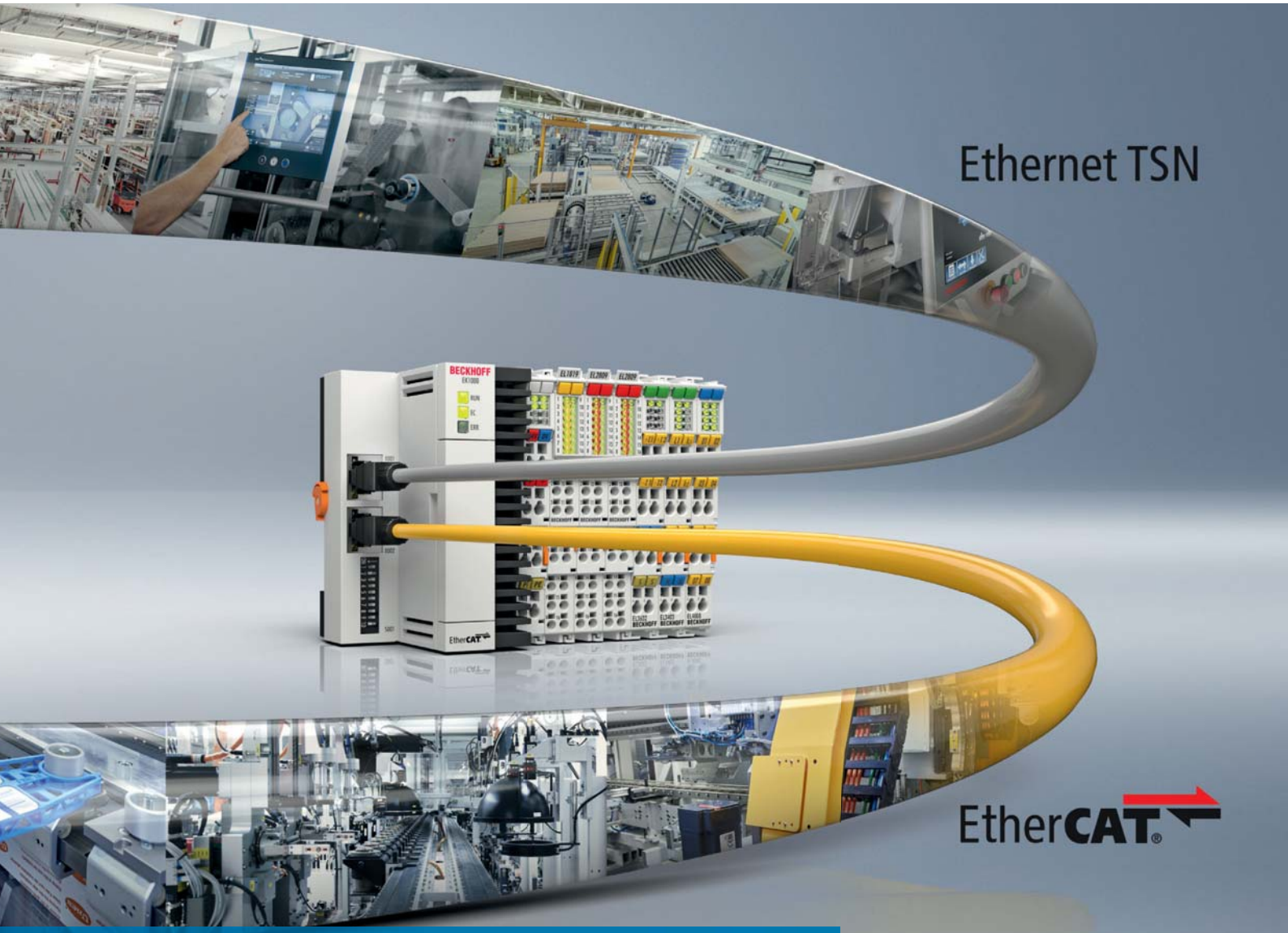
SPS MAGAZIN
SONDERAUSGABE 1/2018
www.sps-magazin.de

INDUSTRIAL COMMUNICATION JOURNAL

ICJ

ETHERNET WIRELESS SECURITY



EtherCAT über geswitchte Ethernet-Netzwerke übertragen

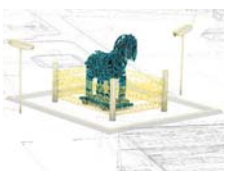
EtherCAT einfach mit TSN kombinieren

Seite 6

BECKHOFF

Bild: Beckhoff Automation GmbH & Co. KG

SECURITY
Offene Steuerungen im Netz
Seite 28



VOM SENSOR IN DIE CLOUD
Lösungen für die Fabrik von morgen
Seite 40

TSN OVER ETHERNET
Switch für die Automatisierung
Seite 45

INDUSTRIENETZE SCHÜTZEN UND VERBINDEN!

WALLIE — Industrial Ethernet Bridge und Firewall

WALLIE, die Industrial Ethernet Bridge und Firewall, schützt Ihr Automatisierungsnetzwerk sicher vor unbefugten Zugriffen. Da WALLIE individuell konfigurierbar ist, kann die Firewall leicht an die Anforderungen Ihrer Maschinennetze angepasst werden. Sollen identische IP-Adressbereiche realisiert werden, fungiert WALLIE als Bridge.

- Einfache Integration von Maschinennetzen in das übergeordnete Produktionsnetz
- Individuelle Konfiguration über Webinterface
- Bridge-Funktionalität für identische IP-Adressbereiche
- NAT (Basic NAT, NAPT und Portforwarding)
- Platzsparende industrietaugliche Bauform zur Hutschienenmontage

www.helmholz.de

Helmholz®
COMPATIBLE WITH YOU

Kai Binder, Chefredakteur

Die Industriekommunikation ist im Wandel. Während die vergangenen Dekaden vor allem von der Diskussion um die beste und schnellste Verbindung der Komponenten innerhalb der Maschine geprägt waren, stellt sich für viele Anwender heute vor allem die Frage, wie die Maschine an überlagerte Systeme angebunden werden sollte – allen voran das Internet bzw. die Cloud.

Von der Maschine zum Produktionssystem

Mit dem Einzug von Ethernet in die Maschine ist es möglich geworden, transparent aus der Leitebene auf nahezu alle Informationen aus der Maschine durchzugreifen. Und mit den Möglichkeiten sind auch die Ansprüche gewachsen. Die Einbindung der gesamten Produktionsinfrastruktur in eine – wie auch immer geartete – Cloudlösung steht daher bei vielen Maschinenbauern ganz oben auf der Agenda, verspricht sie doch einen großen Mehrwert nicht nur für den Endanwender, sondern auch für neue Geschäftsmodelle der Maschinenanbieter.

Mit TSN und OPC UA kommen zwei Technologien in die Anwendung, die die gestiegenen Ansprüche erfüllen könnten. Der Benefit von TSN ist in erster Linie nicht, dass man nun keine Feldbuslösungen innerhalb der Maschine mehr verwenden wird, weil TSN alles ersetzt: Die Realität zeigt, dass selbst nach annähernd zwei Dekaden seit der Einführung von Industrial Ethernet immer noch jedes Jahr mehr klassische Feldbusknoten verkauft werden als im Vorjahr. In vielen Fällen gibt es nämlich keinen Grund bestehende Maschinentypen, die noch klassische Feldbussysteme, einsetzen, auf Ethernet-basierte Systeme umzurüsten.

Auch wenn TSN mittelfristig das Zeug dazu hat, die bisherigen Industrial-Ethernet-Systeme zu ersetzen: Heute liegt der direkte Vorteil von TSN darin, dass die Kommunikation zwischen den Maschinen nun in Echtzeit erfolgen kann.

In der Kombination mit OPC UA, das den Informationsaustausch zwischen Steuerungen unterschiedlicher Hersteller ermöglicht, vereinfacht sich in der Folge die Vernetzung der Maschinen zu einem Gesamtproduktionssystem. Doch OPC-UA kann noch mehr, denn viele überlagerte Systeme sind heute in der Lage OPC-UA-Kommunikation nahtlos einzubinden. Für Anwender bedeutet dies einen immensen Vorteil, den sie in ihren neuen Maschinenkonzepten nutzen können.

Auch die vorliegende Ausgabe des ICJ spiegelt diesen Wandel wider. In diesem Sinne wünsche ich Ihnen viel Spaß bei der Lektüre.

Kai Binder
kbinder@sps-magazin.de

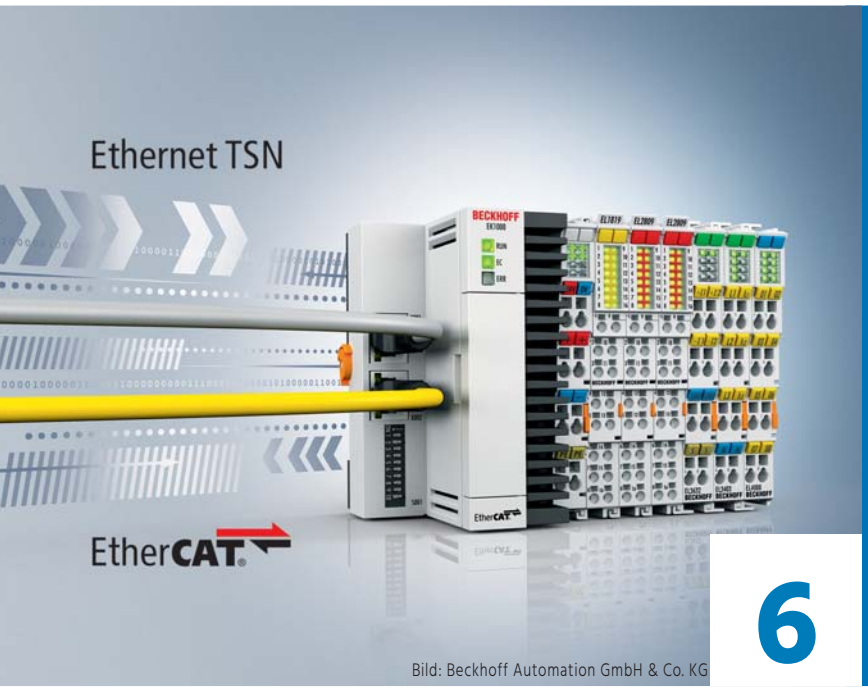


Bild: Beckhoff Automation GmbH & Co. KG

6

TITELSTORY

EtherCAT einfach mit TSN kombinieren

Die Ankopplung eines oder mehrerer EtherCAT-Segmente an ein TSN-Netzwerk erfolgt mit dem EtherCAT-TSN-Koppler EK1000 auf einfache Weise. Das TSN-Netzwerk wird dabei für die Echtzeitanbindung einer abgesetzten Steuerung im Fabriknetz verwendet werden und somit als Topologie-Erweiterung eines EtherCAT-Segments dienen. Zusätzlicher Kommunikationsbedarf, z. B. für Vision-Kameras, kann dann parallel im TSN-Netzwerk eingesammelt und zentral in der Steuerung ausgewertet werden.

OPC UA und TSN kommt zur Anwendung

Bild: Kontron S&T AG

2018 wird das Jahr von OPC UA und TSN
Seite 26

Prozessautomatisierung im IIoT

Bild: PCTEL, Inc.

Die richtige Antenne für das IIoT
Seite 49

Markt-Trends-Technik

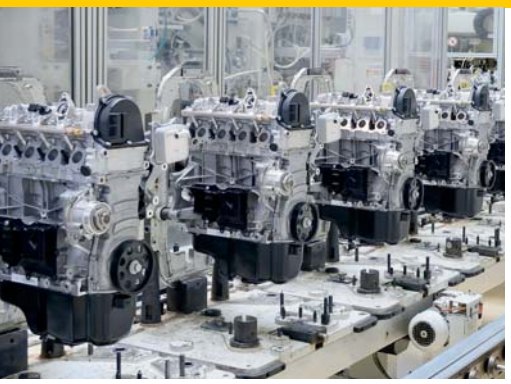
Fachbeiträge

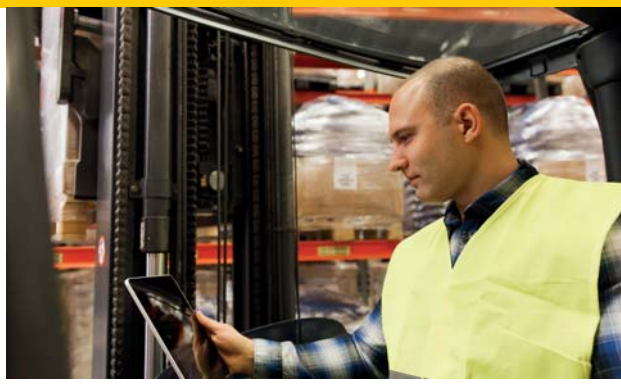
Service

Your Global Automation Partner

TURCK

Industrie 4.0
Daten- und Kommunikations-lösungen





Durchgängige HF/UHF-RFID-Lösungen für Datenerfassung und -vorverarbeitung, Identifikation, Rückverfolgung, Serialisierung

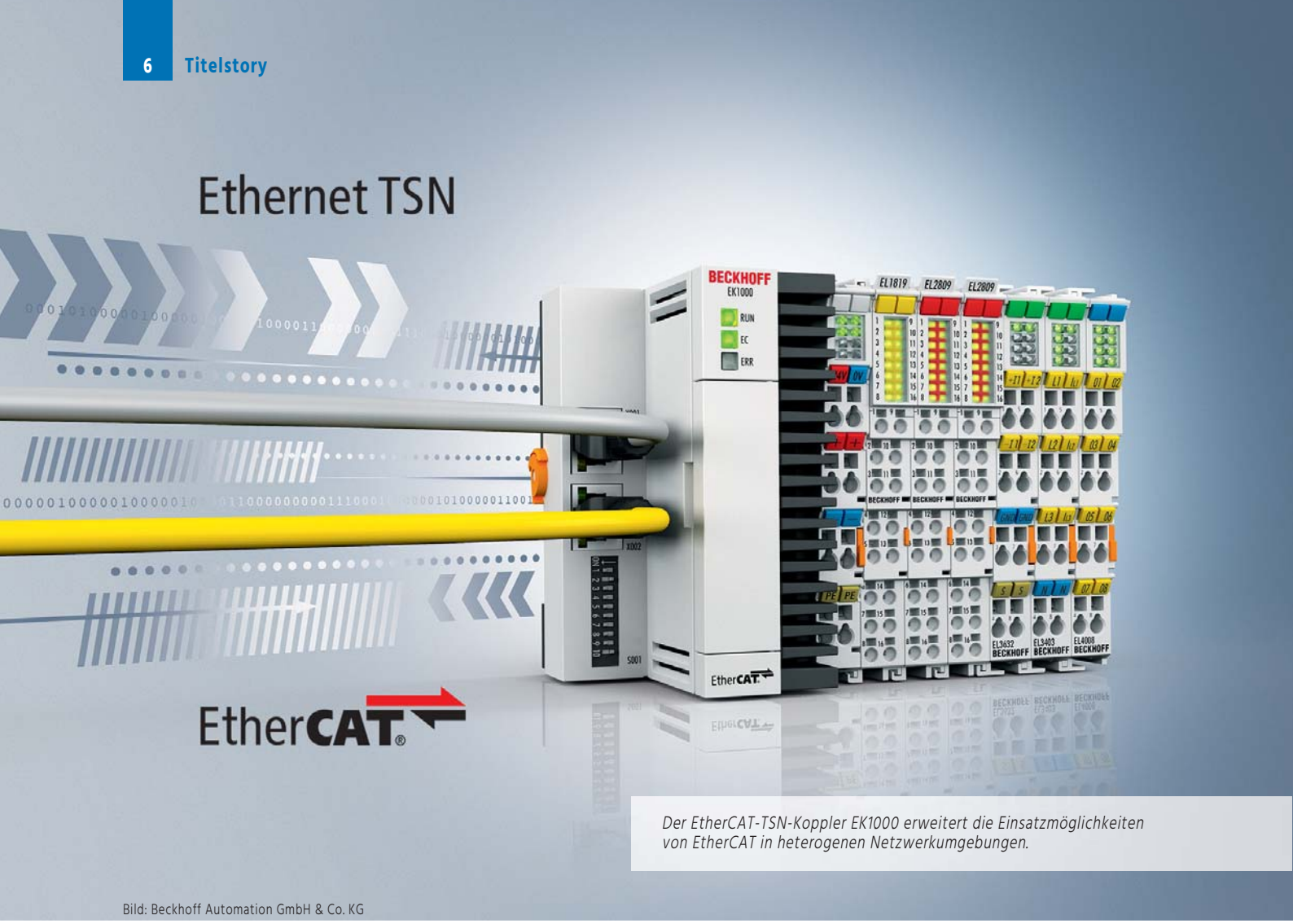
Intelligente Sensor- und Verbindungslösungen mit IO-Link-Kommunikation für maximale Flexibilität

Robuste IP67-I/O-Systeme mit dezentraler Intelligenz und Multiprotokoll-Ethernet-Kommunikation zur einfachen IT-Integration

Hannover Messe
Wir sind für Sie da!
Halle 9, Stand H55

HANNOVER MESSE

www.turck.de/i40



Der EtherCAT-TSN-Koppler EK1000 erweitert die Einsatzmöglichkeiten von EtherCAT in heterogenen Netzwerkumgebungen.

Bild: Beckhoff Automation GmbH & Co. KG

EtherCAT über geswitchte Ethernet-Netzwerke übertragen

EtherCAT einfach mit TSN kombinieren

Die Ankopplung eines oder mehrerer EtherCAT-Segmente an ein TSN-Netzwerk erfolgt mit dem EtherCAT-TSN-Koppler EK1000 auf einfache Weise. Das TSN-Netzwerk wird dabei für die Echtzeitanbindung einer abgesetzten Steuerung im Fabriknetz verwendet werden und somit als Topologie-Erweiterung eines EtherCAT-Segments dienen. Zusätzlicher Kommunikationsbedarf, z. B. für Vision-Kameras, kann dann parallel im TSN-Netzwerk eingesammelt und zentral in der Steuerung ausgewertet werden.

Die Kommunikation zwischen Steuerungen zur Vernetzung von Maschinen und Anlagen erfolgt bereits heute über Standard-Ethernet-Netzwerke. Die Nutzung von Time Sensitive Networking (TSN)-Technologien ermöglicht eine Echtzeitkommunikation in einem solchen Netzwerk: TSN eignet sich, um in einem heterogenen Ethernet-Netzwerk Datenströme (Streams) zu definieren und diese echtzeitfähig und priorisiert durch das Netzwerk zu transportieren.

Für die Kommunikation innerhalb von Maschinen ist EtherCAT die führende Technologie – das Prinzip der Datenverarbeitung on-the-fly ermöglicht eine herausragende Performance und ist prädestiniert, die im industriellen Umfeld zahlreichen kleinen Datenpakete von digitalen und analogen Eingängen in einem EtherCAT-Segment in der Regel mit nur einem Frame zu einem Gesamtprozessabbild zusammenzufügen. Beckhoff verbindet mit dem EtherCAT-TSN-Koppler EK1000 diese beiden Aufgabengebiete auf ein-

Bild: Beckhoff Automation GmbH & Co. KG

Komplementäre Nutzung des Ethernet-Frames für TSN und EtherCAT.

fache Weise und unterstützt die Anbindung von EtherCAT-Segmenten über ein heterogenes Ethernet-Netzwerk an eine abgesetzte EtherCAT-Steuerung.

Aktueller Status der TSN-Entwicklung

TSN ist eine Projektgruppe in IEEE 802.1, in der verschiedene Verfahren zur Verbesserung der Switching-Technologie definiert werden – quasi ein Werkzeugkasten auf Ebene 2 (Data Link Layer). Mit den richtigen Werkzeugen eignet sich TSN, um Daten mit Hilfe von Streams echtzeitfähig durch ein heterogenes Netzwerk zu leiten. Sehr kurze Verzögerungen in den Netzwerkkomponenten, garantierte Bandbreite sowie eine hochgenaue Synchronisierung lassen damit auch Anwendungen für die Vernetzung von Automatisierungsanlagen zu.

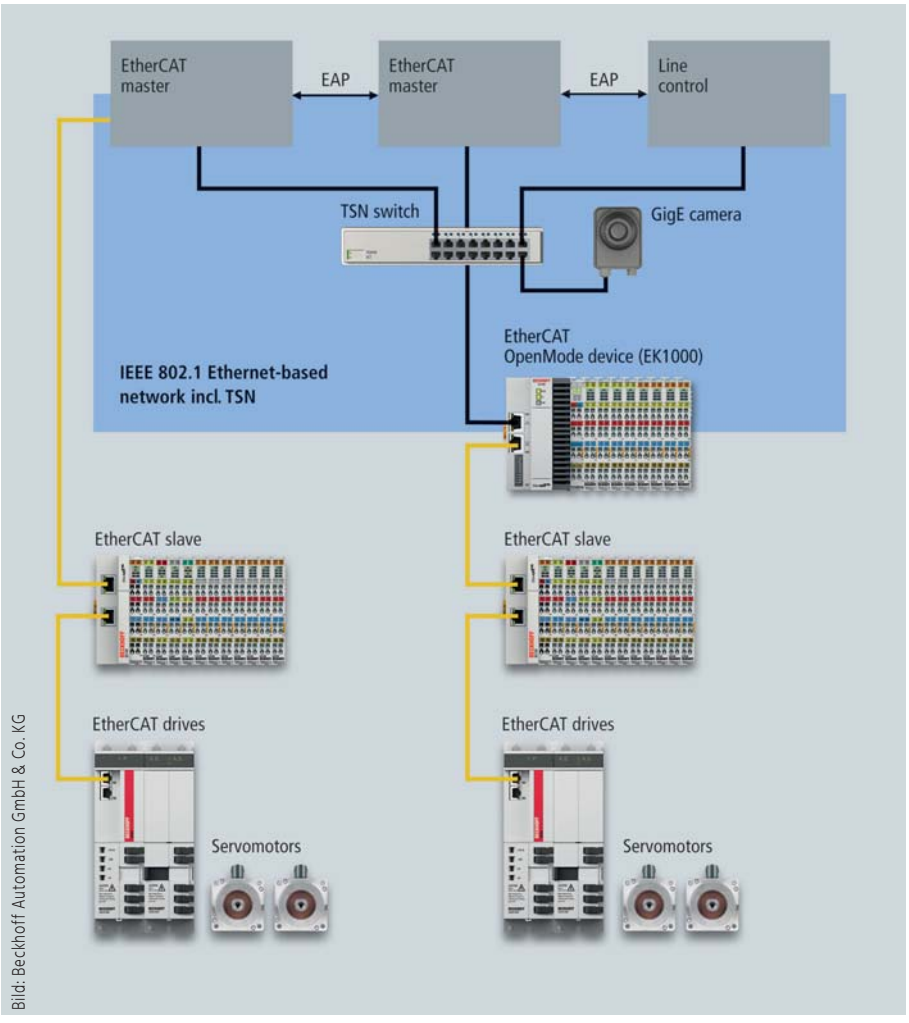


Bild: Beckhoff Automation GmbH & Co. KG

Erweiterung der EtherCAT-Topologie um ein heterogenes Standard-TSN-Netzwerk – EK1000 als Open-Mode-Koppler.

• IEEE 802.1Qbv ist ein Standard zur Verbesserung des Weiterleitungsprozesses von zyklischen, zeitsensitiven Daten (daher Time Sensitive Networking) durch einen vorgeplanten und zeitgesteuerten Datentransfer (Time Aware Shaping, TAS). Weniger zeitkritische Daten werden für diese Zeit geblockt und dadurch Verzögerungen an den Ausgangsports vermieden.

• IEEE 802.1Qbu Frame Preemption: Ein Problem bei der deterministischen Übertragung von zeitkritischen Daten ist die Belegung eines Netzwerk-Ports von einem nichtpriorisierten Frame, z. B. mit bis zu 1.500 Bytes. Eine mögliche Unterbrechung dieser nicht kritischen Ethernet-Frames dient dazu, die Verzögerung für einen zeitkritischen Frame zu reduzieren bzw. zu verhindern, dass ein großer Zeitschlitz vor der Echtzeitphase freigehalten werden muss.

• Der Standard IEEE 802.1AS-REV definiert ein Protokoll zur Synchronisierung von verteilten Uhren auf Basis des Standards IEEE 1588. Erst dadurch ist die genaue Zeitsteuerung in den Komponenten möglich, die für das TAS genutzt wird.

• Weitere Projekte in der IEEE 802.1 beschäftigen sich mit der Konfiguration der Netzwerkteilnehmer und Infrastrukturkomponenten. Der Standard IEEE 802.1Qcc (Stream Reservation Enhancements) definiert eine Verteilung der vorhandenen Bandbreite auf angeforderte Echtzeit-Datenströme (max. 80 %) und garantiert auch nicht priorisierten Daten ein Durchkommen. Die Strategien zur Konfiguration werden noch kontrovers diskutiert: Sie variieren von einem dezentralen An-

> *„Die Nutzung komplementärer Bereiche des Ethernet-Telegramms für TSN und EtherCAT ermöglicht eine einfache Anbindung kompletter EtherCAT-Segmente an ein heterogenes TSN-Netzwerk. Beide Technologien können somit ihre Vorteile dort ausspielen, wofür sie entwickelt wurden.*
>
> *Dr. Guido Beckmann, Beckhoff Automation GmbH & Co. KG*

Bild: Beckhoff Automation GmbH & Co. KG

satz mit hoher Flexibilität bis hin zu einem strikt zentralen Ansatz mit optimierter Performance für das System. Beiden Ansätzen gemein ist die komplexe Aufteilung der verfügbaren Bandbreite auf die angeschlossenen Teilnehmer.

Einsatz und Eigenschaften des EtherCAT-TSN-Kopplers

Beckhoff bietet mit dem EK1000 die Möglichkeit, durch ein TSN-Netzwerk ein oder auch mehrere EtherCAT-Segmente echtzeitfähig von einer Steuerung anzusprechen. So kann das breite Spektrum an EtherCAT-Geräten und EtherCAT-I/O-Klemmen direkt – ohne Änderung in den EtherCAT-Geräten – an die heterogene TSN-Welt angebunden werden.

Der EtherCAT-TSN-Koppler EK1000, als erster Teilnehmer in einem EtherCAT-Segment platziert, übernimmt die Adaption zwischen TSN und EtherCAT basierend auf dem EtherCAT-TSN-Profil, das in der EtherCAT Technology Group (ETG) definiert wurde. Da die verwendeten Spezifikationen in der IEEE-Projektgruppe noch nicht abgeschlossen sind, kann das Profil der ETG zunächst nur als Entwurf zur Verfügung gestellt werden. Eine Liaison zwischen IEEE und ETG stellt sicher, dass EtherCAT auch auf die noch nicht verabschiedeten IEEE 802.1-Spezifikationen zugreifen kann und so die Technologie zeitnah mit TSN eingeführt wird.

Das Profil macht sich dabei den Vorteil zu Nutze, dass beide Technologien komplementäre Bereiche des Ethernet-Frames verwenden: Ein TSN-Stream wird definiert durch den MAC-relevanten Teil im Frame (MAC-Adresse und VLAN Tag), EtherCAT hingegen nutzt nur den Bereich der Nutzdaten des Frames. Somit kann ein TSN-Stream originär ein EtherCAT-Telegramm transportieren, das anschließend direkt durch die EtherCAT-Slaves im EtherCAT-Segment geschickt wird. Im Segment selbst ändert sich nichts, d. h. die Performance des Protokolls, die genaue Synchronisation, die Topologie-Flexibilität, die Diagnosemöglichkeiten und die Einfachheit durch vollautomatische Adressierung der Geräte bleiben erhalten. Gleiches gilt für die freie Auswahl unter den EtherCAT-Geräten am Markt, die nach der Integration von TSN keinerlei Modifikationen benötigen.

Die Stream-Anpassung, mit der das EtherCAT-Segment an das heterogene TSN-Netzwerk angebunden wird, erfolgt entweder im letzten TSN-Switch oder im ersten EtherCAT-Slave-Gerät – dem EK1000. Hierfür ist es lediglich notwendig, die TSN-Stream-ID des empfangenen Frames auf dem Rückweg zum Master auf eine neue TSN-Stream-ID zu ändern und ggf. den Zeitstempel für die verteilten Uhren (Distributed Clocks) im EtherCAT-Frame zu aktualisieren – mehr nicht.

Der EtherCAT-TSN-Koppler, als erster Teilnehmer in einem EtherCAT-Segment platziert, verfügt über zwei Ethernet-Schnittstellen. Einer dieser Ports verbindet den Koppler mit dem Ethernet- bzw. TSN-Netzwerk. Der EK1000 übernimmt dabei den Austausch des Telegramms vom TSN- an den EtherCAT-Port mit minimaler Durchlaufverzögerung. Die bewährten EtherCAT-Eigenschaften, wie z. B. Distributed Clocks und XFC, sowie EtherCAT-fähige Antriebe lassen sich somit auch in einem TSN-Netzwerk nutzen. In einem Netzwerk ohne TSN-Erweiterungen eignet sich der Buskoppler selbstverständlich auch zur Ankopplung eines EtherCAT-Netzwerks an ein Standard-Ethernet-Netzwerk. Die Implementierung von TSN-Technologien (Qbv, AS-REV) im EK1000 stellt die Grundlage für einen deterministischen Datenaustausch zwischen der Steuerung und dem EtherCAT-Segment bereit.

Ausblick

Mit den richtigen ‘Werkzeugen’ aus dem TSN-Werkzeugkasten eignet sich TSN, um in einem heterogenen Ethernet-Netzwerk Datenströme (Streams) zu definieren und diese echtzeitfähig und priorisiert durch das Netzwerk zu transportieren. Dies minimiert Verzögerungszeiten und gewährleistet eine Synchronisierung der Teilnehmer – es ersetzt aber keinesfalls den Echtzeitfeldbus. Feldbusse, wie z. B. EtherCAT, sind extrem effizient und optimiert auf eine einfache Handhabung und Inbetriebnahme; die Diagnose der Teilnehmer im laufenden Betrieb ist auf eine schnelle Fehlerbehebung ausgelegt. TSN sollte dort genutzt werden, wo es deutliche Vorteile bringt: im Fabriknetzwerk. ■

Autor: *Dr. Guido Beckmann,*
Technology Marketing,
Beckhoff Automation GmbH & Co. KG
www.beckhoff.de/ek1000 — www.beckhoff.de/ethercat

Besuchen Sie uns auf
der HMI: Halle 11, Stand C72

Einfach in die Cloud?
Sicher!

