SPS MAGAZIN
SONDERAUSGABE 2/2017
www.sps-magazin.de

INDUSTRIAL COMMUNICATION JOURNAL

ETHERNET WIRELESS SECURITY

Bild: IFM Electronic GmbH

Handling von Sensordaten

Der Weg in die Cloud Seite 6

IM SCHULTERSCHLUSS?
Time Sensitive Networking für den Einsatz in der Industrie
Seite 11

LICHTWELLENLEITER
Wann sind optische Fasern die bessere Alternative zu Kupfer?
Seite 26

WIRELESS & REMOTE
Von der Funktechnik im Feld zu Edge und dem Industrial IoT
ab Seite 36

In die Cloud

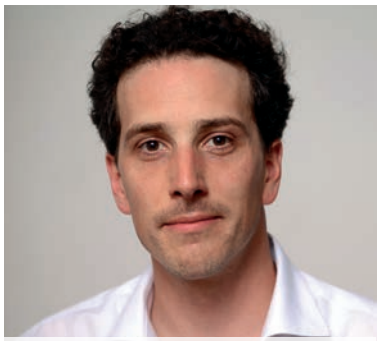
ohne Angst vor Datenklau

WAGO ist die erste Wahl, wenn Sie Ihre Energie- und Prozessdaten sicher verwalten und zur Analyse in die Cloud schicken wollen. Dank Security by Design und des gehärteten Linux®-Betriebssystems unserer Controller bleiben Ihre Daten vor Hackern geschützt. **Das ist die digitale Zukunft!**

www.wago.com/digitale-zukunft/de

WAGO

Generations-übergreifend



Mathis Bayerdörfer, Chefredakteur INDUSTRIAL COMMUNICATION JOURNAL

Die komplette Anbieterschaft der Automatisierungstechnik diskutiert TSN als Echtzeit-Enabler für Standard-Ethernet. Schießt das nicht am Ziel vorbei, angesichts der Tatsache, dass viele Anwender nach wie vor auf klassische Feldbusse setzen oder gerade auf Industrial Ethernet wechseln? Nein, denn die Historie hat gezeigt: Früh übt sich und gut Ding will Weile haben.

Zugegeben: Je nachdem, mit wem man über Ethernet TSN spricht, bekommt man den Eindruck, da komme das neue Kommunikations-Allheilmittel, der große Gleichmacher, auf den die Anwender sehnsüchtig gewartet haben. Doch dem ist entgegenzuhalten: Die Landschaft der industriellen Kommunikation, samt der dort eingesetzten Technik und Technologie, ist sehr heterogen. Das war schon immer so und wird noch lange so bleiben. Die Vielseitigkeit ist letztendlich auch ein Grund, warum das SPS-MAGAZIN diesem Thema mit dem INDUSTRIAL COMMUNICATION JOURNAL seit mehr als zehn Jahren eine Sonderheft-Reihe widmet.

Es ist also nicht weiter verwunderlich, dass auch beim Thema TSN nicht alle ins gleiche Horn stoßen. Zwar korrespondiert die grundlegende Stoßrichtung stets – keiner will der Weiterentwicklung des Standard-Ethernets ihren Benefit für die industrielle Kommunikation absprechen. Wo die Vorteile für den Anwender aber konkret liegen und wie diese im Zusammenspiel mit den bisherigen Lösungen zu erschließen sind, dazu gehen die Meinungen auseinander, wie die Experten-Statements im TSN-Faktecheck dieser Ausgabe zeigen (S. 11).

Um dem Informationsanspruch der Branche gerecht zu werden, berichtet das INDUSTRIAL COMMUNICATION JOURNAL aber generationsübergreifend über Produkte, Lösungen und Trends. Der Anwendungsbeitrag auf Seite 30 liefert ein gutes Beispiel dafür, wie es in der produktionstechnischen Praxis tatsächlich vielerorts läuft. Statt auf OPC UA und TSN zu setzen, ist man dort momentan dabei, von klassischen Feldbussen auf Industrial-Ethernet-Standards umzustellen. Das passiert aber in den seltensten Fällen ad hoc, sondern gut geplant und auf mittel- bis langfristiger Schiene. So lässt sich zusammenfassen: Auch in der industriellen Kommunikation ist nichts beständiger als der Wandel. In diesem Sinne wünsche ich eine interessante Lektüre.

Mathis Bayerdörfer
mbayerdoerfer@sps-magazin.de

Bild: IFM Electronic GmbH

6

TITELSTORY

Der Weg in die Cloud

Für die allermeisten Ansätze von Industrie 4.0 ist eine durchgängige Datenkommunikation von der Feldebene zu übergeordneten Systemen absolute Voraussetzung. Um den Anwender bei dieser Herausforderung zu unterstützen, hat IFM neue Lösungen entwickelt, die sich speziell dem Handling von Sensordaten aus dem Feld auf ihrem Weg in die Datenwolke widmen. Auch eine eigene Cloudlösung stellt das Unternehmen dafür bereit.

Grundlage für das Digital Enterprise

Industrielle Netzwerkdesigns konzipieren, planen und einrichten
Seite 12

Bild: Siemens AG

Sichere Antriebssteuerung

AS-Inteface und FSoE: Antriebe ohne Sicherheits-SPS steuern und überwachen
Seite 28

