Trends wie Predictive Maintenance und Condition Monitoring schrauben die Ansprüche nach oben und zeigen auf, wo sich die Automatisierungstechnik in diesem Segment hin entwickelt. Gleichzeitig müssen sich Maschinenbauer und Endanwender und dem industriellen Internet der

Dinge stellen. „Bei einigen Unternehmen gibt es noch große Vorbehalte in Bezug auf die Cloudlösungen“, schildert Eichmüller die aktuelle Situation. „Diejenigen, die sich aber bereits mit dem Thema beschäftigen, finden sich in einem Dschungel angebotener Lösungen wieder: Von den großen Public-Lösungen, die zwar weit verbreitet, aber nicht auf industrielle Anforderungen abgestimmt sind, bis zu einer Vielzahl an Speziallösungen für bestimmte Industrieanwendungen und -branchen.“ Dazu kommt: Die steigenden Anforderungen in Bezug auf den Fernzugriff betreffen nicht nur aktuelle und kommende Maschinen- generationen. „Immer mehr Betreiber müssen sich intensiv Ge-



Bild: Helmholz GmbH &amp; Co. KG

Die Router der Rex-Familie ermöglichen zusammen mit dem Fernwartungs-Portal myRex24 alle modernen Remote-Funktionen: vom klassischen Fernzugriff, über Überwachungs- und Alarmfunktionen.

danken dazu machen, wie sie ihre gewachsene Fertigungsumgebung fit für die Zukunft halten“, erklärt Eichmüller. „Man muss bedenken, dass viele verbaute SPSen noch nicht mal einen Netzwerkanschluss haben.“

### Zentraler Punkt: Einfach muss es sein

Für solch in die Tage gekommene Steuerungen bietet Helmholz eine Lösung namens Netlink, mit der sich ein Netzwerkzugang unkompliziert nachrüsten lässt. Natürlich stehen auch Router mit Profibus-Schnittstelle wie der Rex300 oder die neuen Rex250 zur Verfügung. Auf dieser Basis sind Maschinen dann auch bereit für moderne Fernwartungskonzepte, mit denen sich Helmholz jetzt verstärkt an den Markt wendet. „Unsere Lösungen stoßen in den Brownfield-Umgebungen der europäischen Industrie auf reges Interesse“, so Eichmüller weiter. Aber nicht nur dort: Auch bei der Ausrüstung neuer Maschinen und Anlagen bringe das Helmholz-Fernwartungskonzept große Vorteile, weil es sehr unkompliziert in der Handhabung ist. Einfache Konfiguration und Inbetriebnahme sind von zentraler Bedeutung. „Maschinenbauer haben abseits ihrer Kernkompetenz immer weniger Ressourcen frei und der Anwender kann, bedingt durch den Fachkräftemangel, auf immer weniger Spezialisten zurückgreifen.“ Das Fernwartungskonzept von Helmholz zielt genau in diese Richtung ab, und zwar mit all seinen Bestandteilen. „Unser Anspruch lautet: Der Remote-Zugriff auf eine Maschine muss so intuitiv und einfach sein, dass sich der Kunde weder auf Hardware- noch auf Software-Seite um Einzelheiten kümmern muss“, erklärt Produktmanager Fabian Slowakiewicz. „Stattdessen kann er sich komplett auf die echten USPs seiner Maschine konzen-

trieren.“ Unter diesem Ansatz hält Helmholz eine abgestimmte Kombination aus den Routern der Rex-Familie und dem Fernwartungsportal myRex24 V2 bereit, die alle modernen Remote-Funktionen umfasst: vom klassischen Fernzugriff, über Überwachungs- und Alarmfunktionen bis hin zum Daten-Logging. „Primär ist unsere Lösung aber darauf ausgelegt, das Leben von Maschinenbauer und Endanwender wirklich zu erleichtern“, so Slowakiewicz, „und dieser Ansatz wurde im Markt sehr erfolgreich aufgenommen.“ Denn einen klassischen Router für die jeweilige Anlage und Anwendung einzubinden, kann mühevoll und zeitintensiv sein. Dazu kommt die Anbindung an übergeordnete Software-Systeme und die Server-Infrastruktur. „Dieser Aufwand rechnet sich für viele Mittelständler einfach nicht“, unterstreicht der Produktmanager. „Deshalb der Fokus auf das Rundum-sorglos-Paket für unsere Kunden: Easy to use und Benutzer-Ergonomie lauten hier die Zauberwörter.“

### Flexibles Portal für die Fernwartung

Ergo: Helmholz will die Integration, Konfiguration und Inbetriebnahme der Fernwartungslösungen wesentlich vereinfachen. Das gelingt, in dem die hauseigenen Rex-Router in ein zeitgemäßes Online-Portal eingebettet werden. „Über unser myRex24 V2 Portal kann die komplette Router-Konfiguration mit wenigen Mausklicks erfolgen“, verspricht Slowakiewicz. Das Portal führt den Nutzer durch alle Schritte der Inbetriebnahme, erklärt grundlegende Eigenschaften und stellt auch eine Online-Hilfe bereit. Zudem stehen vorbereitete Ansichten zur Wahl, je nachdem welche Parameter erfasst und welche Funktionen genutzt werden sollen. „Auf diese Weise wird der Installation der Großteil der Komplexität genommen“, fährt Slowakiewicz fort. Bei einem neuen Router erfolgt die komplette Konfiguration in drei einfachen Schritten:

- Router auswählen und Namen vergeben
- LAN IP-Adresse vergeben (Maschinennetzwerk)
- Daten für die Internetverbindung eingeben (WAN, WIFI oder Mobilfunk)

„ Mit unserer Fernwartungs-lösung kommt man schnell zum Ziel, ohne bei Sicherheit oder Verfügbarkeit Kompromisse eingehen zu müssen.

Karsten Eichmüller, Helmholz



Bild: Helmholz GmbH &amp; Co. KG

Mit dem anschließenden Klick auf den Download-Button steht die komplette Konfiguration zur Verfügung und lässt sich über das Netzwerk oder per USB-Stick auf den Router aufspielen, der sich daraufhin über VPN auf dem myRex24 V2 Portal anmeldet. „So funktioniert Fernwartung heute“, betont Slowakiewicz. „Wenn man will, kann man aber natürlich auch ganz tief in die

Technik und die Details unserer Fernwartungslösung einsteigen.“ Im laufenden Betrieb kann der Anwender über das Fernwartungsportal seine weltweit verteilten Maschinen und Anlagen parallel erreichen. Neben der Visualisierung von Anlagendaten ist es natürlich auch möglich, erfasste Daten aus Auswertung oder Analyse an übergeordnete Systeme weiterzuleiten.

### Passende SPS- und HMI-Technik

Sein Angebot an Steuerungs- und I/O-Technik hat Helmholz ebenfalls auf die Anbindung an das Fernwartungsportal ausgelegt. Aber nicht nur das. Auch die SPSen aus dem Hause Insevis lassen sich zugunsten der Funktionalität mit dem myRex24 V2 Konzept kombinieren. „Wir positionieren unsere Steuerungen vor allem als Alternative und Ergänzung in der S7-Welt“, schildert Insevis-Geschäftsführer Jörg Peters die eigene Ausrichtung. „Wir bauen keine SPSen nach, legen aber großen Wert darauf, dass sie das ähnliche Look&Feel bieten und mit den Siemens-Programmier-Tools kompatibel sind.“ Der Insevis-Slogan 'Make S7 smart and simple' sei kein Marketing-Gag, sondern Programm, führt Peters weiter aus. „Wir wollen es dem Anwender in der S7-Welt so einfach wie möglich machen und decken gleichzeitig Nischen ab, die aus der Sicht des Konzerns nicht rentabel sind.“ So sind die Insevis-SPSen z.B. auch mit Schnittstellen erhältlich, die Siemens im Rahmen seines S7-Portfolios nicht anbietet. Die beiden Firmen Helmholz und Insevis verbindet eine lange partner-

schaftliche Zusammenarbeit. „Unsere Portfolios überlappen sich kaum und passen ausgezeichnet zueinander“, unterstreicht Eichmüller. „So ist über die Jahre zwischen unseren Unternehmen ein besonders Maß an Vertrauen gewachsen.“ Entsprechend will man auch im Bereich der Fernwartung dem Anwender gemeinsam Mehrwert bieten. „Der Anwender will heute auf getestete

„  
Der Anwender will auf  
schlüsselfertige Lösungen  
zugreifen und sich nicht mit  
einzelnen Komponenten bzw.  
deren Anbindung befassen.“  
Jörg Peters, Insevis



Bild: Helmholz GmbH & Co. KG

Lösungen zugreifen und sich nicht mit Details bei der Abstimmung zweier Systeme befassen“, beschreibt Peters die zunehmende Lösungsdenke der Maschinenbauer. „Hier kommen wir dem Kunden gemeinsam entgegen.“ Im Ergebnis müsse er die Geräte von Helmholz und Insevis quasi nur noch zusammenstecken und das System auf die Anwendung abstimmen. „Auf Wunsch bekommt der Kunde den funktionierenden Lösungsansatz dokumentiert als Beispielprogramm für SPS, Panel, Router und Remote-Portal aus einer Hand.“

### Zusammentreffen von Automatisierung und IT

Neben der unkomplizierten Konfiguration und Inbetriebnahme kommt bei myRex24 V2 Portal auch der Offenheit ein hoher Stellenwert zu. Das sei umso wichtiger, als das immer mehr IT-Funktionalität Einzug in die Automatisierung hält: „Das myRex24 V2 Portal bietet beim Zusammentreffen von Automatisierung und IT-Welt einen guten Kompromiss“, hebt Eichmüller hervor. „Die IT-Seite erhält eine Verwaltungs- und Remote-Lösung mit bekannten Standardmechanismen wie OpenVPN. Parallel bleiben die Automatisierer auf bekanntem Terrain und müssen in Aspekten der Fernwartung keine regelmäßigen Umwege über die Administratoren gehen.“ Weitere Vorteile kommen hinsichtlich der Visualisierung direkt an der Maschine hinzu. „Durch unsere Mittelstandsallianz stellen wir ein abgestimmtes System für ihre Aufgaben zur Verfügung“, so Peters. „Da wir unsere SPSen mit zwei Ethernet-Schnittstellen ausgerüstet haben, lassen sich zudem unproblematisch zwei getrennte IP-Kreise für Fabriknetz und Remote-Zugang realisieren.“ Generell ist das Portal komplett offen gehalten, was das Steuerungsfabrikat angeht. „Wir setzen auf Ethernet und



Bild: Helmholz GmbH & Co. KG

Die S7-SPSen von Insevis bieten das gleiche Look&Feel wie Siemens-Steuerungen, decken aber auch Funktionen und Schnittstellen ab, die der Konzern in seinem Portfolio nicht anbietet.

Bild: Helmholz GmbH & Co. KG

OpenVPN“, unterstreicht Eichmüller. „Welche Steuerung letztendlich die Daten liefert ist eher Nebensache und für die Fernwartung selbst nicht relevant.“ Dieser Ansatz kommt u.a. dann zum Tragen, wenn eine einheitliche Fernwartungslösung in gewachsenen Fertigungsumgebungen etabliert werden soll. „Mit dem myRex24 V2 Portal lässt sich die SPS A genauso fernwarten wie die SPS B“, verdeutlicht es Eichmüller. Der Endanwender muss sich also nicht mit unterschiedlichen Geräten oder Software-Tools auseinandersetzen. Dabei orientiert sich das Portal an heutigen und zukünftigen Standards: „Man kann heute nicht mehr sein eigenes Süppchen kochen. Man darf aufkommende Schnittstellen wie OPC UA und MQTT nicht außer acht lassen. Auch wir werden uns damit intensiv beschäftigen“, erklärt Slowakiewicz. Gerade die Fernwartung müsse durchgängig und nahtlos integrierbar sein. „Alles andere ist in Zeiten der fortschreitenden Digitalisierung und dem zunehmenden Fachkräftemangel nicht sinnvoll.“ Auch bei der Router-Einbindung ist das myRex24 V2 Portal prinzipiell offen.



Das Redaktionsgespräch bei Helmholz drehte sich um moderne Steuerungs- und Remote-Lösungen.

### Funktionsumfang nach Maß

Das myRex24-Portal ist in der Public-Version als kostenfreie Fernwartungslösung verfügbar und umfasst dabei alle wichtigen Basisfunktionen. „Diese Grundfunktionalität reicht für die allermeisten Anwendungen aus“, betont Helmholz-Geschäftsführer Eichmüller. Bei abweichenden oder darüber hinaus gehenden Anforderungen lässt sich der Funktionsumfang sehr flexibel und individuell auf die Bedürfnisse des Anwenders zuschneiden. „In jedem Fall erhält der Anwender eine sichere und schlüsselfertige Lösung, die auf die Bedürfnisse im Mittelstand abgestimmt ist.“ Das Portal steht auf Wunsch auch als virtuelle Lösung zur Verfügung, die der Kunde auf seinen eigenen Servern betreiben und verwalten kann. „Dann behält er auch physikalisch die Datenhoheit und ist bis auf Service- und Sicherheitsupdates komplett autark von Helmholz.“ Weil die Datensicherheit generell immer mehr Raum einnimmt, verfolgt das Portal moderne

Security-Ansätze. Selbst wenn die Visualisierung über den Remote-Zugriff freigegeben wird, lassen sich keine Sicherheitsmechanismen an der Maschine oder Anlage umgehen. „Auch

”

**Über unser myRex24-Portal kann die komplette Router-Konfiguration mit wenigen Mausklicks erfolgen.**

*Fabian Slowakiewicz, Helmholz*



Bild: Helmholz GmbH & Co. KG

über das Portal kann nur derjenige das Programm einer SPS ändern, der die entsprechende Zugangsberechtigung hat.