Das ist die digitale Zukunft!

www.wago.com/hmi/de

Übernahme von CIP Safety als chinesischer Nationalstandard

Die ODVA hat mitgeteilt, dass CIP Safety, die Erweiterung des Common Industrial Protocol (CIP) für funktionale Sicherheitsanwendungen, von der Standardization Administration of China (SAC) der Volksrepublik China als chinesischer Nationalstandard GB/Z34066-2017 übernommen wurde. Die Zulassung des Standards wurde vom Chinese Standardization Technical Committee TC124 für 'Industrielle Prozessmessung' unterstützt und das Projekt wurde vom Instrument Technology and Economy Institute (ITEI) geleitet. CIP Safety bietet eine Kommunikation mit abgesichertem Ausfallverhalten zwischen Geräten, wie beispielsweise Sicherheits-E/A-Blöcken, Sicherheitsverriegelungsschaltern, Sicherheitslichtvorhängen und Sicherheits-SPS, in funktionalen Sicherheitsanwendungen bis Safety Integrity Level 3 (SIL3) (entsprechend der Norm IEC61508 und wie vom TÜV Rheinland zertifiziert). CIP Safety ist eine anerkannte Lösung für funktionale Sicherheit, die bereits seit 2005 angewendet wird, als sie zum ersten Mal im CAN-basierten Netzwerk Devicenet der ODVA eingesetzt wurde. Heute ist CIP Safety der Standard für funktionale Sicherheit für Devicenet, Ethernet/IP sowie Sercos III, die Industrial-Ethernet-Technologie, die von Sercos International unterstützt wird. "In den letzten Jahren legte die chinesische Regierung ihr Augenmerk verstärkt auf die Übernahme von Technologien und Standards für Sicherheitsanwendungen", führte Katherine Voss, President von ODVA, aus. "Die Übernahme von CIP Safety als chinesischer Nationalstandard wird in einer verstärkten Annahme der Technologie in China als führende Sicherheitslösung für die Automatisierung von Industrieprozessen resultieren." Die Norm GB/Z34066-2017 wird voraussichtlich im ersten Quartal 2018 veröffentlicht.

ODVA
www.odva.org

Workshop: Physikalische Prüfkriterien für Profinet

Bild: I-V-G Göhringer

Seit vielen Jahren wird Profinet in verschiedenen Branchen eingesetzt und verdrängt nach und nach die seriellen Feldbusse. Das liegt nicht nur an den deutlich höheren Übertragungsraten, sondern auch an der großen Flexibilität. Verschiedene Protokolle laufen parallel und die Topologie lässt sich nahezu beliebig erweitern. Entsprechend hoch sind die Anforderungen an alle Komponenten. Zuletzt wurden strengere Prüfkriterien bei den Devices von der PNO veröffentlicht. Damit stellt sich zwangsläufig die Frage, welche Auswirkung das auf die Systemprüfung im Feld hat. In dem dreieinhalbstündigen Praxis-Workshop werden die wesentlichen physikalischen Prüfkriterien für Profinet-Abnahmemessungen erarbeitet – speziell für die Ersteller von Lastenheften, Konstrukteure, Inbetriebnehmer und Instandhalter. Im Mittelpunkt steht die Bewertung der EMV, die in der täglichen Praxis häufig Störungen in der Datenübertragung verursacht. Physikalische Grundlagen, Erdung, Schirmströme und Störpegel auf der Versorgung runden den Workshop ab.

I-V-G Göhringer
www.i-v-g.de

Workshop: Embedded Cybersecurity

BE.services bietet einen Workshop über Cybersecurity in der industriellen Automatisierung auf dem Automatisierungstreff in Böblingen an. Der Anbieter für Embedded Software in Steuerungssystemen präsentiert diesen Workshop in Zusammenarbeit mit seinem Partner Kaspersky Lab. Die Teilnehmer erhalten einen Überblick über aktuelle Bedrohungen in industriellen Anlagen und erfahren, wie Steuerungssysteme nachhaltig vor Angriffen geschützt werden können. Die stark an Bedeutung gewinnende Norm IEC62443 wird ebenfalls Teil der Veranstaltung sein. Hands-on-Schulungen bieten einen Einblick in die Praxis. Aufgabe der Teilnehmer wird es sein, die richtigen Security Policies für eine Anlage zu konfigurieren, um mögliche Angriffe zu blockieren und zu erkennen. Mehr Information über den Workshop erhalten Sie unter www.automatisierungstreff.com/?page_id=19461.

BE.services GmbH
www.be-services.net

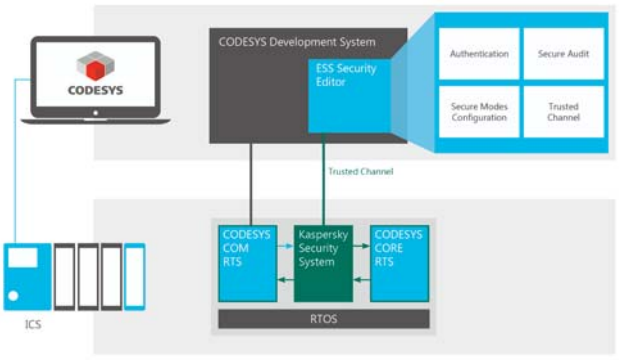


Bild: BE.services GmbH

Die Teilnehmer erhalten einen Überblick über aktuelle Bedrohungen in industriellen Anlagen und erfahren, wie Steuerungssysteme nachhaltig vor Angriffen geschützt werden können.

Industrie 4.0 von Kryptowährung überrascht

Kaum ist der Anfang für Industrie 4.0 geschafft, tauchen am Horizont schon neue Ideen auf. Sie gehen über das bisher Gedachte weit hinaus – man kann noch gar nicht so richtig begreifen, was da auf uns zu kommt. Vielleicht haben Sie zum Jahreswechsel auch den Hype um Kryptowährungen im Allgemeinen und speziell zum Thema Bitcoins mitbekommen. Was nicht so laut durch die Presse ging, ist, dass sich Firmen wie Daimler und Bosch bereits aktiv damit beschäftigen. Laut Pressemitteilungen greifen sich beide Firmen unterschiedliche Applikationen heraus. Bosch beispielsweise investiert in das Berliner Krypto-Startup IOTA. IOTA könnte sich als Standardtechnologie für die vertrauensvolle Kommunikation zwischen Maschinen untereinander und für die Bezahlung im IoT-Bereich etablieren. Daimler macht einen Pilotversuch zur Ausgabe einer Anleihe per Blockchain-Technologie. Es wird kein allzu großer Schritt sein, solche Verfahren auch im Internet der Dinge einzuführen. So könnten sich die unterschiedlichen Maschinen für ihre erbrachten Fertigungs- oder Dienstleistungen gegenseitig bezahlen. Dass Maschinen selbst ihr Geld verwahren, um damit verschiedene Dienstleistungen oder Waren zu kaufen, klingt aus heutiger Sicht natürlich noch sehr surreal. Es wäre eine schöne Möglichkeit, um die Kosten jederzeit transparent und niedrig zu halten und den Standort Deutschland zu stärken. Hoffen wir, dass die Kryptowährungen in die richtigen Bahnen kommen, bevor Spieler und Spekulanten die Idee wieder zerstören. ■

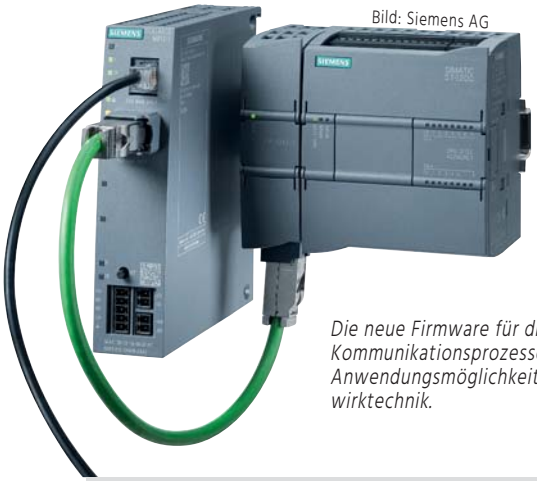
Bild: I-V-G Göhringer

Hans-Ludwig Göhringer ist Geschäftsführer der Firma IVG Göhringer

Modular und flexibel

Siemens erweitert mit der neuen Firmware V3.0 für die Simatic S7-1200 Kommunikationsprozessoren (CPs) die auswählbaren Fernwirkprotokolle für eine flexible Wahl der Leitstellenanbindung. Die neue Firmware unterstützt mehrere Fernwirkprotokolle für unterschiedliche Fernwirkanwendungen mit nur einer Baugruppe. Der Anwender entscheidet sich während der Inbetriebnahme über die TIA (Totally Integrated Automation) Portal- Engineering Software Step 7 V14 SP 1 für eines der verfügbaren Protokolle. Beim CP1243-1 stehen neben TeleControl Basic auch DNP3 und IEC60870-5-104 zur Auswahl.

Bild: Siemens AG



Die neue Firmware für die Simatic S7-1200 Kommunikationsprozessoren erweitert die Anwendungsmöglichkeiten in der Fernwirktechnik.

Siemens AG
www.siemens.de

Zeit ist, was man an der Uhr abliest

Kithara Software hat die Unterstützung des Precision Time Protocol (IEEE1588 v2) bekanntgegeben, mit der sich Netzwerkteilnehmer präzise durch Kithara RealTime Suite synchronisieren lassen. PTP kann beispielsweise zum Bilddatenabgleich von Kameras, Ermitteln genauer Messdaten oder Durchführen paralleler Robotikaufgaben verwendet werden. Der PTP-Stack von Kithara erlaubt die genaue Erzeugung von Zeitstempeln mit Abweichungen im Sub-Mikrosekundenbereich zur genauen Rechner-Synchronisierung. Durch Anbindung an GPS können Computer so selbst weltweit synchronisiert werden. Zur Synchronisation kann der Best-Master-Clock-Algorithmus (BMCA) verwendet werden, der innerhalb eines Netzwerks den Teilnehmer mit der genauesten Systemzeit ermittelt und diese als Referenz für alle weiteren Teilnehmer festlegt.

Bild: Kithara Software GmbH

Mit dem PTP-Stack von Kithara können sowohl Raw-Ethernet als auch IP/UDP als Transportschicht verwendet werden. Für hochpräzises Hardware-Timestamping werden ausgewählte PTP-kompatible Netzwerkcontroller unterstützt.

Kithara Software GmbH
www.kithara.de

Produktrelease Combricks NCI v1.4.3

Mit einem System aus frei wählbaren Modulen auf einer Backplane können Combricks gleich mehrere Funktionen wie Repeater, Relais oder Profinet-Kopplung und viele mehr im Netzwerk abdecken. Durch integrierten Profitrace Over Ethernet kann das Netzwerk zudem jederzeit analysiert werden. Combricks Network Condition Indicator ist ein Tool, das mehrere Combricks-Sets zeitgleich überwacht. Es verfügt über eine Ampelanzeige, die der Ampel in Profitrace ähnelt. Mit dieser Ampel können Sie den Status Ihres Profibus-Netzwerkes überwachen.

Procentec GmbH
www.procentec.de

Für mehr Offenheit in der Peripherie

Bild: Pilz GmbH & Co. KG

Das Remote-I/O-System PSSuniversal 2 wurde um ein Kopfmodul mit Ethernet/IP-Schnittstelle erweitert. Damit passt sich das offene System an seine bereits bestehenden Systemumgebungen an.

Pilz erweitert sein Remote-I/O-System PSSuniversal 2 um ein Kopfmodul mit Ethernet/IP-Schnittstelle. Damit bietet PSSuniversal 2 die notwendige Offenheit für die reibungslose Kommunikation in unterschiedlichen Steuerungsumgebungen auf Ethernet-Basis. Im Remote-I/O-System PSSuniversal 2 steht neben dem neuen Ethernet/IP-Kopfmodul mit CIP Safety bereits ein Kopfmodul mit Profinet/Profisafe-Schnittstelle zur Verfügung. Diese Offenheit erleichtert den Datenaustausch mit den verschiedenen Master-Steuerungen unabhängig von Maschinentyp und vorhandener Systemumgebung. Das Remote-I/O-System lässt sich durch den Tausch des Kopfmoduls für bestehende Systemumgebungen adaptieren. Der Tausch des Kopfmoduls geht einfach und schnell: Anwender speichern dazu ihre Konfigurationsdaten lokal auf microSD-Karte. So können die Daten dann einfach auf das neue Kopfmodul mit Ethernet/IP-Schnittstelle übertragen werden. Die I/O-Module sind dabei universell und identisch für die verschiedenen Sicherheitsprotokolle verwendbar. Das Remote-I/O-System ist eine Lösung für die Peripherie-Erweiterung. Die I/O-Module sind dabei universell und identisch für die verschiedenen Sicherheitsprotokolle verwendbar. Durch den dreiteiligen Systemaufbau bietet das System PSS u2 Installations- und Servicefreundlichkeit. Die Reihenfolge der Bedienung ist intuitiv.

Pilz GmbH & Co. KG
www.pilz.de


Gemeinsam schnell und sicher
zu Ihrer Industrial-IoT-Lösung
Industrial IoT
Cloud Connectivity
>4.000 OEMs
Echtzeit-
kommunikation
Effizienz
Security
Safety
Offenheit
Performance
OPC UA TSN
POWERLINK
POWERLINK und OPC UA TSN –
die Lösung für eine durchgängige
Kommunikationsarchitektur. Effizient,
herstellerunabhängig und optimal für
kürzeste Zykluszeiten und strukturier-
ten Zugriff auf große Datenmengen.
Gestalten Sie mit uns Ihre Zukunft.
www.ethernet-powerlink.org
ETHERNET
POWERLINK
Standardization Group
OPC
FOUNDATION
MEMBER

Ethercat mit TSN in heterogenen Netzwerken

Die ETG hat die Technologieerweiterung in Form eines Profils spezifiziert. Dies vereinfacht die Anpassung an die finalen Versionen der TSN-Technologien, deren Spezifikationen in der IEEE noch nicht abgeschlossen sind. Die ETG unterstützt bereits seit 15 Jahren die TSN-Entwicklung durch Mitarbeit in den IEEE-Gremien und wird bei der Adaption von TSN eng mit der IEEE 802.1 Working Group zusammenarbeiten. Eine Liaison zwischen IEEE und ETG soll sicherstellen, dass Ethercat auch auf die noch nicht verabschiedeten IEEE 802.1 Spezifikationen zugreifen kann und so die Technologie zeitnah mit TSN eingeführt wird.

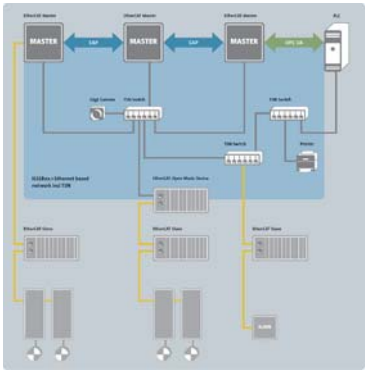


Bild: Ethercat Technology Group

Die Ethercat Technology Group (ETG) hat angekündigt, Ethercat um TSN-Technologien zu ergänzen. Damit sollen die Einsatzmöglichkeiten von Ethercat in heterogenen Netzwerkumgebungen erweitert werden.

EthercatTechnology Group
www.ethercat.org

Embedded-Lösung unterstützt OPC UA und MQTT

Die Produktfamilie der embedded Kommunikationsschnittstellen Anybus Compactcom von HMS Industrial Networks unterstützt künftig auch die IoT-Protokolle OPC UA und MQTT. Dadurch bietet Anybus Compactcom Herstellern von Automatisierungsgeräten und Maschinen einen einfachen Weg ins IIoT und in Industrie 4.0. Denn Hersteller, die bereits Compactcom verwenden, können Daten ihrer Geräte und Maschinen über die Kommunikationsschnittstelle von HMS sicher an IT-Systeme und IoT-Software übermitteln. Anybus CompactCom mit OPC UA und MQTT kann IT-Systemen und IIoT-Anwendungen die Geräte- und Maschinendaten der Feldebene direkt zur Verfügung stellen, was die Kommunikation zwischen Fertigung und IT deutlich vereinfacht.

Bild: HMS Industrial Networks GmbH

Die übermittelten Geräte- und Maschinendaten ermöglichen Anwendern die Datenanalyse im Hinblick auf vorausschauende Wartung und Verbesserung von Fertigungsprozessen.

HMS Industrial Networks GmbH
www.hms-networks.com

Eintrittskarte nach Asien

Speziell für Hersteller von Automatisierungsgeräten, die ihr Geschäftsfeld nach Asien erweitern wollen, hat Hilscher das Spektrum seiner cifX PC-Karten Familie um CC-Link IE Field erweitert. Automatisierungsfirmen steht damit eine PCI Express- sowie eine Low Profile PCI Express-Karte zur Verfügung. Die CC-Link IE Field Karten sind Intelligente Stationen im Netzwerk und bieten eine feste Übertragungsrate von 1Gbit/s. Azyklische Kommunikation kann per SLMP (Seamless Message Protocol) realisiert werden. Die cifX PC-Karten bieten dem Anwender einen einheitlichen Standard für alle am Markt vorhandenen Real-Time-Ethernet- und Feldbus-Systeme, unter anderem CC-Link, CC-Link IE Field und auch CC-Link IE Field Basic.

Bild: Hilscher Gesell. f. Systemautomation mbH

Der gesamte Protokoll-Stack wird auf der PC-Karte abgewickelt. Der Datenaustausch zum Host erfolgt per Dual-Port-Memory oder DMA (Direct Memory Access).

Hilscher Gesell. f. Systemautomation mbH
www.hilscher.com

Serielle Geräteserver in kompakter Bauform

Die serielle Kommunikation ist seit langer Zeit Standard für eine sichere Datenverbindung. Heute hat sich das Ethernet in modernen Automatisierungsanwendungen fest etabliert. Für eine zuverlässige Anbindung bestehender serieller Endgeräte in ein Ethernet Netzwerk, hat ICPDAS die seriellen Geräteserver der tDS-700 Serie entwickelt. Als serielle Schnittstellen stehen bis zu drei verschiedene COM Ports für RS-232 und RS-422/485 bereit. Mit Hilfe der im Lieferumfang enthaltenen VxComm Utility wird ein virtueller COM Port im Windows Betriebssystem eingerichtet. Darauf können bestehende Programme im gleichen Maße zugreifen, wie auf einen reellen COM Port. Die Spannungsversorgung wird über PoE (Power-over-Ethernet) oder ein separates 12-48VDC Netzteil realisiert. Das kompakte Gehäuse ist für die Montage auf DIN-Schiene vorbereitet und nimmt nur wenig Platz in Anspruch.

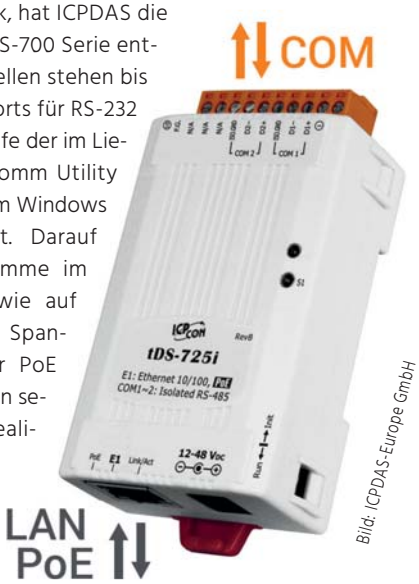


Bild: ICPDAS-Europe GmbH

ICPDAS bietet die tDS-700 Geräteserver jetzt auch als isolierte Variante mit 3.000VDC Isolierung und +/-4kV ESD-Schutz an.

ICPDAS-Europe GmbH
www.icpdas-europe.com

Bereit für Datenkommunikation von morgen

Alles für industrielle Netzwerke

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

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

PHOENIX CONTACT
INSPIRING INNOVATIONS

ION11-18.000.L1

Über BLE direkt vom Sensor in die Steuerung

Die Geräteserie Dataeagle von Schildknecht realisiert die Umsetzung von Funktechnologien wie zum Beispiel Bluetooth auf Kabel wie 4-20mA, Profibus, Profinet, TCP/IP. Das neue Gateway Dataeagle 2730 übernimmt die direkte Übertragung von Sensordaten über Bluetooth Low Energy an das Gateway und von dort mittels RJ 45-Kabelanschluss über Profinet, Ethernet IP, Modbus TCP und anderen zu Steuerungen oder bis in die Cloud. Mit Dataeagle 2730 kann ein Anwender die Vorteile kabelloser Sensoren, etwa an schwer zugänglichen Maschinenteilen oder für die Übertragung der Sensordaten über Bluetooth Low Energy nutzen. Der Vorteil ist, dass die Daten direkt - ohne Zwischenstation wie z.B. Tablets in Hand von Personen - an die Steuerung zur erforderlichen Verarbeitung geschickt werden können. Das bedeutet Zeitgewinn, Sicherheit und Kostensenkung zugleich.

Bild: Schildknecht AG

Mit dem Dataeagle 2730 können Daten direkt an die Steuerung zur Verarbeitung geschickt werden.

Schildknecht AG
www.schildknecht.ag

Smarte Soft- und Hardware für das Industrial IoT

Mit der IoT Gateway Software V2 lassen sich in wenigen Schritten Neu- und Bestandsmaschinen effizient vernetzen und transparent machen. Für den Zugriff auf Produktions- und Maschinendaten lässt sich das webbasierte konfigurierbare Tool über sogenannte Device Apps mit verschiedensten Sensoren, Servern und Steuerungen verbinden. Neu unterstützt werden dabei der kompakte und robuste Multi-Sensor CISS von Bosch, der OPC UA-Vorgänger OPC DA sowie weitere Drittsteuerungssysteme, darunter Beckhoff CX und Allen Bradley/Rockwell ControlLogix. Die Weiterleitung der Daten zwecks Analyse und Auswertung erfolgt über Processing Apps, die neben verschiedenen Cloud-Diensten und On-Premises Lösungen jetzt auch MES Systeme unterstützen sowie einen Generic REST Dienst anbieten.

Eine weitere Neuheit stellt Device Portal dar, über das OEMs, Serviceanbieter und Endanwender verteilte IoT Gateway Instanzen fernverwalten können.

Bild: Bosch Rexroth AG

Bosch Rexroth AG
www.boschrexroth.com

CAN-Transceiver sichern robuste Kommunikation

Mit MAX14878, MAX14879 und MAX14880, den 2,75kV- und 5kV-Familien isolierter CAN-Transceiver von Maxim Integrated können Entwickler eine robuste Kommunikation und eine längere Betriebszeit für industrielle Anwendungen erzielen. Die neue Highspeed-Transceiver-Familie verfügt über eine integrierte galvanische Isolation von bis zu 5kV mit Fehlerschutz und ESD-Eingangsschutz von ±15kV nach HBM (Human Body Model) für erhöhte Betriebszeiten bei rauen und rauschbehafteten Umgebungsbedingungen. Sie arbeiten mit einer Highspeed-CAN-Datenrate von bis zu 1Mbit/s und verfügen über einen Fehlerschutz von ±54V am Empfängereingang. Verfügbar im 16-poligen Wide-Body-SOIC-Gehäuse mit industriekompatiblen Anschlussbelegungen mit 8mm Kriechstrecke sind die Transceiver für den Betrieb in einem Temperaturbereich zwischen -40 und +125°C ausgelegt.

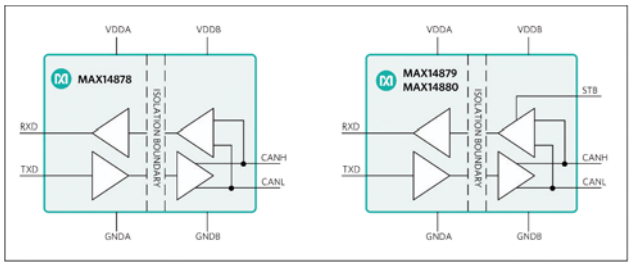


Bild: Maxim Integrated Products GmbH

Die CAN-Transceiver arbeiten mit einer Highspeed-CAN-Datenrate von bis zu 1Mbit/s und verfügen über einen Fehlerschutz von ±54V am Empfängereingang.

Maxim Integrated Products GmbH
www.maximintegrated.com

Erleichterter Fernzugriff

Die Coniugo Go-Module eignen sich für Telematik und Fernwartung in der Automatisierung und Fernwirktechnik. Die Gruppe der BUS-Module, die mit M-BUS, wireless M-BUS und S0-Schnittstelle (Go Impulse Gateway) zur Erfassung von Zählerdaten geeignet ist, ist nun um ein Go-Profibus-Gateway erweitert worden. Zuwachs gibt es auch bei der Temperaturmessung, wo neben den Halbleitersensoren nun ein Go-Modul für Pt1000-Sensoren existiert und neuerdings auch ein Go-Modul für Thermoelemente (unterstützte Typen B, E, J, K, N, R, S, T) angeboten wird. Auch für Schaltausgänge zur Aktivierung von Pumpen, Lüftern und dergleichen gibt es nun ein Relaismodul, das direkt 230V AC schalten kann.

Bild: wireless netcontrol GmbH

Die Module bieten Möglichkeiten zur Datenübertragung, Datenerfassung und zur Ausführung von Schaltsystemen.

wireless netcontrol GmbH
www.wireless-netcontrol.de

Firmware-Update für Industrierouter

Das neue Firmware-Update Icom OS 2.8 für die Industrie-Router MRX und MRO von Insys Icom ermöglicht DMVPN, dynamisches Routing sowie eine Trennung des Datenverkehrs über zwei APNs. Bei der aktuellen Version liegt somit der Fokus auf Funktionen für kritische Infrastrukturen, die weitverzweigte Netze managen, spezielle Sicherheitsaspekte erfüllen und immer verfügbar sein müssen. Das Update unterstützt die dynamischen Routing-Protokolle OSPF, BGP und RIP, um auch in komplexen Installationen für die nötige Verfügbarkeit und Qualität der Datenverbindungen zu sorgen. Für Internetverbindungen über LTE lassen sich zwei APNs parallel nutzen, um den Datenverkehr zu trennen: z.B. ein APN für Betriebsdaten des Routers, der andere für Daten der am Router angeschlossenen lokalen Datenquellen. Das hat einerseits sicherheitsrelevante Vorteile, andererseits dient es der korrekten Verteilung der Kommunikationskosten auf die beteiligten Rollen (z.B. Netz-, EEG-Anlagen- oder Messstellenbetreiber).

Insys Microelectronics GmbH
www.insys-icom.de

GSM-basiertes Fernmeldemodul in 19"-Technik

Das Advanced GSM-Modul ist ein Fernmelde- und Fernwirkgerät, das unter anderem in Zugangskontrollen von Serverräumen oder IT-Zentralen eingesetzt werden kann. Es passt zu den 19"-Racks der Server- und Technikschränke und ist in einem hochwertig verarbeiteten Einschubgehäuse mit 1HE untergebracht. Das Modul bietet folgende Funktionen: 12 Eingänge für schaltende Sensoren, z.B. Türzugangskontakte, Spannungsüberwachung und 4 Eingänge für analoge Sensoren. Diese sind mit Fensterkomparatoren ausgestattet und können die elektrischen Eingangsgrößen in Messwerte umrechnen. Außerdem stehen vier Schaltausgänge mit Wechselkontakt für Fernwirkaufgaben zur Verfügung. Das Modul ermöglicht Ereignismeldungen (z.B. Stromausfall, Stromwiederkehr) über SMS und das Einrichten von kombinierten Ereignissen, etwa wenn ein Türkontakt erst nach 18 Uhr als unerlaubter Zutritt gemeldet werden soll.

Bild: wireless netcontrol GmbH

Das Modul ist mit einem eigenen 6V Akku ausgestattet, der das Gerät im Notfall 24 Stunden in Betrieb hält.

wireless netcontrol GmbH
www.wireless-netcontrol.de

Ethernet-Remote-Module für industrielle Anwendungen

Bei der ED-Serie von Brainboxes für industrielle Anwendungen handelt es sich um kompakte Remote-Module für Ethernet, vertrieben von Meilhaus Electronic. Die Serie ED-000/200 bietet Digital-I/Os, Relais oder eine Interface-Umsetzung zu seriell/RS232. Die Serie ED-500 verfügt hingegen über Analog-I/Os, Digital-I/Os, Relais oder eine Interface-Umsetzung zu seriell/RS232, RS422 und RS485. Darüber hinaus ermöglichen die Module der ES-Serie die Steuerung serieller Geräte über LAN. Es handelt sich hier um Ethernet-zu-seriell-Device-Server mit einem, zwei, vier oder acht seriellen Ports, die serielle Raten bis 1MBaud bieten. Die US-Serie beinhaltet zudem USB-zu-seriell-Adapter für industrielle Anwendungen.

Bild: Meilhaus Electronic GmbH

Anwender haben die Wahl zwischen kompakten Dongle-Gehäusen, einem Gehäuse für die Wandmontage oder Multiport-Boxmodellen.

Meilhaus Electronic GmbH
www.meilhaus.com

LTE Mobilfunkrouter mit vier SIM-Karten-Steckplätzen

Der Industrierouter Smartmotion verfügt über den Mobilfunkstandard LTE mit einer Downloadrate von 100Mbit/s sowie 50Mbit/s im Upload. Durch die zusätzliche Bestückung mit bis zu vier SIM-Karten, können Ausfallzeiten im Mobilfunk reduziert werden. Der Router hat zwei LTE-Mobilfunkeinheiten integriert, so dass stets zwei verschiedene Mobilfunknetze gleichzeitig zur Verfügung stehen, von denen jeweils das beste Netz gewählt wird. Insgesamt sind hier 4 SIM-Kartenhalterungen für eine hohe Ausfallredundanz vorhanden. Ergänzend steht eine WLAN-Schnittstelle zur Verfügung. Ebenso ist eine automatische Umschaltung bei Roaming, bei Überschreitung des Datenvolumens oder manuell möglich. Der Smartmotion unterstützt VPN-Technologien wie OpenVPN oder IPSec IKEv2, die eine sichere Kommunikation gewährleisten. In Verbindung mit dem Lucom Digicluster ist der VPN-Zugriff besonders komfortabel, da sich hier komplette Netze mit nur wenigen Mausklicks verbinden lassen.

Bild: Lucom GmbH

Der Router zeichnet sich durch den Eingangsspannungsbereich von bis zu 60V DC, die höhere Isolationsspannung von 1,5kV der Ethernet-Ports und den Betriebstemperaturbereich von -40 bis 75°C und die hohe Vibrationsbeständigkeit aus.

Lucom GmbH
www.lucom.de

Echtzeit-IEEE1588-Masterstack unter Windows

Der IEEE1588 Stack von TSEP stellt im Standardlieferumfang alle Mittel, die für eine Zeitsynchronisation über sogenannte end-to-end (E2E) Verbindungen notwendig und nach IEEE1588-2008 (Version 2) spezifiziert sind, bereit. Zudem ist ein allgemeiner Synchronisations-Algorithmus enthalten, der Synchronisation im Bereich von 40ns ermöglicht. Es besteht jedoch jederzeit die Möglichkeit, einen eigenen Synchronisations-Algorithmus zu definieren und einfach zu integrieren. Der IEEE1588 Stack ist somit eine gute Wahl für Anwender für die die IEEE1588-Konformität eine notwendige Anforderung ist. Der IEEE1588 Stack ist komplett in C++ und nach dem C++11 Standard entwickelt worden. „Durch die Kooperation mit IntervalZero können wir Echtzeitlösungen unter Windows anbieten. Für TSEP bedeutet diese Kooperation außerdem einen weiteren Schritt in der Entwicklung von Kommunikationslösungen und eine konsequente Fortführung unserer weltweiten Expansion" führt Peter Plazotta, Geschäftsführer von TSEP, aus. IntervalZero transformiert mit dem Produkt RTX64 das Windows-Betriebssystem in ein Echtzeitbetriebssystem (RTOS). Bereits bestehende Partnerschaften ermöglichen Kunden von IntervalZero schon jetzt den Einsatz von Softwarestacks für Ethercat und CANopen, der auf einem eigenen Core, unabhängig von durch Windows verursachte Verzögerungen laufen kann. Mit der Partnerschaft mit TSEP kommt nun ein IEEE1588 Stack hinzu, der kommende Anforderungen an IEEE1588 bzw. PTP (Precision Time Protocol) erfüllt. Der generische Ansatz des IEEE1588-Stacks von TSEP vereint die Möglichkeiten von PTP mit der Echtzeitlösung von IntervalZero unter Windows zu einer sehr interessanten Lösung. Mit der deterministischen Eigenschaft von RTX64 kann der Synchronisations-Algorithmus für den Abgleich mit dem IEEE1588-Masters deutlich präziser realisiert werden.