Bild: Bihl+Wiedemann GmbH

Markt-Trends-Technik

TSN Faktencheck

Protokolle und Standards

Komponenten und Lösungen

Wireless und Remote

Sicherheit

Service

Permanente Netzwerküberwachung

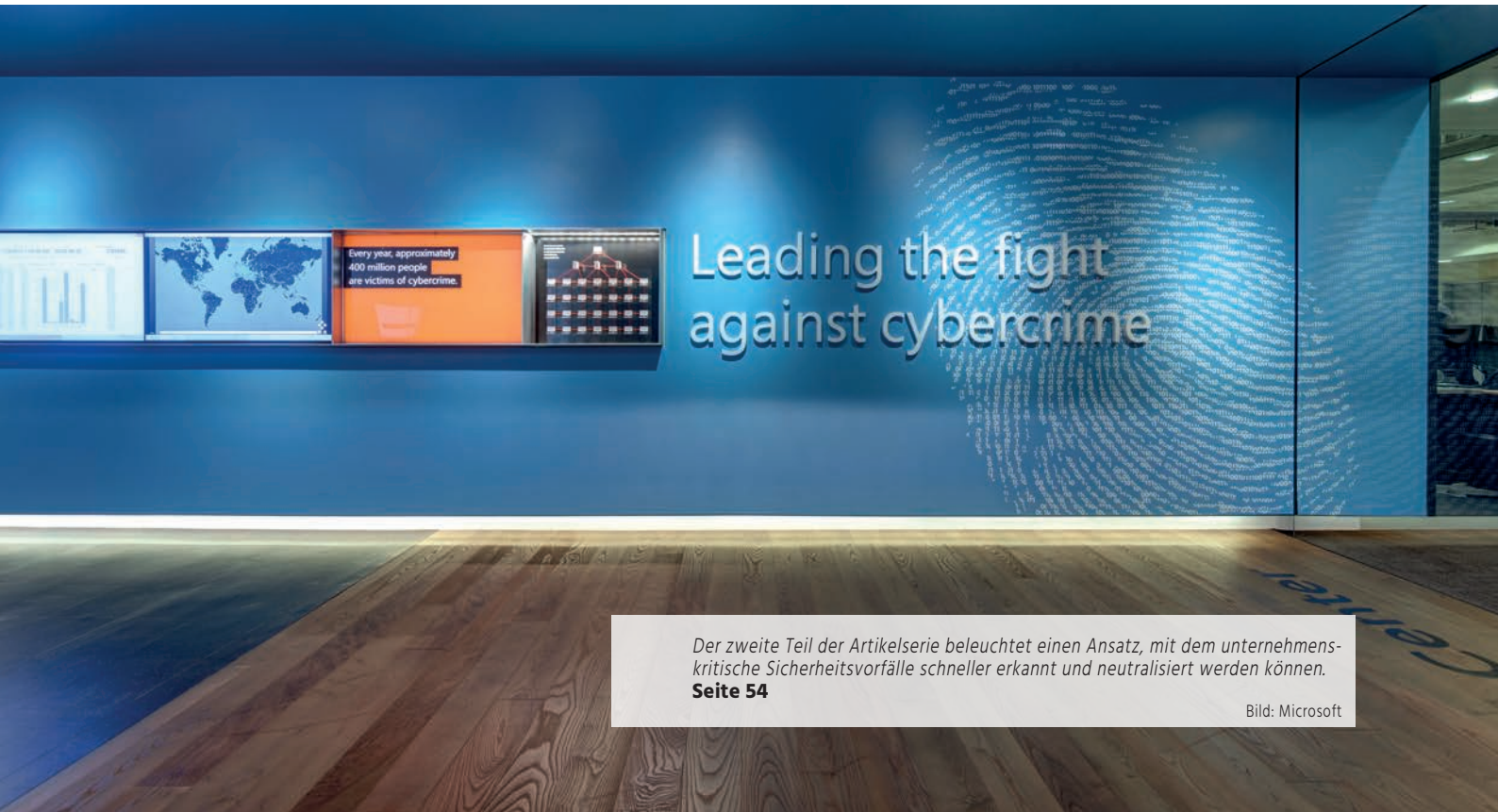
Bild: Indu-Sol GmbH

Monitoring-Software überwacht komplexe Fördernetze
Seite 30

Edge Computing

Bild: © bluebay2014 / thinkstock.de; © stockchairatgfx / thinkstock.de

Produktionsdaten filtern und vorverarbeiten
Seite 36



Der zweite Teil der Artikelserie beleuchtet einen Ansatz, mit dem unternehmenskritische Sicherheitsvorfälle schneller erkannt und neutralisiert werden können.
Seite 54

Bild: Microsoft

Handling von Sensordaten

Der Weg in die Cloud

Für die allermeisten Ansätze von Industrie 4.0 ist eine durchgängige Datenkommunikation von der Feldebene zu übergeordneten Systemen absolute Voraussetzung. Um den Anwender bei dieser Herausforderung zu unterstützen, hat IFM neue Lösungen entwickelt, die sich speziell dem Handling von Sensordaten aus dem Feld auf ihrem Weg in die Datenwolke widmen. Auch eine eigene Cloudlösung stellt das Essener Unternehmen dafür bereit.

Die IO-Link-Produkte von IFM eröffnen dem Anwender eine einfachen Weg, um Sensordaten in übergeordneten Systemen zu verwenden.

Bild: IFM Electronic GmbH

„Industrie 4.0 muss schon bei der ersten Anwendung einen erkennbaren Nutzen bringen", fordert Michael Marhofer, Vorsitzender des Vorstands bei IFM. Seiner Meinung nach werden die Datenmengen, die beispielsweise in einer Produktionsanlage von Sensoren generiert werden, heute häufig aber noch unterschätzt. Aufgabe der Automatisierungsunternehmen sei es daher, Anwendern Lösungen anzubieten, die eine Vorverarbeitung dieser Daten ermöglichen.