### Schuster bleib bei deinem Leisten

Beim Leistungsversprechen für den Anwender setzen Helmholz und Insevis auf die o.g. Redewendung. „Wir kennen unsere Stärken und sichern dem Kunden nur das zu, was wir auch halten können“, stellt Eichmüller klar. „So können wir dem Anwender guten Gewissens versprechen, dass er mit unserer Fernwartungslösung und auch mit der Integration der Insevis-SPSen schnell zum Ziel kommt, ohne bei Sicherheit oder Verfügbarkeit Kompromisse eingehen zu müssen.“ (mby) ■



Die S7-HMIs mit abgesetzter oder integrierter S7-SPS von Insevis mit vielen Zusatzschnittstellen bereits onboard.

Bild: Helmholz GmbH & Co. KG

**Firma:** Helmholz GmbH & Co. KG  
[www.helmholz.de](http://www.helmholz.de)

Direkt zur Marktübersicht
**i-need.de**
[www.i-need.de/?Produkt=21971](http://www.i-need.de/?Produkt=21971)

# Marktspiegel Kabel und Leitungen

**Häufig etwas despektierlich als C-Teile bezeichnet, nehmen Kabel und Leitungen in der industriellen Kommunikation einen großen Stellenwert ein. Denn fallen diese aus, ist die Funktionstüchtigkeit einer Maschine oder Anlage ernsthaft beeinträchtigt.**

Der vorliegende Marktspiegel präsentiert einen Überblick darüber, welche Lösungen derzeit am Markt angeboten werden. Dazu gehören Spezialleitungen für Feldbus-, Ethernet- oder Lichtwellenleiter-Anwendungen. Je nach der in einer bestimmten Applikation geforderten Daten-Übertragungsgeschwindigkeit, richtet sich auch die Wahl der Leitung aus. Gängige Lösungen sind dabei heute CAT 5, 6 oder gar 7 -Leitungen. Letztere erlauben Betriebsfrequenzen bis 600 MHz, Kategorie 7A sogar bis 1.000 MHz. Abhängig von den Umwelteinflüssen, die auf die Leitungen einwirken, sollten diese z.B. EMV- oder ölbeständig sowie flammwidrig sein. Nach den geforderten Biegeradien richtet sich die Flexibilität der Leitung. Viele Anbieter liefern ihre Kabel und Leitungen bereits komplett vorkonfektioniert aus. Immer wichtiger werden zudem Lösungen für den Kabelschutz oder die auch preislich sehr unterschiedlichen Werkzeuge für die effiziente Kabelverarbeitung und -beschriftung.

(jwz) ■



Bild: Automation24 GmbH

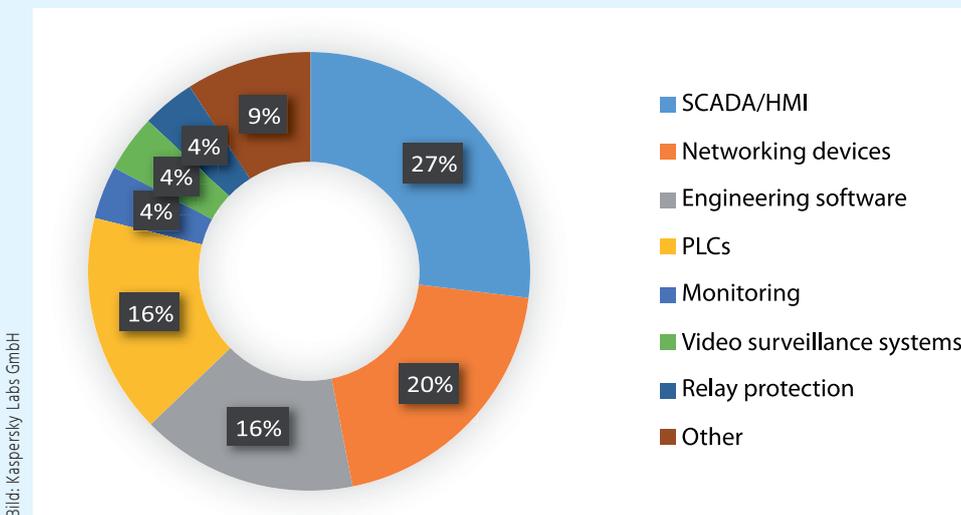
Anbieter	Internet-Adresse	Feldbusleitungen	Sensor-Aktor-Leitung	ASI-Sensor-Aktor-Leitung	CAN / DeviceNet	DeviceNet für Energieführungsnetze	Interbus	Profibus	Profibus PA
Adapt Elektronik	www.adapt.de		•						
Automation24	www.automation24.de		•						
Axon Kabel	www.axon-cable.com								
B&R Industrie-Elektronik	www.br-automation.com		•		•			•	
Balluff	www.balluff.de		•		•	•		•	
Beck Kabel- u. Gehäusetechnik	www.beck-kabelkonfektion.de						•	•	
Bedeu Berkenhoff & Drebes	www.bedeu.com		•	•	•	•	•	•	•
Belden Wire & Cable	www.beldencables-emea.com		•	•	•	•	•	•	•
Thorsten Beulecke Kabelvertrieb	www.beulecke.de		•	•	•	•	•	•	•
BKL Electronic Kreimendahl	www.bkl-electronic.de								
Böhm Kabel	www.boehm-kabel.de		•	•	•	•	•	•	•
Brugg Kabel	www.bruggcables.com								
ConCab kabel	www.concab.de		•	•	•	•	•	•	•
Conductix-Wampfler	www.conductix.de				•	•	•	•	
Conrad Electronic	www.conrad.biz		•	•	•	•	•	•	
Contrinex Sensor	www.contrinex.de		•					•	•
Dannewitz	www.dannewitz.de								
DD Kabelkonfektion Dropulic	www.dropulic.de		•		•	•	•	•	•
DigiComm	www.digicomm.de				•	•	•	•	•
Elektrosil	www.elektrosil.com		•	•	•	•	•	•	•
Eltec Technology	www.eltec-gmbh.de		•	•	•	•	•	•	•
Erni Electronics	www.erni.com		•	•	•	•	•	•	•
Ernst & Engbring	www.eue-kabel.de		•	•	•	•	•	•	•
Escha Bauelemente	www.escha.de		•	•	•	•	•	•	•
ESD Electronics	www.esd.eu		•		•	•	•	•	•
Klaus Faber	www.faberkabel.de		•	•			•	•	•
FCT Electronic	www.fct-electronic.de		•		•	•	•	•	•
Festo	www.festo.de		•	•	•	•	•	•	•
Gebauer & Griller Kabelwerke	www.griller.at		•	•	•	•	•	•	•
Gogatec	www.gogatec.com		•		•	•	•	•	•
W.L. Gore & Associates	www.gore.com				•	•	•	•	•
GSN Greates	www.gsn.sg		•	•	•	•	•	•	•
Harting Deutschland	http://ky.to/www.harting.de		•	•	•	•	•	•	•
Helukabel	www.helukabel.com		•	•	•	•	•	•	•
Hradil Spezialkabel	www.hradil.de				•	•	•	•	•
Huber+Suhner	www.hubersuhner.de								
Hummel	www.hummel.com		•	•	•	•	•	•	•
Igus	www.chainflex.de		•	•	•	•	•	•	•
Indu-Sol	www.indu-sol.com		•	•	•	•	•	•	•
Industrieservice Hoppe	www.ish-industrieservice.de								
IPF Electronic	www.ipf.de		•						
Kabeltec	www.kabeltec.de		•	•	•	•	•	•	•
Kabeltronik Arthur Volland	www.kabeltronik.de		•	•	•	•	•	•	•
Lacon Electronic	www.lacon.de		•	•	•	•	•	•	•
U.I.L.app	www.lappkabel.de		•	•	•	•	•	•	•
Laser 2000	www.laser2000.de								
Leoni Fiber Optics	www.leoni-fiber-optics.com								
Leoni Kerpen	www.leoni-industrial-projects.com				•	•	•	•	•
Leoni Special Cables	www.leoni-industrial-solutions.com				•	•	•	•	•
Letronic	www.letronic.de		•	•	•	•	•	•	•
Lumberg Automation, (Belden)	www.lumberg-automation.com		•	•	•	•	•	•	•
Friedrich Lütze	www.luetze.com		•	•	•	•	•	•	•
Meilhaus Electronic	www.meilhaus.de								
Metz Connect	www.metz-connect.com								
MKU Metrofunk Kabel-Union	www.metrofunk.de								
Murrelektronik	www.murrelektronik.com		•	•	•	•	•	•	•
Mütron Müller	www.muatron.de		•	•	•	•	•	•	•
Nexans Deutschland	www.nexans.de		•	•	•	•	•	•	•
Pepperl+Fuchs	www.pepperl-fuchs.com		•	•	•	•	•	•	•
Phoenix Contact Deutschland	www.phoenixcontact.com		•	•	•	•	•	•	•
SAB Bröckskes	www.sab-kabel.de		•	•	•	•	•	•	•
Siemens	www.siemens.com/simatic-net		•	•					
Sommer cable	www.sommercable.com								
Stecker Express	www.stecker-express.de		•	•					
TE Connectivity	www.te.com		•	•	•	•	•	•	•
TKD Kabel	www.tkd-kabel.de		•	•	•	•	•	•	•
Tsubaki Kabelschlepp	www.kabelschlepp.de		•	•	•	•	•	•	•
Turck	www.turck.com		•	•	•	•	•	•	•
UBF EDV Handel und Beratung	www.ubf.de/shop/lwl-kabel.shtml								
Vogtländisches Kabelwerk (VOKA)	www.voka.de		•		•	•	•	•	•
W+P Products	www.wpro.com								
Wago Kontakttechnik	www.wago.com		•		•	•	•	•	•
Weidmüller	www.weidmueller.de		•	•	•	•	•	•	•
Wieland Electric	www.wieland-electric.com		•	•	•	•	•	•	•
Yamaichi Electronics Deutschland	www.yamaichi.eu								





# Cyberangriffe gegen Industrie-steuerungen nach Branchen

**Welche Branche hat in Zeiten der Industrie 4.0 mit den meisten Cyberattacken zu kämpfen? Kaspersky Lab registrierte zumindest in der zweiten Jahreshälfte 2017 überwiegend viele Cyberattacken gegen Organisationen aus den Branchen Energie sowie Maschinenbau und ICS-Integration. Im aktuellen Kaspersky-CERT-Bericht zu Cyberbedrohungen für industrielle Automationssysteme wurden Angriffe analysiert, die sich gegen Automationssysteme und speziell gegen Rechner für industrielle Steuerungssysteme (ICS, Industrial Control Systems) richten.**



*Kaspersky-Analyse: Scada/HMI-Systeme wurden im 2. Halbjahr 2017 am häufigsten von Malware attackiert.*

Mangelnde Cybersicherheit von Industrieanlagen kann zu erheblichen Konsequenzen für Produktion und den Umsatz führen. Die Experten des Kaspersky ICS CERT zeigen in ihrer aktuellen Analyse die derzeitigen Cybergefahren und Trends für industrielle Systeme auf. So wurden 38,7 Prozent der analysierten ICS-Rechner der Energiebranche und 35,3 Prozent der industriellen Rechner in den Bereichen Maschinenbau und ICS-Integration in der zweiten Jahreshälfte 2017 mindestens einmal von Malware angegriffen. Die Baubranche verzeichnete im Vergleich zum ersten Halbjahr den höchsten Anstieg. Hier waren 31,1 Prozent aller ICS-Rechner von einem Angriff betroffen. Automatisierung ist für diese Branche ein noch neues Gebiet und der Cybersicherheit wird damit noch nicht die nötige Aufmerksamkeit gewidmet. In anderen Branchen wie Nahrungsmittel, Bildung, Gesundheitswesen, Telekommunikation, Industriebeteiligungen, Versorgung und Fertigung lag der Anteil bei knapp unter 30 Prozent. Eine große Mehrheit der Angriffe kann dabei als Zufallstreffer gewertet werden. Die Energiebranche ist Vorreiter beim breiten Einsatz von Automatisierungslösungen, und zählt zu den Branchen mit dem höchsten Rechnereinsatz. Moderne Stromnetze gehören zu den ausgedehntesten Systemen miteinander verbundener Industrieanlagen mit vielen Rechnern, die zugleich relativ gefährdet sind. Die Cybersicherheitsvorfälle der vergangenen Jahre sowie verschärfte Auflagen zwingen Strom- und Energiekonzerne zu einer Anpassung der Cybersicherheit ihrer Systeme im Bereich Operative Technologie

(OT). Weitere, ernste Probleme der letzten Jahre wurden hier von Zulieferern verursacht.