Interval Zero
www.intervalzero.com/german

Phoenix Contact DSL-Router und -Modem getestet

Die Umstellung der analogen Telefonanschlüsse der Deutschen Telekom läuft mit Hochdruck. Ziel ist es, diese Umstellung auf die neue digitale IP-Technologie noch in diesem Jahr abzuschließen. Kunden können dabei auf die All-IP-Tarife der Telekom und die damit verbundene DSL-Technologie umsteigen. Der analoge PSTN-Anschluss (Public Switched Telephone Network) wird weiterhin angeboten. Mittels spezieller POTS-Karten erfolgte in der Vermittlungsstelle eine Umstellung auf IP-Kommunikation. Die bestehende analoge Übertragungstechnik zum Endgerät blieb hierbei erhalten. Die Telekom nennt diesen automatisierten Vorgang `Migration auf die IPbasierte Technologie´. Die neuen Anschlüsse tragen die Bezeichnung `MSAN POTS (Multi Service Access Note – Plain Old Telefone Services´ und fallen unter die Sonderdienste im Netz der Telekom. Kunden, die über ihren analogen Anschluss Dienste wie Haus- und Aufzugsnotruf, Alarmanlagen, Zählerfernauslesung oder Fernwartungsanwendungen betrieben hatten, können das auch zukünftig machen. Lediglich die Hardware zum Anschluss an den entsprechenden ALL-IP- oder MSAN-POTS- Anschluss muss die Anforderungen an die geänderte IP-Kommunikation erfüllen. Die Phoenix Contact-Geräte haben dieses im Labor der Telekom erfolgreich bewiesen.

Bild: Phoenix Contact GmbH & Co. KG

Die Geräte von Phoenix Contact wurden von der Telekom erfolgreich für die neue digitale IP-Technologie getestet.

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

Schnellere Anwendungsentwicklung für Industrial Ethernet

Renesas Electronics präsentiert das neue Solution Kit für die RZ/N1-Mikroprozessoren (MPUs). Das Kit bietet Unterstützung für verschiedene industrielle Netzwerkanwendungen wie SPS, intelligente Netzwerk-Switches, Gateways, Bedienerterminals und dezentrale I/O-Lösungen. Das Kit beschleunigt die Entwicklung und kann bei der Integration von Industrienetzwerk-Protokollen in Kundenanwendungen bis zu sechs Monate Zeit sparen. Das neue Kit enthält ein CPU-Entwicklungsboard auf Basis der RZ/N1S MPU. Zum Lieferumfang gehört zudem ein umfassendes Softwarepaket mit allen Treibern und Middleware, Protokoll-Stack-Mustern, U-Boot und ein BSP auf Linux-Basis, eine spezielle Inter-Prozessor-Kommunikationssoftware sowie ein bedienerfreundliches Pinmuxing Tool. Mit dem Pinmuxing Tool lassen sich C-Code Header-Dateien generieren und damit die Pin-Konfiguration vereinfachen. Die verschiedenen Softwareprogramme und Code-Muster bieten dem Anwender einen vollständigen Satz an Tools und Frameworks, mit denen er seine eigene Anwendung ohne zusätzliche Investitionskosten oder Komplexität aufsetzen kann. Entwickler können jetzt neben Linux, das bereits vom RZ/N1 unterstützt wird, den Einsatz des ThreadX Betriebssystems für das Anwendungssubsystem evaluieren. So können Systementwickler das Betriebssystem entsprechend den spezifischen Anforderungen ihrer Anwendung wählen. Beide Betriebssysteme sind kompatibel zu den wichtigsten Industrial-Ethernet-Protokollen, die auf RZ/N1 implementiert wurden. Für die Entwicklung auf der Basis von Yocto-Linux bietet Renesas entsprechende Yocto Recipes zum Aufbau von Linux, U-Boot und einem Root-Dateisystem. Mit einem Set an Qt-abstrahierten APIs lassen sich auch grafische Bedienoberflächen entwickeln und auf verschiedene Zielsysteme portieren. ThreadX: Renesas stellt ein Muster einer Referenz-Portierung der Express Logic XWare IoT-Plattform bereit, in der ThreadX auf dem Applikationssubsystem läuft. ThreadX wurde speziell für tief eingebettete Echtzeit- und IoT-Anwendungen konzipiert. Es

Bild: Renesas Technology Europe GmbH

Die Hard- und Software des Solution Kits ermöglicht eine schnellere Prototypenerstellung für Ethernet-Protokolle wie Ethercat, Ethernet/IP, Ethernet Powerlink, Profinet, Sercos und CANopen.

bietet leistungsfähige Funktionen für Scheduling, Kommunikation, Synchronisierung, Timer, Speichermanagement und Interrupt-Management. Das neue Solution Kit ermöglicht eine Evaluierung von Codesys, eines hardwareunabhängigen IEC61131-3 Entwicklungssystems für die Programmierung und Erstellung von SPS-Anwendungen. Das System unterstützt unter anderem Industrial Ethernet-Masterstacks für Ethercat, Ethernet/IP, Sercos, CANopen und Profinet. Außerdem kann der im RZ/N1D integrierte LCD-Controller das Codesys Target Visualization Tool nutzen und ermöglicht damit eine Produktentwicklung mit grafischen Visualisierungsscreens. Durch die Codesys-Unterstützung kann der Baustein sowohl als Slave wie auch als Master fungieren. Das erweiterte RZ/N1 Solution Kit für die beiden MPU-Gruppen RZ/N1D und RZ/N1S sind ab sofort bei Renesas Electronics und seinen autorisierten Distributionspartnern erhältlich. Das Solution Kit für RZ/N1L wird im ersten Halbjahr 2018 verfügbar sein.

Renesas Technology Europe GmbH
www.renesas.de

Serielle Adapter für Feldbus und Ethernet

Zahlreiche Geräte in der Automatisierungstechnik wie Antriebe, Sensoren, Bedienterminals, Barcode-Leser und RFID-Leser sind mit einer seriellen Schnittstelle vom Typ RS-232/422/485 ausgestattet.

Für die durchgängige Kommunikation zwischen den Geräten und übergeordneten Einheiten werden diese in Feldbus- oder Industrial-Ethernet-Netzwerke integriert. Die Integration übernehmen Serielle Adapter, die es in unterschiedlichen Bauformen und Anschlussmöglichkeiten gibt. Dabei sind sowohl drahtgebundene als auch drahtlose Ankopplungen möglich. *(ghl)* ■

		
Anbieter	AMC Analytik & Messtechnik GmbH	B&R Industrie-Elektronik GmbH
Produkt-ID.	**14560**	**16082**
Ort	Chemnitz	Bad Homburg
Telefon	0371/ 38388-0	06172/ 4019-0
Internet-Adresse	www.amc-systeme.de	www.br-automation.com
Produktname	EKI-152x-Serie	X67IF1121-1
Serielle Schnittstelle RS232	max. 24	1
Serielle Schnittstelle RS422	max. 16	1
Serielle Schnittstelle RS485	max. 16	1
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar	1-, 2-,4-, 8- und 16-Port-Modelle	
Maße BxHxT	55 x 140 x 95 mm bei 4-Ports	53 x 85 x 42 mm
Montageart	Hutschienenmontage, Wandmontage	Wandmontage, Hutschienenmontage
Anschluss	9pol. D-SUB Buchse / Stecker	Schraubsteckverbinder
Verwendete Ethernetprotokolle	TCP/IP, UDP/IP, Telnet, HTTP, ARP, ICMP, BOOTP	TCP/IP, UDP/IP, HTTP
Unterstützte Industrial Ethernet Kommunikationsprotokolle		Powerlink, Ethercat, EtherNet/IP, Modbus-TCP, Profinet, Sercos-III
Feldbus-Anbindung		ASI, CANopen, DeviceNet, Ethernet, Profibus-DP, Profinet, Sercos, Sicherheitsbus
Konfiguration der Seriellen Adapter	Konfigurations-Software, Internet-Browser (Webbased-Management), Telnet	Konfigurations-Software
Programmierbarkeit bzw. Skripterstellung		Automation Studio
Statusanzeige, Diagnoseinformationen am Seriellen Adapter	Power, LAN, COM	System Diagnostics Manager

					
Anbieter	cd electronic	Comsoft GmbH	Deutschmann Automation Gm bH & Co. KG	esd electronics gmbh	HMS Industrial Networks GmbH
Produkt-ID.	**11260**	**11295**	**11286**	**30211**	**11215**
Ort	Michelstadt	Karlsruhe	Bad Camberg	Hannover	Karlsruhe
Telefon	06061/ 73353	0721/ 9497-283	06434/ 9433-0	0511/ 37298-0	0721/ 989777-000
Internet-Adresse	www.cdelectronic.de	www.comsoft.de	www.deutschmann.de	www.esd.eu	www.hms-networks.de
Produktname	S7-LAN-Modul 9352-LANCON	XPS-E - Int. Profibus DP -RS232/RS422/RS485 Gateway	Unigate CL-Ethercat	CAN-CBX-COM2	Anybus Communicator
Serielle Schnittstelle RS232			on board	✓	1 kombiniert RS-232/422/485
Serielle Schnittstelle RS422			on board	optional	1 kombiniert RS-232/422/485
Serielle Schnittstelle RS485	1		on board		1 kombiniert RS-232/422/485
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar			RS232, 485 und 422 on Board		1 kombiniert RS-232/422/485
Maße BxHxT	65 x 48 x 17 mm	90 x 126 x 38 mm	23 x 100 x 115 mm	22,5 x 99 x 114,5 mm	27 x 120 x 75 mm
Montageart	auf PPI/MPI/Profibus-Schnittst. der Simatic S7 gesteckt	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage;	Hutschienenmontage
Anschluss	9pol. D-SUB Stecker und Huckepack Diagnosebuchse	9pol. D-SUB Buchse / Stecker	Schraubsteckverbinder		D-, 9pol. D-SUB Buchse / Stecker
Verwendete Ethernetprotokolle	TCP/IP, UDP/IP, RFC 1006				TCP/IP
Unterstützte Industrial Ethernet Kommunikationsprotokolle			Ethercat		EtherNet/IP, Profinet, Ethercat, Modbus-TCP, CC-Link IE Field
Feldbus-Anbindung	Profibus-DP, MPI, PPI	Profibus-DP		CANopen	Profibus, Interbus, CANopen, DeviceNet, ControlNet, CC-Link, Lonworks
Konfiguration der Seriellen Adapter	Internet-Browser (Webbased-Management), Konfigurations-Software	keine ext. Hilfsmittel (serielles Konfigurationstool) nötig	Konfigurations-Software oder alternativ über Scriptsprache dadurch sind die Module frei programmierbar		Konfigurations-Software
Programmierbarkeit bzw. Skripterstellung			Scriptsprache mit mächtigem Befehlen z.B. Mathematische, Speicherbearbeitungsbefehle, Ablauf		Konfigurationsprogramm
Statusanzeige, Diagnoseinformationen am Seriellen Adapter	Power, LAN, COM	Profibus Status LEDs, RS-Port Status LED, Profibus Adresse	sowohl für die serielle Seite wie auch für die Busseite (busspezifisch)	Power, COM	COM, Power, LAN

					
B&R Industrie-Elektronik GmbH	Beckhoff Automation GmbH & Co. KG	Beckhoff Automation GmbH & Co. KG	Bihl+Wiedemann GmbH	Bressner Technology GmbH	Bressner Technology GmbH
16086	**11264**	**11266**	**11293**	**11241**	**11252**
Bad Homburg	Verl	Verl	Mannheim	Gröbenzell	Gröbenzell
06172/ 4019-0	05246/ 963-0	05246/ 963-0	0621/ 33996-0	08142/ 47284-0	08142/ 47284-0
www.br-automation.com	www.beckhoff.de	www.beckhoff.de	www.bihl-wiedemann.de	www.bressner.de	www.bressner.de
X20IF1020	EL6021 Serielle Schnittstelle RS422/RS485	KL6021 Serielle Schnittstelle RS422/RS485	AS-i 3.0 RS 232-Master in Edelstahl	SENA LS100 HelloDevice Lite	Digi Connect ES Serie 4/8/16 ports
1	1	1	1	1	4/8/16
	1	1			
					1
12,5 x 99 x 85	12 x 100 x 68	12 x 100 x 68	120 x 75 x 83	72 x 25 x 100	23,5 x 26,90 x 4,20 cm
Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	DIN-Rail mount kit, Wandmontage	Wandmontage
Klemme	Federklemmtechnik	Federklemmtechnik	9pol. D-SUB Buchse / Stecker	9pol. D-SUB Buchse / Stecker	RJ45
TCP/IP, UDP/IP, HTTP	Ethercat	Ethernet, ADS, Ethercat, Modbus TCP, Profinet , Ethernet IP		TCP/IP, UDP/IP, Telnet	TCP/IP, Telnet, UDP/IP, ARP
Powerlink, Ethercat, EtherNet/IP, Modbus-TCP, Profinet, Sercos-III	Ethercat	Ethernet, ADS, Ethercat, Modbus TCP, Profinet, Ethernet IP			
ASI, CANopen, DeviceNet, Ethernet, Profibus-DP, Profinet, Sercos, Sicherheitsbus	Profibus, Profinet, CAN	Lightbus, CANopen, DeviceNet, Profibus-DP, Interbus, Modbus	ASI		
Konfigurations-Software	über COE	über COE	Konfigurations-Software	Serielle Konsole, Konfigurations-Software, Telnet	Konfigurations-Software, Internet-Browser (Webbased-Management), Serielle Konsole, Telnet
Automation Studio	über COE	Registerkommunikation	✓		
System Diagnostics Manager	LED	LED	Power, COM	Power, LAN, COM	Power, LAN, COM

					
ICPDAS-Europe GmbH	IPC2U GmbH	Leine & Linde AB	Lenze SE	Meilhaus Electronic GmbH	MEV Elektronik Service GmbH
30950	**23282**	**23763**	**11301**	**11223**	**17016**
Reutlingen	Langenhagen	Hamburg	Aerzen	Alling	Hilter
07121/ 14324-0	0511/ 807-259-0	040/ 3176758-60	05154/ 82-0	08141/ 5271-0	05424/ 2340-57
www.icpdas-europe.com	http://ipc2u.de	www.leinelinde.de	www.lenze.com	www.meilhaus.de	www.mev-elektronik.de
tDS-700 Serie - Device Server	Profi-2541-SC	CANopen Gateway für EnDat Drehgeber	I/O-System 1000	NetCOM PLUS Serie	Tibbo DS1100
max. 3			1 je Modul	1, 2, 4, 8	1
max. 1			0	1, 2, 4, 8	-
max. 3	1	EnDat	0	1, 2, 4, 8	-
✓				1, 2, 4, 8	
52 x 95 x 27 mm	33 x 127 x 105 mm	85 x 132 x 29 mm	60,5 x 76 x 100 mm	je nach Modell	90 x 48 x 25
Hutschienenmontage	Hutschienenmontage	Hutschienenmontage, Wandmontage	Hutschienenmontage	Wandmontage, DIN-Hutschiene	Hutschienenmontage
RJ45; 9pol. D-SUB Buchse / Stecker	9pol. D-SUB Buchse / ST / SC (Multi-Mode)	M23 oder M12 Stecker	Federklemmtechnik	9-pol. Sub-D, 9pol. D-SUB Buchse / Stecker	9pol. D-SUB Buchse / Stecker
TCP/IP			Ethercat, Modbus TCP, Profinet	TCP/IP, Telnet, HTTP, ARP, ICMP	TCP/IP, UDP/IP, HTTP
Modbus-TCP			Ethercat, Modbus TCP, Profinet	EtherNet/IP	
Ethernet	Profibus	CANopen	CANopen, Profibus, DeviceNet		
Internet-Browser (Webbased-Management); Konfigurations-Software		Konfigurations-Software	über Software	Internet-Browser (Webbased-Management), Serielle Konsole, Telnet	Serielle Konsole
			Parametrierung		Tibbo Basic
Power; LAN; COM	PWR LED, TxD LED, RxD LED	Module/Status	LED	Power, WIFI, RDY	LAN, COM, Power

Alle Einträge basieren auf Angaben der jeweiligen Firmen.

					
Anbieter	Microsens GmbH & Co. KG	National Instruments Germany GmbH	Panasonic Electric Works Europe AG	Phoenix Contact Deutschland GmbH	Phoenix Contact Deutschland GmbH
Produkt-ID.	22811	11207	11231	11247	11248
Ort	Hamm	München	Holzkirchen	Blomberg	Blomberg
Telefon	02381/ 9452-0	089/ 741313-0	08024/ 648-748	05235/ 3-41713	05235/ 3-41713
Internet-Adresse	www.microsens.de	www.ni.com	www.panasonic-electric-works.de	www.phoenixcontact.com	www.phoenixcontact.com
Produktname	Indu.-Medienkonverter RS-232/Glasfaser MS650142	NI ENET-232/2	FP Web-Server	FL Comserver UNI 232/422/485	FL Comserver WLAN 232/422/485
Serielle Schnittstelle RS232	1	2	2	✓, 1 Port	✓, 1 Port
Serielle Schnittstelle RS422				✓, 1 Port	✓, 1 Port
Serielle Schnittstelle RS485				✓, 1 Port	✓, 1 Port
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar				wahlweise RS-232/422/485; einstellbar über WB	wahlweise RS-232/422/48,USB; Konfigurierbar mit SW
Maße BxHxT	38 x 116 x 108 mm	21 x 12,4 x 3,7	25 x 90 x 60 (mm)	22,5 x 99 x 114,5 mm	22,5 x 99 x 114,5 mm
Montageart	Hutschienenmontage	Wandmontage	Hutschienenmontage	Hutschienenmontage, NS 35 nach EN 60715	Hutschienenmontage, NS 35 nach EN 60715
Anschluss	9pol. D-SUB Buchse / Stecker	9pol. D-SUB Buchse / Stecker	9pol. D-SUB Buchse / Stecker, Schraubsteckverbinder	RS-232: 9pol. D-SUB, RS-422/485: Schraubkl. Combicon	RS-232: 9pol. D-SUB, RS-422/485: Combicon, Mini USB
Verwendete Ethernetprotokolle		TCP/IP	TCP/IP, UDP/IP, Telnet, HTTP, ARP, ICMP, RFC 1006	TCP/IP; UDP; Modbus-TCP; TFTP; HTTP; PPP; DHCP; BOOTP; SNMP; RIP; ARP; RARP	TCP/IP; UDP; TFTP; HTTP; DHCP; BOOTP; SNMP; RIP; ARP; RARP
Unterstützte Industrial Ethernet Kommunikationsprotokolle			Modbus-TCP	Modbus-TCP	
Feldbus-Anbindung			Modbus	Modbus/RTU; Modbus/ASCII	
Konfiguration der Seriellen Adapter		Konfigurations-Software, Serielle Konsole	Konfigurations-Software	Internet-Browser (Web-based-Management), Serielle Konsole, Telnet	Konfigurierbar mit Konfigurationssoftware über RS-232- Schnittstelle oder USB
Programmierbarkeit bzw. Skripterstellung		Programmierung über LabVIEW oder C/C++/VB	-		
Statusanzeige, Diagnoseinformationen am Seriellen Adapter		Power, LAN, COM	Power, LAN, COM	Spannungsversorgung 24V; Ethernet-Schnittstelle: Link, Datenaktivität, Betriebsart Vollduplex, Übertragungsgeschwindigkeit 100 MBit/s; RS-232/422/485 Sende- und Empfangsdaten; Gerätefehler	Spannungsversorgung 24V; RS-232/422/485 Sende- und Empfangsdaten; 4 stufiger LED-Bargraf und 2 Schaltkontakte zur Anzeige der empfangenen Funkleistung

					
Anbieter	Schneider Electric GmbH	Sigmatek GmbH & Co KG	Spectra GmbH & Co. KG	Spectra GmbH & Co. KG	Sphinx Computer Vertriebs GmbH
Produkt-ID.	11254	22847	11277	11278	11255
Ort	Ratingen	Lamprechtshausen	Reutlingen	Reutlingen	Laudenbach
Telefon	01805/ 753575	0043 6274/ 4321-0	07121/ 1432-10	07121/ 14321-0	06201/ 75437
Internet-Adresse	www.schneiderelectric.de	www.sigmatek-automation.com	www.spectra.de	www.spectra.de	www.sphinxcomputer.de
Produktname	ETG100, ETG1000, ETG3000	ISE 031	JetPort 5601-EU V3.0	I-7530	NPort 5230
Serielle Schnittstelle RS232		✓	1	1	1
Serielle Schnittstelle RS422			1	1	1
Serielle Schnittstelle RS485		✓	1	1	1
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar	1	✓	✓	1	1
Maße BxHxT		12,5 x 103,5 x 72 mm	110 x 114,8 x29,6 mm	72 x 33 x 118 mm	67 x 22 x 100,4 mm
Montageart	Hutschienenmontage	Hutschienenmontage	DIN-Schienenmontage, Wandmontage	Wandmontage, DIN-Schienenmontage	Wandmontage, Hutschienenmontage
Anschluss	9pol. D-SUB Buchse / Stecker, RJ45	Federzugklemme	RJ45	9-pol. D-SUB Buchse / Schraub-Steckklemme	Schraubsteckverbinder
Verwendete Ethernetprotokolle	TCP/IP, HTTP	Varan	IP, TCP, UDP, ICMP, DHCP, BootP, ARP/RARP, SSH, SNMP, HTTPS, SNTP, SMTP		TCP/IP, UDP/IP, Telnet, HTTP, BOOTP, IICMP, DHCP, DNS, SMTP, SNMP
Unterstützte Industrial Ethernet Kommunikationsprotokolle	Modbus-TCP	Varan			
Feldbus-Anbindung				CAN Bus	
Konfiguration der Seriellen Adapter	Konfigurations-Software	Engineering Tool Lasal	Internet-Browser (webbased Management), Konfigurations-Software	Internet-Browser (Webbased-Management), Konfigurations-Software	Internet-Browser (Webbased-Management), Konfigurations-Software, Serielle Konsole, Telnet
Programmierbarkeit bzw. Skripterstellung					
Statusanzeige, Diagnoseinformationen am Seriellen Adapter		Power, COM	Power, LAN, COM	Power, LAN, COM	Power, LAN, COM

					
Plug-In Electronic GmbH **14004** Alling 08141/ 3697-0 www.plug-in.de	Plug-In Electronic GmbH **22798** Alling 08141/ 3697-0 www.plug-in24.com	Pro-face Deutschland GmbH **11239** Solingen 0212/ 25826-0 www.pro-face.de	Process-Informatik Entwicklungsgesellschaft mbH **23402** Wäschenbeuren 07172/ 92666-0 www.process-informatik.de	Quinx AG **32744** Reinach 0041/62/ 76700-40 www.quinx.com	Rockwell Automation GmbH **11292** Düsseldorf 0211/ 41553-0 www.rockwellautomation.de
ES-357	ES-279	GP4201TM	S7-LAN - TCPIP für jede Simtaic S7	Netzwerkadapter DITB-702W	1761-NET-ENI, 1761-NET-ENIW
1 1 1	8		1x MPI / Profibus	1	1 0 0
1		1x RS232/422/485		1	
64 x 91,6 x 25,1 mm	215 x 56 x 123 mm	98 x 55 x 57 mm	65 x 43 x 17 mm (wie ein Profibus-Anschlussstecker)		52 x 118 x 65 mm
Wandmontage	Wandmontage	Wandmontage, Hutschienenmontage	direkt auf die MPI/Profibus-Schnittstelle der Steuerung	Wandmontage	Wandmontage, Hutschienenmontage
Schraubsteckverbinder	9pol. D-SUB Buchse / Stecker, RJ45	9pol. D-SUB Stecker	9pol. D-Sub St. u. Buchse (für Weitergabe d. belegt. Stp.)	9pol. D-SUB Buchse / Stecker	Mini-DIN
TCP/IP	TCP/IP	TCP/IP, UDP/IP	HTTP, RFC 1006, TCP/IP, UDP/IP, ARP,DHCP	TCP/IP; UDP/IP; Telnet; HTTP; ARP; ICMP; WPA; WEP; SNMP; AutoIP; DHCP; TFTP	TCP/IP
		Modbus-TCP, S7-Ethernet, MtM-ASCII, Omron, Mitsubishi, etc., weitere Ethernet Treiber verfügbar	RFC1006 / S7-TCP/IP kompatibel zu CP343-1		EtherNet/IP
			Profibus / MPI		
Internet-Browser (Webbased-Management)	Internet-Browser (Webbased-Management)	über Konfigurationssoftware GP-Pro EX Speicherbefehle in umfangreicher Scriptsprache verfügbar	integrierter WebBrowser oder Konfigurationstool TIC	Quinx DNC-In-The-Box	Konfigurations-Software
Power, LAN, COM	Power, LAN, COM	Power, LAN	Betriebszustand / Linkstatus, Kommunikation	Power; LAN	Power

					
Sphinx Computer Vertriebs GmbH **11256** Laudenbach 06201/ 75437 www.sphinxcomputer.de	SSV Software Systems GmbH **11229** Hannover 0511/ 40000-13 www.ssv-embedded.de	Traeger Industry Components GmbH **11244** Etzenricht 0961/ 48230-0 www.traeger.de	VS Vision Systems GmbH **11271** Norderstedt 040/ 528401-0 www.visionsystems.de	VS Vision Systems GmbH **25411** Norderstedt 040/ 528401-21 www.visionsystems.de	W&T Wiesemann & Theis GmbH **11212** Wuppertal 0202/ 2680-110 www.WuT.de
NPort 5400 Series	IGW/900	S7-LAN TCP/IP für jede Simatic S7	NetCom Plus 811	NetCom Plus 213	Com-Server PoE 3x Isolated
4 4 4	1	1x MPI / Profibus	8		
4	1			2	3
67 x 22 x 100,4 mm	22,5 x 90 x 118 mm	15 x 65 x 45 mm (Größe eines Profibussteckers)	196 x 44 x 147 mm	115 x 73 x 25 mm	45 x 75 x 105 mm
Wandmontage, Hutschienenmontage	Hutschienenmontage	wird direkt auf Profibus / MPI-Schnittstelle gesteckt	Hutschienenmontage, Wandmontage, Rackmount	Wandmontage, Hutschienenmontage	Wandmontage; Hutschienenmontage
9pol. D-SUB Buchse / Stecker o. Schraubsteckverbinder	Schraubsteckverbinder	9pol. D-SUB Buchse / Stecker, Schraubsteckverbinder	9pol. D-SUB Stecker	9pol. D-SUB Stecker	9pol. D-SUB Buchse / Stecker; RJ45
TCP/IP, UDP/IP, Telnet, HTTP, BOOTP, IICMP, DHCP, DNS, SMTP, SNMP	TCP/IP, UDP/IP, Telnet, HTTP	HTTP, RFC 1006, TCP/IP, UDP/IP, ARP, DHCP	TCP/IP, UDP, Telnet, PPP, DHCP, ICMP, HTTP, LPD, SNMP V1/2c/3, DNS, openVPN	TCP/IP, UDP/IP, Telnet, HTTP, ARP, ICMP, BOOTP	TCP/IP; UDP/IP; Telnet; HTTP; ARP; BOOTP
		RFC1006 / S7-TCP/IP kompatibel zum CP 343-1			
	CANopen	Profibus / MPI			Ethernet
Internet-Browser (Webbased-Management), Konfigurations-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Serielle Konsole, Telnet	Konfigurations-Software, Internet-Browser (Webbased-Management)	Internet-Browser (Webbased-Management), Konfigurations-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfigurations-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management); Konfigurati- ons-Software; Serielle Konsole; Telnet; Internet-Brow.
	frei programmierbar über C, C++ o.ä.				
Power, LAN, COM	Power, LAN, COM	Power, LAN	Power, LAN, COM	Power, LAN, COM	Power; LAN; COM

Alle Einträge basieren auf Angaben der jeweiligen Firmen.