IO-Link als Basis für Industrie 4.0

Diesem Anspruch folgend hat das Unternehmen IFM kürzlich verschiedene Neuheiten vorgestellt. Darunter auch eine Anzahl an Produkten, die um eine IO-Link-Schnittstelle ergänzt wurden. Denn bei IFM ist man fest überzeugt: IO-Link ist das Fundament für eine erfolgreiche Umsetzung der Industrie 4.0-Konzepte. „Der Datenhaufen muss an der Quelle sortiert werden", bringt Peter Wienzek, Manager Business Development Systems, eine zentrale Anforderung auf den Punkt. Der IO-Link-Standards als moderne Alternative zur analogen Schnittstellen wie 4...20 mA bringt in dieser Hinsicht das Potenzial mit, die herkömmliche Messwertübertragung zu ersetzen. Aufgrund des digitalen Übertragungsprinzips sind verfälschte Werte durch Störungen auf der Leitung praktisch ausgeschlossen. Ein weiterer Vorteil der IO-Link-Übertragung ist die Möglichkeit, ergänzende Informationen – etwa Statusinformationen des Sensors – gleichzeitig mit zu übertragen. Auch bei der Konfiguration von Sensoren bietet IO-Link Vorteile: Die Parametrierung lässt sich z.B. direkt von einem IO-Master übertragen, so dass ein aufwändiges Einstellen am Sensor entfallen kann. Folgerichtig haben fast alle neuen Produkte des Unternehmens standardmäßig eine IO-Link-Schnittstelle – aktuell sind es rund 500 und jährlich kommen 100 bis 150 weitere Produkte hinzu. Seine neue Generation an IO-Link Mastern hat IFM besonders robust ausgelegt. Sie verfügt über zwei Ethernet-Ports mit Switch für Profinet. Zur Konfiguration der angeschlossenen Sensoren und Aktuatoren wird die Software LR Device eingesetzt. Das Tool findet alle IO-Link-Master im Ethernet-Netzwerk und erstellt eine Übersicht über die gesamte Anlage.

Kommunikation mit der Leitebene

Sensoren müssen als Sinnesorgane einer Maschine oder Anlage nicht nur Messwerte erfassen und Signale ausgeben, sondern diese auch nahtlos kommunizieren. Möglichst einfach von der Sensorebene über Steuerungs- und Leitebene bis hinauf zur Unternehmensebene. Nur so lassen sich viele Vorteile von Industrie 4.0 überhaupt erst umsetzen. Mit IO-Link-Anbindung der Sensoren eröffnet sich dem Anwender eine einfache Möglichkeit, Daten aus dem Feld für übergeordnete Systeme zu verwenden. In der Regel verarbeitet jedoch eine SPS die Daten der angeschlossenen Sensoren und eine Weiterleitung an die Leitebene ist nicht vorgesehen. Will man eine solche Weiterleitung implementieren, muss das SPS-Programm geändert werden. Um dies zu vermeiden, können Daten von Sensoren, die

über eine IO-Link-Schnittstelle verfügen, direkt an übergeordnete Systeme weitergereicht werden. Hierzu ist allerdings ein Werkzeug notwendig, das verschiedene Datenquellen verarbeiten und mit allen üblichen Protokollen zusammenarbeiten kann. Ein solches Werkzeug stellt IFM mit dem Linerecorder-Framework zur Verfügung. Das System besteht aus mehreren Software-Modulen, mit denen sich eine durchgängige Kommunikation realisieren lässt. Der Linerecorder Agent Connectivity Port ist zum Beispiel ein Software-Gateway, das eine bidirektionale Kommunikation zwischen einer großen Zahl unterschiedlicher Schnittstellen erlaubt. Damit ist eine Kommunikation zwischen SAP-Systemen auf der einen Seite und den Daten der Geräte aus der Feld-, Steuerungs- und Leitebene andererseits möglich. „Viele Sensorinformationen, die für vorausschauende Wartung oder Energieverbrauchsmessung benötigt werden, sind für die Steuerungsaufgaben in der Maschine nicht nötig und daher in der SPS nicht verfügbar", erklärt Wienzek. „Aus diesem Grund haben wir einen zweiten Kommunikationsweg unter Umgehung der Steuerungsebene geöffnet." Diesen bezeichnet IFM als Y-Kommunikation, da die Daten wie in den beiden Armen des Buchstaben Y einmal zur SPS gelangen und auf der anderen Seite direkt in die Unternehmensleitebene.

Maschinen und Anlagen einfach überwachen

In dem Software-Framework ist mit dem Linerecorder Smartobserver auch ein System zur Visualisierung enthalten, mit dem der Anwender den Zustand von Maschinen und Anlagen einfach überwachen kann. Die Visualisierung des Smartobservers lässt sich sehr einfach entsprechend der Nutzerwünsche anpassen. Das Linerecorder-Framework macht viele Anwendungen möglich, bei denen Sensordaten eine Rolle spielen. Typisches Beispiel ist die zustandsorientierte Wartung von Maschinen. Sensoren erfassen dabei Vibrationen, die den Verschleiß eines Lagers innerhalb der Maschine ankündigen. Aufgrund der Sensordaten lässt sich der Austausch des Lagers rechtzeitig planen. Sowohl Maschinenstillstände durch einen plötzlichen Lagerschaden als auch unnötige Wartungsarbeiten können so vermieden werden. Ein anderes Beispiel ist die Überwachung von Druckluftanlagen. Sensoren, die den Druckluftverbrauch messen, sind in vielen Maschinen bereits vorhanden, um den Betrieb sicherzustellen. Die Daten dieser Sensoren können verwendet werden, um Druckluftlecks zu erkennen und so beheben zu können. Dies funktioniert aber nur, wenn die Sensordaten an einem übergeordneten System zur Verfügung stehen, was mit der Kommunikation über den Y-Weg und dem Linerecorder-Framework problemlos möglich ist.

Bild: IFM Electronic GmbH

Mit dem Ansatz des Y-Wegs von IFM gelangen Daten aus dem Feld einerseits zur SPS und andererseits direkt in die Unternehmensleitebene.

Bild: IFM Electronic GmbH

Damit der Anwender die für ihn wichtigen Daten stets im Blick hat, ist das Cockpit des Linerecorder Smartobserver frei konfigurierbar.