## Bemühungen noch nicht ausreichend

„Die Ergebnisse unsere Untersuchung attackierter ICS-Rechner aus verschiedenen Branchen haben uns überrascht. So zeigt z.B. der große Prozentsatz angegriffener ICS-Rechner bei Unternehmen der Strom- und Energiebranche, dass deren Bemühungen um die Cybersicherheit ihrer Automationssysteme nach einigen schweren Vorfällen nicht ausreichen. Noch sind zahlreiche Schlupflöcher offen für Cyberangreifer“, sagt Evgeny Goncharov, Leiter des Kaspersky Lab ICS CERT.

## Krypto-Malware bei Industrierechnern angekommen

Auch ICS-Rechner erfahren seit September 2017 verstärkt Angriffe mit Krypto-Malware. Die Experten von Kaspersky ICS CERT führen dies auf den allgemeinen Trend Hype von Bitcom und Co. zurück. Haben schädliche Mining-Aktivitäten zum heimlichen Schürfen digitaler Währungen auf Rechnern im industriellen Umfeld einen bestimmten Umfang erreicht, hat dies negative Auswirkungen auf die Leistung und Stabilität der ICS-Rechner. Von Februar 2017 bis Januar 2018 griff Mining-Malware 3,3 Prozent aller Rechner zur industriellen Automation an. In den meisten Fällen erfolgten die Attacken rein zufällig.

Weitere Zahlen aus dem aktuellen Kaspersky-Bericht:

- Bei 37,8 Prozent aller ICS-Rechner, die über Kaspersky-Lösungen geschützt waren, wurden Infektionsversuche blockiert (1,4 Prozentpunkte weniger als im Vorjahreszeitraum).
- Das Internet bleibt mit 22,7 Prozent Hauptquelle für ICS-Infektionen. Die Angriffe stiegen gegenüber der ersten Jahreshälfte 2017 um 2,3 Prozent.
- Die Zahl der in der zweiten Jahreshälfte gefundenen Malware-Modifikationen auf ICS-Rechnern stieg von 18.000 auf über 18.900.
- 2017 wurden 10,8 Prozent aller ICS-Rechner von Botnetz-Agenten angegriffen. Die Angriffe erfolgten über das Internet, aber auch über Wechseldatenträger und Emails.
- Die Experten von Kaspersky ICS CERT fanden im Jahr 2017 63mSchwachstellen in Industrie- und IoT-Systemen, von den 26 durch die Hersteller beseitigt wurden.

„Generell verzeichnen wir im Vergleich zum Jahr 2016 einen leichten Rückgang bei den ICS-Angriffen – vermutlich ein Zeichen dafür, dass Unternehmen der ICS-Cybersicherheit mehr Aufmerksamkeit widmen, beispielsweise mittels Mitarbeiterschulungen und von Audits (Überprüfungen) der industriellen Segmente ihrer Netzwerke. Das ist ein gutes Zeichen, denn für Unternehmen ist es von größter Bedeutung, proaktiv Maßnahmen zu ergreifen, mit denen zukünftige Cybervoralleinsätze vermieden werden können“, sagt Evgeny Goncharov.

## Schutzempfehlungen des Kaspersky CERT

- Regelmäßige Updates von Betriebssystem, Anwendungs-Software und Sicherheitslösungen auf allen Systemen, die zum industriellen Netzwerk im Unternehmen gehören.
- Einschränkung des Netzwerk-Verkehrs über Ports und Protokolle auf Edge-Routern und innerhalb des OT-Netzwerks.
- Audits der Zugangskontrollen auf die ICS-Komponenten im industriellen Netz des Unternehmens einschließlich seiner Grenzen.
- Einsatz von Endpoint-Sicherheitslösungen für ICS-Server, Workstations und HMIs, um OT und industrielle Infrastruktur vor zufälligen Cyberangriffen zu schützen.
- Einsatz von Lösungen zum Monitoring des Netzwerkverkehrs sowie zur Analyse und zur Erkennung gezielter Angriffe.



Mehr Informationen zu den Cyberbedrohungen für industrielle Automationssysteme enthält der aktuelle Kaspersky-Bericht. ■

Kaspersky Labs GmbH  
www.kaspersky.de

# Compliance im Multi-Cloud-Zeitalter

**Die Multi-Cloud ist heute Realität. Dazu kommt, dass Public Clouds grundsätzlich weltweit verteilt sind. Dies führt zu neuen Herausforderungen bei Compliance und Datenschutz. Denn hier sind oft nationale Regeln zu berücksichtigen.**

Viele Cloud Service Provider (CSP) erfüllen inzwischen die verschiedenen Compliance-Regeln durch eigene Rechenzentren, die sich im jeweiligen Rechtsraum – etwa der EU – befinden. Damit ist für die Kunden jedoch nur ein Teil der Aufgaben erledigt. Denn sie müssen sich trotzdem um die Einhaltung der Richtlinien bemühen, die sie selbst betreffen. Dies gilt insbesondere für den Nachweis, wo welche personenbezogenen Daten gespeichert sind. Daher müssen Unternehmen sämtliche Daten analysieren, die sie in die Cloud übertragen wollen. Eventuell müssen einige hochvertrauliche Daten im eigenen Rechenzentrum bleiben.

## Umfassende Compliance

Häufig übersehen wird die Tatsache, dass personenbezogene Daten nicht nur in der Produktivphase zu schützen sind, sondern auch während der Design-, Entwicklungs-, Implementierungs- und Testphase. Durch eine Referenzarchitektur lässt sich erkennen, wo Compliance-Anforderungen anzuwenden sind. Unternehmen sollten einen erfahrenen Partner einbinden, der mit den verschiede-



nen Compliance-Anforderungen und Vorschriften vertraut ist. Ein solcher Managed Service Provider (MSP) stellt sicher, dass das Unternehmen sowohl bei der Architektur der Umgebung regelkonform ist als auch die Cloud-Sicherheitskontrollen konsequent implementiert und durchsetzt.

## Fazit

Compliance kann eine große Hürde für die Cloud-Nutzung darstellen. Eine Zusammenarbeit mit einem MSP hilft, die zahlreichen Vorschriften und Anforderungen zu erfüllen. ■

RackSpace Germany GmbH  
www.rackspace.com/de



Bild: Microsoft Deutschland GmbH

Security Intelligence Report Interactive Highlights (Beta)

## Hacker bevorzugen einfache Angriffsmöglichkeiten wie Phishing

**Nur drei Prozent der Cyber-Angriffe erfolgen heute über das Umgehen von Sicherheitsmaßnahmen, etwa über Trojaner. Das geht aus Microsofts aktuellem Security Intelligence Report (SIR) hervor. Er zeigt, dass Angreifer zunehmend nach einfachen Wegen für ihre Angriffe auf IT-Infrastrukturen, Firmennetze und Rechner suchen.**

Dasu gehört das Social Engineering: Hacker versuchen Zugang zu vertraulichen Daten, Geräten oder Netzwerken über den persönlichen Kontakt zu bekommen. Erfolgt diese Manipulation per Email oder Telefon spricht man vom Phishing. Phishing war im zweiten Halbjahr 2017 die häufigste Bedrohung in der Email-Kommunikation über Office 365 mit einem Anteil von mehr als 50 Prozent. Aufwändigere Methoden wie das Umgehen von Sicherheitsmaßnahmen, etwa über Trojaner, fallen dagegen mit nur drei Prozent Anteil weniger ins Gewicht.

Die wichtigsten Erkenntnisse des Reports:

- Phishing hat in der zweiten Jahreshälfte 2017 die größte Bedrohung für die E-Mail-Kommunikation über Office 365 dargestellt. Ebenso sind schlecht gesicherte Cloud-Apps ein einfaches Ziel für Angreifer: Bei 79 Prozent der SaaS-Speicher-Applikationen und bei 86 Prozent der SaaS-Kollaborations-Anwendungen werden Daten während der Übertragung und im Ruhezustand nicht verschlüsselt.
- Automatisierte Schadprogramme wie Botnets bedrohen nach wie vor Millionen von Rechnern weltweit. Die Programme ermöglichen es den Angreifern, Computer mit Malware zu infizieren. Cyberkriminelle nutzen Botnets mit dem Ziel, Infrastrukturen aus infizierten Rechnern aufzubauen, über die sie sensible Daten auspähen und erpressen können.
- Ransomware hat im Jahr 2017 verschiedene Netzwerke attackiert und ist weiterhin eine Gefahr. Bei dieser Methode versuchen Cyberkriminelle Rechner, Geräte oder Dateien zu sperren, um ihre Opfer anschließend zu erpressen. Zur Familie der Ransomware gehören WannaCrypt, Petya/NotPetya und BadRabbit.

„Der Security Intelligence Report zeigt einmal mehr den Wert intelligenter und integrierter Sicherheitsmechanismen“, sagt Michael Kranawetter, National Security Officer bei Microsoft Deutschland. „Moderne Schutzmaßnahmen wie biometrische Multifaktor-Authentifizierung oder cloudbasierte Security Intelligence Lösungen wie Windows Defender Advanced Threat Protection (ATP) oder Azure Security Center bieten Unternehmen konkrete Werkzeuge für ihre Sicherheitsverwaltung.“ Der Report basiert auf zwischen Februar 2017 und Januar 2018 erhobenen Daten aus Unternehmensnetzwerken und Cloud-Diensten, darunter Windows, Bing, Office 365 und Azure. Für seine Analysen scannt Microsoft monatlich rund 400 Milliarden Emails, verarbeitet 450 Milliarden Authentifizierungen und analysiert rund 18 Milliarden Webseiten sowie mehr als 1,2 Milliarden Geräte nach potenziellen Bedrohungen und Angriffsversuchen. Bei der Auswertung werden nur solche Computer berücksichtigt, die Sicherheitslösungen von Microsoft zur Echtzeitüberwachung nutzen und deren Administratoren oder Benutzer sich für die Bereitstellung von Daten an Microsoft einverstanden erklärt haben. Zu jedem der im SIR beschriebenen Bedrohungsszenarien liefert der Report auch Tipps und Hinweise, wie man sich vor solchen Angriffen schützen kann und welche Microsoft-Technologien sowie Sicherheitsprodukte von Microsoft-Partnern dabei helfen. ■



## IT-Experte Andreas Schlechter: Produktionsrechner und -anlagen sind Sicherheitsrisiko



Bild: Telonic GmbH

Geschäftsführer Andreas Schlechter von Telonic

# VDMA bestätigt: Maschinenbau ist nicht Hacker-Ready

**Die vor allem mittelständisch geprägte Maschinenbauindustrie in Deutschland ist nicht ausreichend auf Cyberkriminalität vorbereitet – weder auf den Angriff, noch auf die Folgen. Zu dem Ergebnis kommt eine Studie des VDMA, dem mit 3.200 Mitgliedern größten Verband der Unternehmen des Maschinenbaus in Deutschland und Europa.**

**K**napp die Hälfte der Unternehmen arbeitet laut VDMA mit einem veralteten Schutz vor Angriffen aus dem Netz. In der Praxis sind vor allem Rechner in Produktionsanlagen reich an Risiken: „Betriebsrechner in Industrieanlagen sind häufig mit älteren Betriebssystemen wie Windows XP ausgestattet und erfüllen damit nicht die aktuellen Sicherheitsrichtlinien. In den Betrieben werden Fertigungsanlagen wesentlich weniger auf Cyberattacken überwacht, als die Rechner der Mitarbeiter“, sagt Andreas Schlechter, Geschäftsführer von Telonic. Das Kölner Systemhaus implementiert proaktive Sicherheitslösungen für IT-Netze und setzt umfangreiche drahtlose sowie drahtgebundene Netzwerke um.

### Millionenschäden zu erwarten

Befürchtet werden Betriebsunterbrechungen, die neben Ausfällen auch für Reputationsschäden sorgen. Ein Produktionsstopp kann die Auslieferung an Kunden verzögern. Den möglichen Schaden durch Cyber-Attacken schätzen die durch den VDMA befragten Firmen mehrheitlich in Bereichen zwischen 500.000 bis 1 Mio.€ ein. Bei mittelständischen Unternehmen kann das auch existenziell bedrohlich werden. „Pleite durch Hacker – das darf nicht passieren. Das mangelnde Bewusstsein für Sicherheitslücken werden Hacker ausnutzen. Daher gilt es, Schutzmechanismen zu implementieren. Ansonsten wird die Industrie 4.0 zur größten Gefahr für alle Unternehmen“, er-

klärt Telonic-Geschäftsführer Andreas Schlechter. Sein Unternehmen betreut mit mehr als 120 Mitarbeitern Kunden aus dem Mittelstand sowie der Konzernwelt und setzt dazu innovative Technologien zur Überwachung eines Netzwerks auf verdächtige Aktivitäten ein.