					
Anbieter	W&T Wiesemann & Theis GmbH	Wachendorff Prozesstechnik GmbH & Co. KG	Wachendorff Prozesstechnik GmbH & Co. KG	Wachendorff Prozesstechnik GmbH & Co. KG	Wago Kontakttechnik GmbH & Co. KG
Produkt-ID.	**14276**	**11281**	**25430**	**30556**	**11299**
Ort	Wuppertal	Geisenheim	Geisenheim	Geisenheim	Minden
Telefon	0202/ 2680-110	06722/ 9965-20	06722/ 9965-20	06722/ 9965-20	0571/ 887-0
Internet-Adresse	www.WuT.de	www.wachendorff-prozesstechnik.de	www.wachendorff-prozesstechnik.de	www.wachendorff-prozesstechnik.de	www.wago.com
Produktname	USB-Server Industry Isochron	Data Station Plus	1-Kanal-Serielle Schnittstelle RS-232 (ST5211)	Pegelwandler HD67038-25-A1	Serielle Schnittstelle RS-232/RS-485 (750-652)
Serielle Schnittstelle RS232		2	1	1	1
Serielle Schnittstelle RS422		1			1
Serielle Schnittstelle RS485		1		1	1
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar					1
Maße BxHxT	105 x 75 x 22 mm	79 x 135 x 105 mm	12 x 99 x 70 mm	23 x 120 x 107 mm	12 x 65 x 100 mm
Montageart	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage
Anschluss	USB-Buchse Typ A	RJ12 und RJ45 Stecker; Kabeladapter erhältlich	Abnehmbare Anschlussebene in Federzugklemmte.	1 x RS232 (9-polig Sub-D Stecker)	Cage Clamp
Verwendete Ethernetprotokolle	TCP/IP; UDP/IP; HTTP; ARP; BOOTP	TCP/IP, Telnet, UDP/IP, HTTP	TCP/IP, UDP/IP, HTTP, BOOTP		TCP/IP, UDP/IP, HTTP, BOOTP/DHCP, SNMP, SNTP, DNS, FTP
Unterstützte Industrial Ethernet Kommunikationsprotokolle		Modbus-TCP	Ethercat, EtherNet/IP, Modbus-TCP, Profinet		Profinet, Modbus/TCP, EtherNet/IP, Sercos III, BACnet, KNX IP, Ethercat
Feldbus-Anbindung	Ethernet	BACnet	Modbus-TCP/RTU, Profinet, Profibus, Ethercat, EtherNet/IP, Powerlink,CANopen,DeviceNet, CC-Link		Profibus DP, Modbus, LonWorks, Lightbus, Interbus, DeviceNet,CANopen, BACnet, CC-Link, IEC 60870-5
Konfiguration der Seriellen Adapter	Internet-Browser (Webbased-Management); Konfigurations-Software	Konfigurations-Software	Konfigurations-Software (IOGuidePro) o. über Gerätebeschr. (je n. Feldbus: GSD-/GSDML-, EDS, XML)	kostenlose Konfigurationssoftware SW67038 zur Parametrierung des Gerätes	Wago-I/O-CHECK oder GSD-/GSDML-Dateien
Programmierbarkeit bzw. Skripterstellung		Programmierbar durch C-Programmiersprache		kostenlose Konfigurationssoftware SW67038 zur Parametrierung des Gerätes	Registerkommunikation
Statusanzeige, Diagnoseinformationen am Seriellen Adapter	Power; LAN; COM	Power, LAN, COM	5x LED für Modul- und Kommunikationsstatus	4x LED: Signalanzeige für Versorgung und Kommunikation	LED

					
Anbieter	Wago Kontakttechnik GmbH & Co. KG	Weidmüller GmbH & Co. KG	Weidmüller GmbH & Co. KG	Welotec GmbH	Welotec GmbH
Produkt-ID.	**17300**	**11225**	**22775**	**22772**	**22774**
Ort	Minden	Detmold	Detmold	Laer	Laer
Telefon	0571/ 887-0	05231/ 1428-259	05231/ 1428-259	02554/ 9130-16	02554/ 9130-16
Internet-Adresse	www.wago.com	www.weidmueller.de	www.weidmueller.de	www.welotec.com	www.welotec.com
Produktname	Serielle Schnittst. RS-232/RS-485 (750-652/040-000)	IE-CS-2TX-2RS232/485	IE-GW-MB-2TX-1RS232/485	Serieller Geräteserver - SE5002-S5is	Serieller Geräteserver - SE5002
Serielle Schnittstelle RS232	1	2	1		
Serielle Schnittstelle RS422	1	2	1		
Serielle Schnittstelle RS485	1	2	1		
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar	1	2	1	2	2
Maße BxHxT	12 x 65 x 100 mm	36 x 140 x 105 mm	29 x 124,5 x 89,2 mm	90 x 63 x 45 mm	90 x 63 x 45 mm
Montageart	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Wandmontage, Hutschienenmontage	Hutschienenmontage, Wandmontage
Anschluss	Cage Clamp	2 x 9pol. D-SUB Stecker für RS232/422/485	RS-232: 9pol. D-SUB Stecker, RS-422/485: Steckv.	5-pol. Terminal Block (3,81mm)	9pol. D-SUB Buchse / Stecker
Verwendete Ethernetprotokolle	TCP/IP, UDP/IP, HTTP, BOOTP/DHCP, SNMP, SNTP, DNS, FTP	ICMP, IP, TCP, UDP, DHCP, BOOTP, Telnet, Rtelnet, DNS, SNMP, HTTP, SMTP, SNTP, IGMP	TCP/IP, UDP, Modbus-TCP, HTTP, DHCP, BOOTP, SNMP	ICMP, TCP (UDP)/IP, DHCP Client, SNMP, SMTP, HTTP, Telnet	ICMP, TCP (UDP)/IP, DHCP Client, SNMP, SMTP, HTTP, Telnet
Unterstützte Industrial Ethernet Kommunikationsprotokolle	Profinet, Modbus/TCP, EtherNet/IP, Sercos III, BACnet, KNX IP, Ethercat		Modbus-TCP		
Feldbus-Anbindung	Profibus DP, Modbus, LonWorks, Lightbus, Interbus, DeviceNet,CANopen, BACnet, CC-Link, IEC 60870-5		Modbus/RTU , Modbus/ASCII		
Konfiguration der Seriellen Adapter	Wago-I/O-CHECK oder GSD-/GSDML-Dateien	Internet-Browser (Webbased-Management), Konfigurations-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfigurations-Software, Telnet	Web Page, Telnet, Serial console, Windows utility	Web Page, Telnet, Serial console, Windows utility
Programmierbarkeit bzw. Skripterstellung	Registerkommunikation				
Statusanzeige, Diagnoseinformationen am Seriellen Adapter	LED	Spannungsversorgung 1 und 2, Ethernet-Schnittstelle, Übertragungsgeschwindigkeit 10 oder 100 MBit/s, RS-232/422/485 Sende- und Empfangsstatus	Spannungsversorgung 1 und 2, Ethernet-Schnittstelle, Übertragungsgeschwindigkeit 10 oder 100 MBit/s, RS-232/422/485 Sende- und Empfangsstatus	LAN, RUN, COM1Tx, COM2Tx, COM1Rx, COM2Rx	LAN, RUN, COM1Tx, COM2Tx, COM1Rx, COM2Rx

Alle Einträge basieren auf Angaben der jeweiligen Firmen.

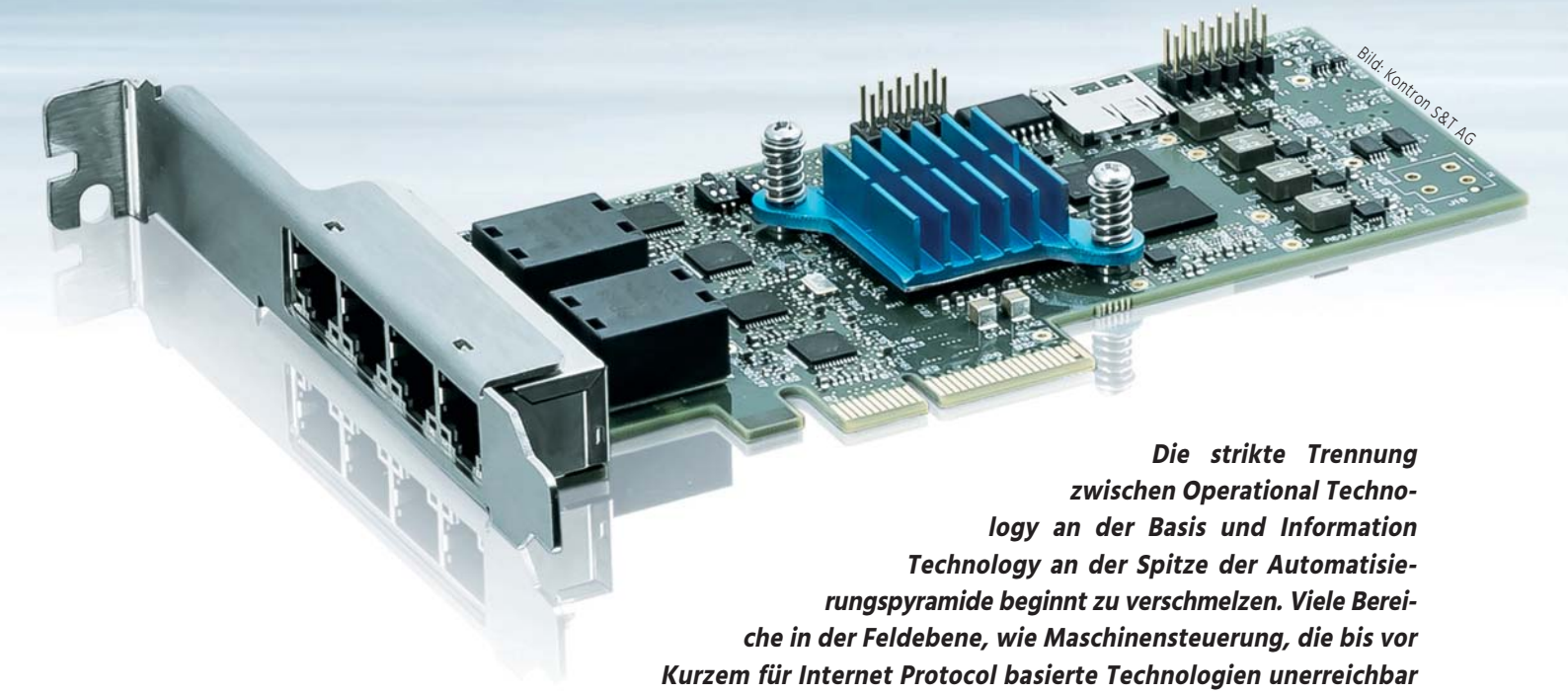
OPC UA-Komponenten

In einer immer vernetzteren Welt ist Security eine der zentralen Grundanforderungen. Auch dies ist einer der Erfolgsfaktoren von OPC UA. Innerhalb weniger Jahre hat sich OPC UA als ein zentraler Standard bei der Lösung der Kommunikationsaufgaben entwickelt – vor allem, aber nicht nur, in der Industrie.

Der Austausch von Informationen über Hersteller- und Protokollgrenzen hinweg steht bei OPC UA im Vordergrund. Hier bietet das System einzigartige Möglichkeiten, die dazu geführt haben, dass sich viele entsprechend zu OPC UA als Kommunikations-Framework committed haben. Dabei waren die eingebauten Sicherheitsmechanismen vermutlich in vielen Fällen mit entscheidend. Die OPC Foundation hat diese Sicherheitsmechanismen nicht neu erfunden, sondern orientiert sich an den Webservice-Securityspezifikationen. Neben der Authentifizierung und Autorisierung kommt als dritte Komponente eine Verschlüsselung zum Einsatz. Die Umsetzung hat weltweit viele Securityexperten überzeugt – so auch das Bundesamt für Sicherheit in der Informationstechnik. Das IIoT braucht eine starke Sicherheitsarchitektur. OPC UA ist ein Baustein, der diese Anforderungen der Unternehmen sehr gut unterstützt. *(kbn)* ■

Internet Protocol statt Feldbus

2018 wird das Jahr von OPC UA und TSN



Die strikte Trennung zwischen Operational Technology an der Basis und Information Technology an der Spitze der Automatisierungspyramide beginnt zu verschmelzen. Viele Bereiche in der Feldebene, wie Maschinensteuerung, die bis vor Kurzem für Internet Protocol basierte Technologien unerreichbar schienen, stehen plötzlich vor einer Zeitenwende. Verantwortlich für den unaufhaltsamen Trend sind unter anderem die rasante Weiterentwicklung von Embedded Hardware zu IoT-Devices und Technologien wie Cloud Computing. Doch um sich in einem anspruchsvollen Industrieumfeld zu etablieren, braucht es auch entsprechende Standards. Open Platform Communications Unified Architecture (IEC62541 OPC UA) in Verbindung mit Time Sensitive Networking (IEEE 802.1 TSN) sind die beiden Standards, die sich rasant durchsetzen. TSN beginnt, den klassischen Feldbus-Spezifikationen Konkurrenz zu machen und hat sogar das Potential, diese mittelfristig zu ersetzen.

Um einen Standard zu etablieren, braucht es immer Player auf Hersteller- und Anwenderseite, die mit aller Kraft daran arbeiten, den Markt dafür zu bereiten. Die großen IT-Anbieter, allen voran Microsoft mit seinem Cloud-Angebot Azure IoT Edge, dringen immer weiter an die Basis der Automatisierungspyramide vor. Kontron hat sich deshalb entschlossen, viele seiner Embedded PCs und Workstations – teilweise auch als Embedded Server – für das Fog- und Edge-Computing mit Microsoft Azure IoT Edge Services zertifizieren zu lassen. Auf der Seite der Standards setzt Kontron voll auf OPC UA und TSN. Der OPC UA Foundation, die den Standard weiterentwickelt und definiert, gehören mittlerweile mehr als 300 renommierte Unternehmen an, darunter auch Kontron. Der Standard, den Microsoft mitentwickelt hat, stellt die Verbindung zwischen der Feldebene und der IT-Ebene her. Um sicher zu gehen, dass der Standard erfolgreich wird, hat Microsoft die entsprechende Spezifikation öffentlich gemacht und bietet die Implementation als Open Source Software an. TSN ermöglicht konvergente Ethernet-basierende Netzwerke, auf denen parallel zum IT-Datenverkehr auch zeitsynchronisierte, deterministische Kommunikation möglich ist, wie sie bei zeitkritischen Maschinensteuerungen und Prozessen unabdingbar sind.

Highlight: Die Kontron TSN-Netzwerkkarte

Ende November 2017 zeigte Kontron die erste Version seiner Standardnetzwerkkarte (NIC), die Time Sensitive Networking (TSN) ermöglicht. Die Spezifikationen des TSN sorgen dafür, dass Datenpakete garantiert zeitgerecht und hoch verfügbar zugestellt werden. Im industriellen Umfeld kann konvergentes, Ethernet-basiertes TSN

Bild: Kontron S&T AG

mit garantierter Latenz und Quality of Service (QoS) mit Zeitsynchronisation proprietäre Feldbussysteme beispielsweise bei der Maschinensteuerung in der Fertigung ergänzen und mittelfristig ersetzen und gleichzeitig nahtlos bis in die IT-Ebene kommunizieren. 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 sternförmigen TSN-Netzwerk verbunden werden. So lassen sich beispielsweise die Kontron Box PCs, 19-Zoll-Server und Workstations der KBox C-Serie, ZINC19 und HPW Produktfamilien problemlos für TSN erweitern. Die TSN-Netzwerkkarte von Kontron umfasst einen integrierten Switch für redundante Netzwerke mit zwei oder vier externen sowie einem internen (via PCIe) Gigabit-Ethernet-Ports. Sie erfüllt alle Spezifikationen gemäß IEEE 802.1 wie Timing und Synchronisation, Traffic Scheduling, Frame Preemption, Stream Reserveration Protocol und weitere. Im FPGA lassen sich zukünftige Erweiterungen durch Software-Updates integrieren. Die TSN-Netzwerkkarte ist für raue Industrieumgebungen entwickelt und kann im industriellen Temperaturbereich von -40 bis +85°C betrieben werden.

2018: Das Jahr von TSN

Mit der Netzwerkkarte und Microsoft Azure Cloud Unterstützung wird Kontron seinen Beitrag zur schnellen Verbreitung von TSN und des OPC UA Standards leisten. Seit der Embedded World 2018 ist ein Starterkit auf Systembasis für TSN erhältlich. Zudem wird die Karte mit Private Labeling angeboten, so dass Maschinenhersteller, Automatisierer und Systemintegratoren die TSN-Karte unter Ihrem Brand in ihre Geräte einbauen und damit ihren Kunden Time-to-market Vorteile für die Integration in TSN-Netze ermöglichen können. Feldbusse werden sicher auf absehbare Zeit nicht ganz verschwinden, TSN in Verbindung mit OPC UA wird sie aber nach und nach ablösen. Bei der Prüfung von Produktionsprozessen im Rahmen von Digitalisierungsstrategien dürfte der IP-Standard immer dann vorgezogen werden, wenn es technisch möglich ist. Und mit OPC UA und der entsprechenden TSN-fähigen Hardware wird plötzlich vieles denkbar. Im Verbund mit S&T ist Kontron nicht nur gut aufgestellt, entsprechende Hardware zu liefern, sondern auch vorintegrierte Cloud-Lösungen beispielsweise für Microsoft Azure IoT Edge Services sowie weitere Software, Services und Beratungsleistungen. ■

Autor: ***Norbert Hauser,***
Vice President Marketing,
Kontron S&T AG
www.kontron.de

Bild: Bachmann Electronic GmbH

Security: Offene Steuerungen im Netz

Wenn Industrie 4.0 Realität werden soll, dann müssen die Systeme sicher mit dem Internet verbunden werden können. Bachmann Electronic rückt das Thema Security daher in den Mittelpunkt. Die Österreicher suchen den Dialog mit den Kunden – nicht nur um ihre Security-Technik zu vermarkten, sondern um gemeinsam mit den Kunden Gefahren zu definieren, auszuschalten und voneinander zu lernen.

ICJ Sie haben auf der letzten SPS IPC Drives ein trojanisches Pferd auf Ihren Messestand gestellt. Was wollten Sie damit demonstrieren?

Christoph Scherrer: *Das Pferd war eingezäunt, von uns und unserer State-of-the-Art Technologie gebändigt. Wichtig ist uns: Unsere Industriekunden dürfen Trojanische Pferde oder Schadsoftware oder Angreifer nicht unwissend in die Produktion lassen, wir wollen aufklären und beim Schutz helfen, denn aus unserer Sicht wird zu wenig über Security gesprochen, die Ausrüster und die Anwender meiden das Thema. Wir brauchen aber den Austausch mit unseren Kunden, um gemeinsam Lösungen zur Verteidigung zu entwickeln.*

ICJ Sind die Anwender unwissend?

Scherrer: *Ja, viele schon. Unwissenheit ist eines der größten Einfallstore für Angreifer. Beispielsweise Shodan.io. Mit der Suchmaschine können Sie offene, nicht geschützte Steuerungen weltweit finden – viele unserer Industriekunden waren überrascht, als wir ihnen die Suchmaschinenergebnisse präsentierten. Das HMI einer Brauerei in Italien anschauen? Kein Problem, alles schnell zu finden. Oder nehmen Sie Google-Dorking. Das ist ein passiver Angriff, mit dem sich Nutzernamen und Passwörter, E-Mail-Adressen, geheime Dokumente, private Finanzdaten und Sicherheitslücken auf Webseiten herausfinden lassen. Angreifer nutzen zudem weitere Suchmaschinen, um offene Steuerungen oder IoT-Geräte zu finden – was im Netz hängt, muss geschützt werden, sonst wird es nichts mit Industrie 4.0, denn es sind nicht nur kriminelle Profis, die auf Jagd nach ICSs gehen, sondern auch Scriptkiddies, die mutwillig zerstören wollen. Das gilt auch für die Fernwartung. Für uns bedeutet das: Wir müssen den Kunden für Security in der Automatisierung sensibilisieren. Ein erster wichtiger Schritt wäre das Ende der Standardpasswörter oder Standard-Betriebseinstellungen und konsequentes Patchen. Unser Solution Center bietet dem User deshalb regelmäßige Updates für sein System an.*

ICJ Das tun ja viele Unternehmen und Aufklärung ist wichtig, aber was tun Sie technisch?

Scherrer: *Klar, wir verschlüsseln Daten und wir haben viel Erfahrung in der Sicherung kritischer Infrastrukturen. Verschlüsselte Speicherbereiche und Dateien schützen kritische Daten wie beispielsweise Log-Files oder Rezepte. Feingranulare Zugriffskontrolle ermöglicht die Freigabe oder das Verbot zum Zugriff auf einzelne Dateien und sogar Variablen, für jeden Benutzer. Überwacht wird dies durch ein zentrales Security-Protokoll, welches jeden An- und Abmeldevorgang sowie sämtliche verändernden Zugriffe aufzeichnet und somit auch im Garantiefall als hilfreiches Instrument dient. Und: Wir können über offene Schnittstellen weitere kryptografische Anwendungen anbinden.*

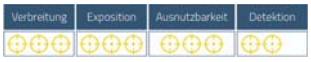
10 Bedrohungen für die Industrie

Über IT-Angriffe sprechen nur wenige Unternehmen. Viele Verantwortliche wissen nicht um die Gefahren. Bachmann Electronic fasst die Ergebnisse des deutschen Bundesministeriums für Sicherheit in der Informationstechnik (BSI) zusammen.

1. Social Engineering und Phishing

Durch meist nicht-technische Handlungen Zugang zu Informationen oder IT-Systemen erlangen.

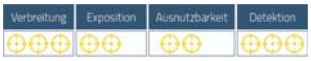
Schutz: Security-Awareness-Training, Sicherheitsrichtlinien, etablieren von Alarmierungswegen, Device Control, Zutrittskontrollen



2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware

Wechseldatenträger wie USB-Sticks sind sehr weit verbreitet.
Mitarbeiter des Unternehmens verwenden diese häufig sowohl in Office- als auch in ICS-Netzen.

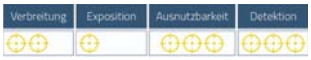
Schutz: Etablieren strikter organisatorischer Vorgaben und technischer Kontrollen



3. Infektion mit Schadsoftware über Internet und Intranet

Unternehmensnetze nutzen Standardkomponenten wie Betriebssysteme, Webserver und Datenbanken. Browser oder E-Mail-Clients sind i. d. R. an das Internet angebunden.

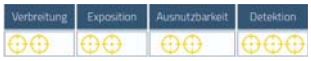
Schutz: Firewalls, VPN, Updates, Überwachung/Monitoring von Logfiles, Beschränkung der im Unternehmen frei verfügbaren Informationen



4. Einbruch über Fernwartungszugänge

In ICS-Installationen sind externe Zugänge für Wartungszwecke weit verbreitet. Häufig existieren dabei z. B. Default-Zugänge mit Standardpasswörtern oder sogar fest kodierten Passwörtern.

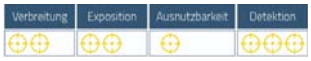
Schutz: Standardnutzer/-passwörter löschen, SSL/TLS-Verschlüsselung, Pre-Shared-Keys, Zertifikate, granulare Segmentierung der Netze, Firewall, Freischaltung von Fernzugängen durch internes Personal, Protokollierung von Fernzugriffen, Zugänge personalisieren, Audits



5. Menschliches Fehlverhalten und Sabotage

Das im Umfeld eines ICS tätige Personal nimmt eine besondere Stellung bzgl. der Sicherheit ein.

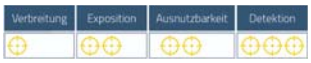
Schutz: Etablieren des 'Need-to-know'-Prinzips, Policies, automatische Überwachung von Systemzuständen und -konfigurationen



6. Internet-verbundene Steuerungskomponenten

Oftmals werden ICS-Komponenten wie speicherprogrammierbare Steuerungen direkt mit dem Internet verbunden.

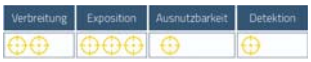
Schutz: Keine direkte Verbindung von Steuerungskomponenten mit dem Internet, Standardpasswörter ändern, Firewall, Patches



7. Technisches Fehlverhalten und höhere Gewalt

Software-Fehler in sicherheitsspezifischen Komponenten und ICS-Komponenten, die zu unvorhergesehenem Fehlverhalten führen können, lassen sich ebenso wenig ausschließen, wie mögliche Hardwaredefekte und Netzwerkausfälle.

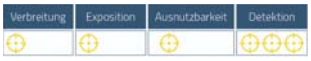
Schutz: Aufbau eines Notfallmanagements, Tausch- oder Ersatzgeräte, Test- und Staging-Systeme, Nutzung von standardisierten Schnittstellen, redundante Auslegung, Zulieferer prüfen



8. Kompromittierung von Extranet und Cloud-Komponenten

Der in der konventionellen IT verbreitete Trend zum Outsourcing von IT-Komponenten hält mittlerweile auch in ICS Einzug.

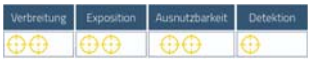
Schutz: Service Level Agreement, zertifizierte Anbieter wählen, Private Cloud-Nutzung, kryptografische Mechanismen, VPN



9. (D) DoS-Angriff

Die Kommunikation zwischen den Komponenten eines ICS kann sowohl über drahtgebundene als auch über drahtlose Verbindungen erfolgen. Werden diese Verbindungen gestört, können beispielsweise Mess- und Steuerdaten nicht mehr übertragen werden. Beispiel: Überlastung einer Komponente durch eine sehr hohe Anzahl von Anfragen, sodass keine fristgerechte Antwort mehr ausgeliefert werden kann.

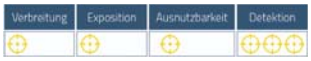
Schutz: Härtung von Netzzugängen, Nutzung dedizierter, kabelgebundener Verbindungen für kritische Funktionen, Intrusion Detection Systeme (IDS) zur Detektion von Angriffen, redundante Anbindung unter Verwendung unterschiedlicher Protokolle



10. Kompromittierung von Smartphones im Produktionsumfeld

Die Anzeige sowie die Veränderung von Betriebs- oder Produktionsparametern auf einem Smartphone oder Tablet wird bei immer mehr ICS-Komponenten als zusätzliche Produkteigenschaft beworben und eingesetzt.

Schutz: Nur lesenden Zugriff, Mobile Device Management, VPN, zertifizierte App-Stores, keine Verwendung von Apps zum direkten Zugriff auf ICS



Reicht das, um für alle Gefahren gewappnet zu sein?

Scherrer: *Nein, sicher nicht. Wir statten unsere M1-Steuerungen zusätzlich mit Funktionen zur Bandbreitenbegrenzung des Netzwerks aus, um die Robustheit gegen absichtliche und unabsichtliche Netzwerkstörungen zu erhöhen. Echtzeitprozesse werden durch Überlastung der Netzwerkschnittstelle nicht gestört. Die bereits erwähnten Maßnahmen zur Zugriffskontrolle und -überwachung sind auch hier wirksam. Diese helfen beim Verhindern unautorisierter Funktionsaufrufe und auch im Fall des Falles bei der Eingrenzung potenzieller Fehlerquellen. Der Betrieb eines komplexen Maschinenparks erfordert ein durchgängiges und zentralisiertes Management der User, ihrer Passwörter und Berechtigungen sowie der Zertifikate. Ebenso müssen Security-Protokolle zentral gesammelt und analysiert werden. Hier bietet Bachmann Unterstützung für die Protokolle LDAP, SCEP und syslog.*

Was müssen Industrieanwender aus Ihrer Sicht tun?

Scherrer: *Wir können Systeme und Ausführungsrechte einschränken und empfehlen den Kunden ein Sicherheitsmanagement mit klaren Richtlinien und einer Rechtevergabe – denn das größte Risiko sind Mitarbeiter im Betrieb, die unwissend oder weil sie frustriert sind die Prozesse zerstören. Unser Automatisierungssystem bietet im Fall der Fälle auch einen Backup- und Recovery-Mechanismus an. Doch wir sollten uns auch bewusst sein: Viele Angriffe registrieren die Unternehmen erst viele Monate nach der eigentlichen Attacke.* ■

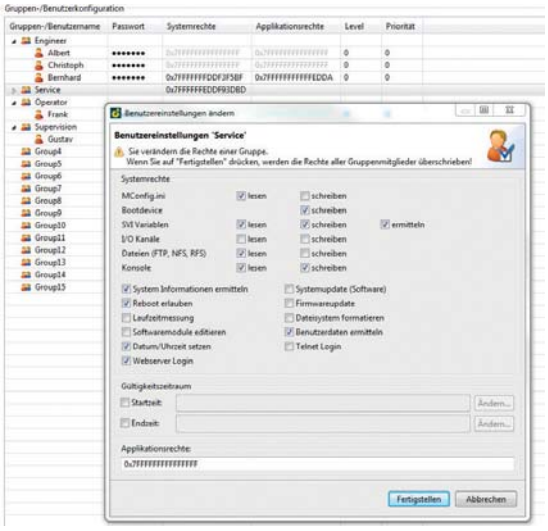


Bild: Bachmann Electronic GmbH

Zentralisiertes Management der User und ihrer individuellen Zugriffsrechte

Christoph Scherrer ist Product Manager Safety and Security bei Bachmann Electronic aus Feldkirch. Scherrer studierte Elektrotechnik an der Technischen Universität in Wien und forschte an der Hochschule zu Themen der funktionalen Sicherheit.

Bachmann Electronic GmbH
www.bachmann.info

Bild: ©jamesteohart / istockphoto.com

LPWAN-Funktechnologie auf dem Vormarsch

Infrastruktur für das Internet of Things

Analysten schätzen, dass 2020 weltweit mehr als 20Mrd. Geräte und Sensoren vernetzt sein werden. Dies erfordert auch einen erheblichen Ausbau der Infrastruktur. In diesem Kontext etablieren sich unter dem Dachbegriff LPWAN (Low Power Wide Area Network) weltweit neue Funknetze. Sie eignen sich im industriellen Umfeld aufgrund ihrer Eigenschaften insbesondere für die Vernetzung von Sensoren.

Der Dachbegriff LPWAN bezeichnet Funktechnologien, die mit wenig Energie betrieben werden können, eine gute Gebäudedurchdringung ermöglichen — bis in Kellergeschosse hinein — und mit denen eine Versorgung vom Campus bis zur internationalen Abdeckung große Gebiete möglich wird. Die hohe Reichweite und Durchdringung geht bislang allerdings zu Lasten der Bandbreite und der Latenz, so dass diese Technologie vor allem als Speziallösung zur Vernetzung von Sensoren, also zum Transport geringer Datenmengen und mit geringen Anforderungen an die Übertragungsgeschwindigkeit und Latenz gilt. Sie ist also nicht geeignet für die Übertragung von Bilddaten oder umfangreichen Maschinendaten im industriellen Umfeld. Als Gegenspieler zum bekannten, breitbandigen Mobilfunkangebot ist sie daher nicht zu sehen (siehe Tabelle 1).

LPWAN in Deutschland und Europa

LPWAN-Technologien bauen teilweise auf existierenden, global heterogenen Mobilfunk-Infrastrukturen (LTE) auf, so dass es eine Reihe von Standards gibt, die gerade auch für globale Projekte Relevanz haben können (Tabelle 2). Die Auswahl der Technologie ist hier jedoch sehr simpel, da sie ausschließlich von der geografischen Region beziehungsweise der zugrundeliegenden LTE-Infrastruktur abhängt. Und – um es noch einfacher zu machen – unterstützen die Hersteller mehrere LPWAN-Technologien auf einem Modul, wodurch die Lösungen mit derselben Hardware weltweit in verschiedenen LPWAN-Mobilfunknetzen eingesetzt werden können.

Situation in Deutschland

Für den Raum Deutschland/Europa ist vor allem der Standard NB-IoT relevant, der netzseitig seit Mitte 2017 in einigen Regionen im Netz der Deutschen Telekom verfügbar ist und auch schon zu Testzwecken genutzt werden kann. Die Netzaufrüstung geschieht über ein Software-Update in den Mobilfunknetzen, so dass mit einer schnellen Flächendeckung bei allen Netzbetreibern zu rechnen ist. Aktuell bieten bereits drei Hersteller Module für NB-IoT an, die jeweils auf den Chips von Huawei aufbauen. Entwickler können heute folglich Module der Hersteller beziehen und sowohl im Mobilfunknetz der Deutschen Telekom als auch in den Laboren der anderen Mobilfunkanbietern oder von Huawei testen.

	LPWAN	2G/3G/4G
Bandbreite	-	+
Latenz	-	+
Reichweite	+	-
Abdeckung/Penetration	+	-
Anzahl Basisstationen	+	-
Kosten Verbinung	+	-
Energieverbraucht	+	-

Bild: Q-loud GmbH

Tabelle 1

	LTE Cat 1	LTE Cat 0	LTE Cat M1	NB-IoT
3GPP Release [info]	Release 8	Release 12	Release 13	Release 13
Downlink Spitzenwert	10 Mbps	1 Mbps	< 1 Mbps	150 kbps
Uplink Spitzenwert	5 Mbps	1 Mbps	< 1 Mbps	150 kbps
Empfängerbandbreite des Endgeräts	20 MHz	20 MHz	1,4 MHz	200 kHz
Max. Sendeleistung des Endgeräts	23 dBm	23 dBm	23 oder 20 dBm	23 oder 20 dBm
Duplexmodus	Vollduplex	Halbduplex (opt.)	Halbduplex (opt.)	Halbduplex

Quellen: Rohde & Schwarz NB-IOT

Bild: Rohde & Schwarz

Tabelle 2

Angebote in lizenzfreien Frequenzbändern

Neben dem NB-IoT Angebot der Mobilfunkanbieter, deren Betrieb in lizenzierten Frequenzbändern erfolgt, entstehen mit Sigfox und LoRa parallel weitere LPWAN-Angebote, die im lizenzfreien ISM-Band im Frequenzbereich 868MHz betrieben werden können. Sigfox wird unter den Bedingungen der Sigfox-Allianz angeboten, so dass prinzipiell auch ein internationales Roaming zwischen Netzen möglich ist. Eher national oder auch lokal zu sehen sind die LoRa-Angebote mit eher niedrigen Eintrittsschwellen. Um eine Großstadt flächendeckend zu versorgen bedarf es beispielsweise weniger als ein Dutzend Antennenstandorte mit Strom und Internetzugang. Dies motiviert aktuell Unternehmen, Städte oder Kommunen auch einfach und kostengünstig eigene Netze aufzubauen.