Sicher in die Cloud

Weil Vorteile wie gesteigerte Verfügbarkeit, ein globaler Zugriff auf Daten oder eingesparte Hardware-Kosten auf der Hand liegen, sind Cloud-Lösungen in vielen Industriebereichen auf dem Vormarsch, z.B. im Maschinenbau. Mit entsprechenden Lösungen lassen sich Remote-Dienstleistungen und neue Geschäftsmodelle realisieren, ohne dass die Software aufwändig implementiert werden muss. Unter dem Slogan „Vertrauen durch Sicherheit" bietet IFM deshalb jetzt auch eine eigene Cloud an. So sollen Kunden die Vorteile von Cloud und durchgängiger Datenkommunikation zusammen nutzen können. Die ERP-Konnektivität der Daten wird durch die Nutzung der Plattform von SAP garantiert. Um Vorbehalte gegenüber Cloud-Lösungen auszuräumen, setzt IFM an dieser Stelle auf hohe Standards in Bezug auf Datenschutz und Sicherheit. Ein Zertifikatemanagement und eine E2E-Verschlüsselung der Daten schützt vor unberechtigten Zugriffen. Außergewöhnlich ist zudem, dass die Datenhoheit vollständig beim Kunden verbleibt. Eine Nutzung oder der Verkauf der Daten an Dritte wird ausgeschlossen. Damit – und mit dem in Software gegossenen Applikations-Know-how – will sich IFM von den meisten Cloud-Anbietern abheben. Durch die Branchenkenntnisse des Unternehmens stehen dem Kunden abgestimmte Lösungen im industriellen Umfeld zur Verfügung. Da die Lösungen in Form von SaaS (Software as a Service) angeboten werden, ist die für die Implementierung benötigte Zeit auch in Verbindung mit SAP sehr kurz. Zusätzlich profitieren die Kunden von geringen Investitionen und einem weltweiten Support 24/7. ■

Firma: **IFM Electronic GmbH**
www.ifm.com

Feldbusse weiter nachgefragt

Dass heute oft von modernen Kommunikationstechnologien wie OPC UA, IO-Link oder auch Safety-Protokollen die Rede ist, darf nicht darüber hinwegtäuschen, dass die klassischen Feldbusse von der Mehrheit der Maschinenbauer auch zukünftig genutzt werden. Insgesamt wird aber die Bedeutung der modernen Technologien stark steigen. Auch der Einsatz von Ethernet-Protokollen und Funktechnologien wird weiter zunehmen.

Zu diesen Ergebnissen kommt eine aktuelle unabhängige Marktstudie mit dem Titel 'Industrielle Kommunikation'. Im Rahmen der Wiederholung von Studien aus den Jahren 2004, 2008 und 2013 gaben im Januar/Februar 2017 deutschlandweit knapp 300 Maschinenbauunternehmen Auskunft über das Einsatzverhalten und über zukünftige Entwicklungen in den Bereichen Industrie 4.0, Feldbus/Ethernet und Wireless.

Vernetzung schreitet voran

Die Verknüpfung von Automatisierungs- und IT-Netz schreitet weiter voran: Mehr als 80 Prozent der Maschinenbauer erwarten zukünftig Industrie-4.0-Eigenschaften vom Automatisierungsnetz. Die größte Rolle spielen hier Plug&Play und die einheitliche Datenbeschreibung. Jedes vierte Unternehmen rechnet aber auch mit der Anbindung an eine Private Cloud, wobei sich abzeichnet, dass OPC UA dabei eine wichtige Rolle spielen wird. Bemerkenswert dabei ist, dass derzeit nur 37 Prozent der Unternehmen der Security in der Maschinen-/Feldebene einen hohen Stellenwert beimessen.

Ethernet im Einsatz

Ethernet löst herkömmliche Feldbussysteme immer weiter ab: Fast alle Maschinenbauer (96 Prozent) setzen sie mittlerweile ein. Am meisten verbreitet sind dabei Profinet im Feld und TCP/IP auf der Leitebene. Allerdings handelt es sich bei der Umstellung um einen langwierigen Prozess, da auch weiterhin fast drei von vier Unternehmen Feldbussysteme einsetzen werden. Gerade CAN- und ASi-Bus-Nutzer planen überwiegend auch zukünftig mit diesen Vernetzungsarten. Eine steigende Rolle

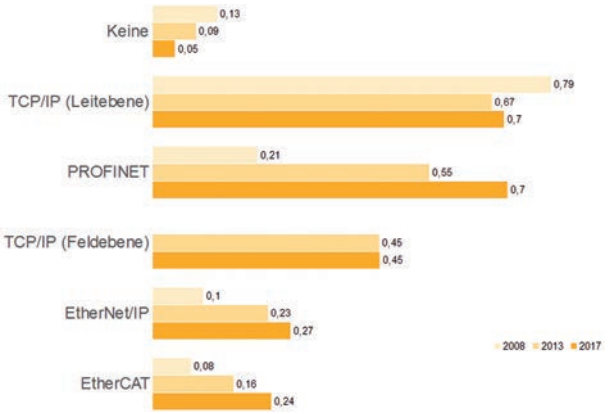


Bild: © Michaela Rothhöff/FH Südwestfalen

nimmt Ethernet im Bereich der funktionalen Sicherheit ein, denn demnächst werden immer mehr Safety-Protokolle auf Ethernet-Basis verwendet.

Sorgenkind Funktechnologien

Die Nutzung von Funktechnologien ist zwar in den letzten Jahren gestiegen, aber bei weitem nicht in dem Ausmaß, wie vor einigen Jahren prognostiziert. So planten z.B. 2013 knapp 40 Prozent der Unternehmen die kabellose Anbindung von Bediengeräten für die Zukunft, real sind es aber heute erst 20 Prozent. Die Studie wurde von Michaela Rothhöft, wissenschaftliche Mitarbeiterin der Fachhochschule Südwestfalen, freiberuflich mit Unterstützung des VDMA-Arbeitskreises Steuerungstechnik durchgeführt.

www.marktstudien.org

50.000 Downloads auf SourceForge

Bild: Ethernet Powerlink Standardization Group (EPSG)

Mehr als 50.000-mal wurde der OpenPowerlink-Stack mittlerweile von SourceForge heruntergeladen. „OpenPowerlink ist durch seine Open-Source-Charakteristik einzigartig am Automatisierungsmarkt – das schlägt sich in den Downloadzahlen nieder", kommentiert EPSG-Geschäftsführer Stefan Schönegger. OpenPowerlink ist ein Protokollstack, der für die Implementierung des Echtzeit-Ethernet-Kommunikationsstandards Powerlink verwendet wird. Er erfüllt alle Anforderungen, die an Open-Source-Software gestellt werden und eignet sich für Master- und Slave-Implementierungen. OpenPowerlink ist eine softwarebasierte Lösung. Abhängig von der Anforderung lässt sich das Protokoll auf FPGAs, MCUs, ARM- oder x86-Prozessoren portieren. Als Betriebssystem kommt meist Linux, bevorzugt mit Echtzeiterweiterung, zum Einsatz. Wahlweise lässt sich OpenPowerlink auch ohne Betriebssystem oder mit Windows verwenden. Da keine spezielle Hardware nötig ist und der Software-Stack als Open-Source zur Verfügung steht, ist OpenPowerlink nicht nur für Maschinen- und Anlagenbauer, sondern auch für Universitäten und Forschungseinrichtungen interessant.