### Nicht einmal versichert

Die deutliche Mehrheit (88 Prozent) der vom VDMA befragten Unternehmen ist nicht einmal gegen die möglichen Auswirkungen einer Cyber-Attacke versichert. Insgesamt wurden 244 Firmen mit einem Umsatz von bis zu 75Mio.€ jährlich durch den VDMA und seine Tochter VSMA befragt. Der geschützte Datenaustausch in Produktionsbereichen ist derweil nicht so einfach umzusetzen wie die eines Client-PCs in der Verwaltung. Verantwortlich dafür sind Altsysteme, die sich nicht mehr updaten lassen, aber auch vorhandene Fernwartungsschnittstellen, die herstellenseitig benötigt werden. In diesen Fällen müsse dringend am Schutz des gesamten Netzwerkes gearbeitet werden, so Andreas Schlechter. ■

### Die Telonic GmbH

Die Telonic GmbH ist ein Systemhaus für Netzwerk und Security. Seit der Gründung 1979 ist das Unternehmen in Familienbesitz und betreut Kunden in zahlreichen Branchen - von Verwaltung, Industrie und Logistik über Bank- und Finanzwesen bis zu Konzernen aus der Energieversorgung. Durch den klaren Fokus auf Netzwerk- und IT-Sicherheitslösungen verfügt Telonic über zahlreiche Best Practice-Erfahrungen und agiert als Systemintegrator für führende Soft- und Hardwarehersteller. Neben der herstellerunabhängigen Analyse realisiert Telonic die Projekte und sorgt auch für die laufende Betreuung und anfallende Schulungsmaßnahmen. Mehr als 120 Mitarbeiter stehen dazu bundesweit den Kunden zur Verfügung.

Telonic GmbH  
www.telonic.de

**Neue McAfee-Umfrage zeigt den Stand aktueller Cyber-Sicherheit auf und empfiehlt organisatorische Strategien, um Cyber-Bedrohungen entgegenzuwirken**

# Verbesserte Automatisierung und Einsatz von 'Gamification'

**Das Sicherheitsunternehmen McAfee veröffentlicht im April den neuen Bericht 'Winning the Game', der die wichtigsten Herausforderungen für IT-Sicherheitsunternehmen hinsichtlich aktueller Bedrohungen untersucht. Eine Umfrage (siehe Kasten 'Methodik') ergab, dass Automatisierung in Security Operations Centern (SOC) und 'Gamification' am Arbeitsplatz entscheidend sind, um Cyber-Kriminelle in ihrem eigenen Spiel zu schlagen. Ist dies auch eine Möglichkeit für Bedrohungen in der Produktion? Machen wir uns ein Bild über diesen aktuellen Trend in der Bekämpfung von Cyberangriffen ...**

Für Grant Bourzikas, Chief Information Security Officer bei McAfee ist die Überforderung der Anwender eines der größten Einfallstore für Cyberangriffe: „Da Cyber-Sicherheitsverletzungen mittlerweile die Norm für Unternehmen sind, müssen wir einen Arbeitsplatz schaffen, der es den Cyber-Sicherheitsbeauftragten ermöglicht, ihr Bestes zu leisten. Es ist unerlässlich die Mitarbeiter am Arbeitsplatz zufriedenzustellen, um sicherzustellen, dass Unternehmen die Komplexität in dem ohnehin schon hochgesteckten Spiel gegen Cyber-Kriminalität nicht noch weiter erhöhen.“

## Automatisierung

Durch die Verknüpfung menschlicher Intelligenz mit automatisierten Aufgaben, dem sogenannten Human-Machine-Teaming, können automatisierte Programme grundlegende Sicherheitsprotokolle handhaben, während die IT-Spezialisten Bedrohungen proaktiv bewältigen können. Hier einige der Ergebnisse der Umfrage:

- 81 Prozent der Befragten glauben, dass die Cyber-Sicherheit ihres Unternehmens durch mehr Automatisierung sicherer wäre.
- Ein Viertel gibt an, dass Automatisierung Zeit für Innovationen und Mehrwertarbeit schafft.

### Methodik

McAfee beauftragte den Marktforscher Vanson Bourne mit der Befragung von 300 Senior Security Managern und 650 Sicherheitsexperten in öffentlichen und privaten Organisationen mit mindestens 500 Mitarbeitern in den USA, Großbritannien, Deutschland, Frankreich, Singapur, Australien und Japan. Ziel der Untersuchung war es, einen Einblick in die wichtigsten Herausforderungen zu gewinnen, denen sich IT-Sicherheitsorganisationen in Bezug auf Bedrohungen, Technologieinvestitionen und Fähigkeiten gegenübersehen, und die Strategien und Techniken zu identifizieren, mit denen sie sich durchsetzen können.

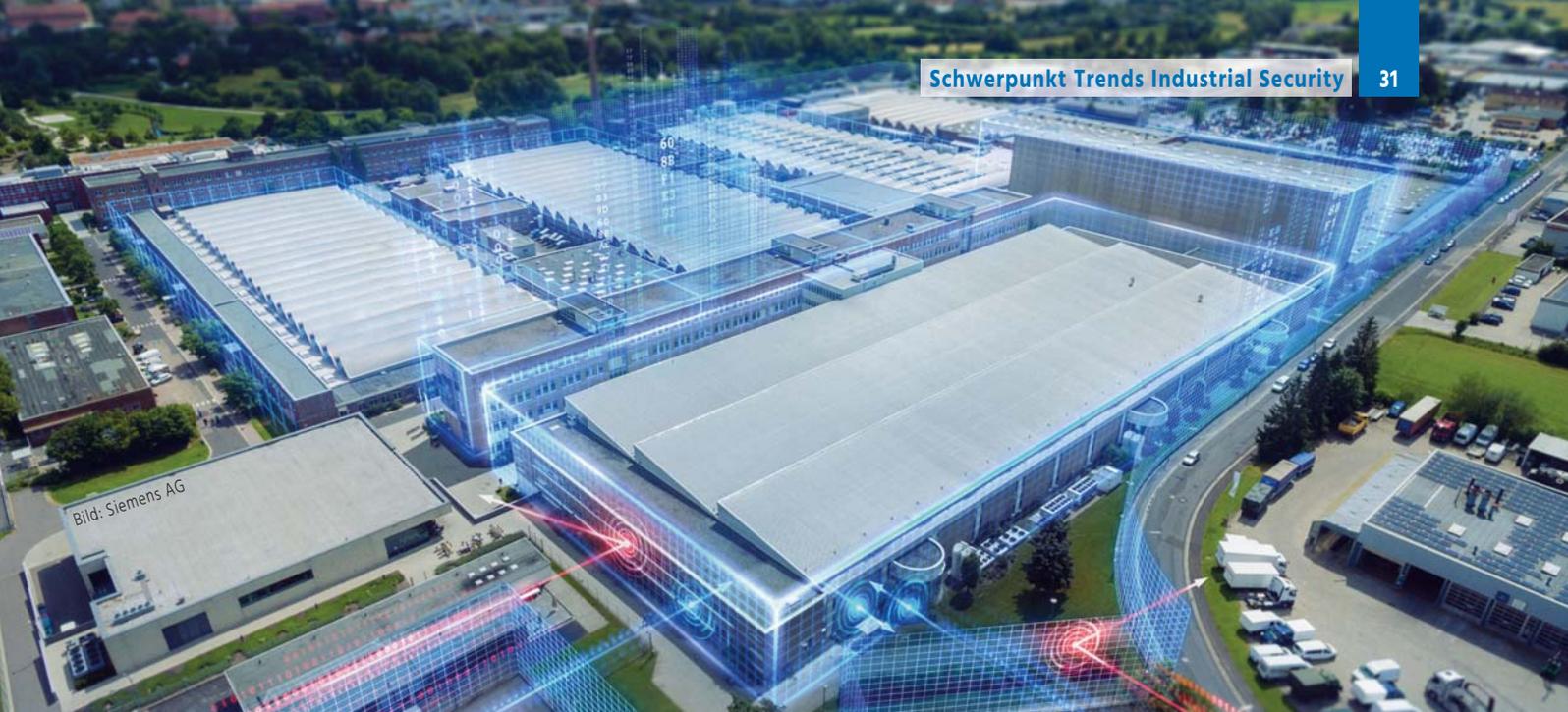
- Fast ein Drittel (32 Prozent) derjenigen, die nicht in Automatisierung investieren, geben an, dass dies auf fehlende interne Möglichkeiten zurückzuführen ist.

## Gamification

Gamification, ein Konzept, bei dem spieltypische Elemente und Prozesse in spielfremden Kontext angewandt werden, gewinnt als Werkzeug zur Förderung einer leistungsfähigeren Cyber-Sicherheitsorganisation zunehmend an Bedeutung. In vielen Organisationen werden bereits entsprechende 'Spielübungen' durchgeführt. Ganze 96 Prozent derjenigen, die Gaming am Arbeitsplatz einsetzen, berichten ausschließlich von Vorteilen. Mehr als die Hälfte (57 Prozent) erkennen einen Zusammenhang zwischen dem Einsatz von Gaming und erhöhter Konzentration der IT-Mitarbeiter. 43 Prozent erkennen an, dass das Gaming eine Teamwork-Kultur erschafft, die für ein effektives Cyber-Sicherheitsteam erforderlich ist.

## Die nächste Generation von Cyber-Bedrohungsjägern

Die Ergebnisse des Berichts deuten darauf hin, dass Gamer dem Fachkräftemangel im Bereich Cyber-Sicherheit entgegenwirken können. 92 Prozent der Befragten glauben, dass Gamer durch das Spielen Fähigkeiten entwickeln, die für die Jagd auf Cyber-Sicherheitsbedrohungen entscheidend sind: Logik, Ausdauer, ein Verständnis der Gegner und eine neue Perspektive im Vergleich zu traditionellen Cyber-Sicherheitseinstellungen. Drei Viertel der Führungskräfte sagen, dass sie es in Betracht ziehen würden, einen Gamer einzustellen auch wenn keine Erfahrung im Cyber-Sicherheitsbereich vorliegt. Mehr als drei Viertel der Befragten geben an, dass die Generation, die mit Videospiele aufgewachsen ist, stärkere Kandidaten im Bereich Cyber-Sicherheit sind als herkömmliche Mitarbeiter. ■



Siemens stellt auf der Hannover Messe 2018 eine Lösung zur Anomalieerkennung in industriellen Netzwerken vor. Mit 'Industrial Anomaly Detection' lassen sich sicherheitsrelevante Vorfälle wie unerlaubtes Eindringen oder Schadsoftware erkennen und darauf aufbauend Gegenmaßnahmen ergreifen.

# Siemens Industrieanlagenschutz mit Firewalls von Palo Alto Networks

**Siemens kooperiert mit dem IT-Security-Unternehmen Palo Alto Networks, um den Schutz von Industrieunternehmen vor Cyber-Attacken zu erhöhen. Hierfür wird Siemens die Next Generation Firewalls von Palo Alto Networks bei Unternehmen der Fertigungs- und Prozessindustrie einsetzen. Sie sollen die zunehmend komplexen Schnittstellen zwischen Büro- und Automatisierungnetzwerken auf einem hohen Sicherheitsniveau absichern. Die Kunden können aus einer Vielzahl an Schutzstufen auswählen und diese entsprechend ihren Anforderungen einstellen. Die Firewalls ergänzen die Industrial Security Appliances Scalance S von Siemens, die für den Schutz von Geräten und Netzwerksegmenten eingesetzt werden.**

Im Zuge der wachsenden Digitalisierung sind Industrieunternehmen zunehmend mit komplexen und ausgefeilten Sicherheitsbedrohungen konfrontiert. Sie müssen daher in der Lage sein, überholte Netzwerkstrukturen zu erneuern und industrielle Umgebungen abzusichern, um die Transparenz zu erhöhen, Produktionsprozesse nachhaltig abzusichern und Wachstum zu ermöglichen. Aufgrund unterschiedlicher Netzwerkstrukturen und Applikationen variieren die Sicherheitsanforderungen je nach Branche stark. Im Rahmen seiner Industrial Security Services bietet Siemens hierfür die Firewalls von Palo Alto Networks. Damit lässt sich die Angriffsfläche und das Risiko zufälliger, unbeabsichtigter Security-Vorfälle reduzieren – etwa durch Netzwerksegmentierung oder eine rollenbasierte Zugriffskontrolle, bei der gemäß IEC62443-Standard die Zugriffsrechte von Benutzern und Prozessen bedarfsgerecht reduziert werden. Zudem ermöglichen die Firewalls einen gesicherten Zugang für die Mitarbeiter eines Unternehmens sowie dessen Lieferanten und Partner. Angesichts zunehmend ausgefeilter Bedrohungen für Kontrollsysteme (Industrial Control Systems/ICS bzw. Supervisory Control and Data Acquisition/SCADA) können Nutzer so auch von den inhärenten Schutzfunktionen der Firewalls und den Security Services profitieren, um bekannten und unbekanntem Bedrohungen zu begegnen.