Bewertung der Angebote

Es ist davon auszugehen, dass bezüglich der Flächendeckung die Mobilfunker in der Lage sein werden, den Vorteil einer bereits vorhandenen Infrastruktur zu nutzen. Vermutlich werden sich hier auch sehr schnell internationale Roaming-Möglichkeiten ergeben. Dieses Angebot ist insbesondere für Anwender attraktiv, die hohe Anforderungen an eine geografische Verfügbarkeit und ggf. auch an eine mobile Nutzung haben. Die Modulkosten und der Verbindungspreis je SIM-Karte sind allerdings aktuell noch relativ hoch, so dass bei wirklichen Massenanwendungen die Berücksichtigung von Alternativen wie z.B. lokale Netze mit einer Anbindung über Gateways sinnvoll ist. Sigfox bietet schon heute eine internationale Abdeckung an. Jedoch ist das Netz gerade in Deutschland nicht flächendeckend ausgebaut. Die Hardware ist relativ kostengünstig verfügbar; zudem gibt es spezialisierte Entwickler, die bei der Umsetzung unterstützen. Das Konsortium investiert erheblich in den Netzaufbau und hat demnach einen hohen Kapitalbedarf, der durch regelmäßige Investitionsrunden gedeckt wird. Der Aufbau eines LoRa-Netzes hat die geringsten Eintrittsbarrieren, so dass dies gerade für Campus oder regionale Anwender attraktiv sein sollte. Denn hierfür gibt es bereits kostengünstige Hardware, und die geringen Aufbaukosten sollten sich auch in für den Nutzer preiswerte Verbindungskosten umsetzen lassen. Unklar ist, ob wirklich flächendeckende Angebote entstehen werden und wie sich der parallele Betrieb unterschiedlicher LoRa-Netze auf die Verbindungsqualität auswirken wird. Dies hat insbesondere dann Relevanz, wenn LoRa ein Erfolg wird und sehr viele Geräte in unterschiedlichen Netzen, aber im selben Frequenzband um die limitierte Bandbreite konkurrieren.

Fazit

Mit der wachsenden industriellen Vernetzung steigt die Notwendigkeit eines Ausbaus der Infrastrukturen. Hierfür etablieren sich derzeit mit LPWAN neue Technologien, die das bestehende Angebot deutlich ergänzen. Eine Option stellen sie immer dann dar, wenn die Bandbreiten- und Latenzrestriktionen akzeptabel sowie die angebotenen Merkmale – insbesondere Stromverbrauch und Gebäudeversorgung – in Verbindung mit geringeren Kosten für das angestrebte Szenario relevant sind. Eine 'One-fits-all-Lösung' ist aber selbst bei diesen neuen Technologien nicht auszumachen: Es gibt kein Angebot, das in allen Eigenschaften den anderen überlegen ist. Daher ist der Auswahlentscheidung stets eine detaillierte Anforderungsanalyse voranzustellen – nur so lässt sich die individuell passende Technologie ermitteln und zum Einsatz bringen. ■

Autor: ***Christian J. Pereira,***
Geschäftsführer,
Q-loud GmbH
www.q-loud.de

Bild: Ergon Informatik AG

Voraussetzung für eine sichere Industrie 4.0

Firewalls für sichere industrielle Web-Anwendungen

Die Vernetzung von Industrieprozessen resultiert in einem hohen Sicherheitsrisiko durch IT-Angriffe. Daher sollten Unternehmen frühzeitig skalierbare Maßnahmen zum Schutz ihrer Anlagen ergreifen, wenn sie Industrie-4.0-Konzepte anwenden möchten.

Das Ziel von Industrie 4.0 ist es, dass Fabriken zu Smart Factories werden und mit weniger Personal immer kürzere Produktzyklen und steigende Produktvarianten zu niedrigen Kosten realisieren können. Um diese Potentiale auszuschöpfen, sind allerdings erhebliche Investitionen erforderlich. Daher ist dieses Thema weit oben in der Agenda der Chefs deutscher Industrieunternehmen. Aber im Industrie-4.0-Konzept muss auch die IT-Sicherheit berücksichtigt werden. Und das entlang der kompletten Wertschöpfungskette eines Produktes. IT-Sicherheit ist eine grundlegende Herausforderung, da die hohe Flexibilität von Industrie 4.0 eine absolute Vernetzung verlangt. Steuerungen müssen beispielsweise große Datenmengen verarbeiten und brauchen eine Vielzahl von offenen Schnittstellen für die Kommunikation mit der industriellen Umgebung.

IT-Security in einer untergeordneten Rolle

IT-Security hat in der Vergangenheit für Fabriken eine geringe Rolle gespielt, da oftmals davon ausgegangen wurde, dass Fertigungsnetze nur in sehr geringer Form oder gar nicht mit externen Netzen gekoppelt würden. In der Praxis jedoch zeigt sich, dass viele Fabriknetze im Zuge der Digitalisierung mit dem Internet verbunden werden. Dabei spielen zum Beispiel Fernwartungsanwendungen eine Rolle. Industrie 4.0 hebt somit die organisatorische Trennung von Office- und Fertigungs-IT auf. Meist sind sensible Konstruktionsdaten von einem Ingenieur erarbeitet worden, die in der Fertigung oder in einem anderen Bereich verwendet werden. Gezielte Angriffe erfolgen nicht nur in den Anlagen selber, sondern können auch über einen Einstieg im Büro-

Bilder: Ergon Informatik AG

bereich erfolgen. Von diesem Einstiegspunkt werden dann weitere Angriffe im Unternehmen durchgeführt, bis hin zu den Produktions- und Steuerungsanlagen. Eine Trennung der Sicherheitsmaßnahmen für verschiedene Unternehmensbereiche ist daher nicht erfolgreich. Angriffe können nur mit einem ganzheitlichen Ansatz verhindert werden.

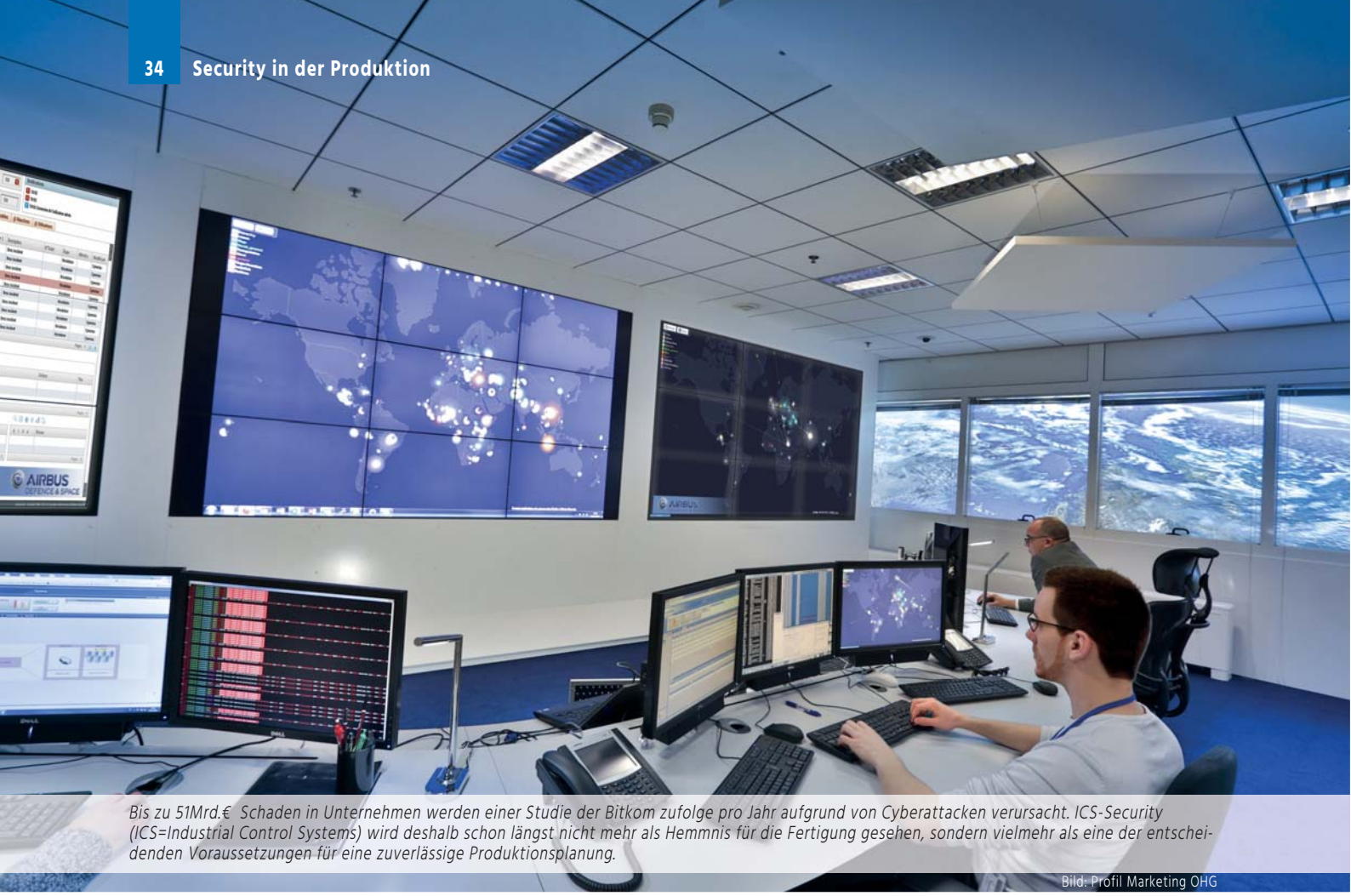
Gefährdete Web-Anwendungen

Das Unternehmen hat im Bürobereich meist viele Web-Anwendungen installiert zu verschiedensten Zwecken: zur E-Mail-Kommunikation, für den Austausch mit Kunden und Lieferanten, aber auch um Industrie 4.0 zu steuern. Durch moderne ERP-Systeme wie SAP oder Oracle, können Lieferanten direkt auf Systemteilbereiche zugreifen und verschiedene Firmenniederlassungen werden direkt miteinander verbunden, um Produktionsprozesse und Warenbestellungen zu automatisieren und zu optimieren. Maschinen beginnen miteinander auf direktem Weg zu kommunizieren. Auch dieser Kommunikationskanal wird immer häufiger mittels sogenannter Webservices von außen zugänglich gemacht. Verbunden mit deren Nutzung ist aber immer eine sichere, digitale Authentifizierung der jeweiligen User erforderlich. Die Integrität von Daten und Identitäten der User muss gewährleistet sein. Eine lückenlose Sicherung und Kontrolle der Web-Applikationen ist daher unverzichtbar.

Traditionelle Lösungen greifen nicht

Unternehmen sind sich jedoch den Gefahren selten bewusst, die durch die Einbindung von Web-Anwendungen entstehen. Klassische Netzwerk-Firewalls schützen nicht gegen Angriffe auf Applikationsebene und oft erhalten schlecht geprüfte Identitäten Zugriff auf sensitive Daten. Die häufig eingesetzten traditionellen Virenschutz- und Firewall-Lösungen greifen hier nicht. Dabei sind 75 Prozent aller Web-Anwendungen verwundbar und damit einer potenziellen Gefährdung ausgesetzt. Wie lässt sich nun dennoch die Sicherheit der Web-Anwendungen mit vertretbarem Aufwand realisieren? Eine praktikable Lösung bieten moderne Lösungen im Bereich Web Application Security: Web Application Firewalls (WAF) können diese Gefahren abwehren. Sie kontrollieren den Inhalt aller gestellten Anfragen und lassen Gefährdungen nicht durch. Da eine WAF den Anwendungen vorgelagert ist, sind alle Applikationen dahinter sicher: Unternehmen können auch neue Anwendungen hinzufügen und die Web Application Firewall schützt sie automatisch mit. Die Sicherheit der Applikationen und Daten wird jedoch erst ausreichend, wenn nicht nur der Inhalt der Anfragen geprüft wird, sondern auch die Identität der Anfragensteller. Das erledigt eine Authentifizierungsplattform. Die vorgelagerte Kombination aus Authentifizierungsplattform und Web Application Firewall schützt Anwendungen vor den bekannten OWASP Top 10-Bedrohungen. Compliance Anforderungen können durch den vorgelagerten Schutz schnell erfüllt und angepasst werden. Außerdem amortisieren sich die Aufwände mit jeder weiteren Applikation, die angeschlossen wird. Um die Benutzerfreundlichkeit – ein entscheidender Faktor für den Erfolg der Digitalisierung – zu steigern sollten auch Single Sign-on und Benutzerselbstverwaltung umgesetzt werden. Statt ein separates Passwort für jede Anwendung zu vergeben, können die Applikationen im bestehenden Single-Sign-on (SSO)-Verbund integriert werden. Der kombinierte Schutz ermöglicht außerdem die Verteilung verschiedener Rollen, die mit entsprechenden Zugriffsrechten ausgestattet sind. So können unbekannte Identitäten beispielsweise nur die öffentliche Website ansehen. Lieferanten hingegen können auf alle für sie relevanten Daten zugreifen, während Unternehmen Mitarbeitern umfassenden Zugriff gewähren können. ■

Autor: ***Gernot Bekk-Huber,***
Head of Marketing bei Airlock,
Ergon Informatik AG
www.airlock.com/de



Bis zu 51Mrd.€ Schaden in Unternehmen werden einer Studie der Bitkom zufolge pro Jahr aufgrund von Cyberattacken verursacht. ICS-Security (ICS=Industrial Control Systems) wird deshalb schon längst nicht mehr als Hemmnis für die Fertigung gesehen, sondern vielmehr als eine der entscheidenden Voraussetzungen für eine zuverlässige Produktionsplanung.

Bild: Profil Marketing OHG

Hightech-Manufacturing:

Angriffe auf die Produktions-infrastruktur abwehren

Wer künftig am Wertschöpfungspotenzial von Smart-Industry-Lösungen partizipieren möchte, muss in punkto Sicherheit umdenken. Denn mit zunehmender Komplexität des Lieferkettenökosystems steigen auch die potenziellen Risiken. Cybersecurity ist damit längst kein Selbstzweck mehr, sondern eine der entscheidenden unternehmerischen Voraussetzungen für den Erhalt der Wettbewerbsfähigkeit in Zeiten der digitalen Transformation.

Wenn es um die Digitalisierung der Wirtschaft geht, überschlagen sich inzwischen die Wachstumsprognosen. Folgt man führenden Wirtschaftsexperten, so warten auf die deutsche Industrie brachliegende Wertschöpfungspotenziale im dreistelligen Milliardenbereich. Eine 2014 durchgeführte Studie des Bitkom-Verbandes schätzt etwa, dass sich durch Industrie 4.0 allein in den Fertigungsbereichen Automotive, Maschinenbau und Elektronik bis zum Jahr 2025 eine zusätzliche Wertschöpfung in Höhe von rund 50Mrd.€ ergeben könnte. Handlungsbedarf ist indessen noch nicht in allen Wirtschaftsbereichen in gleichem Maße gegeben. Die Industrie, im speziellen die Hightech-Fertigung, sieht sich bereits heute einem enormen Digitalisierungszwang ausgesetzt. Denn immer kürzer werdende Produktzyklen und steigender Wettbewerbsdruck machen die digitale Fabrik schon allein aufgrund ihres hohen Optimierungspotenzials für die immer komplexer werdenden Lieferketten zu einem der entscheidenden Zukunftsfaktoren. Zumal der Produktionsprozess eines Flugzeugs, Automobils oder die Herstellung eines Smartphones heute nicht mehr aus einer einzelnen Lieferkette besteht, sondern vielmehr die Summe aus hunderten von verzahnten, exakt aufeinander abgestimmten Wertschöpfungsprozessen und Fertigungsschritten darstellt. Unter diesen Vorzeichen auf Industrie 4.0 zu verzichten, hieße, hart erarbeitete Technologievorsprünge preiszugeben und damit langsam aber sicher seine Marktrelevanz zu verlieren. Auch wenn jeder Technologiehersteller im Rahmen der digitalen Transformation seine ganz eigenen Strategien entwickeln und umsetzen muss, so teilen alle Smart-Industry-Konzepte letztlich ein gemeinsames Paradigma: Die Fertigung der Zukunft ist datengetrieben, vernetzt und transparent. Produktionsprozess, Materialfluss und ERP-Informationen verschmelzen, gleichzeitig wächst die Anzahl von Echtzeitdatenströmen und Verbindungen exponentiell an – und damit auch die Zahl möglicher Sicherheitslücken. Schon jetzt zeigt sich, dass 'klassische' Sicherheitskonzepte, die hauptsächlich auf einer Tren-

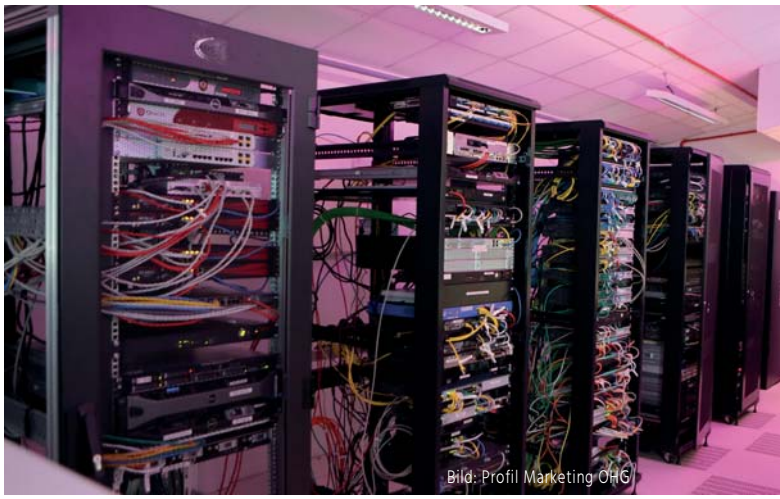
nung von Produktionssystemen und Office-IT beruhen, den Herausforderungen der digitalen Fabrik nicht mehr standhalten werden. Eine Strategie des digitalen Wandels muss deshalb auch die Voraussetzungen für den sicheren Betrieb neuer Technologien einschließen, bei denen die Grenzen zwischen IT-Ebene und Produktionssystemen zunehmend verschwinden. Die technologische Neuausrichtung bietet hierbei einen perfekten Einstiegspunkt für eine grundlegende sicherheitstechnische Bestandsaufnahme und die Bewertung möglicher Sicherheitsrisiken, gerade im Hinblick auf die Planung der eigenen digitalen Agenda.

Gewachsene Strukturen werden zum Sicherheitsproblem

Auch wenn die industrielle Digitalisierung oftmals als Revolution dargestellt wird, so gleicht sie im Prinzip einem kontinuierlichen Prozess, der bereits in den achtziger und neunziger Jahren begonnen hat. Als die moderne Automatisierungstechnik ihren Anfang nahm, steckte das Internet noch in den Kinderschuhen. Niemand hat seinerzeit ernsthaft an die Möglichkeit gedacht, Produktionssysteme mit dem Internet zu verbinden. Industriesteuersysteme wurden als isolierte Einheit betrachtet – Sicherheitsfunktionen wie Authentifizierungsmechanismen, Passwortmanagement oder Zugriffsbeschränkungen waren demnach nicht notwendig und auf Protokollebene schlichtweg nicht vorgesehen. Für ein Produktions-Subsystem genügte es, per Zweidrahtleitung oder Funk an eine höhere Hierarchie wie beispielsweise ein SPS-System angeschlossen zu sein, denn praktische Vorteile wie Echtzeitfähigkeit und Zuverlässigkeit waren die entscheidenden Parameter im Produktionsverbund. Doch trotz der hohen Echtzeitanforderungen ist das Zeitalter des Internets nicht spurlos an der Fertigungsebene vorbeigezogen. Wo die Flexibilität von TCP/IP von Nutzen war oder Kosten eingespart werden konnten, wurden in den vergangenen Jahren viele Verbindungen auf das IP-Protokoll umgestellt – jedoch nicht immer mit der notwendigen Systematik und nur selten mit dem entsprechenden IT-Sicherheitsbewusstsein. Einer der Haupttreiber war dabei die Bereitstellung von Fernzugängen. Technikern und Wartungspersonal von Anlagen-Herstellern sollte ein schneller Zugriff auf die Managementoberflächen von Produktionssystemen ermöglicht werden, um Konfigurationsänderungen vorzunehmen, den Status von Maschinen einzusehen oder wichtige Updates einzuspielen – und dies, ohne dabei hohe Arbeits- oder Anreisekosten zu verursachen. Als Folge entstanden so organisch gewachsene Vernetzungsstrukturen mit einer heterogenen Architektur aus industriespezifischen Protokollen, lokalen Netzknoten mit Anbindung an die Office-IT und mehr oder weniger offenen Internet-Zugängen – meist mäßig dokumentiert, unzureichend segmentiert und mangels verfügbarer Richtlinien auch ohne einheitliche Standards für Zugriffsmanagement und Passwortsicherheit.

Vom Silo-Denken zum fachübergreifenden Konsens

Bei Produktionsspezialisten und Automatisierern mag der Mix-and-Match-Zustand vieler Industrienetze zunächst keine Bedenken auslösen. Denn immerhin werden Funktionen, die die Betriebssicherheit von Anlagen gefährden könnten, auf Feldebene getrennt ausgeführt und redundant ausgelegt. Sicherheitsrelevante Grenzwerte wie Maximaldrücke oder Drehzahlen von Pumpen sind ohnehin hartkodiert. Hinzu kommt, dass die verwendeten industriespezifischen Protokolle für mögliche Angreifer eine hohe technische Hürde darstellen. Angesichts der Entwicklung der vergangenen Jahre reichen diese Aspekte für sich allein jedoch nicht mehr aus. Denn nicht nur die Anzahl der IP-Verbindungen hat bereits stark zugenommen, sondern auch die Bedrohungslage selbst ist heute eine völlig andere als vielleicht noch vor fünf Jahren. Spätestens seit dem Auftauchen von Stuxnet sowie weiteren, auf Industrienetze spezialisierten Malwarevarianten wird die Diskussion über Sicherheit in Produktionssystemen verstärkt in der Öffentlichkeit geführt. Hinzu kommt, dass inzwischen auch spezialisierte Suchmaschinen existieren, die gezielt nach offenen Internetverbindungen mit produktionsspezifischen Protokollen suchen können. Eine aktuelle ICS-Security-Studie (ICS=Industrial Control Systems) des Sicherheitsspezialisten Kaspersky Lab lieferte unlängst rund 26.000 unsichere ICS-Komponenten, die allein in Deutschland problemlos über das Internet erreichbar waren. Das dies kein wünschenswerter Ist-Zustand für den reibungslosen Betrieb einer Produktionsumgebung sein kann, ist mittlerweile fachübergreifender Konsens. Auch das ursprüngliche Silo-Denken zwischen IT-Verantwortlichen und Produktionsleitern löst sich dank zunehmender Berichterstattung, vermehrter Aufklärung in Forschung und Lehre sowie standardisierter Sicherheitsrichtlinien (IEC62443) mehr und mehr auf. Inzwischen werden professionell koordinierte Sicherheitsinitiativen von den meisten Produktionsleitern begrüßt oder sogar aktiv gefordert. Immerhin sind sie letztlich für einen reibungslosen Fertigungsablauf und einen effizienten Anlagen-Output verantwortlich. Ein komplexer Hackerangriff oder ein auf Industrieanlagen spezialisierter Schädling gefährdet diese Zielsetzung. Laut dem BSI vergehen 227 Tage, bis eine gezielte Attacke auf ein Unternehmen bemerkt wird – so lange sitzt der Angreifer im Durchschnitt im Unternehmen, kann spionieren, Manipulationen vorbereiten, ohne dass jemand weiß, dass ein Problem vorliegt. Schon ein einzelner Sicherheitsvorfall kann zu langanhaltenden und sehr teuren Produktionsausfällen oder zur Offenlegung brisanter Betriebsgeheimnisse führen – speziell in der Hochtechnologiefertigung wie auch beim Aufbau der Produktionsumgebung selbst, denn in der Architektur



Die technologische Neuausrichtung bietet einen guten Einstiegspunkt für eine sicherheitstechnische Bestandsaufnahme und die Bewertung möglicher Sicherheitsrisiken, gerade im Hinblick auf die Planung der eigenen digitalen Agenda.


Bild: Profil Marketing OHG

Im Rahmen seiner Security-Services entwickelt Airbus CyberSecurity ganzheitliche Sicherheitsstrategien, die auf einer Risikoanalsyse basieren mit der Zielsetzung den Top-Risiken wirksam zu begegnen.

von Feldbusebene und MES-Systemen sowie der Parametrisierung von speicherprogrammierbaren Steuerungen steckt mitunter jahrzehntelanges Entwicklungs-Know-how und damit geistiges Eigentum, das unbedingt geschützt werden muss. Bis zu 51Mrd.€ Schaden in Unternehmen werden pro Jahr, so eine Studie der Bitkom, aufgrund von Cyberattacken verursacht. ICS-Security wird deshalb schon längst nicht mehr als Hemmnis für die Fertigung gesehen, sondern vielmehr als eine der entscheidenden Voraussetzungen für eine zuverlässige Produktionsplanung. Dieses Umdenken war zwingend nötig, denn ohne die Fachkenntnis von Produktionstechnikern und Prozessleitingenieuren lassen sich Fertigungsumgebungen nicht praxisgerecht absichern. Erst ein interdisziplinärer Ansatz, bei dem die Sichtweisen von IT- und Produktionsspezialisten sinnvoll zusammengeführt werden, ist in der Lage, Echtzeitanforderungen und Sicherheitsmechanismen zu einem ausbalancierten Sicherheitskonzept zu verbinden. Dabei müssen auch IT-Security-Spezialisten ihre Sichtweisen überprüfen und gegebenenfalls einen nachhaltigen Perspektivwechsel vornehmen, denn auch ein übertriebener Einsatz von IT-Security-Maßnahmen ist in der Feldebene nicht zielführend. Er würde letztlich in einen starren Produktionsverbund münden, der an den Praxisanforderungen der Fertigungsumgebung vorbeigeht. Deshalb gilt gerade bei der Absicherung von Fertigungsumgebungen: 'One-size-fits-all'-Lösungen sind meist fehl am Platze, entscheidend sind die individuellen Anforderungen des einzelnen Betreibers.

Risikobewertung führt zum zuverlässigen Produktionsverbund

Für einen Security-Anbieter liegt die Herausforderung bei der Absicherung von Produktionsumgebungen deshalb vor allem darin, maßgeschneiderte Sicherheitskonzepte zu finden, die sich technisch und organisatorisch nahtlos in die vorhandenen Fertigungsabläufe einbetten lassen. Voraussetzung hierfür sind nicht nur theoretische Grundlagenkenntnisse und ein gut ausgebildetes Spezialisten-Team, sondern auch ein hohes Maß an Praxiserfahrung. Als eines der führenden Hochtechnologieunternehmen Europas blickt Airbus auf eine lange Tradition in der Fertigung von Hightech-Produkten mit hohem Schutzbedarf zurück. Viele Erfahrungswerte und analytische Methoden des Geschäftsbereichs CyberSecurity stammen dabei direkt aus dem unternehmenseigenen operativen ICS-Umfeld und haben sich in der Praxis schon vielfach bewährt. Industrial Security ist, wie auch der digitale Wandel insgesamt, kein definierter Endzustand, sondern ein kontinuierlicher Prozess. Ein grundlegender erster Schritt auf dem Weg zu einer validen ICS-Sicherheitsstrategie muss deshalb eine detaillierte Risikoanalyse sein. Diese Vorgehensweise empfiehlt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Im ICS-Security-Kompendium des BSI heißt es hierzu: „Die Durchführung einer wiederkehrenden (regelmäßigen bzw. anlassbezogenen) Risikoanalyse wird als verpflichtend angesehen". Im Rahmen seiner umfassenden Security-Services entwickelt Airbus CyberSecurity ganzheitliche Sicherheitsstrategien, die exakt auf solch einer Analyse basieren. Zielsetzung ist dabei, in direkter Zusammenarbeit mit IT- und Produktions-Teams des Betreibers die fünf Top-Risiken zu identifizieren und zu dokumentieren sowie praktikable Gegenmaßnahmen zu empfehlen.

Die Zielsetzungen umfassen im Einzelnen:

- Den Aufbau von sicheren Remote-Zugängen für Wartung und Analyse
- Die Absicherung des Produktionsverbundes sowie die Isolierung oder Überwachung von mit Schwachstellen behafteten Altsystemen durch passive Security Sensoren
- Die Sicherung von Endpoints, Datenbanken und Servern (MES, HMI-Stationen, Notebooks und Mobilgeräten)
- Die sichere Nutzung von portablen Medien wie USB-Sticks oder CDs

Wissenstransfer und die Bereitstellung einer Methodik für eine kontinuierliche Risikoanalyse

Die Absicherung von Produktionsanlagen ist gerade für Hochtechnologieunternehmen eine komplexe Herausforderung mit zuweilen hohem Kostenaufwand. Vor dem Hintergrund von Industrie 4.0 und IoT (Internet of Things) ist eine sicherheitstechnische Bestandsaufnahme jedoch unumgänglich, um den digitalen Wandel auf eine solide Basis zu stellen. Ein Security-Assessment bietet dazu einen sinnvollen Einstiegspunkt und ist der Grundstein für alle weiteren Handlungsempfehlungen sowie den Aufbau einer langfristigen Sicherheitsstrategie. Die Kosten der Analyse bleiben dabei in einem überschaubaren Rahmen und amortisieren sich schnell durch die Minimierung von Ausfallrisiken sowie einen insgesamt zuverlässigeren Produktionsverbund. ■

Autor: ***Daniel Scheerer,***
Portfolio Manager OT Security,
Airbus CyberSecurity
www.airbus-cyber-security.com/de/

Bild: Phoenix Contact Deutschland GmbH

PoE-Injektoren versorgen Ethernet-Geräte über ein gemeinsames Kabel mit Energie und Daten.

Neue PoE-Injektoren mit zusätzlichen Funktionen

Höhere Anlagenverfügbarkeit bei kürzerer Installationszeit

In einer zunehmend vernetzten Welt kommt dem durchgehenden Zugriff auf die Daten aller Prozesse eine große Bedeutung zu. Das Power-over-Ethernet-Verfahren unterstützt bei ihrer einfachen Integration in bestehende Netzwerke. Durch den Einsatz der neuen PoE-Injektoren von Phoenix Contact spart der Anwender viel Zeit bei der Installation und schützt die angebundenen Geräte sowie die Datenübertragung vor Überspannungen, unterschiedlichen Potentialen und EMV-Einflüssen.