Ethernet Powerlink Standardization Group (EPSG)
www.ethernet-powerlink.org

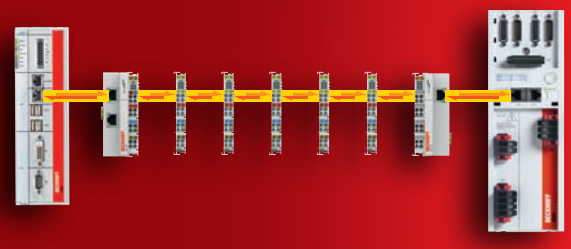
EtherCAT-Klemmen.
Das schnelle All-in-One-System für alle Automatisierungsfunktionen.

Das Beckhoff-I/O-System integriert Klemmen für:

- Alle digitalen/analogen Standardsignaltypen
- Antriebstechnik, wie z. B. Schrittmotoren, AC/DC-Motoren
- Gateways zur Einbindung unterlagerter Feldbussysteme
- Hochpräzise Messtechnik, Condition Monitoring
- TwinSAFE PLC und Safety-I/Os
- Highspeed-Automation (XFC)

www.beckhoff.de/EtherCAT-Klemmen

- Echtzeit-Ethernet bis zur I/O-Ebene
- Geringe Systemkosten
- Flexible Topologie
- Maximale Performance
- Einfache Konfiguration
- Feldbussysteme und Safety-Geräte integrierbar



Ethernet bis in die Klemme: mit Vollduplex-Ethernet im Ring und einem Telegramm für mehrere Teilnehmer. Anschluss direkt am Standard-Ethernet-Port.

New Automation Technology **BECKHOFF**

IO-Link-Safety-Spezifikation freigegeben

Bild: Profibus Nutzerorganisation e.V.

Mit der Freigabe und Veröffentlichung der IO-Link- Safety-Spezifikation durch die IO-Link Community sowie der erfolgreichen Konzeptbeurteilung durch den TÜV Süd steht der Umsetzung in Systeme und Geräte nichts mehr im Wege. So wie IO-Link ist auch IO-Link Safety Feldbus- und System-unabhängig. Erreicht wird dies durch die Umsetzung der vielen am Markt verfügbaren Safety-Protokolle zu IO-Link Safety im Master. Die IO-Link Safety Devices bleiben damit weltweit einheitlich. Bedenkt man, dass es bereits heute mit den 4.000 Device-Typen wesentlich mehr gibt als IO-Link Master, liegen die Vorteile auf der Hand. Soll ein neuer Markt oder ein neues System für IO-Link Safety erschlossen werden, so muss nur ein entsprechender IO-Link Safety Master entwickelt werden. Alle vorhandenen IO-Link Safety Devices können unverändert verwendet werden. Auf Basis der vorliegenden Spezifikation können jetzt die Hersteller beginnen, IO-Link Safety in ihre Systeme zu integrieren. Hand in Hand werden parallel dazu die Testspezifikation und Testsysteme sowie die Zertifizierung vorbereitet.

Profibus Nutzerorganisation e.V.
www.profibus.com

Neuer Vorstand beim AutomationML e.V.

Anfang Mai fand in Fulda die jährliche, ordentliche Mitgliederversammlung des AutomationML statt, auf der der Vorsitz im Vorstand getauscht wurde. Vorsitzender ist jetzt Dr. Andreas Gössling von Hilscher. Jürgen Kübler (Bild) von Daimler, bisher Vorsitzender, bleibt als Beisitzer Mitglied des Vereinsvorstands. Dadurch sollen neben dem Automobilsektor auch andere Industrien ein Signal zur Mitarbeit im Verein erhalten. Neu in den Vorstand gewählt wurde Daniel Wolff von Inpro.

Bild: Daimler AG

AutomationML e.V.
www.automationml.org

ODVA startet Projekt XDS

Die ODVA hat eine neue technische Strategie für die Entwicklung von Standards und Tools der nächsten Generation digitaler Beschreibungenen für Gerätedaten eingeleitet – das 'Project XDS'. Schwerpunktmäßig konzentriert es sich auf die Entwicklung von Spezifikationen für Workflow-gesteuerte Gerätebeschreibungsdateien für die Geräteintegration und für digitalisierte Geschäftsmodelle. Phase 1 von XDS ist bereits im Gange - diese Phase wird von einem Ad-hoc-Ausschuss unter der Leitung des ODVA-Vorstandes durchgeführt und beinhaltet die Erstellung des Gesamtplanes für das Projekt, darunter u.a. die Zuordnung nativer Gerätedaten zu Geräteintegrationsworkflows, die Referenzarchitektur für die Verwendung der XDS-basierten Geräteintegrationsdateien und die Syntax bzw. das Format, die von XDS-Gerätebeschreibungsdateien zu verwenden sind. Phase 2 steht unter der Leitung der ODVA Special Interest Group, die sich auf das Verfassen und Veröffentlichen der XDS-Spezifikation konzentriert. Phase 2 soll 2018 starten. Beginnend mit Ethernet/IP, ODVAs industriellem Ethernet-Netzwerk und dem Ethernet/IP-Kernkonzept für standardmäßige Ethernet- und Internet-Technologien, verfolgt ODVA die Idee, die Verlagerung von Gerätedaten von der Werkshalle zum Enterprise zu vereinfachen. Darüber hinaus bietet ODVAs Common Industrial Protocol, das als 'CIP' bekannt ist und von Ethernet/IP und ODVAs anderen industriellen Netzwerktechnologien verwendet wird, ein kontextbasiertes Repository für Gerätedaten. Zusammen bilden die Technologien die Basis für die Definition einer ganzheitlichen Beschreibungsdatei, um die digitalisierte Darstellung eines Geräts abzubilden. Project XDS definiert die Technologien und Standards für 'XDS'-Gerätebeschreibungsdateien, die auf einem gemeinsamen Format und einer gemeinsamen Syntax basieren und somit eine Workflow-gesteuerte Integration für Netzwerk- und Sicherheitskonfigurationen, Netzwerk- und Sicherheitsdiagnosen sowie Gerätekonfigurationen bzw. Gerätediagnosen ermöglichen.