## Industrial Security Services

Die Siemens Industrial Security Services Dienstleistungen für die Sicherheit von Industrieanlagen gemäß dem Standard IEC62443. Sowohl Kunden mit Siemens-Komponenten wie auch mit einer Ausstattung von Drittanbietern können diese Dienste in Anspruch nehmen, die von einem Schutzkonzept auf mehreren Ebenen ausgehen: Dieses umfasst die Anlagenbestandserfassung und -verfolgung, das Erkennen und Schließen von Sicherheitslücken, Netzwerk-Segmentierung, Sicherheitsmanagement für Industrieanlagen, Bewältigung von Sicherheitsvorfällen (Incident Handling) und weitere Beratungsleistungen in Sicherheitsfragen. Siemens verfügt auch über ein umfassendes Product Computer Emergency Response Team (ProductCERT) - ein Notfall-Reaktionsteam für Produkte und Computer - für Siemens-Lösungen. ■

# Bessere Verteidigung gegen industrielle Schadsoftware

## **Spezialisierte Ransomware bedroht zunehmend industrielle Steuerungssysteme**

**Seit der Entdeckung von Stuxnet im Jahr 2010 gab es bei industrieller Schadsoftware einige evolutionäre technologische Sprünge, aber auch massive Schäden sowohl bei Unternehmen als auch bei staatlichen Einrichtungen. Malware für ICS (Industriesteuerungen) ist nicht mehr länger eine Waffe, die nur Insidern zur Verfügung steht und die lediglich zur Wirtschaftsspionage genutzt wird.**

An aktuellen Beispielen wie LogicLocker (Ransomware), Industroyer aber auch Trisis (Triton/Hatman) lässt sich ablesen, dass Angreifer heute auch Wirtschaftssabotage im Sinn haben. Unterstützt wird die These von den zurückliegenden Vorfällen rund um das ukrainische Stromnetz Mitte Dezember 2015. Leider sind diese Angriffe immer erfolgreicher, was nicht nur daran liegt, dass sie immer ausgefeilter und zielgerichteter erfolgen, sondern auch, weil viele Hersteller und Unternehmen es versäumen in die Sicherheit der Systeme zu investieren.

### Sabotage-Malware – ein aktueller Überblick

Am Anfang stand eine Software, die dafür entwickelt wurde, die Urananreicherung in Zentrifugen zu sabotieren. Mit Stuxnet wurde für die Welt der Industriesteuerung im Grunde genommen die Büchse der Pandora geöffnet. Wie einschneidend dieses Ereignis für die Branche war, ist daran erkennbar, dass alle nachfolgenden Bedrohungen mit Stuxnet verglichen werden. Die Malware zeigte, dass Automatisierungssysteme ähnlich durch Softwaremanipulationen gefährdet sein können wie IT-Systeme. Eine direkte Konsequenz war, dass nach dem Aufdecken von Stuxnet, Sicherheitsexperten auf der ganzen Welt begannen, gezielt nach Schwachstellen in Industriesoftware zu suchen. Die Schwachstellenmeldungen stiegen daraufhin sprunghaft an. Eine beliebte Quelle, die auf unsichere, direkt am Internet betriebene Industriesysteme hinweist, ist noch heute die Webseite <https://www.shodan.io/explore/category/industrial-control-systems>. Die erste Ransomware, die nachweislich auch Industriesteuerungen in Geiselschaft nehmen kann, ist LogicLocker. Diese wurde als Proof-of-Concept entwickelt und ist bisher noch nicht im Feld aufgetaucht, deshalb ist es schwer zu sagen, wie gefährlich diese Bedrohung wirklich ist.

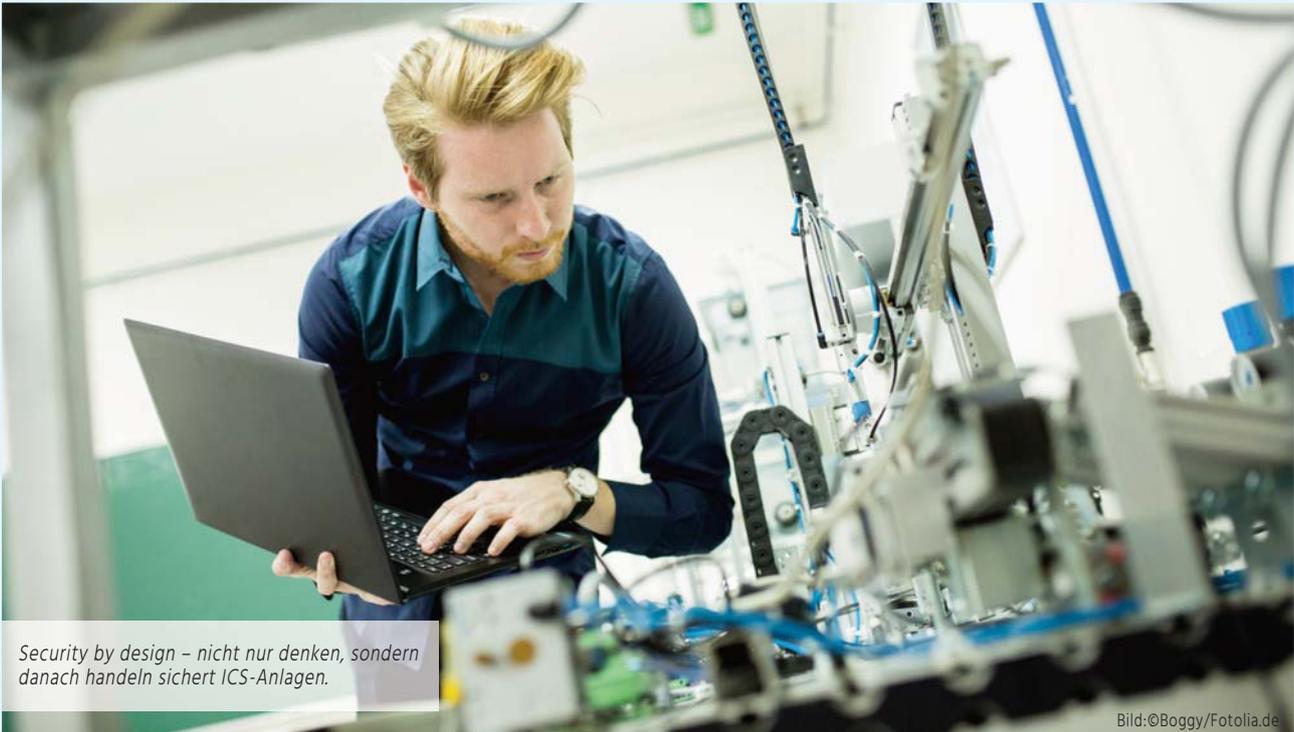
### Industroyer

Anders verhält es sich mit Industroyer. Die Schadsoftware löscht alle Registry-Keys, die mit bestimmten System-Services in Verbindung stehen, überschreibt bestimmte ICS-Konfigurationsdateien auf den Festplatten und manipuliert Daten auf Netzwerklaufwerken, die mit einer bestimmten Controller-Software

in Verbindung stehen. Darüber hinaus werden auch gewöhnliche Windowsdaten überschrieben. Die Schadsoftware war auch in der Lage eine Konfigurationsdatei auszulesen, stoppte alle Master-Prozesse eines Energieautomatisierungssystems auf dem Host des Opfers, tarnte sich als neuer Master und löste autonom vier Arten von Schalthandlungen aus. Sie scheint außerdem für den Stromausfall in der Ukraine verantwortlich zu sein, Angriffe mit dieser Software auf Stromnetze in Deutschland sind ebenfalls prinzipiell denkbar, da die gleiche IEC-Protokollfamilie auch von deutschen EVUs eingesetzt wird. Bislang zielt sie primär auf kritische Energieinfrastrukturen, sie wurde jedoch auch in anderen Infrastrukturen entdeckt. Triton/Trisis/Hatman stehen für ein und dieselbe Malware, die Ende 2017 auf einem SIS (Safety Instrumented System)-Controller gefunden wurde. Sie modifiziert mit einem py2exe kompilierten Python Script den Speicher der Anwendung auf dem Controller. Allerdings kann das Script noch deutlich mehr. Die erste bekannt gewordene Infektion trat auf einem Windows-PC auf, der mit einem SIS-Gerät verbunden war und die daraufhin das Verhalten des Geräts veränderte. Die Spuren, die dabei hinterlassen werden, können von der Malware wieder gelöscht werden, sodass eine forensische Untersuchung nach der Entdeckung sehr schwierig ist. Wirklich bemerkenswert ist jedoch, dass die Schadsoftware nicht nach Schwachstellen im SIS selbst sucht, sondern sich das Design der Netzwerkarchitektur zunutze macht, um den Angreifern die Möglichkeit zu geben, die Befehle direkt an die Controller zu senden. Das vermutliche Ziel dieser Malware war die kritischen Betriebszustände des primären Automatisierungssystems zu erzeugen und dann zu unterbinden, sodass das Safety System (SIS) das Eintreten dieser Betriebszustände verhindert.

### Ansatz: Professioneller Umgang mit Schwachstellen

Die Werkzeuge, mit denen Sicherheitsforscher und Hacker gegenüber Industriesystemen auftreten, sind ebenfalls umfangreicher geworden. Viele Programme zur Netzwerkprüfung inkludieren zumindest Module, die Industriesteuerungen am Netzwerk als solche identifizieren und nicht mehr als unbekannte Geräte klassifizieren. Für gängige Hacking-Werkzeuge wie das Metasploit-Framework existieren durchaus auch of-



*Security by design – nicht nur denken, sondern danach handeln sichert ICS-Anlagen.*

Bild: ©Boggy/Fotolia.de

fensivere Funktionen: Befehle zum Stoppen und Starten von speicherprogrammierenden Steuerungen (SPS) werden nachgebildet oder spezifische Angriffe auf Implementierungsschwachstellen bereitgestellt. Automatisierungshersteller haben bereits begonnen, professioneller mit Sicherheitschwachstellen umzugehen. Die meisten Automatisierungshersteller haben nun endlich die ersten Gehversuche im Umgang mit Sicherheitsschwachstellen hinter sich, in vielen Fällen ist daraus eine eigene Sicherheitsorganisation entstanden. Mitunter ist sogar ein eigenes Geschäftsfeld entwickelt worden, in dem Anlagenbetreibern Zusatzdienste wie Patch- und Update-Management, Risikoanalysen oder der Aufbau von Sicherheitskonzepten angeboten werden. Ein großes Problem liegt weiterhin im Bereich Security Know-how in der Industrie. Die Industrie als Ganzes muss nun lernen, mit Security umzugehen. Security war bisher kein Kernthema der Industrieunternehmen, und wenn dann typischerweise eher den IT-Abteilungen oder –Unternehmen zugeordnet. Durch Industrie 4.0 und eine noch stärkere Durchdringung von Software in Industrieanlagen sowie die stärkere Vernetzung muss Security aber ebenso gut umgesetzt werden. Dies ist nur möglich, wenn das Industriepersonal auch mit dem richtigen Security Know-how ausgestattet ist. Spezialisierte Schulungen und Zertifizierungen zum Thema Industrial Security sind ebenfalls erst in den letzten zwei bis drei Jahren nach Stuxnet entstanden. Besonders hervorzuheben ist beispielsweise die Zertifizierung GIAC Global Industrial Cyber Security Professional (GICSP), für die in Zusammenarbeit mit dem SANS Institute ein Training entwickelt wurde, um Anlagen- und Industrietechniker besser auf Security-Fragestellungen vorzubereiten und IT-Sicherheitsexperten in die Welt der ICS einzuführen. Wichtig ist, dass beide Seiten die gleiche Sprache sprechen und Lösungsansätze zusammen entwickeln, um die Systeme besser zu schützen.