Als herstellerübergreifender IEEE-Standard hat sich Power over Ethernet (PoE) seit mehr als zehn Jahren in industriellen Anwendungen etabliert. Durch die Verwendung der PoE-Technologie lässt sich der Verdrahtungsaufwand reduzieren. Außerdem gestaltet sich die Vernetzung flexibler und die schlanke PoE-Verkabelung senkt die Installationskosten. Abgesetzte Netzwerkteilnehmer, die sich beispielsweise im Außenbereich von Gebäuden befinden, benötigen nämlich nur eine Leitung zur Übermittlung von Daten und Energie. Bei den anzukoppelnden Geräten geht es beispielsweise um Access Points, Zutrittskontrollen oder die erheblich steigenden Anwendungen mit einer Kameraüberwachung. Im Bürobereich hat sich Power over Ethernet längst zur Versorgung von Voice-over-IP-Telefonen (VoIP) durchgesetzt. Bei der PoE-Technologie wird die Energie für das zu beliefernde Gerät über die Datenleitung transportiert. Die dazu erforderliche Leistung handeln der Abnehmer – das Powered Device (PD) – und der Versorger – das Power Sourcing Equipment (PSE) – elektrisch untereinander aus. Anschließend wird die Versorgungsspannung über die nicht genutzten Leitungen der achtadrigen Verkabelung bis zu einer Übertragungsgeschwindigkeit von 100MBit/s gespeist (Modus A). Alternativ ist eine sogenannte Phantom-

speisung mit einer Datenrate bis 1GBit/s moduliert über die Datenleitungen möglich (Modus B). Der Modus wird selbständig ausgehandelt, lässt sich aber auf Wunsch über Dip-Schalter fest vorgeben. Das PSE kann ein Mehrport-PoE-Switch oder ein PoE-Injektor als Stand-Alone-Lösung sein.

Internes Netzteil mit galvanischer Trennung

Für die verschiedenen Leistungsklassen stellt Phoenix Contact zur Hannover Messe 2018 neue PoE-Injektoren zur Verfügung. Mit bis zu 30W Versorgung erfüllen die Geräte die Standards IEEE802.3 af (15,4W) und 802.3 at (30W). Obwohl der kommende Standard IEEE802.3 bt derzeit noch nicht verabschiedet ist, sind die PoE-Injektoren bereits optional entsprechend ausgelegt. Die 60W-Komponenten können z.B. leistungsstarke PTZ-Kameras (Pan Tilt Zoom – Schwenken, Neigen, Zoomen) beliefern, die oftmals eine integrierte Infrarotheizung umfassen, um das Beschlagen der Scheibe zu verhindern. Zu diesem Zweck ist eine höhere Leistung notwendig, als sie der bisherige PoE-Standard IEEE802.3 at bis 30W bereitstellen kann. Neben den unterschiedlichen Leistungsklassen bis 60W zeichnen sich die PoE-Injektoren durch einen weiten Betriebstemperaturbereich von -40 bis 75°C aus. Die Geräte werden über einen redundanten Eingangsspannungsbereich von 18 bis 57VDC versorgt und erlauben somit die Verwendung von 24VDC- und 48VDC-Netzteilen. Zur Absicherung von Kurzschlüssen auf der PoE-Versorgungsleitung bietet das interne Netzteil eine galvanische Trennung. Diese schützt den PoE-Injektor, aber auch vorgeschaltete Netzteile und andere Komponenten im Versorgungssegment vor der Zerstörung durch einen Kurzschluss zwischen den PoE-führenden Datenleitungen und gegen den Kabelschirm. So lassen sich erhebliche Kosten vermeiden. Zudem ist die Nutzung von galvanisch getrennten Netzteilen in zahlreichen Anwendungen vorgeschrieben.

Bild: Phoenix Contact Deutschland GmbH

Die PoE-Injektoren stehen in RJ45-, Schraub-, Push-in- und IDC-Schnellanschlusstechnik zur Verfügung.

Integrierter Schutz vor eingekoppelten Spannungen

Erstmals verfügen die PoE-Injektoren wahlweise über einen integrierten Überspannungsschutz. Dies, weil Ethernet-Schnittstellen mit niedrigen Signalpegeln bei hohen Frequenzen arbeiten. Das macht sie besonders empfindlich in Bezug auf Überspannungen, die zur Zerstörung der teuren Netzwerkkomponenten führen können. Gerade bei einer Gebäude- oder Schaltschrank-übergreifenden Verkabelung sind die Geräte bei einkoppelnden Spannungen gefährdet. Der in die Injektoren eingebaute Überspannungsschutz entspricht dem Standard DIN EN61643-21 mit der IEC-Prüfklasse C2. Dabei ist der feldseitige, PoE-führende Port als Überspannungsschutz-Schnittstelle gedacht. Die Lösung sichert alle acht Signalwege ab. Die neuen PoE-Injektoren überzeugen ferner durch eine patentierte Schirmstromüberwachung. Ist die Installation durch verschiedene Potentialbezüge gekennzeichnet, können Ausgleichsströme über den Kabelschirm fließen. Daraus resultieren unter Umständen eine Beschädigung kostspieliger Betriebsmittel und damit der Stillstand der kompletten Fertigung. Daher beinhalten die PoE-Injektoren INJ 2000 eine einfache Diagnose. Vorhandene Ausgleichsströme oder eingekoppelte Ströme auf der PoE-führenden Leitung werden messtechnisch ermittelt und über eine LED angezeigt. Diese leuchtet bei einem Kabelschirmstrom ab 30mA auf. Dem Anwender wird somit visualisiert, dass in seiner gesamten Installation ein generelles Erdungsproblem vorliegt. Einzelne Schaltschränke oder Gebäudeteile sind also möglicherweise nicht sachgerecht untereinander potentialverbunden oder bei der Kabelverlegung gibt es zu viele Einkopplungsmöglichkeiten für elektromagnetische Einflüsse.

Der integrierte Überspannungsschutz und die Schirmstrom-Überwachung erhöhen die Anlagenverfügbarkeit.

Bild: Phoenix Contact Deutschland GmbH

Patch-Panel für viele Anschlusstechnologien

Die PoE-Injektoren verfügen erstmals über eine integrierte Patch-Panel-Funktion. Die bisher übliche RJ45-Buchse für beide Ethernet-Ports wird durch Klemmtechnologien zum Anschluss der PoE-führenden Feldleitung ergänzt. Durch die einfache Anbindung der Leitung an den Injektor entfällt folglich die aufwändige Montage eines RJ45-Steckverbinders mit speziellem Werkzeug. Ebenso erübrigt sich das Platzieren eines separaten Patch-Panels mit einem Verbindungs-Patchkabel. Das spart Kosten und Platz auf der Tragschiene. Wie bereits erwähnt, unterstützen die neuen PoE-Injektoren unterschiedliche Anschlusstechnologien, um die individuellen Wünsche der Anwender zu erfüllen. Aufgrund der einfachen,

schnellen und sicheren Installation wird der Zeitbedarf so um bis zu 60 Prozent reduziert, was die Montage wirtschaftlich gestaltet. Je nach gewählter Variante legt der Mitarbeiter die PoE-führende Feldverkabelung auf die Schraub-, Push-in- oder IDC-Anschlussklemmen auf. Neben der üblicherweise verwendeten Schraubanschlusstechnik erlaubt die Push-in-Klemme eine komfortable Ankopplung. Die größte Zeitersparnis eröffnet allerdings die IDC-Schnellanschlusstechnik. Bei diesem Schneidklemmverfahren werden die Einzeladern nicht mehr abisoliert, sondern die Drähte einfach in den Schacht geschoben und die Klemme mit dem Finger geschlossen. Auf der Unterseite des geöffneten Deckels ist der Farbcode zum Anschließen der Drähte gemäß TIA 568A, TIA 568B und Profinet abgedruckt. Außerdem zeigt eine Strichmarkierung die korrekte Abmantellänge des Kabels an. Nachdem der Anschluss erfolgt ist, wird der Klappdeckel geschlossen. Er bedeckt nun den Anschlussraum der Feldkabelseite mit den Anschlussklemmen sowie der Schirmkontaktierung und sorgt so für ein einheitliches Installationsbild. Abgesehen vom optischen Aspekt werden die empfindlichen Anschlussdrähte vor äußeren Einflüssen geschützt.

Der Kabelschirm wird einfach und werkzeuglos bei gleichzeitiger Zugentlastung angebunden.

Bild: Phoenix Contact Deutschland GmbH

Kabelschirm-Kontaktierung mit Zugentlastung

Die PoE-Injektoren INJ 2000 mit Patch-Panel-Funktion verfügen ferner über eine neue und patentierte Art der Schirmkontaktierung. Sie ermöglicht die werkzeuglose Anbindung des Kabelschirms mit einer gleichzeitigen Zugentlastung. Eine Schirm-Kontaktierungsfeder drückt das Kabel mit dem nach hinten über den Kabelmantel geführten Schirmgeflecht an eine Kontaktierungsfläche, die sich direkt auf der Leiterbahn befindet. Dazu wird das Kabel einfach in den Schacht gelegt und das Federblech mit dem Finger zugedrückt, bis es am Gehäuse verrastet. Auf diese Weise haftet nicht nur der Kabelschirm großflächig an; das Kabel erhält zudem eine Zugentlastung von bis zu 50 Newton. Zum Lösen der Verbindung muss der Anwender die Verriegelung lediglich mit einem Schraubendreher aufhebeln. Schließt er den Gehäusedeckel nach dem Kabelanschluss mit einem leichten Druck, öffnet sich die Schirmkontaktierung selbst bei starken Vibrationen nicht. Die Schirmung ist also sicher sowie direkt über die Tragschiene mit dem Erdpotential verbunden. Alle auf dem Kabelschirm befindlichen Störungen können so abgeleitet werden.

Fazit

Die neuen PoE-Injektoren von Phoenix Contact versorgen im Feld installierte Geräte über ein Kabel mit Daten und Spannung bis 60W. Neue Funktionen wie der integrierte Überspannungsschutz und die Schirmstromüberwachung stellen einen störungsfreien Betrieb der Applikation sicher, während das eingebaute Patch-Panel die Installationskosten senkt und Platz im Schaltschrank spart. Aufgrund des weiten Betriebstemperaturbereichs und der hohen Übertragungsrate bis 1GBit/s bieten sich die Geräte u.a. zur Belieferung von Überwachungskameras an. ■

Autor: ***Bernd Rosenbaum,***
Produktmanager Communication Interfaces,
Phoenix Contact Electronics GmbH
www.phoenixcontact.de/webcode/#1789

Neue Ethernet-Patch-Panel zur schnellen Verkabelung

Patch-Panels dienen der strukturierten Verkabelung und sparen viel Zeit bei der Installation.

Bild: Phoenix Contact Deutschland GmbH

Die Anschlusstechniken und Schutzmechanismen der PoE-Injektoren kommen auch in den acht neuen Ethernet-Patch-Panels von Phoenix Contact zum Einsatz, die in zwei Funktionsgruppen zur Verfügung stehen. Die passiven Übergabemodule erlauben eine einfache und schnelle Verbindung zwischen der Feld- und Schaltschrankverkabelung. Neben den Standard-Modulen in kompakter Bauform umfassen die neuen Patch-Panels einen integrierten Überspannungsschutz. Er sichert die angekoppelten Endgeräte ab und trägt damit zu einer hohen Anlagenverfügbarkeit bei. Das gilt für die zusätzliche Schirmstromüberwachung, denn eine LED zeigt Erdungsprobleme in der Anwendung an. Verschiedene Technologien wie IDC-, Schraub- und Push-in-Anschlusstechnik erleichtern die Anbindung des Feldkabels. Bei gleichzeitiger Zugentlastung wird der Kabelschirm werkzeuglos angeschlossen, was zu einer deutlichen Zeitersparnis führt

Kontinuierliche Weiterentwicklung bringt maximale Sicherheit und Flexibilität:

Kommunikationslösungen für die Fabrik von morgen

Es braucht keine Glaskugel um sagen zu können, dass in fünf bis zehn Jahren cloudbasierte Datenspeicherung und die entsprechende Analyse in der Automatisierungstechnik Stand der Technik sein werden. Auch wenn es bei der praktischen Umsetzung noch viele Fragezeichen gibt, ist die Richtung vorgegeben. Wer heute auf die Integration cloudbasierter Kommunikationslösungen verzichtet, nur weil es bislang noch kein standardisiertes Patentrezept gibt, läuft Gefahr den Anschluss zu verpassen.

Bevor man über die Zukunft industrieller Anlagen spricht und welche Rolle datenbasierende Geschäftsmodelle dabei künftig spielen, sollte man einen Blick auf den aktuellen Stand der Technik werfen. Typischerweise sind industrielle Anlagen mit mindestens einer oder mehreren Speicherprogrammierbaren Steuerungen (SPS) ausgerüstet. Wo mehrere SPSen im Einsatz sind, stammen sie nicht selten von unterschiedlichen Herstellern. Nach heutigem Stand verbleiben in den meisten Anwendungen Prozess- und Anlagedaten noch in der Fertigungsebene, werden also nicht auf Planungsebene genutzt. Zudem sind vielen Geräteherstellern, Anlagenbauern, Maschinenbauern und Systemintegratoren nach wie vor die Vorteile unklar, die Industrie 4.0 bzw. IIoT allen Beteiligten in diesem Zusammenhang bringen kann. Deshalb vorab einige der Vorteile im Kurzüberblick.

Viele Vorteile

Während der Produktion fallen in der Anlage Unmengen an Daten an. Sammelt man diese Daten zentral und analysiert sie mit den entsprechenden Tools, lassen sich Fertigungsprozesse optimieren, das ist keinem neu. Weitere Vorteile entstehen jedoch, wenn man diese Daten in der Cloud ablegt, denn dann können sie Anlagenbetreiber gemeinsam mit ihren Geräteherstellern oder Maschinenlieferanten untersuchen und zusammen Prozesse verbessern. Für Maschinenbauer entsteht über cloudbasierte Datenspeicherung und Analyse die Möglichkeit, Wartungsverträge und -zyklen ideal an die Bedürfnisse der Anwender anpassen. Zudem wird in vielen Fällen Fernwartung möglich und bei Problemen kann aus der Ferne geholfen werden. So lassen sich viele Anlagenstillstände vermeiden oder Stillstandzeiten deutlich verkürzen. Auch vorausschauende Wartung wird damit einfacher. Zudem lassen sich Pay-per-Use-Anwendungen mit Cloud-Lösungen sehr gut realisieren: Anbieter von Dienstleistungen oder Arbeitsmitteln können ihre Vertriebskonzepte dahingehend umstellen, dass der Verbraucher nur das bezahlt, was er wirklich auch nutzt. Wo bei Verbrauchsgütern Nachschub geliefert werden muss, lassen sich automatisiert Bestellungen auslösen und dadurch die Logistik vereinfachen. Zusätzlich profitiert auch der Anlagenbetreiber durch die cloudbasierte Datenspeicherung und Analyse von der vorausschauenden Wartung und standortübergreifenden Optimierung von Materialfluss und Logistik.

Viele Vorbehalte

Aus theoretischer Sicht überzeugen die möglichen Vorteile Gerätehersteller, Anlagenbauer, Maschinenbauer und Systemintegratoren längst. Allerdings müssen diese Vorteile auch in der Praxis nutzbar werden. Hier stößt die Cloud-Kommunikation auf ganz unterschiedliche Vorurteile und Hürden. Da in dem Bereich noch Standards fehlen, haben viele z.B. Angst aufs falsche Pferd zu setzen. Deshalb abzuwarten und erst einmal nicht aktiv zu werden, ist jedoch das Schlechteste was

IIoT Gateway für den Maschinenbau

Der Router eWON 205 Flexy ist ein vielseitiges Gateway für Industrie 4.0 bzw. IIoT (Industrial Internet of Things). Es wurde speziell für den Maschinenbauer konzipiert, der seinen Kunden mithilfe von Maschinendaten einen Mehrwert gegenüber dem klassischen Fernzugriff bieten möchte. Zu den Funktionen gehören Alarmmanagement, Erfassung von Maschinendaten sowie Aufzeichnung historischer Daten. Zudem können mithilfe des Routers wichtige Kennzahlen (KPIs) für die Analyse und vorausschauende Wartung erhoben werden. Standardmäßig mit Ethernet-Anschluss ausgestattet, können bei Bedarf noch zwei zusätzliche Erweiterungskarten (z.B. für WLAN, LTE, MPI, seriell etc.) eingesteckt werden. Darüber hinaus ist die Datenintegration in eigene Systeme oder Cloud-Plattformen über Programmierschnittstellen (APIs) möglich. Auch die HTTPS-Skripterstellung oder MQTT sind Optionen, um nur einige der unterstützten Protokolle zu nennen.

Ideal für Maschinenbauer und Anlagenbetreiber: Das neue IIoT-Gateway eWON Flexy 205.

Bild: HMS Industrial Networks GmbH

man tun kann. Denn auch in puncto Cloud-Kommunikation gilt: Der frühe Vogel fängt den Wurm. Wer frühzeitig in die Technologie einsteigt, läuft natürlich Gefahr, die falsche Technologie zu wählen. Aber mit der gesammelten Erfahrung einen Richtungswechsel einzuleiten ist einfacher, als völlig unerfahren und verspätet in die Thematik einzusteigen und bis dahin Mitbewerbern den Markt zu überlassen. Eine weitere Einstiegshürde liegt darin, dass in industriellen Anlagen ganz unterschiedliche Steuerungen und Kommunikationsbusse eingesetzt werden. Eine passende Lösung für die Cloud-Kommunikation zu finden, ist nicht ganz einfach. Auch die teilweise verhältnismäßig hohen Investitionen schrecken viele ab. Richtig genutzt spart man jedoch die Mehrkosten für die Kommunikationslösung im laufenden Betrieb sehr schnell durch die erzielten Effizienzsteigerungen wieder ein.

Ist sicher wirklich sicher?

Neben fehlendem Wissen um die Vorteile cloudbasierter Kommunikationslösungen und die bereits vorhanden Lösungen entscheidet oft noch die Angst gegen den Einsatz. Ist die Datenübertragung wirklich sicher? Schaffe ich nicht Einfallstore für Hacker in meine Produktion? Wem gehören die Prozessdaten, dem Anlagenbetreiber oder dem Maschinenbauer bzw. Gerätehersteller oder Systemintegrator? Um auf diese Fragen Antworten geben zu können, haben die Experten für industrielle Kommunikation von HMS auch im vergangenen Jahr ihre Produkte kontinuierlich weiterentwickelt. So wurden ihre Kommunikationslösungen nach der ISO27001 zertifiziert. Die Norm befasst sich mit Informationssicherheit innerhalb von Organisationen und spezifiziert Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems. Dank dieser und einer Star-Zertifizierung (Security Test Audit Report) haben Anwender die Sicherheit, dass ihre Daten mit den Lösungen der Kommunikationsexperten auch wirklich sicher übertragen und abgelegt werden.

Praktische Lösungen für Neu- und Bestandsanlagen

Während in Neuanlagen (Greenfield) heute direkt Lösungen für die Cloud-Kommunikation integriert werden, gilt es diese in den kommenden Jahren in vielen Bestandsanlagen (Brownfield) nachzurüsten. Beide Anwendungsfälle stellen ganz unterschiedliche Anforderungen. Bei Brownfield-Applikationen hat man es oft noch mit alten SPSen und heterogenen Netzen zu tun, während bei Neuanlagen moderne Kommunikationsstandards wie OPC UA, MQTT oder TSN gefordert werden. HMS hat schon heute für beide Anwendungsfälle die passenden Lösungen im Angebot: Nicht nur bei Neu-Anlagen, sondern auch bei Bestandsanlagen können die IIoT-Gateways eWON Flexy (Vertrieb in Deutschland über Wachendorff Prozesstechnik) ihre Vorteile ausspielen. Sie passen sich flexibel an unterschiedlichste Steuerungen an, beherrschen nicht nur neue Kommunikationsstandards, sondern kommunizieren auch über ältere Kommunikationsstandards (z.B. MPI), wie man sie in Bestandsanlagen vorfindet. Damit lassen sich unterschiedlichste Steuerungen in ein Gesamtkonzept integrieren. Für Gerätehersteller bietet HMS mit den neuen Multi-Protokolllösungen der Anybus CompactCom-Familie die Möglichkeit, die Protokolle OPC UA und MQTT zusätzlich zur Echtzeitkommunikation über Profinet und Ethernet/IP zu nutzen. Die neuen Kommunikationsmodule sind abwärtskompatibel zu den bestehenden Modulen. Gerätehersteller können durch einen einfachen Modultausch ihre Automatisierungsgeräte mit den modernen Kommunikationsstandards nachrüsten. Mit den Kommunikationsmodulen lässt sich so einerseits die Echtzeitkommunikation abwickeln und andererseits die Anbindung an industrielle IT-Systeme über nur einen Ethernet-Anschluss realisieren. Bei alledem sollte man nicht vergessen: Im Industrial Internet of Things (IIoT) geht es weniger um Dinge als vielmehr um Daten. Wie man Big Data analysiert und sinnvoll nutzt, stellt viele Anwender vor ebenso große Herausforderungen wie die Suche nach der passenden Daten-Kommunikationslösung. HMS hat dazu ein großes Partnernetzwerk aufgebaut, das mit entsprechenden Tools und Know-how beratend zur Seite steht. ■

Autor: *Thilo Döring,*
Geschäftsführer
HMS Industrial Networks GmbH
www.hms-networks.de

Embedded Kommunikationsschnittstelle mit OPC UA und MQTT

IIoT Kommunikation zum Nachrüsten: Die Anybus Kommunikationsmodule unterstützen jetzt auch OPC UA und MQTT.

Die Produktfamilie der Embedded-Kommunikationsschnittstellen Anybus CompactCom unterstützt nun auch die IoT-Protokolle OPC UA und MQTT. Damit haben Gerätehersteller und Maschinenbauer, die Anybus CompactCom einsetzen, eine einfache Möglichkeit, Daten im Umfeld von Industrie 4.0 bzw. IIoT sicher auszutauschen. Neben diesen Kommunikationsschnittstellen bietet CompactCom weitere Möglichkeiten, industrielle Hardware mit IT-Systemen und IoT-Software zu verbinden, z.B. über integrierte, anpassbare Webseiten und die Unterstützung von Web Services, E-Mail und FTP. Anwendern, die spezielle Anforderungen bezüglich der Kommunikation zwischen Fertigung und IT haben, bietet das CompactCom mit dem Socket Interface und dem transparenten Ethernet-Kanal größtmögliche Flexibilität, um eigene IT-Funktionen zu realisieren. Unabhängig davon wickelt das CompactCom weiterhin die gesamte Kommunikation mit dem industriellen Fertigungsnetzwerk ab.

Ob serielle Schnittstellen, Ethernet-Multiprotokoll-Technologie oder vorausschauende Wartung – Turcks 2COM-Modul ist ein Universalwerkzeug für die Automatisierung.

Einfache Anbindung von RS232-, RS485- und Modbus-RTU-Geräten an Ethernet-Netzwerke

Zurück in die Zukunft

Serielle Schnittstellen spielen nach wie vor eine große Rolle in vielen Bereichen der industriellen Automation. Das gute Preis-Leistungs-Verhältnis ist dafür ausschlaggebend. Aus diesem Grund erweitert Turck das Portfolio der TBEN-S-Familie um das Block-I/O-Modul TBEN-S-2COM. Wir stellen das System im Folgenden vor.

Das IP67-Block-I/O-Modul TBEN-S-2COM bietet zwei serielle Schnittstellen und vier I/O-Kanäle. Zur Steuerung kommuniziert es über Turcks Multiprotokoll-Technologie mit Profinet, Ethernet/IP oder Modbus TCP. Damit ist es für den globalen Einsatz in Neuanlagen ebenso geeignet wie für Retrofit-Projekte. Es reduziert Kosten, da es beispielsweise Barcode-Scanner über Buskabel auch mit Energie versorgt oder die Anbindung von bis zu 64 Modbus-RTU-Servern erlaubt – optimal für Pick-to-Light-Anwendungen. Und wer auf die Zukunft vorbereitet sein möchte, bringt mit dem 2COM-Modul seine seriellen Schnittstellen in die Industrie-4.0-Ära: Die parallele Kommunikation über Profinet (zur Steuerung) und Modbus TCP an Edge-Gateways oder Data-Hubs ermöglicht die intelligente Auswertung von Gerätedaten zur vorausschauenden Wartung.

Serielle Schnittstellen immer noch weit verbreitet

Während serielle Schnittstellen in der IT-Welt weitestgehend durch Ethernet und USB abgelöst sind, haben sie in der Industrieautomation bis heute einen guten Stand. Nicht nur lange genutzte Geräte haben die Schnittstelle an Bord, auch viele neue Produkte, von Barcode-Scannern und Lichtvorhängen über Drucker, Waagen

und Bedienterminals, aber nicht zuletzt auch viele Antriebe kommunizieren über diese Schnittstellen. Auch deshalb legt Turck jetzt sein ultrakompaktes IP67-Ethernet-I/O-Modul zur Anbindung von seriellen Schnittstellen neu auf. Das TBEN-S2-2COM-4DXP bietet neben den beiden Ports für RS232 oder RS485 vier digitale Ein- oder Ausgänge. Die Charakteristik der seriellen Ports (RS232, RS485 oder Modbus RTU) kann frei gewählt werden. Die I/Os lassen sich dabei konfigurationslos als Ein- oder Ausgang nutzen.

Verdrahtung im Feld spart Zeit und Kosten

Die neuen TBEN-S-Module erleichtern das Anbinden von Geräten mit serieller Schnittstelle erheblich. Abhängig von der gewählten Anschlusstechnik erreichen die Module Schutzart IP65/67 oder sogar IP69K und sind daher direkt im Feld auf der Maschine einsetzbar. Das verkürzt die Verdrahtungswege vom Modul zu den Geräten vor Ort. Vom I/O-Modul wird dann nur noch eine Ethernet- und eine Power-Versorgung zum Schaltschrank geführt. Beide Leitungen, Power und Ethernet, können von Modul zu Modul als sogenannte 'Daisy Chain' durchgeschleift werden, müssen also im Idealfall nur einmal vom Schaltschrank ins Feld geführt werden. Kleinere Geräte wie Barcodescanner versorgt das TBEN-S-2COM über den Bus-Stecker mit Leistung – auch hier verringert das I/O-Modul den Zeitaufwand und Kosten für Verdrahtung.

Konfigurieren statt Programmieren – Modbus RTU an Board

Neben Einsparungen beim Verdrahtungsaufwand profitieren Anwender der Module auch davon, dass der Programmieraufwand für die Kommunikation mit Modbus-RTU-Geräten reduziert ist. Üblicherweise müssen Modbus-Zugriffe in der Steuerungsumgebung selbstständig programmiert und verarbeitet

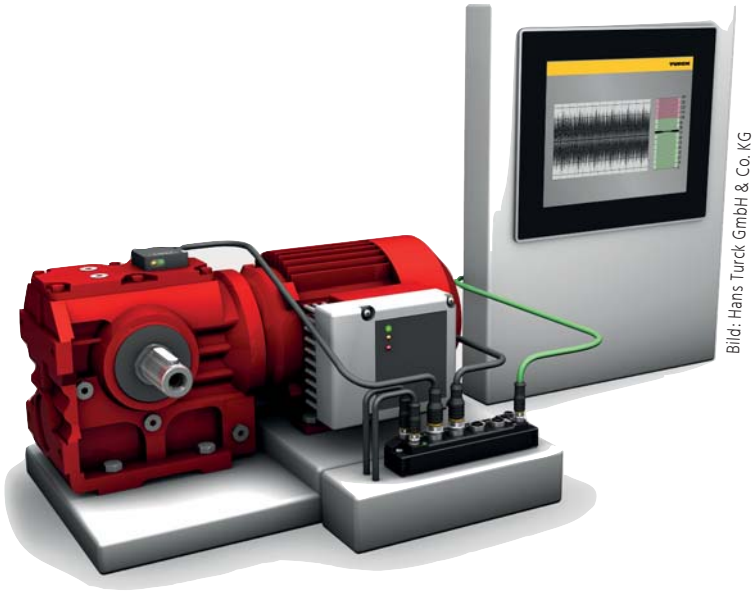


Bild: Hans Turck GmbH & Co. KG

Über RS485 können bis zu 32 Motoren pro COM-Port mit dem TBEN-S2-2COM verbunden werden. Der Sensor für Vibration und Temperatur wird ebenfalls via RS485 mit dem Modul verbunden. So lassen sich Lagerschäden frühzeitig diagnostizieren, um geplante Wartungen durchzuführen.

werden. Bei Turcks seriellem Modul ist Modbus RTU integriert. Der Nutzer muss lediglich Adressen und Prozessdatenbereiche konfigurieren. Danach übernimmt das Modul die Protokollverarbeitung und tauscht Prozessdaten mit der Steuerung aus. Komplizierte Funktionsbausteine für Modbus werden nicht benötigt. Damit ist das Modul der perfekte Counterpart für zahlreiche Modbus-RTU-Geräte, wie etwa intelligente Sensorik oder auch die Lichtvorhänge von Turcks Optosensorik-Partner Banner Engineering. Beispielsweise können bis zu 64 Pick-to-Light-Sensoren der K50-Serie von Banner an nur einem I/O-Modul betrieben werden. Kostengünstiger lassen sich Pick-to-Light-Anwendungen kaum aufbauen. Auch für Retrofitprojekte ist das 2COM-Modul das Bindeglied, um bestehende Modbus-RTU-Teilnehmer in Industrial-Ethernet-Netze zu integrieren.

Motorensteuerung mit vorausschauender Wartung

Gerade in den Branchen Fördertechnik, Logistik und Verpackungstechnik werden häufig Motoren mit seriellen Schnittstellen verwendet. Ein gutes Beispiel sind die Movimot-Motoren von SEW Eurodrive. In der Betriebsart RS485 können bis zu 32 Motoren pro COM-Port mit dem TBEN-S2-2COM verbunden werden. Mit dem QM42VT2 von Banner steht darüber hinaus ein Sensor zur Überwachung von Vibration und Temperatur zur Verfügung, der ebenfalls via RS485 mit dem Modul verbunden werden kann. Montiert direkt am Antrieb, lassen sich Lagerschäden auf diese Weise frühzeitig diagnostizieren, um geplante Wartungen durchzuführen. Eine einfache und effiziente Möglichkeit, vorausschauende Wartung zu betreiben.