ODVA Inc.
www.odva.org

Powerlink wird IEEE61158-Standard

Wie EPSG Ende Mai mitteilte, wurde Powerlink vom IEEE (Institute of Electrical and Electronics Engineers) als internationaler Standard IEEE61158 verabschiedet. Es sei das einzige Industrial-Ethernet, das diesen Status erreicht habe. Die IEEE-Standards zu TSN und Powerlink sind damit aus Sicht des Verbands zentrale Komponenten für industrielle Echtzeitkommunikation. Die IEEE-Arbeitsgruppe 'Industrial real-time communication' hat in den vergangenen zwei Jahren an der Definition eines Industrial-Ethernet-Standards gearbeitet. Im März hat die Arbeitsgruppe schließlich mit einer Zustimmung von 97% Powerlink als alleinigen IEEE-Standard verabschiedet.

Ethernet Powerlink Standardization Group
www.ethernet-powerlink.org

Time Sensitive Networking

Mehrwert im Schulterschluss?

In der Branche wird TSN als Weiterentwicklung des Ethernet-Standards aktuell stark diskutiert. Bislang ist Standard-Ethernet für Anwendungen in der Automatisierung nicht geeignet, weil es weder deterministisch noch echtzeitfähig ist. TSN könnte das ändern. Wird es damit zum Alleinherrscher der industriellen Kommunikation oder stellen sich gerade im Zusammenspiel mit klassischen Feldbus- und Industrial-Ethernet-Standards Vorteile für den Anwender ein? Das INDUSTRIAL COMMUNICATION JOURNAL hat verschiedene Experten gefragt.

Vielversprechende Lösung

In der Nutzerorganisation von Profibus und Profinet halten wir TSN für eine sehr vielversprechende Lösung für die industrielle Kommunikation im Zeitalter von Industrie 4.0. Damit wird es möglich sein, die Vorteile von Ethernet aus der IT-Welt, wie z. B. eine hohe Bandbreite, mit den Errungenschaften der Fertigungswelt, z. B. Echtzeitfähigkeit, zu kombinieren. So entsteht ein zukunftssicheres Echtzeit-Ethernet-System für die industrielle Automatisierung. Vor allem die hohe Bandbreite, z. B. durch GBit, aber auch der Einsatz von Standard-Ethernet-Chips sind Vorteile gegenüber den heutigen Systemen. In PI werden wir TSN als einen weiteren Layer 2 – neben den heute verfügbaren RT und IRT – für Profinet nutzbar machen. Dabei ist uns wichtig, die heutige Anwendersicht in Profinet beizubehalten. Das heißt, dass auch künftige TSN-basierte Profinet-Geräte die gleichen Dienste wie die heutigen Geräte anbieten und auch die Netzwerkkonfiguration in der Feldebene analog zu der bekannten Lösung funktioniert. Somit senken wir die Hürde für die Anwender, in Zukunft auch TSN-Geräte einzusetzen. Applikationen müssen nicht aufwendig neu programmiert werden. Profinet-Geräte auf TSN-Basis werden sich eben wie Profinet-Geräte anfühlen. Es geht darum vorhandenes Know-How zu nutzen und den Wandel so einfach wie möglich zu gestalten. Dazu sind aber auch noch einige Hausaufgaben zu erledigen, beispielsweise wie TSN-Netzwerke herstellerübergreifend konfiguriert werden. Vor allem in Hinblick auf konvergente Netzwerke. Denn eine der Stärken von Profinet ist, dass neben dem zyklischen Echtzeit-Datenaustausch auch immer parallel zusätzlicher Ethernet-Traffic möglich ist. In der Zukunft wird das vor allem auch OPC UA sein, um beispielsweise Maschinen an die IT-Welt anzuschließen. Neben Profinet werden damit auch andere Protokolle TSN nutzen. In der Nutzerorganisation PI sehen wir uns mit unserer breiten Mitgliederbasis in der idealen Position diese Entwicklung voranzutreiben und zu standardisieren. ■

> *„Es geht darum, vorhandenes Know-How zu nutzen und den Wandel so einfach wie möglich zu gestalten.*
>
> *Karsten Schneider, Chairman, Profibus & Profinet International*

Bild: Profibus Nutzerorganisation e.V.

Ethercat profitiert von TSN

Für Ethercat ist TSN das Beste, was passieren konnte. TSN ist ja ein Bündel von Projekten des entsprechenden IEEE802.1-Arbeitskreises, von denen viele die Verbesserung der Echtzeitfähigkeit von Ethernet zum Ziel haben, einige für die industrielle Kommunikation interessant sind und erst manche abgeschlossen sind. Und Ethercat wird von diesen Ergebnissen profitieren, sobald sie verfügbar sind und wo sie Sinn machen: bei der Vernetzung von Steuerungen, aber auch für neuartige Systemarchitekturen. So kommt Ethercat ja in der Regel mit einem einzigen Frame pro Zyklus aus – nicht mit einem pro Netzwerkknoten. Damit kann man ein abgesetztes Ethercat-Segment elegant und schlank mit einem einzigen Frame versorgen, in Zukunft auch deterministisch mit Hilfe von TSN-Technologien. Daran arbeiten wir, und das ist eine wunderbare Ergänzung unseres Systems. Passend zum postfaktischen Zeitalter sind ja über TSN die schönsten Mythen im Umlauf. Von abenteuerlichen Zykluszeiten bis hin zur Aussage, TSN sei die Sauce, mit der man ein fades Ethernet-Gericht zu einem scharfen Echtzeit-