## Fazit

Die größte Herausforderung bleibt weiter bestehen: Auch wenn Hersteller begonnen haben, Konzepte wie Security by Design in neue Produkte zu integrieren, läuft der größte Teil von Industrieanlagen noch immer mit der älteren 'Legacy'-Technologie nach dem Motto 'Never Change a Running System' (auch bei Updates nicht) und damit eher spärlichem Sicherheitsdesign. Es liegt also in der Verantwortung der Systemintegratoren und Anlagenbetreiber, die Security von bestehenden Anlagen zu verbessern, indem bei entsprechenden Wartungsfenstern auch Sicherheitsmechanismen nachgerüstet werden. Welche Maßnahmen hier am effektivsten für die jeweilige Anlage sind, sollte mit ausreichender Vorbereitung gemeinsam mit internen oder externen Fachleuten in einer Risiko- oder Schwachstellenanalyse geklärt werden. Denn leider belegen die eingangs aufgeführten Bedrohungen, dass sie sich stetig vermehren und immer mehr Angreifer ihre Zeit auf die Weiterentwicklung aufwenden. ICS zu manipulieren, zu sabotieren oder aber in Geiselschaft zu nehmen, bleibt für Angreifer ein lohnenswertes Ziel. ■

**Autor:** Prof. Thomas Brandstetter,  
Trainer beim SANS Institute und Senior Security Consultant,  
Limes Security GmbH  
[www.limesecurity.com/de](http://www.limesecurity.com/de)

# Wie können Industrieunternehmen ihre IT-Angriffsfläche erkennen und verringern?

**Während sich Assets stetig weiterentwickelten, veränderten sich traditionelle Tools, wie Antivirenprogramme, kaum. Sie decken nach wie vor nur Server, Desktops und Netzwerkinfrastrukturen ab. Doch um die gesamte Angriffsfläche zu erkennen, ist ein neuer, umfassender Ansatz nötig. Um diesen zu beschreiben, hat sich der Begriff Cyber Exposure etabliert. Cyber Exposure konzentriert sich darauf, wo Schwachstellen bestehen und wie diese reduziert werden können. Tenable erklärt, welche Schritte beim Umgang mit Cyber Exposure wichtig sind.**



Bild: Tenable Network Security

Die Digitalisierung im Arbeitsleben erlaubt effiziente Arbeitsmethoden und ein flexibles Geschäftsleben. Auch in Industrieunternehmen gibt es eine Vielzahl an neuen, smarten Geräten im Unternehmensnetz, Web- und Cloud-Applikationen. Hinzu kommt die zunehmende Vernetzung von Industrie- und Steueranlagen, um Vorgänge zu flexibilisieren und optimieren. Doch stellt sich zugleich die Frage, wie Unternehmen diese Automatisierungsumgebungen und Industrieanlagen sowie Kritis sichern können. Denn die Kehrseite der Medaille sind neue Angriffsflächen für Hacker. Die Antwort: Es ist nötig, sämtliche Geräte im Netz zu identifizieren, alle Schwachstellen zu kennen und möglichst durchgängig zu scannen, um Verwundbarkeiten so schnell wie möglich zu entdecken. Unternehmen müssen ihre gesamte IT-Angriffsfläche kennen.

## Entdecken

IT-Verantwortliche können nur die Geräte und Assets im Netzwerk schützen, die sie auch kennen. Deshalb gilt als höchste Priorität, sämtliche Assets umgehend zu identifizieren – in IT, Cloud, IoT (Internet of Things) und OT (Operational Technology).

## Bewerten

Auch Industrieunternehmen müssen den Zustand aller Assets bewerten können: Welche Schwachstellen gibt es? Wo bestehen Fehlkonfigurationen? Welche Indikatoren für Probleme in den Systemen gibt es?

## Analysieren

Schwachstellen müssen im Kontext analysiert werden, nach Schwere der Schwachstelle, dem Bedrohungskontext und der Relevanz des betroffenen Assets: Wo ist das Unternehmensnetzwerk anfällig, welche Schwachstellen sollten aufgrund des geschäftlichen Risikos priorisiert werden, welche sind zunächst weniger wichtig?

## Beheben

Sind die Schwachstellen nach Dringlichkeit priorisiert, müssen die Wichtigsten zuerst behoben werden – mit der jeweils richtigen Technik.

## Erfassen

Letzter Schritt ist eine wichtige Aufgabe für die IT-Verantwortlichen: Die Cyber Exposure muss geformt und analysiert werden, um bessere geschäftliche und technologische Entscheidungen treffen zu können. Die durch die Digitale Transformation ausgelöste Beschleunigung mündet zwangsläufig in neuen Sicherheits Herausforderungen, die nach modernen Strategien verlangen. Nur wenn Verantwortliche die Schwachstellenproblematik systematisch angehen und sich ihrer Cyber Exposure bewusst sind, können sie ihre gesamte Angriffsfläche identifizieren und verringern. ■

# IT- und Netzwerksicherheit

**Ohne Security wird Industrie 4.0 nicht erfolgreich werden können. Nur wenn sich Betreiber von Produktionsanlagen darauf verlassen können, dass ihre Daten und Assets sicher geschützt sind, werden sie auch die Digitalisierung weiter vorantreiben.**

**O**bwohl immer häufiger Angriffe erfolgreich sind, die den Menschen als Schwachstelle ausnutzen, dürfen technische Security-Maßnahmen nicht vernachlässigt werden. Unternehmen haben also zwei wichtige Aufgabenfelder: Einerseits immer wieder die Aufmerksamkeit der Mitarbeiter für Security im Unternehmen zu schärfen und gleichzeitig die technische Security-Infrastruktur auf dem Laufenden zu halten. Das macht eines deutlich: Sicherheit ist kein Zustand sondern eine permanente Aufgabe. ■



Industrial IT

ads-tec GmbH  
72622 Nürtingen | Tel: +49 7022 2522-0  
sales@ads-tec.de  
www.ads-tec.de



## Big-LinX® IoT-Service-Plattform Die sichere Basis für Industrie 4.0

Sichere Kommunikation im Internet of Things (IoT) mit Big-LinX – der professionellen IoT-Service-Plattform von ADS-TEC für eine weltweite Vernetzung von Maschinen und Anlagen.

ADS-TEC Firewalls der IRF2000 Serie schützen alle Ihre Produktionsumgebungen. Maximale Authentifizierungssicherheit durch Smartcards und Servicefreigabe durch den Kunden.

- Connectivity
- Device Management
- Condition Monitoring
- Fernwartung
- Dokumentationsablage für jedes Endgerät

Erfahren Sie mehr unter  
[www.ads-tec.de](http://www.ads-tec.de)



MPL AG Elektronikunternehmen  
CH-5405 Dättwil | Tel.:+41 56 483 34 34  
info@mpl.ch  
www.mpl.ch

## Rugged Industrial Ethernet Firewall, Router, Switch, Embedded Computers



100% in der Schweiz entworfen und hergestellt

### Highlights

- 10 Jahre Verfügbarkeit
- Mehr als 20 Jahre reparierbar
- Openframe bis IP67-Gehäuse
- OEM / kundenspez. Lösungen

### Features

- managed & unmanaged Switch
- Media Converter
- Firewall / Router
- -40°C to +85°C



Siemens AG  
Process Industries and Drives  
Process Automation  
[www.siemens.de/scalance-s](http://www.siemens.de/scalance-s)



## Digitale Schutzengel für industrielle Kommunikationsnetzwerke

### SCALANCE S

Kennen Sie wirklich alle Gefahren, die im Netzwerk lauern und Ihr industrielles Kommunikationsnetzwerk bedrohen?

Die digitalen Schutzengel von Siemens schon: Industrial Security Appliances SCALANCE S!

Sie sorgen für Sicherheit auf der industriellen Zellebene und sind ein entscheidender Baustein von Defense in Depth – dem tiefengestaffelten Industrial Security-Konzept – basierend auf den Empfehlungen der IEC 62443.

Verstärken Sie Ihre Netzwerksicherheit mit Industrial Security Appliances SCALANCE S!



[siemens.de/scalance-s](http://siemens.de/scalance-s)

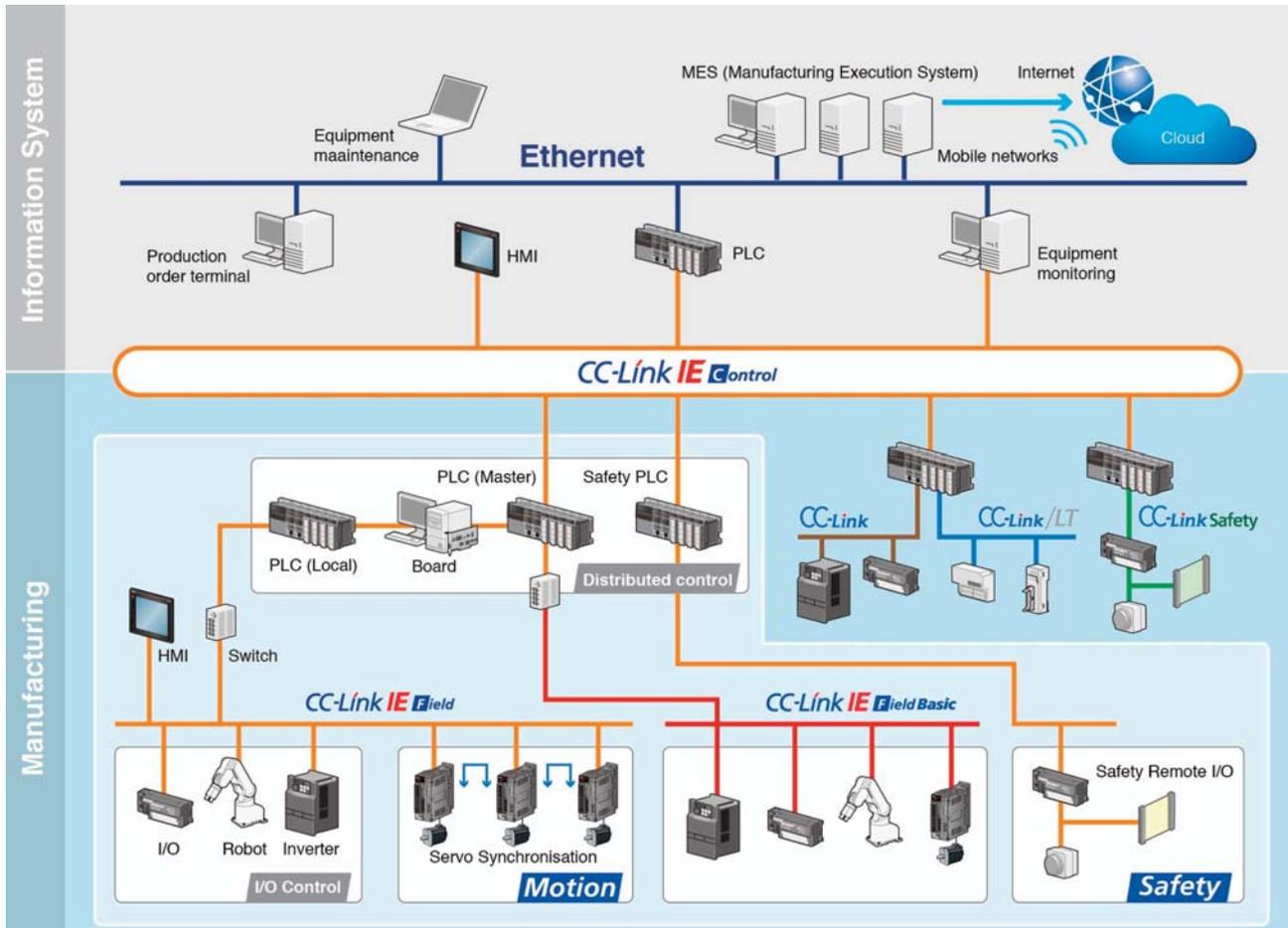


Bild: CC-Link Partner Association

# Toyota stellt Motorenwerk auf CC-Link IE um

**Das Management von Toyotas Motoren- und Getriebewerk im polnischen Wałbrzych wollte die Verfügbarkeit der Produktionslinien und die Datentransparenz verbessern. Dabei sollte das zu implementierende Netzwerk nicht nur die erforderliche Leistung bieten, sondern auch Komponenten unterschiedlicher Hersteller integrieren können. Mit der offenen Gigabit-Technologie CC-Link IE, der Industrial-Ethernet-Technologie mit der derzeit größten Bandbreite, gelang das Vorhaben ohne Probleme.**

Toyota Motor Manufacturing Poland (TMMP) ist die größte Motoren- und Getriebefertigung von Toyota in Europa und verteilt sich auf die beiden Standorte Wałbrzych und Jelcz-Laskowice im Südwesten Polens. Während die größeren Toyota-Motoren im Werk Jelcz-Laskowice mit einer Kapazität von 180.000 Einheiten pro Jahr produziert werden, findet der Großteil der Motorenproduktion sowie die Herstellung von Getrieben im Werk Wałbrzych statt. Das 1999 errichtete Werk Wałbrzych nahm im April 2002 die Produktion auf und produziert heute mehr als 633.000 Einheiten pro Jahr. Im Dreischichtbetrieb ist auch eine Kapazität von über einer Million Einheiten realisierbar. Das Werk stellt unter anderem den 1-Liter-Benzinmotor für den Toyota Aygo und weitestgehend baugleiche Fahrzeuge von Citroen und Peugeot her. Produziert werden außerdem Kurbelwellen und Pleuelstangen für Toyota Manufacturing UK (TMUK) im britischen Deeside, wo die Motoren für den Aveniris und Auris entstehen, sowie Zahnradrohlinge und geschmiedete Hohlzylinder für das Toyota-Werk in Indien. Mit einer Gesamtfläche von 520.000m<sup>2</sup>, einschließlich rund 100.000m<sup>2</sup> Maschinenhalle, beherbergt das

Werk in Wałbrzych Linien für die Motorenmontage sowie Schmiedelinien. Als die Produktionslinien gebaut wurden, waren die Anforderungen an die Datenkommunikation noch relativ gering. Die Notwendigkeit, immer größere Datenmengen zu extrahieren, um die Fertigungsprozesse besser kontrollieren zu können, veranlasste das Unternehmen zur Neubewertung seiner Netzwerkanforderungen. Dabei sollten die Netzwerksysteme sowohl im Bereich der Motorenmontage als auch in der Schmiedesparte modernisiert werden.