Zusätzliche Kommunikation auch parallel zur SPS

Eine weitere Eigenschaft der Komponenten öffnet Perspektiven in Richtung Industrie 4.0. Wie alle Geräte der TBEN-Familie unterstützt auch das TBEN-S2-2COM Turcks Ethernet-Multiprotokoll-Technologie, die den Einsatz der Geräte in Profinet-, EtherNet/IP- und Modbus-TCP-Netzen ermöglicht. Über Modbus kann dabei parallel zu bestehenden Steuerungsverbindungen auf das Gerät zugegriffen werden. Am Beispiel der Motorensteuerung mit vorausschauender Wartung lassen sich die Daten vom Vibrationssensor so zum Beispiel zur weiteren Analyse direkt an überlagerte Systeme, wie Edge-Gateways, Daten-Hubs oder Cloud-Systeme versenden. Viele gängige Systeme, wie Microsoft Azure, IBM Bluemix, aber auch OPC-UA-Server von Matricon und Kepware unterstützen die Kommunikation via Modbus TCP.

Eckdaten:

- Ultrakompakte Abmessungen (B x L x H) 32x144x32mm
- Zwei COM Ports, konfigurierbar als RS232 oder RS485
- Datenraten von 9,6Kbit/s bis 230,4kbit/s
- Je 192 Bytes Eingangs- und Ausgangsdaten pro Port
- Integrierte Modbus RTU Client Funktion
- Vier universelle digitale Ein- oder Ausgänge
- Ethernet-Multiprotokoll (PROFINET IO, Ethernet/IP, Modbus TCP)
- Ethernet Switch mit zwei M8 Ports
- Ethernet Medienredundanz (MRP, DLR)
- M8 Spannungsversorgung mit zwei galvanisch getrennten Gruppen
- Schutzart: IP65/IP67/IP69K
- Erweiterter Temperaturbereich von -40 bis 70°C

ARGEE macht Modul zur Kleinsteuerung (FLC)

Wie alle aktuellen TBEN-Modelle verfügt auch das 2COM-Modul über die browserbasierte Programmierumgebung ARGEE. Damit können SPS-Funktionen direkt auf den Modulen der Block-I/O-Reihen TBEN-L, TBEN-S, BL compact und FEN20 programmiert werden. Mit solchen Field Logic Controllern (FLC) lassen sich einfache Steuerungsfunktionen auf die I/O-Module auslagern, was die zentrale Steuerung und die Buskommunikation entlastet. Die Programmierumgebung ist eine einfache Web-Applikation. Dazu ist lediglich ein PC mit einem Webbrowser wie Chrome oder Firefox erforderlich. Einfache Anforderungen sind mit ARGEE auf den Turck-Block-I/O-Modulen auch autark realisierbar. Die Programmierung ist denkbar einfach. Im Simple-Modus, der einem Kontaktplan-Editor entspricht, können über Drop-Down-Felder die Ein- und Ausgänge mit Boole'schen Operatoren und Aktionen verknüpft werden. Das Programmieren grundlegender Funktionen ist damit ohne Kenntnis einer Programmiersprache möglich. Im Professional-Modus steht dann der volle Funktionsumfang zur Verfügung, womit sich beispielsweise auch Ablaufdiagramme realisieren lassen. ■

Die browserbasierte Programmierumgebung ARGEE lässt sich auch mit mobilen Geräten bedienen.

Autor: **Aurel Buda,**
Produktmanager Fabrikautomation Systeme,
Hans Turck GmbH & Co. KG
www.turck.com

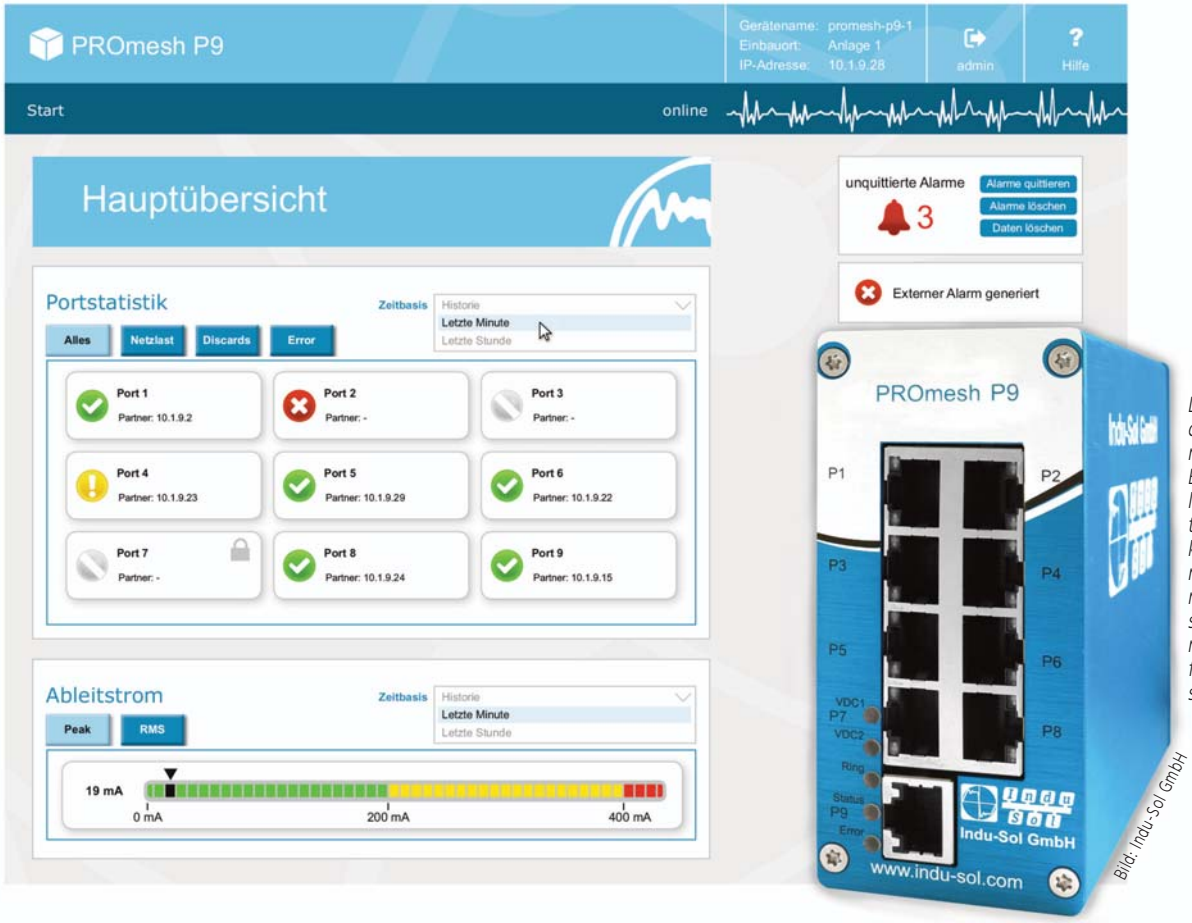


Bild: Indu-Sol GmbH

Die Entwicklung des Switches PROmesh P9 bildet die Basis für eine völlig neue Generation Infrastrukturkomponenten, die neben der Steuerung von Datenströmen mehr und mehr Diagnosefunktionen bereitstellen muss.

Einfache Handhabung trotz hoher Funktionalität

Der Switch für die Automatisierungsbranche

Im Zuge von Industrie 4.0 kommt dem Netzwerkmanagement einschließlich der Überwachung auf Stabilität und Sicherheit eine wesentlich größere Bedeutung zu, als ihm derzeit in der Automatisierung beigemessen wird. Durch die Weiterentwicklung des IEEE 802.XXX-Standards wird die Ethernet-Kommunikation in vollem Umfang Einzug in die Automatisierung halten. Mit Time-Sensitive Networking (TSN) werden vielschichtige Anwendungen gleichzeitig ablaufen, die SPS verliert ihre zentrale Stellung in der Netzwerküberwachung und das Netzwerk wird Mittel zum Zweck. Das heißt: Seine Funktionalität, Sicherheit und Zuverlässigkeit werden von den Anwendungen vorausgesetzt und deshalb nicht gesondert unterstützt. In diesem Zusammenhang wird dem Switch künftig eine zentrale Rolle zukommen, die viele der derzeit am Markt verfügbaren nicht erfüllen.

Die Netzwerkexperten von Indu-Sol haben in den vergangenen Jahren Trends in der industriellen Kommunikation oft frühzeitig erkannt und Forderungen nach Qualitätsparametern und deren Einhaltung maßgeblich mitgeprägt. Ziel ist es dabei stets, die Zuverlässigkeit und Langlebigkeit industrieller Datenkommunikation sicherzustellen – auch und erst recht unter den Bedingungen einer hochvernetzten Produktion. Die scheinbar unbegrenzten neuen Möglichkeiten der Datenkommunikation, die steigende Bandbreite und niedrige Latenzen sollten uns Anwender aber nicht davon abhalten, gewohnte Selbstverständlichkeiten in Bezug auf standardisierte Diagnosen – 'Maintenance Signals' – sowie die Notwendigkeit eines umfangreichen Netzwerk-Monitorings weiterhin einzufordern. Im Zuge von Industrie 4.0 stellt sich Indu-Sol die Frage, welchen Einfluss die absehbare Technologieentwicklung auf Stabilität und Zuverlässigkeit der Kommunikation haben wird und für welche Situationen im Netz es kurz-, mittel- und langfristig neuer Lösungen bedarf.

Fortschritt stellt erhöhte Anforderungen

Bislang werden in den meisten Fällen der industriellen Automation Maschinen- und Hallennetz noch getrennt betrachtet. Im Zuge von Industrie 4.0 wird es hier immer stärker zu einer Verschmelzung kommen. Karl-Heinz Richter, Geschäftsführer Marketing & Vertrieb der Indu-Sol GmbH, erwartet in diesem Zusammenhang einen Trend: „Trotz sichtbarem Gerangel um Zuständigkeiten verschmilzt die Informationstechnologie (IT) zunehmend mit der Automatisierung (OT – Operational Technology), wobei die Verantwortlichen noch immer um eine gewisse Abgrenzung bemüht sind. Es ist abzusehen, dass mittelfristig Strukturen und Performance der Kommunikationsnetze von den Anwendern vorausgesetzt werden und dass die Themen Betreuung, Wartung und Pflege von externen Dienstleisternübernommen werden. Sprich: Die Verantwortung und somit Sicherstellung der Verfügbarkeit wird ausgelagert, wie wir das in der IT heute schon sehen. Der Wandel hat eingesetzt und es gilt, sich darauf vorzubereiten." Mit dem Switch Promesh P9, den Indu-Sol auf der SPS IPC Drives 2017 in Nürnberg präsentierte, legt das Technologieunternehmen den Grundstein dafür, dieser Entwicklung zu begegnen.

Warum jetzt noch ein Switch, wo doch schon so viele am Markt erhältlich sind?

Switches werden heute in den vielfältigsten Varianten angeboten. Die meisten entstammen jedoch der IT-Welt. Richter erklärt dazu: „Wenn wir über Switches für die zukünftigen Anwendungen im OT-Bereich sprechen, müssen wir eine ganz andere Sichtweise als die Officewelt an den Tag legen. So stellen Switches von Haus aus zum Beispiel vergleichsweise wenige Informationen zur Netzwerkdiagnose, d.h. zum Netzwerkzustand an sich, zur Verfügung. Permanente Überwachung, Telegrammanalyse, Anomalieerkennung, Warnung vor dem Ausfall – all das sind Forderungen im Sinne von Predictive Maintenance, welche neben der eigentlichen Switch-Funktion abzudecken sind. In zunehmendem Maße kommunizieren dezentrale Intelligenzen eigenständig miteinander, die Netzwerke werden immer größer

Bild: ©eyetronic/fotolia.com

Wie beim Verkehr auf einer Großstadt-Kreuzung müssen Switches im Netzwerk die Kommunikation verschiedenster Teilnehmer auch bei hohen Lasten effektiv koordinieren. Im Netzwerk besteht zusätzlich die Herausforderung, dass die 'Straßen' nur einspurig sind und nicht überholt werden kann.

Der Switch PROmesh P9 überwacht permanent Netzlast, Telegramme und sogar Ableitströme und dokumentiert sie für eine schnelle Fehlersuche."

Bild: Indu-Sol GmbH

und weitläufiger, der smarte Sensor stellt seine Information mehreren Abnehmern gleichzeitig zur Verfügung und die Kommunikation läuft mehr und mehr „an der Steuerung vorbei". Somit verliert die Steuerung ihre zentrale Stellung bei der Netzwerküberwachung und steht für diese Aufgabe nur noch begrenzt zur Verfügung. Im Sinne des weiteren Technologiewandels hin zu durchgängiger Ethernet-Kommunikation kommt dem Switch eine noch nie gekannte zentrale Bedeutung zu, welche es gilt, entwicklungsseitig vorzubereiten." Die Switches von morgen werden neben ihrer Funktion als intelligente und robuste Schaltzentralen für Datenströme zusätzlich mit umfangreichen Funktionen zur Netzwerkdiagnose ausgestattet sein. Mit der Entwicklung des Promesh P9 wurde bei Indu-Sol eine Basis gelegt, die vielfältige Optionen der Vervollkommnung eröffnet. Dass sie mehr als nur eine Erweiterung des Indu-Sol Produktportfolios ist, zeigt die Aussage von Richter: „Wir werden uns in den nächsten Jahren neben der Dienstleistung mehr um die Netzwerkverantwortung bei unseren Kunden bemühen und fortführend auch Komplettangebote zur Netzwerkausrüstung im OT-Bereich anstreben. Ob eigenständig oder in Allianzen mit gleichgesinnten Mittelständlern, wird sich in nächster Zeit zeigen. Dass wir für unsere nächsten Entwicklungsschritte mehr brauchen als nur einen Switch, ist uns klar. Ein nächster Schritt könnte unsere derzeit in der Entwicklung befindliche Fog Cloudlösung sein."

Auf die Bedürfnisse der Automatisierer zugeschnitten

Was macht den Promesh P9 einzigartig? Neben seiner sehr guten Performance zeichnet sich der Indu-Sol Switch durch seine anwenderorientierte Bedieneroberfläche aus. Im Webinterface stehen direkt auf der Startseite wichtige Informationen zu Portstatus und Portbelegung auf einen Blick zur Verfügung und werden dem Anlagenbetreiber in vertrauten Ampelfarben visualisiert. So werden beispielsweise neben der prinzipiellen Verfügbarkeit und Nachbarschaftserkennung eines Ports die Netzlast, Discards und Errors erfasst und mit voreingestellten Triggerwerten permanent abgeglichen. Ein Alarmmanagement über einen potentialfreien Kontakt, per E-Mail oder zentraler SNMP-Abfrage stellen eine rechtzeitige Warnung vor dem Aus-

fall sicher. Alle Unregelmäßigkeiten werden intern dokumentiert und als Snapshot festgehalten. Ersten positiven Feedbacks von Nutzern aus der Automotivebranche zufolge haben vor allem die einfachen und klar dargestellten Informationen einen bedeutenden Nutzen für das Wartungs- und Instandhaltungspersonal.

Ableitströme im Blick

Außerdem greift die Entwicklung des Promesh P9 ein Thema auf, das im IT-Bereich so gut wie nicht auftaucht, in der komplexen Automatisierungstechnik aber durchaus beachtet werden muss: Potentialausgleichsströme, die über den Schirm der Datenleitungen in den Switch abgeleitet werden. Diese können zu Unregelmäßigkeiten im Datenverkehr führen und sogar Geräte zerstören. Eine speziell integrierte Messschaltung überwacht zu diesem Zweck diese sogenannten Ableitströme permanent und speichert bei Überschreitung die Werte einschließlich des Frequenzverlaufs. Mit einer kontinuierlichen Messung über das gesamte Frequenzspektrum (20kHz) sowie einer Erfassung von Mittelwerten (RMS-Messung) und Spitzenwerten (Peaks) werden Ursachen und Zusammenhänge für EMV-Störungen nachvollziehbar. Übersteigt dieser Ableitstrom einen Wert von 200mA (effektiv) und 400mA (Peak), so stellt dies eine Gefahr für die störungsfreie Kommunikation dar und es erfolgt eine zielgerichtete Warnung. Mit dieser Funktion trägt der Promesh P9 gleichzeitig einer noch im Entwurf befindlichen Handlungsempfehlung der Nutzerorganisation Profibus & Profinet International (PI) mit dem Titel „Funktionserdung und Schirmung von Profibus und Profinet“ Rechnung. In ihr wird ganz klar die Forderung gestellt, eine Überwachungsmöglichkeit zur Prüfung des aktuellen Schirmstromniveaus vorzusehen.

Präzises Monitoring durch dezentrale Datenerfassung und zentrale Auswertung

Obwohl wir uns von der IT-Umgebung gern distanzieren und die eigene Welt der Automatisierung voranstellen, können wir doch zum Thema Netzwerkmonitoring noch eine Menge von der IT lernen bzw. sogar übernehmen. Indu-Sol bietet mit Blick darauf hierzu bereits seit vielen Jahren eine Serverlösung unter Verwendung der Software Promanage an. Sie fragt im Minutentakt alle SNMP-fähigen Netzwerkkomponenten ab und erstellt über 365 Tage eine minutenaktuelle Statistik. Ziel ist es, an einer zentralen Stelle die Informationen zum Netzwerkzustand zu sammeln und dem Wartungs- und Instandhaltungspersonal zur Verfügung zu stellen. Damit lässt sich frühzeitig feststellen, wann sich Zustände verändern und welche Trends sich abzeichnen. Darüber hinaus lassen sich aber auch dezentral im Promesh P9 individuelle Schwellenwerte für alle überwachten Größen wie z.B. Netzlast, Discards, Errors und Ableitströme einstellen und eine Warnung über den potentialfreien Kontakt oder per SNMP-Trap absetzen. Indu-Sol möchte mit der Veröffentlichung von Promesh P9 neben der Erweiterung seines Portfolios vor allem eine Diskussion über Entwicklungstendenzen in der Automatisierungstechnik anregen, ohne den Blick in der Glaskugel zu haben. Der erste Schritt ist gemacht. ■

Bild: Indu-Sol GmbH

Das übersichtliche Webinterface macht Portbelegung und -status direkt auf einen Blick sichtbar; mit wenigen Klicks lassen sich weitere Details darstellen.

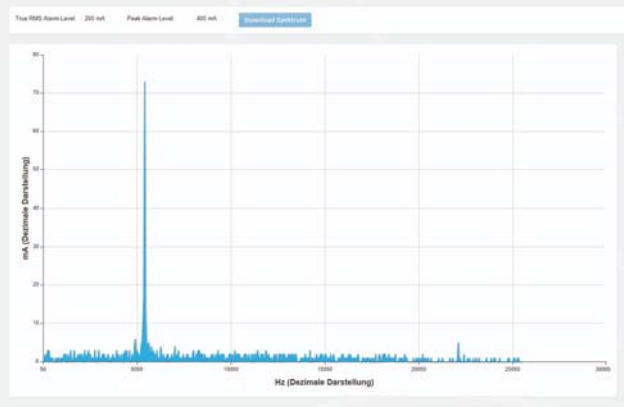


Bild: Indu-Sol GmbH

Der Switch überwacht Ableitströme permanent über das gesamte Frequenzspektrum (20kHz) und macht so Ursachen und Zusammenhänge für EMV-Störungen nachvollziehbar.

Promesh P9 im Überblick

- Volle Profinet-Funktionalität
- 9x100 Mbit/s RJ45 Ports
- Ableitstromüberwachung inkl. Frequenzspektrum
- Grafische Anzeige der Portauslastung (millisekundengenau)
- Optimierte Schirmkontaktierung
- Kompakte Bauform
- Anzeige von Discards auf der Web-Oberfläche
- Einfacher Gerätetausch mit Wechselmedium
- Mirror Port, VLAN, SNTP, SMTP und DHCP
- Redundante Spannungsversorgung

Autor: **Christian Wiesel, Marketing, Indu-Sol GmbH**
www.indu-sol.com

Bild: National Instruments Germany GmbH

Die neuen cDAQ Chassis sind für eine Stoßfestigkeit bis 50g und Vibrationsfestigkeit bis 5g ausgelegt.

Die neuen Ethernet-Chassis von National Instruments mit 4 und 8 Steckplätzen bieten eine deterministische Synchronisierung über Ethernet für verteilte Mess- und Prüfsysteme.

NI CompactDAQ unterstützt jetzt Time-Sensitive Network

National Instruments stellt zwei neue Ethernet-Chassis mit unterschiedlicher Steckplatzanzahl vor, cDAQ-9185 und cDAQ-9189, die eine deterministische Synchronisierung über aktuelle Ethernet-Standards unterstützen. NI verbindet damit Time-Sensitive Networking (TSN) mit robuster CompactDAQ-Hardware für verteilte Messungen im Netzwerk.

Die Art und Weise, wie physikalische Systeme getestet werden, verändert sich rasant, da Messsysteme zunehmend vom Kontrollraum näher an das Testobjekt rücken. Dies sorgt zwar einerseits für eine schnellere Installation, geringere Kosten bei Verkabelung und Verdrahtung sowie eine höhere Messgenauigkeit. Andererseits ergeben sich dadurch jedoch Herausforderungen bei der Synchronisierung und Systemverwaltung, insbesondere bei aktuell in der Industrie eingesetzten Netzwerktechnologien. NI ist aktiv an der Definition von Time-Sensitive Networking (TSN) beteiligt – der Weiterentwicklung des IEEE-802.1-Ethernet-Standards – um für verteilte Systeme eine nahtlose Zeitsynchronisierung, geringe Latenz und die Zusammenführung sowohl zeitkritischer als auch allgemeiner Netzwerkdaten zu ermöglichen. Die Chassis cDAQ-9185 und cDAQ-9189 unterstützen genaue Zeitsynchronisierungen über TSN, wodurch sich verteilte Systeme einfacher skalieren lassen, und bieten u. a.:

- Präzises Netzwerk-Timing ohne zusätzliche Synchronisationsleitungen für nahtlos synchronisierte Messungen
- Einfaches Daisy-Chaining über einen integrierten Netzwerk-Switch für die schnelle Einrichtung und Erweiterung verteilter Anwendungen
- Betriebstemperaturen von -40 bis 70°C, Stoßfestigkeit bis 50g und Vibrationsfestigkeit bis 5g für einen zuverlässigen Betrieb in rauen Umgebungen
- Softwareabstraktion über den Treiber NI-DAQmx, der für eine einfachere Programmierung mehrere Chassis automatisch synchronisiert

„Die neuen Chassis synchronisieren Messungen automatisch über einen Netzwerktakt. Dadurch wird eine genaue Synchronisierung über größere Entfernungen möglich, was wiederum die Einrichtung und Verwaltung von verteilten Systemen und Systemen mit hoher Kanalanzahl vereinfacht“, so Todd Walter, Chief Marketing Manager des DAQ and Embedded Lead User Teams bei NI. „Dank dieser innovativen Synchronisationsmethode in Kombination mit den Signalverarbeitungsbibliotheken der Systemdesignsoftware LabVIEW können Anwender zügig Daten erfassen sowie analysieren und Tests somit schneller und effizienter durchführen. CompactDAQ und LabVIEW unterstützen Anwender bereits seit mehr als zehn Jahren bei der Anpassung ihrer Datenerfassungssysteme an unterschiedliche Anwendungsanforderungen. Dank der Investitionen von NI in aktuelle Synchronisations- und Kommunikationstechnologien sind die neuen CompactDAQ-Chassis mit den nötigen Funktionen für die Erstellung leistungsstarker und robuster Datenerfassungssysteme für hochgradig verteilte Sensoren ausgestattet und eignen sich sowohl für aktuelle als auch zukünftige Anforderungen verteilter Mess- und Prüfanwendungen. ■

Firma: ***National Instruments Germany GmbH***
www.ni.com/germany

Direkt zur Marktübersicht i-need.de ***www.i-need.de/?f7729***

Bild: PCTEL, Inc.

In Produktionsumgebungen hängt der Erfolg eines IIoT-Netzwerks maßgeblich von der Leistung der Antenne ab.

Tipps für die Auswahl der richtigen Übertragungslösungen

Die richtige Antenne für das IIoT

Durch das 'Industrial Internet of Things' (IIoT) erlebt die Industrieproduktion derzeit eine radikale Transformation. Allerdings sind IIoT-Netzwerke auf einwandfreie Konnektivität angewiesen: Für stationäre Anlagen ist die kabelgestützte Datenkommunikation eine Option, jedoch arbeiten viele IIoT-Netze kabellos. Dabei gilt: Ein drahtloses Netzwerk ist nur so gut wie seine schlechteste Antenne. Der drahtlose Datenaustausch im Internet der Dinge verlangt nach Hochleistungsantennen an jedem Knotenpunkt der Kommunikationskette. Bei der Auswahl der richtigen Lösungen und Übertragungstechnologien gibt es einiges zu beachten.

Prozessautomatisierung und die damit verbundenen IIoT-Anwendungen verlangen nach drahtloser Netzwerktechnologie, die sich auf dem neuesten Stand befindet. Das drahtlose Überwachen und Steuern technischer Prozesse mittels eines Computersystems (engl. 'Scada') gibt es zwar schon eine ganze Weile, aber die moderne Prozessautomatisierung schraubt die Anforderungen an die drahtlose Vernetzung noch einmal nach oben. IIoT bedeutet perfekte Konnektivität immer und überall, und zwar von Maschine zu Maschine (M2M) und von der Maschine zum Personal (M2P).

Drahtlostechnologien für das Internet der Dinge

Bei IIoT-Anwendungen, die mit relativ wenig Bandbreite auskommen, werden die alten VHF- und UHF-Netze, die mit ISA100 oder GSM arbeiteten, gerade durch LPWAN-Technologien ersetzt – z.B.

NB-IoT, LoRA und SigFox. LPWAN verbindet niedrige Latenzraten und geringen Energieverbrauch mit großflächiger Abdeckung, z.B. in einer Werkshalle. Einige LPWAN-Technologien unterstützen auch Fernüberwachungsanwendungen, bei denen eine Datenübertragung über große Entfernungen erforderlich ist. Doch können die Herausforderungen einer 'überfüllten' Industrieumgebung für LPWAN auch schnell zu viel werden. Dann kommen sog. vermaschte Netze (Mesh-Netzwerke) ins Spiel. Dabei handelt es sich um zwischengeschaltete Antennen, die als Knotenpunkte dienen und Signale von isolierten Antennen auffangen und an andere Empfänger im Netz weiterleiten. Bei automatischen Prozessen, wie z.B. Selbstheizsystemen, kann auf diese Weise die zuverlässige Kommunikation zwischen lokalen Ressourcen sichergestellt werden. Zu den verbreitetsten Drahtlosprotokollen für Mesh-Netzwerke gehören Zigbee und WirelessHart. Datenintensive Applikationen wie z.B. die Videoüberwachung hingegen benötigen Breitband-Standards, die auch mit großen und schnell getakteten Datenmengen zurechtkommen, z.B. WLAN oder LTE. Bei Anwendungen im unlizenzierten Spektrum bietet sich häufig WLAN an. LTE zeichnet sich durch relativ niedrige Latenzraten aus und kann in Spektren eingesetzt werden, die von einem Carrier geleast werden, oder in einem privaten Spektrum. Auch die Technik MulteFire kann LTE-Anwendungen ermöglichen, dann allerdings unter ausschließlicher Verwendung unlizenzierter Spektren. Es wird erwartet, dass 5G-Netze demnächst sogar noch höhere Datendurchsatzraten und niedrigere Latenzen unterstützen, und zwar sowohl im drahtlosen Bereich als auch im Millimeterwellenspektrum.

IIoT-Netzwerke sind auf einwandfreie Konnektivität angewiesen – diese wiederum lässt sich nur mit der richtigen Antenne erreichen.

Bild: PCTEL, Inc.

Auswahl von Antennen für IIoT-Anwendungen

Nicht nur in Produktionsumgebungen entscheidet die Leistung der Antenne, ob eine Übertragung den Empfänger erreicht und wie viel Datenvolumen übertragen werden kann. Dabei ist die maximale Ausbreitung der Funkwellen nicht zwangsläufig ideal, da sich überlappende Systeme gegenseitig stören können. IIoT-Antennen müssen daher gerade so viel Reichweite haben, wie für ihre Aufgabe unbedingt erforderlich ist. Gleichzeitig sollten sie große Datenmengen bei minimalen Interferenzen übermitteln, platzsparend sein und auch widrigen Umständen trotzen. Bezüglich der Strahlungscharakteristik stehen verschiedene Antennendiagramme zur Auswahl, je nach Aufgabenstellung und Platzierung der Antenne im Netz. In einem Netz mag die direkte Übertragung von Punkt zu Punkt (PTP) gefordert sein, in einem anderen von Punkt zu Mehrpunkt (PTMP). Die einfache PTP-Datenübermittlung erfordert gewöhnlich eine Richtantenne, während der Kommunikation mit vielen Empfängern (PTMP) mit einer Rundstrahlantenne besser gedient wäre. Der Netzentwickler kann natürlich auch für eine PTP-Anwendung eine Rundstrahlantenne einplanen und so Flexibilität gewinnen. Dies wäre z.B. eine Lösung für ein Mesh-Netzwerk mit zahlreichen mobilen Elementen: Dort überträgt eine Antenne zwar aus rein technischer Sicht nur PTP, aber zu verschiedenen Zeiten in unterschiedliche Richtungen – je nachdem, wo die nächste Antenne empfangsbereit ist. Doch unabhängig von Richt- oder Rundstrahlantenne kommt es auf das optimale Antennendiagramm an, damit die Abdeckung zuverlässig gewährleistet bleibt und Interferenzen minimiert werden. Zur Optimierung von Datendurchsatz und Abdeckung verfügen IIoT-Antennen über diverse technische Lösungen. Die sog. MIMO-Technologie (Multiple Input, Multiple Output) ermöglicht es der Antenne, Datenströme auf derselben Fre-

Die moderne Prozessautomatisierung stellt ganz neue Anforderungen an die drahtlose Vernetzung.

Bild: PCTEL, Inc.

quenz voneinander zu unterscheiden – das kommt datenintensiven Anwendungen wie Videoüberwachung zugute. Viele MIMO-Antennen verfügen zusätzlich über doppelte Polarisierung, was die Netzwerkkonnektivität dank Isolierung der HF-Eingänge weiter stabilisiert. Netze, die mehrere HF-Frequenzen verwenden, benötigen Multibandantennen, die mehrere Antennenelemente in einem Gehäuse vereinigen. Besonders hochqualitative Multibandantennen verfügen über Port-To-Port-Isolation, was nicht nur Interferenzen zwischen den Frequenzen verringert, sondern das Endprodukt auch noch kompakt macht.

Platzsparende und robuste Lösungen

Bei der Auswahl und Platzierung von IIoT-Antennen kommt es natürlich auch darauf an, wertvollen Platz für die eigentliche Produktion zu sparen. Das heißt, die Antenne muss nicht nur leistungsstark, sondern auch noch platzsparend sein. Eine häufige Lösung besteht darin, die Antenne in das Gerät zu integrieren, das sie bedienen soll. Komplexe Geräte (wie z.B. Zeilensensoren) enthalten manchmal ein komplettes, integriertes HF-System, wohingegen Router und WAPs oft einfach nur über ein Mobilfunkgerät und eine Antenne verfügen. Eine solche Konstruktion spart Platz und vereinfacht die Installation. Bei externen Antennen kommt auch noch die Flexibilität bei der Montage ins Spiel: Üblicherweise benötigen Antennen eine bestimmte Art von metallischem Untergrund ('Groundplane'). Doch Antennen, die für IIoT optimiert sind, können da montiert werden, wo Platz ist, unabhängig vom Untergrund. Für bestimmte Anwendungen muss die Antenne besonders robust sein, um widrigen Umständen oder auch der Manipulation durch Unbefugte zu wiederstehen. Ein Sensor in einem Gefriergerät für Lebensmittel zum Beispiel benötigt eine Antenne mit einem Gehäuse, das auch tiefen Temperaturen und Feuchtigkeit wiedersteht; ein anderer Sensor, der eine stark vibrierende Maschine überwacht, muss entsprechend daran angepasst sein. Ganz besonders wichtig sind gehärtete Gehäuse für drahtlose Netzwerke im Außenbereich, wo die Antenne verschiedensten, oft widrigen Klimaeinflüssen oder auch Vandalismus ausgesetzt sein kann. Die meisten qualitativ hochwertigen Antennensysteme zeichnen sich durch sehr robuste und flache Gehäuse aus, die gut gegen Wasser und Staub geschützt und vandalismussicher sind.