System aufpeppt: einfach drüber leeren und fertig. Während mit Dr. Karl Weber ein Mitarbeiter des ETG-Headquarters seit fast 15 Jahren ein aktives Mitglied des IEEE TSN-Arbeitskreises ist, haben viele TSN-Lautsprecher ihre Informationen aus zweiter oder dritter Hand. Und so kündigen manche schon ihre Industrial-Ethernet-Lösungen ab, um sie durch TSN zu ergänzen oder gar zu ersetzen: der nächste große Technologiebruch rollt an, und er führt bereits zu deutlich verstärkter Nachfrage nach Ethercat, das ja in ganz anderen Performance-Regionen zu Hause ist. Und zwar ohne IT-Abteilung für die Konfiguration des Netzwerks. Mit einer einzigen stabilen Version ohne Technologiebrüche, und mit der größten Gerätevielfalt im Markt. Nicht umsonst sind alleine in den letzten zwölf Monaten fast 600 Firmen neu in die ETG eingetreten – mehr als je zuvor. ■

> *„Passend zum postfaktischen Zeitalter sind über TSN die schönsten Mythen im Umlauf.*
> *Martin Rostan, Executive Director, Ethercat Technology Group*

Bild: Ethercat Technology Group

TSN löst das Problem nicht allein

Die meisten Kommunikationsprotokolle, die auf Ethernet basieren, lassen sich auch mit Ethernet TSN kombinieren. Am grundlegenden Problem würde das jedoch nichts ändern: die Protokolle sind untereinander nicht kompatibel. In den Zeiten des Industrial IoT ist das nicht mehr der richtige Weg. Eine Grundvoraussetzung für das industrielle Internet der Dinge ist die durchgehende Konnektivität aller Systeme. Diese Konnektivität lässt sich aber nicht erreichen, wenn jede Maschine in einem Fertigungsverbund eine andere Sprache spricht –TSN alleine löst diese Problemstellung nicht. Für uns ist TSN in der industriellen Umgebung daher nur sinnvoll, wenn es mit OPC UA kombiniert wird. Dann können wir die durchgehende und schnittstellenfreie Kommunikation erreichen, die wir für die Produktion der Zukunft benötigen. Die Differenzierung der Hersteller untereinander wird in Zukunft nicht mehr über unterschiedliche Protokolle oberhalb der Steuerungsebene erfolgen. Der Zusammenschluss zahlreicher namhafter Hersteller, um OPC UA TSN voranzutreiben, unterstreicht diesen Wandel. ■

> *„TSN ist in der industriellen Umgebung nur sinnvoll, wenn es mit OPC UA kombiniert wird.*
> *Sebastian Sachse, Technology Manager Open Automation, B&R*

Bild: Bernecker + Rainer Industrie-Elektronik Ges.m.b.H.

Herstellerübergreifender Kommunikationsstandard

> *„Standard-Ethernet-Komponenten mit integrierter Echtzeitfähigkeit machen spezielle Hardware-Implementierungen überflüssig.*
> *Peter Lutz, Managing Director, Sercos International e.V.*

Bild: Sercos International e.V.

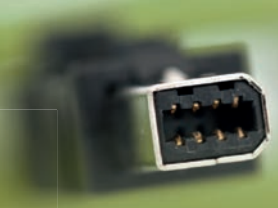
Ethernet TSN leistet einen wichtigen Beitrag, um die Konvergenz von herkömmlichen Echtzeit-Ethernet-Lösungen zu einer einheitlichen, standardisierten und durchgängigen Netzwerkinfrastruktur herbeizuführen. Denn die Verfügbarkeit von Standard-Ethernet-Komponenten mit integrierter Echtzeitfähigkeit macht spezielle Hardware-Implementierungen überflüssig. Zudem erlaubt Ethernet TSN, dass verschiedene Ethernet-basierte Protokolle in einer gemeinsamen Netzwerkinfrastruktur koexistieren können. Damit

kann auf einen einheitlichen und herstellerübergreifenden Kommunikationsstandard aufgesetzt werden. Konventionelle Feldbusse können aufgrund ihrer Übertragungsphysik und des verwendeten Busprotokolls nur über spezifische Kommunikations-Gateways in TSN-basierte Netzwerke integriert werden. Dasselbe gilt auch für Ethernet-Feldbusse, die zwar die Ethernet-Physik nutzen, aber ein proprietäres Protokoll verwenden. Eine nahtlose Integration ist lediglich für Echtzeit-Ethernet-Protokolle möglich, die die Physik und das Protokoll von Ethernet kompatibel verwenden. Solche Lösungen können direkt ohne jegliche Zusatzhardware angebunden werden und profitieren dabei von der Übertragungscharakteristik von TSN. So lassen sich beispielsweise Sercos-Geräte, die auf Fast Ethernet mit 100Mbit/s Full-Duplex basieren, auch in einer 1 oder 10Gb/s basierenden Netzwerkinfrastruktur betreiben. Auch kann der Sercos Master räumlich abgesetzt von den Sercos Slaves betrieben werden, wodurch Edge-Controller-Konzepte mit einer zentralen Steuerung von dezentralen Peripheriegeräten realisiert werden können. Ein Proof-of-Concept, das erstmalig auf der SPS/IPC/Drives 2016 präsentiert wurde, zeigt auf, dass das Sercos-Protokoll gemeinsam mit beliebigen anderen Ethernet-Protokollen (z.B. Video-Streams) über eine einheitliche, TSN-basierte Netzwerkinfrastruktur übertragen werden kann. Das Sercos-Protokoll muss dazu nicht verändert werden. Die Ethernet-TSN-Komponenten sind lediglich so zu konfigurieren, dass das Sercos-Protokoll hochprior in einem festen Zeitraster (Zeitschlitz) übertragen wird. Die Untersuchung des Echtzeitverhaltens zeigte, dass sich (trotz bzw. wegen TSN) die Fehler in der Zeitsynchronisation auf einen zweistelligen Nanosekundenbereich beschränken. Somit werden weder Funktionalität noch Echtzeitcharakteristik von Sercos eingeschränkt. Auch können bestehende Tools, wie beispielsweise der Sercos Monitor als Diagnose- und Analysewerkzeug, weiterhin vollumfänglich verwendet werden. ■

Hintergrund: Was ist TSN?