## Modernisierung der Schmiedelinie

Der Modernisierungsbedarf der Netzwerke der Schmiedelinien war erheblich, wie Damian Mroziński, Manufacturing Engineering Manager bei TMMP, erklärt: „Wir haben neun Schmiedelinien, die sich jeweils aus einer Anzahl unterschiedlicher Maschinen zusammensetzen. Die größte ist eine 5.000-Tonnen-Pressen, die ursprünglich separat konstruiert wurde. Bislang gab es nur einen rudimentären Datenaustausch zwischen den einzelnen

Bilder: CC-Link Partner Association



CC-Link IE, die weltweit einzige offene Gigabit-Netzwerktechnologie für industrielles Ethernet, bot eine Reihe klar erkennbarer Vorteile für die Motorenmontage.

Maschinen. Wir brauchten aber die Möglichkeit, größere Datenmengen von Maschine zu Maschine zu übertragen, und daher ein Netzwerk zur Anbindung der jeweiligen Maschinensteuerungen.“ CC-Link IE (Industrial Ethernet) und die Feldbusversion CC-Link boten sich an. „Wir haben uns für CC-Link-Technologien entschieden, weil sie so einfach zu implementieren sind“, sagt Mroziński. „Insgesamt haben wir 13 Stationen integriert, wobei CC-Link IE für die Kommunikation zwischen den Maschinen sorgt und CC-Link für den Datentransfer zwischen der einzelnen Maschine und ihren Subsystemen, wie unseren Fanuc-Robotern. Trotz der vermeintlich komplexen Anforderungen konnten wir die gesamte Installation während unseres jährlich planmäßigen zweiwöchigen Stillstands zum Abschluss bringen.“

### Motorenmontage

Die Recherche der Optionen führte TMMP zu CC-Link IE, der weltweit einzigen offenen Gigabit-Netzwerktechnologie für industrielles Ethernet. Hierin erkannte das Unternehmen eine Reihe von Vorteilen für die Motorenmontage. Andrzej Zębek, TMMP Assistant Manager, Maintenance Engineering: „In der Motorenmontage haben wir vier Linien: eine für die innere Montage, eine für die Kopfmontage, eine für die mittlere Montage und eine für die Fertigstellung. Wir wollten nicht nur eine bessere Datentransparenz über diese Linien hinweg sicherstellen, sondern auch Produkte von Drittanbietern integrieren, darunter GOT2000 HMIs von Mitsubishi Electric und E/A-Blöcke mit Schutzklasse IP67 von Balluff. Das Ziel war der Aufbau eines Poka-Yoke-Systems zur Verbesserung der Qualität in Montagebereichen mit manueller Bauteilkommissionierung. Hierfür brauchten wir ein Netzwerk, das uns die Freiheit lässt, Produkte von verschiedenen Anbietern zu wählen.“ Wartungsingenieur Radosław Serafin ergänzt: „Wir wollten insgesamt rund 2.000 E/A-Punkte integrieren und viele Geräte verschiedener Hersteller miteinander verbinden – u.a. 48 HMIs von Mitsubishi Electric – und dabei schnellen Datenaustausch gewährleisten. Wir wollten uns für die Zukunft nicht an die Produkte einer bestimmten Marke binden – das war sehr wichtig bei diesem Projekt.“ TMMP entschied sich für CC-Link IE, weil es nicht nur die erforderlichen Kommunikationsgeschwindigkeiten als flexible und modulare Lösung bereitstellt. Bei über 1.700 CC-Link IE-



Die Offenheit von CC-Link IE war für Toyota entscheidend, denn so bleibt es dem Unternehmen unbenommen, Produkte von führenden Anbietern wie Balluff und Mitsubishi Electric einzubeziehen.

war die Offenheit mit entscheidend, denn so bleibt es dem Unternehmen unbenommen, Produkte von führenden Anbietern wie Balluff und Mitsubishi Electric einzubeziehen.“ Die Technologie hat sich schnell bewährt: TMMP genießt höchste Verfügbarkeit, größere Datentransparenz und verbesserte Qualität über die gesamte Produktionslinie, die alle 50 Sekunden einen neuen Motor herstellen kann. Das bestätigt auch Damian Mroziński: „CC-Link IE war schnell und einfach zu implementieren und ist völlig unkompliziert in der Handhabung.“

### Die Vorteile einer stärker vernetzten Produktion

TMMP profitiert bereits von den Vorteilen der Installation in der Motorenfertigung und in der Schmiedelinie. Nicht nur hat sich das CC-Link IE-Netzwerk als außerordentlich robust erwiesen, sondern dank der Diagnosefähigkeiten können auch eventuelle Probleme sehr schnell behoben werden. Damit ist die Modernisierung aber nicht abgeschlossen, wie Mroziński erklärt: „Die Umstellung der einzelnen Schmiedelinie war eigentlich ein Pilotprojekt, um den Nutzen erfassen zu können. Wir planen nun sukzessive die Einführung der CC-Link IE-Technologie auf den anderen Schmiedelinien.“ Künftig könnte die höhere Datentransparenz TMMP auch wichtige Werkzeuge auf dem Weg zur Industrie 4.0 an die Hand geben. Als Grundlage für die Vernetzung von Produktionsmaschinen und Feldgeräten ist das Netzwerk bereit für eine breitere Anbindung an übergeordnete Unternehmenssysteme. Diese Art von Konnektivität ermöglicht es den Herstellern, den Herausforderungen der Produktion von morgen zu begegnen. John Browett zieht folgendes Fazit: „Wir freuen uns sehr, dass ein großer internationaler Konzern wie Toyota CC-Link IE und CC-Link in seinen Fertigungslinien einsetzt. Dies ist ein sehr guter Beleg für die vielen Vorteile, die diese robuste, zuverlässige und offene Netzwerktechnologie bietet.“



**Autor:** John Browett,  
General Manager,  
CC-Link Partner Association – Europe  
[eu.cc-link.org](http://eu.cc-link.org)



Bild: Harting KGaA

## Neuer LWL-Steckverbinder bringt hohe Bandbreiten auch unter Tage

***In Tunnelbohrprojekten und im Bergbau hält die Digitalisierung genauso Einzug wie in der Industrieautomation oder dem Consumerbereich. Aber im Unterschied zu den letzten beiden, sind die Anforderungen unter der Erde und in anderen rauen Umfeldern um ein Vielfaches höher. Große Entfernungen und gleichzeitig hohe, notwendige Bandbreiten machen Lichtwellenleiter (LWL) zum unumgänglichen Leitmedium.***

**D**a optische Schnittstellen bekanntermaßen sehr empfindlich gegenüber Verschmutzungen sind, musste man sich für Minen- und Tunnelbaubetriebe eine Lösung einfallen lassen. Bei Harting heißt die Lösung für hohe Datenraten unter extremen Bedingungen Expanded Beam Cable Assembly. So sind HD-TV an Maschinen und Anlagen, wie auch die Ortung von Personal für Notfälle bis in die letzten Winkel einer Grube kein Problem mehr.

### Digitalisierung hält Einzug im Bergbau

Eine Öllampe, Schlägel und Eisen, manchmal auch noch ein Kanarienvogel. Dies sind die Utensilien, die der Bergmann Gezähe nennt, und die für den Abbau untertage vor 200 Jahren notwendig waren. Heutige Minen und Bergbaubetriebe erinnern wenig an diese Zeit, wenn man Maschinen, Förderanlagen und die ausgefeilte Technik hinter Tunnelbau oder Rohstoffgewin-



Das hermaphroditische Steckgesicht macht das Cable Assembly unabhängig von einer Verlegerichtung.

Bild: Harting KGaA

nung betrachtet. Auch hier hält die Digitalisierung Einzug und verbessert Wirtschaftlichkeit und Sicherheit durch immer mehr Transparenz in Echtzeit. Bohrwagen, Radlader, Walzenlader und Sprengwagen sind nur einige Geräte eines großen Bergbaubetriebes, die man in Zukunft besser überwachen möchte. Neben wirtschaftlichen Interessen wie Fördermengenmessung in Echtzeit oder die Menge des eingesetzten Sprengstoffes, gilt es auch die Sicherheit zu erhöhen. Durch moderne Überwachungssysteme können live Maschinen und Personen geortet und im Notfall schneller gefunden und gerettet werden. Aber wie finden all diese Daten ihren weiten Weg an die Erdoberfläche? Nimmt man den Bau des Gotthardt-Tunnels als Beispiel, waren dies zum Ende der Bauphase je Seite gute 25km, die es zu überbrücken galt. Eine Ethernetübertragung über Kupferkabel schließt sich damit aus, LWL bzw. deren Schnittstellen sind nicht für den Einsatz in derartigem Terrain geeignet. Sie überbrücken lange Distanzen mit großer Bandbreite, aber sind letztendlich doch zu empfindlich. Bis jetzt.

### Endlich robust

Optische Steckverbinder, die auf keramischen Ferrulen, wie ST, SC, LC und E2000 basieren, verbinden die Glasfasern mit

Hilfe eines physikalischen Kontakts der polierten Faserendflächen. Weit verbreitet ist diese Art von Steckverbindern bereits in LANs, WANs und in Rechenzentren. Besonders beliebt für diese Bereiche sind sie deshalb, da die trockenen, sauberen und klimatisierten Bedingungen eine zuverlässige Umgebung in der optischen Verkabelung zur Verfügung stellen. Jedoch müssen diese IP20-Steckverbinder für den Einsatz im Außenbereich mit unterschiedlichen Gehäusen konfiguriert werden, um Schutzgrade bis IP65/IP67 zu erlangen. Nur so können sie für den Außeneinsatz verwendet werden. Zumindest solange sie gesteckt sind. Wird die Schnittstelle geöffnet, ist eine Kontamination unter den extrem rauen Bedingungen untertage unvermeidbar. Denn in Bereichen, in denen optische Verbindungen oft auf- und abgebaut oder wo Anlagen und Anlagenteile regelmäßig örtlich verändert werden, ist eine Beschädigung dieser Ferrulen nicht zu verhindern. Dabei spielt es keine Rolle, ob sie mit einem zusätzlichen IP65/67 Gehäuse geschützt werden oder nicht. Kritisch ist eine Öffnung der optischen Verbindung immer. Minimale Mengen Staub, Feuchtigkeit oder andere Verunreinigungen gelangen schnell auf die Ferrulen und verhindern eine erfolgreiche Übertragung. Trotz schwerer äußerer Bedingungen und Schwierigkeiten im Bergbau, steigt die

Nachfrage und der Bedarf an Datenkommunikation sowie an einer Anbindung an das Firmennetzwerk. Für weite Übertragungstrecken und gleichzeitig hohes Datenaufkommen bleibt also doch nur der Weg über Lichtwellenleiter. Allerdings mit einem neuartigen und robusten Steckverbinder, dem Schmutz und Wasser nichts anhaben können und der einfach zu reinigen ist.

Mögliche Aufgaben im Bergbau sind:

- Fernsteuerung der Maschinen aus einer Leitstelle
- HD-Videoüberwachung der Anlagen und Maschinen
- Netzwerkanbindung an das Firmennetz zur Abfrage von Daten, Leistung und Ertrag
- Anbindung der WLAN Router innerhalb der Anlagen für Telefonie, Ortung von Fahrzeugen, Gegenständen und Personen
- Übermittlung von Aufträgen an Arbeitsmaschinen oder Transportfahrzeuge

Ein wichtiger Grund dafür ist, dass die Mitarbeiter im Bergbau oder Tunnelbau weder die Zeit noch das notwendige Material für eine ordentliche und Standard-Fiber-Optik-Steckverbinder konforme Reinigung haben. Maschinenstillstand und Förderausfälle kosten Firmen in diesen Bereichen enorme Summen und müssen zwingend vermieden werden.



Bild: Harting KGaA

Das Expanded Beam Cable Assembly wurde für widrigste Arbeitsumgebungen entwickelt.

nun in den gegenüberliegenden Stecker eingekoppelt und mit der Linse des zweiten Steckers wieder zurück auf den Faserdurchmesser kollimiert (in gerader Linie geführt) werden. Dieser Vorgang wird in der Optik als Kollimation bezeichnet und ermöglicht so, dass die Lichtstrahlen wieder von der Faser aufgenommen werden können. Der daraus resultierende Vorteil ist klar ersichtlich: da nun zwischen den Steckern der übertragene Lichtstrahldurchmesser um das 40-fache erweitert wurde, ist eine Staubverschmutzung mit einer Größe von 0,020mm keine Störung mehr. In einer IP20 Lösung hätte eine Staubverschmutzung dieser Größenordnung zu einer Verbindungstrennung geführt. Der Expanded Beam Steckverbinder besitzt die Schutzklasse IP68 und ist zudem deutlich einfacher zu reinigen. Zwar wird er standardmäßig mit einer Schutzkappe ausgeliefert, die im ungesteckten Zustand die

Linzen und Gewinde schützen soll, aber auch ungeschützt sind Staub und Wasser kein Problem. Einfach die Kontaktfläche abspülen, mit einem Tuch oder an der Kleidung grob abwischen und verbinden, fertig. So sorgen Digitalisierung und I4.0 für eine bessere Prozessüberwachung und mehr Sicherheit im Bergbau. GLÜCK AUF!