Hochleistungsantennen an jedem Knotenpunkt der Kommunikationskette ermöglichen einen reibungslosen und schnellen drahtlosen Datenaustausch.

Bild: PCTEL, Inc.

Bild: PCTEL, Inc.

Multibandantennen, die mehrere Antennenelemente in einem Gehäuse vereinigen, eignen sich besonders für Netze mit mehreren HF-Frequenzen.

Gut vernetzt – dank der optimalen Antenne

Die 4. industrielle Revolution ist in vollem Gange. Wer jetzt die Bedeutung leistungsstarker Antennentechnologien unterschätzt, läuft Gefahr, den Anschluss zu verlieren – im wahrsten Sinne des Wortes. Dank Datenkommunikation in Echtzeit zwischen Produktionsanlagen und dem Mitarbeiter im Leitstand agieren Unternehmen effizienter und beschleunigen gleich auch noch die Produktion. Doch hängt der potenzielle Vorteil stark von der Qualität der Antenne ab: Antennen, die im Rahmen des Internets der Dinge eingesetzt werden ('IIoT'), müssen flexibel genug sein, um eine große Bandbreite von HF-Frequenzen und Anwendungen abzudecken; gleichzeitig aber auch robust genug, um unter extremsten Bedingungen zuverlässig zu funktionieren, und schließlich auch noch kompakt genug, um auch dort eingesetzt zu werden, wo Platz Mangelware ist. Die Auswahl und Installation von Antennen für industrielle IoT-Anwendungen erfordert Sachverstand und sorgfältige Planung. Experten wie PCTEL stehen den Anwendern gerne beratend zur Seite. ■

Autor: **Leo Nieminen,**
Regional Sales Manager EMEA & India,
PCTEL, Inc.
www.antenna.com

Hacken für mehr Sicherheit

Hochregallager: Schwachstelle Steuerung

Die Transport- und Logistikkette ist für eine störungsfreie Produktion überlebenswichtig. Gehackte Container-Terminals, Automobilzulieferer und Logistikprozesse; fast stündlich müssen Unternehmen, Institute, Behörden und Verwaltungen Hackerangriffe abwehren, vorausgesetzt das Unternehmen verfügt über die technischen Möglichkeiten und Expertisen. Die Edelstahlservice GmbH aus Sulz am Neckar setzt bereits im Vorfeld auf Prävention und ließ nicht nur das Hochregallager von Experten auf Schwachstellen untersuchen. Das Ergebnis: Nicht nur die Steuerung konnte mit einfachen Mitteln gehackt werden.

Bild: CSP GmbH

Die letzten großen Attacken mit dem Wanna-Cry-Virus und Petya zeigten welches wirtschaftliches und sicherheitsrelevantes Ausmaß durch Hackerangriffe haben können. Das Ergebnis: Wie alle anderen Unternehmen, die Prozesstechnik einsetzen sind auch Steuerungsprozesse in der Intralogistik anfällig für Manipulation sowie Zerstörung. Die Logistikbranche und damit auch die laufende Produktion gerät immer stärker ins Visier von Cyberkriminellen. Das bestätigen Studienergebnisse von Oliver Wyman, einer international agierenden Strategieberatung. Mit der zunehmenden Digitalisierung der Prozessekette bei Verladern, Spediteuren, Transportunternehmen und Infrastrukturbetreibern wachsen die Gefahren von Datenmissbrauch und -klau. Demnach drohen der weltweiten Logistikbranche bereits 2020 rund sechs Milliarden Euro an Schäden durch Cyberkriminalität, warnen Wyman Analysten. Allein in Deutschland könnte sich der Schaden auf 450 Millionen Euro belaufen. Die Berater zeigen auf, dass es bei der Abwehr von Cyberrisiken auf eine Kombination von Technologie und Mitarbeitern ankommt. Logistiker, die Cybersicherheit zu einem Teil ihres Angebotsportfolios machen, können sich vom Wettbewerb abheben und das Risiko zu einer Chance machen.

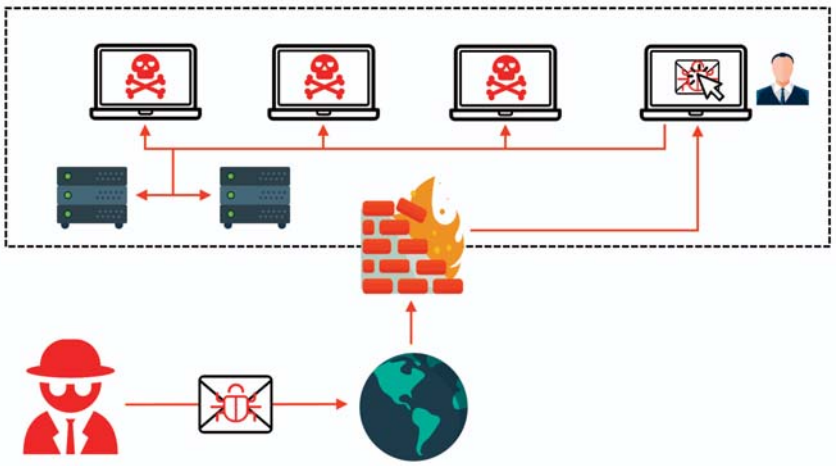


Bild: CSPI GmbH

Durch Drive-By (über den Webbrowser) oder über eine E-Mail Kampagne, wird dem Opfer ein Link präsentiert über den dann schadhafte Inhalte, wie zum Beispiel WannaCry auf das Zielsystem heruntergeladen werden.

Cyberattacken gekonnt abwehren

„Bis auf immer clevere Pishingattacken, diese sehen oftmals aus wie ernsthafte Bestellungen, waren wir bisher nicht übermäßig von Angriffen bedroht. Dennoch ist es uns wichtig Cyberangriffe und Manipulationen weitestgehend ausschließen zu können. Daher haben wir uns entschlossen die IT Sicherheit zu überprüfen", so Sven Leuthe, Projektleiter Edelstahlservice GmbH. „Bei der letzten Angriffswelle waren drei Depots unserer Transportdienstleiter betroffen. Wir waren verblüfft, dass sich die S7 Steuerung von den Sicherheitsexperten der CSPi GmbH so einfach knacken ließ. Ohne Zugriff auf unser Hochregallager könnten wir auch nicht mehr liefern, auch ungewollte Zugriffe auf andere Systeme (wie Email oder ERP) wollen wir ausschließen, da diese Angreifern weitgehende Manipulationsmöglichkeiten bieten würden. Wir hatten z.B. auch schon Versuche von externen Mailversendern, die sich als Mitglieder der Geschäftsleitung Ausgaben und versuchten die Buchhaltung dazu zu bringen eine geheime Überweisung auf fremde Konten zu tätigen", beschreibt Leuthe. Im Zuge der Überprüfung konnten noch weitere ungeschützte Anwendungen eliminiert werden. Derzeit werde auch ein neues Büro mit verstärkten Sicherheitstools ausgebaut. Dazu gehört z.B. auch ein besser gesicherter Zugang zu Server- und Technikräumen. „Werden neue Pishingversuche erkannt, so geht ein Screenshot via Mail an unsere vier bundesweit aufgestellten Niederlassungen mit Hinweisen wie man diese Mails erkennen kann um bei den Mitarbeitern ein Bewusstsein für die Bedrohungen zu schaffen, ergänzt Leuthe. Maurice Al-Khaliedy, Sicherheitsexperte bei der CSPi GmbH in Köln ist als Praktiker deutschlandweit unterwegs und unterstützte das Unternehmen bei der Identifizierung von Schwachstellen und möglichen Angriffsvektoren im Bereich der IT und der Operational Technology (OT). „Dazu gehören auch LiveHacks, die in der Praxis Schwachstellen der IT-K vor Augen führen. Grundsätzlich kann man sagen, das die Produktion und Logistik wie bei allen anderen Unternehmen, die Prozesstechnik einsetzen zu behandeln sind. Alles was mit der Automatisierung von Prozessen zu tun hat ist anfällig für die Manipulation sowie deren Zerstörung. Es spielt auch keine Rolle welche Produkthersteller in dem Unternehmen eingesetzt worden sind. Siemens, Wago, Phönix, Schneider Electric um nur einige zu nennen, alle haben mehr oder weniger Schwachstellen in Ihren Komponenten (SPS)", so der Sicherheitsexperte. Zum Schutz vor durchbrechenden Hacker- und CEO Fraudangriffen müssen Unternehmen umdenken. Die Frage die sich stellt, ist zu überprüfen, ob die aktuelle IT/OT-Infrastruktur hinsichtlich der Sicherheit noch zeitgemäß ist. „Es sollte geprüft werden, ob die Infrastruktur auf mögliche Schwachstellen und Angriffsvektoren untersucht werden sollte. In den meisten Fällen sind nach einem solchen Assessment erhebliche Mängel festgestellt worden", ergänzt Al-Khaliedy. ■

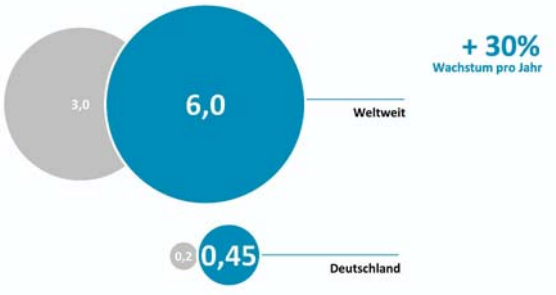


Bild: CSPI GmbH / Oliver Wyman-Analyse

Direkte Kosten von Cyberangriffen weltweit und in Deutschland 2017 vs. 2020, in Milliarden Euro. Berücksichtigt keine indirekten Kosten wie Reputationsschäden und IP-Verlust. Umfasst Frachttransport, Infrastruktur und letzte Meile (keinen Personentransport)

Autor: **IWP Wissenschaftsredaktion**
Uwe Manzke
www.umweltdienstleister.de

- Anzeige -

Wireless-Produkte

Die Funktechnik ist nicht nur komfortabel, sie löst auch Aufgaben, die anders gar nicht zu realisieren wären. Im industriellen Umfeld ist sie ein wesentlicher Mitspieler von Industrie 4.0 und IIoT. Hier gibt es Lösungen für die unterschiedlichsten Aufgaben.

Dass wir heute von Funkübertragungen sprechen, liegt im Ursprung der Entwicklung der Technologie. Als Guglielmo Marconi im ausgehenden 19. Jahrhundert seine Experimente zur drahtlosen Übertragung machte, wurden die elektromagnetischen Wellen noch durch tatsächliche Funkenentladungen erzeugt. Auch der Firmenname Telefunken verrät, wie die Anfangstage der Drahtlostechnologie aussahen. Heute gibt es neue Herausforderungen. Dabei geht es nicht immer nur um höhere Übertragungsraten, sondern auch um die drastische Reduzierung des Stromverbrauchs, um mobilen Geräten eine möglichst lange Batterielaufzeit zu verschaffen. So sind heute komplett drahtlose Rauchwarnmelder mit Batterielaufzeiten von 10 Jahren fast schon ein Standardprodukt. Das IoT braucht solche Lösungen für einen wirtschaftlich sinnvollen Betrieb von mobilen Geräten. Die Zuverlässigkeit von Funklösungen ist heute hingegen kaum noch ein Thema: Selbst für Safety-Funktionen kommt Funk heute zum Einsatz – zum Glück ganz ohne Funken. *(kbn)*

Bild: Fotolia/©zapp2photo

Quarze und Oszillatoren

Taktgeber für industrielle Echtzeitsysteme

Die Automatisierungstechnik basiert zunehmend auf Industrial Ethernet – und das aus gutem Grund: Die Technik vereint Echtzeitfähigkeit mit der Robustheit und Sicherheit der Feldbusse. Damit sie auch die harten Echtzeitanforderungen der Steuer- und Feldebene erfüllt, sind Quarze und Oszillatoren mit hoher Signalgenauigkeit und Zuverlässigkeit gefragt.

Die klassischen Feldbusse kommen noch in 48 Prozent der derzeit neu realisierten industriellen Netzwerke zum Einsatz, auf Industrial Ethernet entfallen 46 Prozent, so die Einschätzung von HMS Industrial Networks (Stand März 2017). Doch diese Verteilung wird sich bald drastisch ändern. Denn für die Feldbusse geht HMS von einem jährlichen Wachstum von vier Prozent aus, für Industrial Ethernet sind es ganze 22 Prozent. So ist der Marktanteil von Industrial Ethernet bereits deutlich von 38 Prozent (2016) auf 46 Prozent (2017) gestiegen. Andere Analysten ermitteln zwar etwas abweichende Zahlen, alle zeigen jedoch den Trend zum Industrial Ethernet. Durch ihre Fähigkeit, Echtzeit-Leistung mit der Belastbarkeit und Sicherheit von Feldbus-Lösungen zu vereinen, entspricht die Technik den aktuellen Bedürfnissen der Industrieautomatisierung. Zudem ermöglicht Industrial Ethernet eine durchgängige Kommunikation vom Aktor oder Sensor auf der Feldebene bis zu den Systemen der Leit- und Unternehmensebene, da die EDV-Systeme der Unternehmen bereits auf Ethernet basieren. Aktuell stehen viele, jedoch untereinander inkompatible Anwendungsprotokolle zur Verfügung, z.B. Ethernet/IP, Ethercat, Sercos, Profinet oder Powerlink. Die größten Marktanteile haben laut HMS derzeit EtherNet/IP, Profinet und Ethercat. Viele Maschinen- und Anlagenbauer nutzen sie zur Steigerung der Performance und um den Prozesses für den Anwender benutzerfreundlicher zu gestalten – vor allem wenn es auf hohe Zuverlässigkeit und Ausfallsicherheit ankommt.

Schnell und flexibel: Ethercat

Die bei weitem schnellste Technologie ist Ethercat, zudem bietet sie eine außerordentliche Synchronisationsgenauigkeit im Nanosekunden-Bereich. Mit ihren kurzen Reaktionszeiten beschleunigt sie alle Applikationen mit Weiterschaltbedingungen. Da Ethercat die CPU bei gleicher Zykluszeit um rund ein Drittel weniger beansprucht als andere Bussysteme, bildet sie die Basis für höhere Performance und Genauigkeit bei niedrigeren Kosten – und damit Steuerungs- und Regelungskonzepte, die mit herkömmlichen Feldbussystemen nicht realisierbar sind. Hierfür wird das Protokoll komplett in Hardware bearbeitet, unabhängig von Laufzeiten der Software-Implementierung. Der Datenaustausch folgt dem Master-Slave-Modell, hinsichtlich der Topologie bietet Ethercat uneingeschränkte Flexibilität: Es unterstützt die Linien-, Baum- und Sterntopologie sowie jede Kombination daraus. Die Knotenzahl ist nahezu unbegrenzt. Damit macht das System die von den Feldbussen her bekannten Strukturen auch für Ethernet verfügbar. Das Protokoll eignet sich für den Einsatz in zeitkritischen Motion-Control-Anwendungen, beispielsweise in Verpackungsmaschinen, CNC-Maschinen, Robotik und Hydraulikregelungen. Die Entwicklung und Verbreitung der ursprünglich von Beckhoff entwickelten Technologie treibt weltweit die Ethercat Technology Group (ETG) voran. Die Gruppe hat das Conformance-Test-Tool entwickelt, mit dem die Interoperabilität und Protokollkonformität von Ethercat-

Geräten sichergestellt wird. Außerdem unterstützt sie ihre Mitglieder bei der Implementierung und bietet Schulungen an. Die ETG ist mit über 4.400 Mitgliedern – darunter auch Rutronik – die größte Industrial-Ethernet-Nutzerorganisation weltweit.

Harte und weiche Echtzeit

Während die Kommunikation der Systeme in der Leit- und Unternehmensebene nicht sehr zeitkritisch ist und lediglich weiche Echtzeitanforderung stellt, ist in der Steuer- und Feldebene zunehmend harte Echtzeit gefordert. Damit die unterschiedlichen Systemkomponenten einer vielschichtigen Anlage sauber zusammenarbeiten können, ist ein sicherer und schneller Datenaustausch gefordert. Hierfür müssen die Netzwerke außer einem schnellen Real-Time-Verhalten auch geringe Abweichungen und synchronisierte Abläufe in den Netzwerkknoten sicherstellen. Die exakte Synchronisierung ist vor allem dann wichtig, wenn räumlich verteilte Prozesse gleichzeitige Aktionen erfordern, z.B. in Applikationen, in denen mehrere Servo-Antriebe gleichzeitig koordinierte Bewegungen ausführen. Verteilt abgeglichene Uhren, sogenannte Distributed Clocks, stellen hier eine hochgenaue, netzwerkweite Zeitbasis zur Verfügung. Diese Forderungen und Funktionen gehen über den einfachen Ethernet-Standard hinaus. Sie lassen sich in verschieden realisierbaren Hardwarelösungen implementieren, z.B. mit FPGAs, ASICs oder vollintegrierten Controllern. Für den Signaltakt sind Quarze, Oszillatoren oder Real Time Clocks mit hoher Signalqualität und Zuverlässigkeit erforderlich.

Präzise und zuverlässige Quarze und Oszillatoren

Quarze und Oszillatoren, die sowohl weiche als auch harte Echtzeitanforderungen mit kurzen Zykluszeiten und niedrigem Jitter verbinden, bietet EPSON. Mit seinem breiten Portfolio hochwertiger frequenzbestimmender Bauelemente deckt der Hersteller jeden Bedarf der aktuellen Protokolle ab. Die Komponenten eignen sich für unterschiedliche Applikationen, z.B. Human Machine Interface (HMI), Programmable Logic Controller (PLC) oder Motion Controller (Servomotoren, FA Kamera, Sensoren) und Frequenz-Inverter. MEMS-Oszillatoren gelten zwar als mechanisch belastbarer, was gerade für raue industrielle Anwendungen von Vorteil ist. Doch bezüglich Präzision, Phasenrauschen und Temperaturstabilität haben quarzbasierende Oszillatoren immer noch die Nase vorn. In die stark verbreiteten Ethercat-Asics ET1100/ET1200 von Beckhoff sind viele Algorithmen des Protokolls in Hardware integriert. Sie verfügen über Distributed-Clocks, die die hochpräzise Synchronisation (<1µs) der Ethercat-Slaves ermöglichen. Für Standardfrequenzen der Industrieprotokolle mit einer Anforderung von +/-50ppm über -40 bis +85°C empfiehlt sich die 2.5x2.0-Serie SG-210STF, mit gleicher Charakteristik auch in 7x5 (SG7050) und 5x3.2 (SG5032) verfügbar. Den erweiterten Temperaturbereich bis 105°C oder 125°C deckt die SG-210S*B-Serie ab. Für Nicht-Standardfrequenzen, kleine Stückzahlen und kurze Lieferzeiten empfehlen sich die programmierbaren Quarzoszillatoren der SG-8018- und SG-8101-Serie. Diese kommen mit einer internen PLL-Schaltung, die die entsprechenden Frequenzen erzeugt. Die neue Serie SG-8101 hat einen erweiterten Temperaturbereich bis zu 105°C und kann auch unter rauen Umweltbedingungen zum Einsatz kommen. Außerdem zeichnet sie sich durch eine um ca. 66 Prozent engere Frequenztoleranz (±50 bis ±15ppm) und einen um 50 Prozent niedrigeren Stromverbrauch gegenüber vergleichbaren Produkten aus. Damit tragen die Quarzoszillatoren der SG-8101 Serie erheblich zu den Systemeigenschaften mit harter Echtzeit, niedrigen Stromverbrauch und schnelleren Entwicklungszyklen bei. Sie eignen sich auch für kleinere Produktionsmengen, es gibt sie in mehreren Baugrößen von 7mm x 5mm bis 2,5mm x 2mm, wobei bei Epson-Oszillatoren immer gilt: je kleiner, desto günstiger. Die neue Serie SG-8018 ist die günstigste PLL-Serie von Epson, die per Standard bereits mit +/-50ppm über -40 bis 105°C spezifiziert ist und zukünftige Anforderungen bezüglich Betriebstemperatur bereits erfüllt. Auch hier sind alle Bauformen von 7mmx5mm bis 2,5mmx2mm verfügbar.

Bild: Epson

Quarzoszillatoren, die auch harte Echtzeitanforderungen erfüllen, bietet z.B. Epson.

Echtzeituhren für höchste Genauigkeit

Ist eine noch höhere Präzision erforderlich, sind Echtzeituhren (Real Time Clocks, RTC) das Mittel der Wahl. Diese separaten Module bieten ein einfacheres Design dank integriertem Quarz, eine hohe Zuverlässigkeit und niedrige Stromaufnahme und können z.B. als BackUp Funktion eingesetzt werden. Für höchste Genauigkeit, die bei vernetzten Systemen zunehmend wichtiger wird, hat die RX8900CE Serie von Epson eine integrierte Temperaturkompensation. Damit kann sie etwa die zeitliche Zuordnung verschiedener Ereignisse in Relation zueinander setzen. Die RTCs haben eine Ganggenauigkeit von bis zu ±3,4x10^{-6} bei Temperaturen von -40 bis +85°C. Sowohl bei den Oszillatoren als auch bei den Echtzeituhren führt der Hersteller die Abstimmung des Quarzes durch. Damit ist keine große Untersuchung des Designs notwendig, was die Time-to-Market deutlich verkürzt. Um den Quarz optimal an das Design anzupassen – und so Zeit und Geld zu sparen – bietet Epson außerdem einen Evaluation Service an. Rutronik unterstützt bei der Auswahl und vermittelt zwischen Hersteller und Kunden. ■

Autor: *Jochen Neller,*
Technischer Support Inductors & Timing Devices,
Rutronik Elektronische Bauelemente GmbH
www.rutronik.com/de

Vorschau Industrial Communication Journal 2018

	Protokolle und Standards	Komponenten und Lösungen	Wireless und Remote	Sicherheit	Industrielle Kommunikation 4.0
Ausgabe I ET: 28.03.2018 RS: 28.02.2018	Profibus und Profinet AS-Interface	OPC UA als Backbone für Industrie 4.0 Kommunikations-lösungen für die Antriebstechnik Serielle Adapter für Ethernet *mit Marktübersicht*	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
Ausgabe II ET: 15.05.2018 RS: 17.04.2018	Ethercat Modbus TCP/IP CC-Link	Kabel und Verbindungstechnik *mit Marktspiegel* 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
Ausgabe III 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 *mit Marktübersicht* Funk in der Feldebene	Antiviren-Software für die Industrie Sicher kommunizieren mit Profisafe Security *mit Marktübersicht*	Industrial IoT Cloud & M2M Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN
Ausgabe IV ET: 19.11.2018 RS: 22.10.2018	Ethernet Powerlink Sercos IO-Link	Diagnose und (Fern-) Wartung IO-Systeme mit Feldbus/ Ethernet-Ankopplung *mit Marktübersicht*	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

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),
Clara Luise Josuttis (clj),
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

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 Götze,
Fabienne Heßler, Melissa Hoffmann,
Ronja Kaledat, Moritz Klös,
Timo Lange, Ann-Christin Lölkes,
Nadin Rühl, Verena Vornam

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

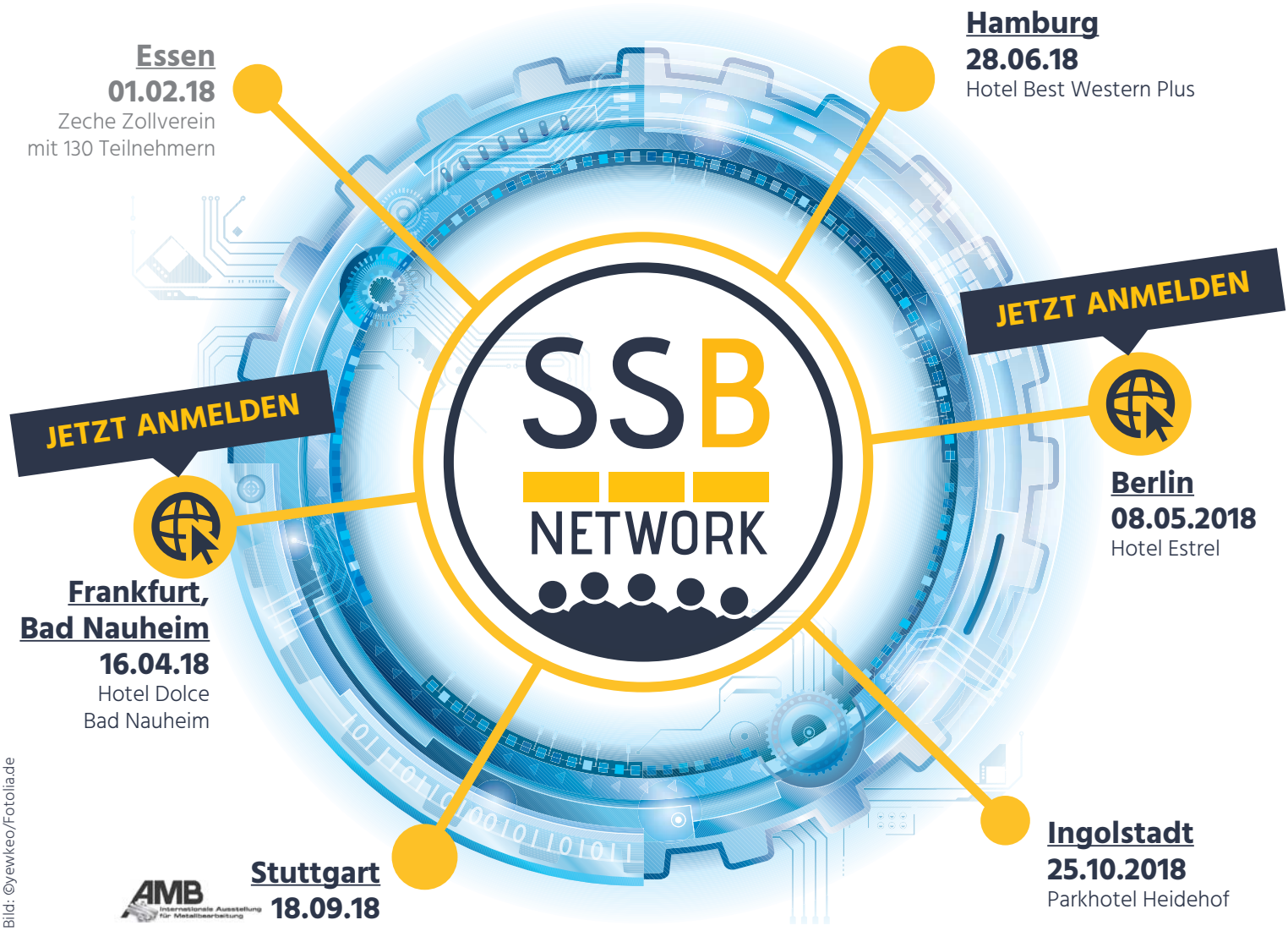
JAHRESABONNEMENT
SPS-MAGAZIN: (18 Hefte)
Inland: 99€ (inkl. MwSt. + Porto)
Ausland: 115€ (inkl. Porto)

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

ISSN 0935-0187
Vertriebskennzeichen G30449

NETWORK SCHALTSCHRANKBAU2018

Neuste Entwicklungen zuerst erfahren und miteinander austauschen!



Essen
01.02.18
Zeche Zollverein
mit 130 Teilnehmern

Hamburg
28.06.18
Hotel Best Western Plus

Berlin
08.05.2018
Hotel Estrel

Frankfurt,
Bad Nauheim
16.04.18
Hotel Dolce
Bad Nauheim

Stuttgart
18.09.18

Ingolstadt
25.10.2018
Parkhotel Heidehof

Bild: ©yewkeo/Fotolia.de

- **Relevante VDE/DKE-Normen**
- **UL-Normung für den nordamerikanischen Markt**
- **Digitalisierung im Schaltanlagenbau**
- **Planungstools und Software**
- **EMV- und Störlichtbogenschutz**

Treffen Sie Kollegen aus Ihrer Branche und pflegen Sie Kontakte in angenehmer Atmosphäre. Freuen Sie sich auf spannende Fachvorträge zu aktuellen Themen rund um den Schaltanlagenbau. Unsere Industriepartner zeigen neuste Entwicklungen und beantworten Ihre Fragen.

Jetzt Anmelden

ssb-magazin.de/network04

Unsere Industriepartner:

Manometer LEO 5 mit LoRaWAN

LoRa

ISM Band

Funk-Manometer Sender und Remote-Display

GSM-2 mit Pegelsonde Serie 36 XiW

GSM

LOW POWER PRESSURE SENSORS

OPTIMIZED FOR

INTERNET OF THINGS

Bluetooth

Schnittstellen-Konverter K-114 BT für digitale + analoge Druckmessgeräte

GSM-2 Box mit Drucktransmitter Serie 23 SY

RFID

Bluetooth SMART

Manometer LEO 5 mit Bluetooth classic

RFID Datenlogger Serie 21 DC

RFID Drucktransponder Serie 21 D

Funk-Drucktransmitter mit Bluetooth smart

KELLER unplugged!

Das Internet der Dinge beginnt mit einem Sensor.

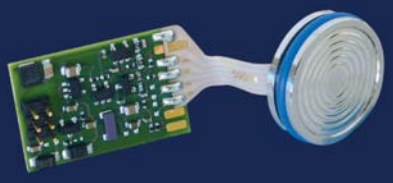
Drucktransmitter und Pegelsonden mit digitalen Schnittstellen sind wie geschaffen für IoT-Lösungen.
Niedrige Versorgungsspannungen und optimierter Stromverbrauch, ideal für batteriebetriebene Funk-Lösungen.
Druckbereiche: 0,3…1000 bar / ATEX-Zertifizierung / Druck- und Temperaturinformationen

D-Linie Drucktransmitter

- I²C-Interface bis 5 m Kabel
- 1,8…3,6 V (optimiert für Knopfzellen)
- 20 µW @ 1 S/s und 1,8 V
- Gesamtfehlerband ± 0,7 %FS @ -10…80 °C

X-Linie Drucktransmitter

- RS485-Interface bis 1,4 km Kabel
- 3,2…32 V (optimiert für 3,6 V Lithium-Zellen)
- 100 µW @ 1 S/min und 3,2 V
- Gesamtfehlerband ± 0,1 %FS @ -10…80 °C



Hannover Messe I Halle 11 I Stand A72

KELLER

keller-druck.com