## Hartings Lösung

Hartings Expanded Beam Kabelkonfektion ist die Lösung für den Einsatz von Glasfasern untertage und innerhalb rauer Industriefelder. Diese Lösung wurde designed, um in den härtesten, rauesten und schmutzigsten Situationen jeglicher Anwendung eine zuverlässige optische Verbindung zu gewährleisten. Zudem ist ein regelmäßiges Auf- und Abbauen der Verkabelung in diesen rauen Zonen problemlos realisierbar. Sogar eine Verlängerung der optischen Verbindung ist einfach durch den Anschluss eines weiteren Kabels möglich, ohne hierbei auf die Verlege-Richtung achten zu müssen. Durch das hermaphroditische Steckgesicht, ist ein zusätzlicher Adapter ebenfalls nicht von Nöten, womit nur zwei von mehreren Vorteilen dieser Technik aufgezeigt werden. Hartings Lösung ist daher in Bereichen anwendbar, die extremen äußeren Bedingungen ausgesetzt sind. Bergbau und Tunnelbohrmaschinen sind nur zwei der vielen möglichen Anwendungen.

## Der direkte Vergleich

Bei ferrulenbasierten Steckverbindern wird die Glasfaser in die Ferrule eines Standard Fiber Optik Steckverbinders eingeklebt. Wichtig für die Faserendfläche ist, dass diese geschliffen und poliert sein muss. So können dann die zu verbindenden Stecker die Faserendflächen in Kontakt bringen, womit Licht von einer Faser in die andere eingekoppelt wird. Die lichtführenden Bereiche der Fasern haben je nach Fasertyp einen Durchmesser von 0,009mm bis 0,065mm. Folglich lässt bereits die kleinste Verschmutzung in genau diesem minimalen Bereich die Dämpfung des optischen Signals sehr schnell wachsen, wodurch die Verbindung getrennt wird. Wie schon der Name sagt, erweitert Hartings Expanded Beam Connector den Durchmesser des Lichtstrahls mit dem Einsatz einer Linse um den Faktor 40. Der erweiterte Lichtstrahl kann

## Vorteile im Überblick

Aus der ganzen Lösung, die Harting seinen Kunden bietet, ergeben sich noch weitere Vorteile, die den Einsatz in rauen, industriellen Zonen erleichtert:

- Aluminium Gehäuse, gummiertes Gehäuse, Kappe und Knickschutz (mechanische Schutzvorrichtungen)
- Kabel und Stecker in RAL 1021 – erleichtert die Unterscheidung zu anderen Kabeln
- Kabeleigenschaften:  $\Delta T = -40\text{ °C bis }+85\text{ °C}$ ;  $F = 600\text{N}$ ;
- 2 und 4 Fasern in single- und multimode Ausführung
- Einfaches Verlängern der Verbindung durch Verwendung mehrerer Kabel
- Kein Vertauschen von Tx und Rx möglich (bei der Verlängerung)
- Design: hermaphroditisch, das heißt kein male oder female – ermöglicht so immer die richtige Zuordnung beim Stecken.
- Durch die stets richtige Zuordnung des Steckgesichts werden Beschädigungen vermieden. ■

**Autor:** Frans Oudshoorn,  
Global Product Manager Fiber Optic Cable Assemblies,  
Harting Customised Solutions

**Autor:** Jonas Diekmann,  
Fachredakteur,  
Harting Electronics  
[www.harting.com/de](http://www.harting.com/de)

# Ethercat-Komponenten

**Man mag es kaum glauben, aber der Ethercat-Standard wird in diesem Jahr bereits 15 Jahre alt. Im April 2003 wurde das System vorgestellt.**

Der Fokus bei der Entwicklung von Ethercat lag von Beginn an auf geringen Zykluszeiten ( $\leq 100\mu\text{s}$ ) und einem kleinen Jitter ( $\leq 1\mu\text{s}$ ) für hohe Synchronisationsanforderungen insbesondere im Antriebsbereich. Das Funktionsprinzip von Ethercat ist so einfach wie genial: Ethercat-Geräte verarbeiten die Ethernet-Pakete quasi 'On-The-Fly'. Alle Teilnehmer entnehmen dem Frame beim Durchlauf die für sie bestimmten Daten und fügen die eigenen Daten ein. Daraus entsteht die außergewöhnlich hohe Performance. Heute ist Ethercat ein ausgewachsenes System mit Lösungen für nahezu jeden Anwendungsfall. Mit Safety-over-Ethercat wird das Thema 'Funktionale Sicherheit' abgedeckt und Ethercat P (P für Power) überträgt gleichzeitig noch die Energie zum Busteilnehmer. Und auch der Integration von TSN hat Ethercat sich bereits angenommen: Als erste große Feldbusorganisation hat die ETG im vergangenen Jahr ein TSN-Profil veröffentlicht, das spezifiziert, wie Ethercat die TSN-Technologie nutzen wird (siehe S. 13f).

## BECKHOFF

Beckhoff Automation GmbH & Co. KG  
33415 Verl | Tel.: +49 5246 963-0  
info@beckhoff.de  
www.beckhoff.de

### Durchgängig Highspeed-Ethernet.



- Ethernet bis in die Klemme – vollständige Durchgängigkeit
- Ethernet-Prozessinterface, skalierbar von 1 Bit bis 64 kByte
- Ethernet-Lösung für die Feldebene
- exaktes Timing und synchronisierbar



esd electronics GmbH  
30165 Hannover | Tel.: +49 511 37298-0  
info@esd.eu  
www.esd.eu

### Modernste EtherCAT-Lösungen für Ihre Anwendung



- **Software**  
EtherCAT Master-Stack, EtherCAT-Slave-Stack und Konfigurationstool EtherCAT-Workbench
- **Gateways und Bridges**  
Kommunikationsmodule von CAN zu EtherCAT oder EtherCAT zu EtherCAT zum Datenaustausch, zur Synchronisation etc.
- **Slave Hardware**  
PCI Express, PMC und XMC Interface-Karten, IO-Module
- **Starterkit, Master-Selector**
- **Workshops und Schulungen**

Anlagenbau, Industrie und Gebäude

## SCHALTSCHRANKBAU

Methoden - Komponenten - Workflow

### Immer aktuell!

Die neuen Normen und  
Normenentwürfe der DKE **VDE DIN**



Das Magazin 'Schaltschrankbau' berichtet als erste Fachzeitschrift über relevante Technologien, Produkte, Normen und Trends für Hersteller von Schaltschränken und bietet aktuelles Wissen für Unternehmen aus Handwerk und Industrie.

Bild: ©sdecoret-FOTOLIA.com

ssb-magazin.de

# Vorschau Industrial Communication Journal 2018

	Protokolle und Standards	Komponenten und Lösungen	Wireless und Remote	Sicherheit	Industrielle Kommunikation 4.0
<b>Ausgabe I</b> ET: 28.03.2018 RS: 28.02.2018	Profibus und Profinet AS-Interface	OPC UA als Backbone für Industrie 4.0  Kommunikationslösungen für die Antriebstechnik  Serielle Adapter für Ethernet <i>mit Marktübersicht</i>	Industrielle Mobilfunk-Standards und -Lösungen	Redundante Kommunikation (PSP, HSR etc.)  Plagiats- und Know-how-Schutz  Sicher kommunizieren mit FSoE	Industrial IoT Cloud & M2M  Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN
<b>Ausgabe II</b> ET: 15.05.2018 RS: 17.04.2018	Ethercat Modbus TCP/IP CC-Link	Kabel und Verbindungstechnik <i>mit Marktspiegel</i>  Lichtwellenleiter & Optic Fibre (LWL)	Machine-to-Machine-Kommunikation (M2M)  MQTT und AMQP	IT-Sicherheitsgesetz  Sicher kommunizieren mit Opensafety	Industrial IoT Cloud & M2M  Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN
<b>Ausgabe III</b> ET: 05.10.2018 RS: 07.09.2018	Ethernet/IP Varan CAN/CANopen	Power over Ethernet (PoE und PoE+)  Installations- und Datenmanagement	WLAN für die Industrie <i>mit Marktübersicht</i>  Funk in der Feldebene	Antiviren-Software für die Industrie  Sicher kommunizieren mit Profisafe  Security <i>mit Marktübersicht</i>	Industrial IoT Cloud & M2M  Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN
<b>Ausgabe IV</b> ET: 19.11.2018 RS: 22.10.2018	Ethernet Powerlink Sercos IO-Link	Diagnose und (Fern-)Wartung  IO-Systeme mit Feldbus/ Ethernet-Ankopplung <i>mit Marktübersicht</i>	NFC und Bluetooth	Sicherheit mit RFID  Zugriffsschutz und Firewalls  Sicher kommunizieren mit CIP Safety	Industrial IoT Cloud & M2M  Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN

ET: Erscheinungstermin, RS: Redaktionsschluss

## Inserentenverzeichnis

ads-tec GmbH .....	35	IBHsoftec Gesellschaft für Automatisierungstechnik mbH.....	13
Beckhoff Automation GmbH & Co. KG .....	9, 41	MKU Metrofunk Kabel-Union GmbH.....	43
eks Engel FOS GmbH & Co. KG .....	19	Moxa Europe GmbH .....	17
esd electronics GmbH .....	41	MPL AG .....	35
Helmholz GmbH & Co. KG .....	44	Siemens AG .....	Titel, 35
HELUKABEL GmbH .....	3	WAGO Kontakttechnik GmbH & Co. KG .....	2

## Impressum

### VERLAG/POSTANSCHRIFT:

Technik-Dokumentations-Verlag  
TeDo Verlag GmbH®  
Postfach 2140, 35009 Marburg

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

Internet: www.sps-magazin.de

### LIEFERANSCHRIFT:

TeDo Verlag GmbH  
Zu den Sandbeeten 2  
35043 Marburg

### VERLEGER & HERAUSGEBER:

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

### REDAKTION:

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

### WEITERE MITARBEITER:

Inka Bach, Bastian Fitz, Tamara Gerlach,  
Anja Giesen, Frauke Itzerott, Pascal Jenke,  
Victoria Kraft, Kristine Meier,  
Melanie Novak, Kristina Sirjanow,  
Florian Streitenberger, Natalie Weigel  
Sarah-Lena Schmitt

### ANZEIGEN:

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

### ANZEIGENDISPOSITION:

Michaela Preiß  
Tel. 06421/3086-0  
Es gilt die Preisliste der Mediadaten 2018.

### GRAFIK & SATZ:

Anja Beyer, Tobias Götz,  
Fabienne Heßler, Melissa Hoffmann,  
Kathrin Hoß, Ronja Kaledat,  
Moritz Klös, Timo Lange,  
Ann-Christin Lölkes, Nadin Rühl

### DRUCK:

Offset vierfarbig  
L.N. Schaffrath GmbH & Co. KG  
Marktweg 42 - 50, 47608 Geldern

### 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

### JAHRESABONNEMENT

SPS-MAGAZIN: (18 Hefte)  
Inland: 99€ (inkl. MwSt. + Porto)  
Ausland: 115€ (inkl. Porto)

### EINZELBEZUG:

5,90€ pro Einzelheft  
(inkl. MwSt., zzgl. Porto)

### ISSN

### Vertriebskennzeichen

0935-0187

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.

© Copyright by TeDo Verlag GmbH, Marburg.



# Die DNA von Metrofunk

für Systemerhalt  
hinter der Kulisse



**Metrofunk Kabel-Union GmbH**  
D-12111 Berlin, Tel. 030 79 01 86 0  
info@metrofunk.de – www.metrofunk.de



Bis zu 64 Peripherie-Module



Powermodul im Buskoppler integriert

EtherCAT

## ETHERCAT – FÜR DAS TB20 I/O-SYSTEM

Hohe Leistungsfähigkeit, flexible Topologie

Das TB20 I/O-System mit EtherCAT-Buskoppler zeichnet sich durch seine hohe Leistungsfähigkeit, seine flexible Topologie und die einfache Handhabung aus. So schaffen Sie zukunftsorientierte Automatisierungskonzepte in Ihren Industrie-Anlagen.

- Buskoppler mit folgenden EtherCAT-Funktionen:
  - Modular Device Profile (MDP), automatisches Mapping, CoE-Objektverzeichnis
- 1024 Bytes Eingangs/Ausgangs-Datenwww
- Reduzierte Wartungs- und Stillstandszeiten durch Hot-Plug fähige Module
- TB20-ToolBox – einfache Konfiguration, Simulation und Diagnose des Systems