TSN bezeichnet eine Reihe von Standards, an denen die Time-Sensitive Networking Task Group (IEEE802.1) arbeitet. Diese Standardisierungsgruppe der IEEE ist aus der bis Ende 2012 bestehenden Audio/Video Bridging Task Group (AVB) hervorgegangen und setzt deren Arbeit fort. Die neu entstehenden Standards sollen Mechanismen zur Übertragung von Daten über Ethernet-Netze definieren, u.a. sollen die Erweiterungen des Bridging-Standards IEEE802.1Q eine Übertragung mit sehr geringer Latenz und hoher Verfügbarkeit möglich machen. Ein potenzieller Anwendungsbereich für TSN sind konvergente Echtzeit-Steuerungsnetze für den Automobilbau und die Fertigungsindustrie.

VARAN



REAL-TIME ETHERNET

SICHER

Jede Nachricht wird vom Empfänger sofort rückbestätigt. Unquittierte Nachrichten werden noch im selben Buszyklus wiederholt.

EINFACH

Der gesamte Befehlssatz wurde auf wenige Kommandos reduziert. Die VARAN-Bus-Implementierung ist somit sehr einfach realisierbar.

KOSTENGÜNSTIG

Durch die Verwendung von Standard-Komponenten liegt die VARAN-Anbindung auf dem Preisniveau einer herkömmlichen Feldbusanbindung.

OFFEN

Die unabhängige VARAN-BUS-NUTZERORGANISATION hält die Rechte an der Technologie. Jedes Mitglied der VNO entscheidet über die Weiterentwicklung mit.

VARAN-BUS-NUTZERORGANISATION (VNO)

www.varan-bus.net

Kommunikation über TSN

Echtzeit für die Modellfabrik

Die Technologie-Initiative SmartFactory KL hat im Rahmen der Weiterentwicklung ihrer Industrie-4.0-Produktionsanlage einen TSN-Demonstrator vorgestellt, an dem Echtzeitkommunikation vorgeführt wird.

Bild: Technologie-Initiative SmartFactoryKL e.V.

Die Produktionsanlage des SmartFactoryKL-Partnerkonsortiums soll noch in diesem Jahr mit TSN-Kommunikation ausgerüstet werden.

Der TSN-Demonstrator wurde mit technologischer Unterstützung von sechs Partnern aus Industrie und Wissenschaft realisiert: Belden/Hirschmann, Bosch Rexroth, Industrielle Steuerungstechnik, TenAsys, ISW/Universität Stuttgart und InES (Universität Zürich). Er führt vor, wie eine echtzeit- und multiprotokollfähige Netzwerkinfrastruktur auf Basis von TSN bereitgestellt werden kann.

Bildverabeitung und Echtzeit-Antriebsansteuerung parallel

Als Use-Case dient die synchrone Ansteuerung zweier Antriebe mit Echtzeit-Steuerungsdaten über TSN-Ethernet. Über diese Infrastruktur werden gleichzeitig Video-Streams einer Webcam, wie sie zum Beispiel für die Qualitätsdatenerfassung über ein Machine-Vision-System zum Einsatz kommen könnte, zu einem Remote-Display übertragen. Dabei wird die Echtzeitkommunikation ohne Beeinträchtigung aufrechterhalten. „TSN wird die Welt der Industrienetze durcheinander rütteln“, versichert Prof. Detlef Zühlke, Vorstandsvorsitzender der SmartFactoryKL und Leiter des Forschungsbereichs Innovative Fabriksysteme am DFKI. „Wir stellen uns diesem Thema mit einer Technologiedemonstration, die wir, sobald Produkte am Markt verfügbar sind, auf unsere Industrie-4.0-Produktionsanlage ausweiten werden.“ Das soll noch im laufenden Jahr der Fall sein. ■

SmartFactory KL e.V.
www.smartfactory-kl.de

Zukunft der industriellen Kommunikation

TSN als Firmware Update

Hilscher ist als IIC-Mitglied dem TSN Testbed beigetreten. Ziel ist es, TSN zukünftig als Firmware Upgrade anzubieten, und dadurch Standard-Echtzeit-Ethernet-Geräte in TSN-fähige Geräte zu wandeln.

Ein erster Test im Rahmen eines Plugfestes war erfolgreich. Ein mit netX51-Chip für Profinet ausgestatteter Lasersensor von Sick wurde in die Echtzeit-Ethernet-Kommunikation des TSN-Testbeds integriert.

Mit TSN positioniert

Die netX-Familie wird in einer Vielzahl von Anwendungen und Gerätefamilien rund um den Globus eingesetzt. Die Schlüsselwerte der TSN-basierten Protokolle können daher auf unkomplizierte Weise in die industriellen OEMs integriert werden. Mit der Teilnahme am IIC-Testbed will Hilscher seine Position im Bereich der Kommunikationstechnik auch in Zukunft unterstreichen. Das Testbed in Europa, am Bosch Rexroth Standort für IoT-bezogene Steuerungs- und Kommunikationslösungen in Erbach errichtet, hat erfolgreich gezeigt:

- Synchronisierung von Geräten zum Zweck eines über ein Netzwerk bereitgestelltes gemeinsames und präzise Zeitsynchronisation
- Herstellen von TSN-Datenverkehr zwischen verschiedenen Anbietern
- Übermittlung von I/O-Daten über TSN
- Nachweis der Fähigkeit von TSN, kritische Datenübertragung aus dem Datenverkehr mit hoher Bandbreite zu schützen. ■

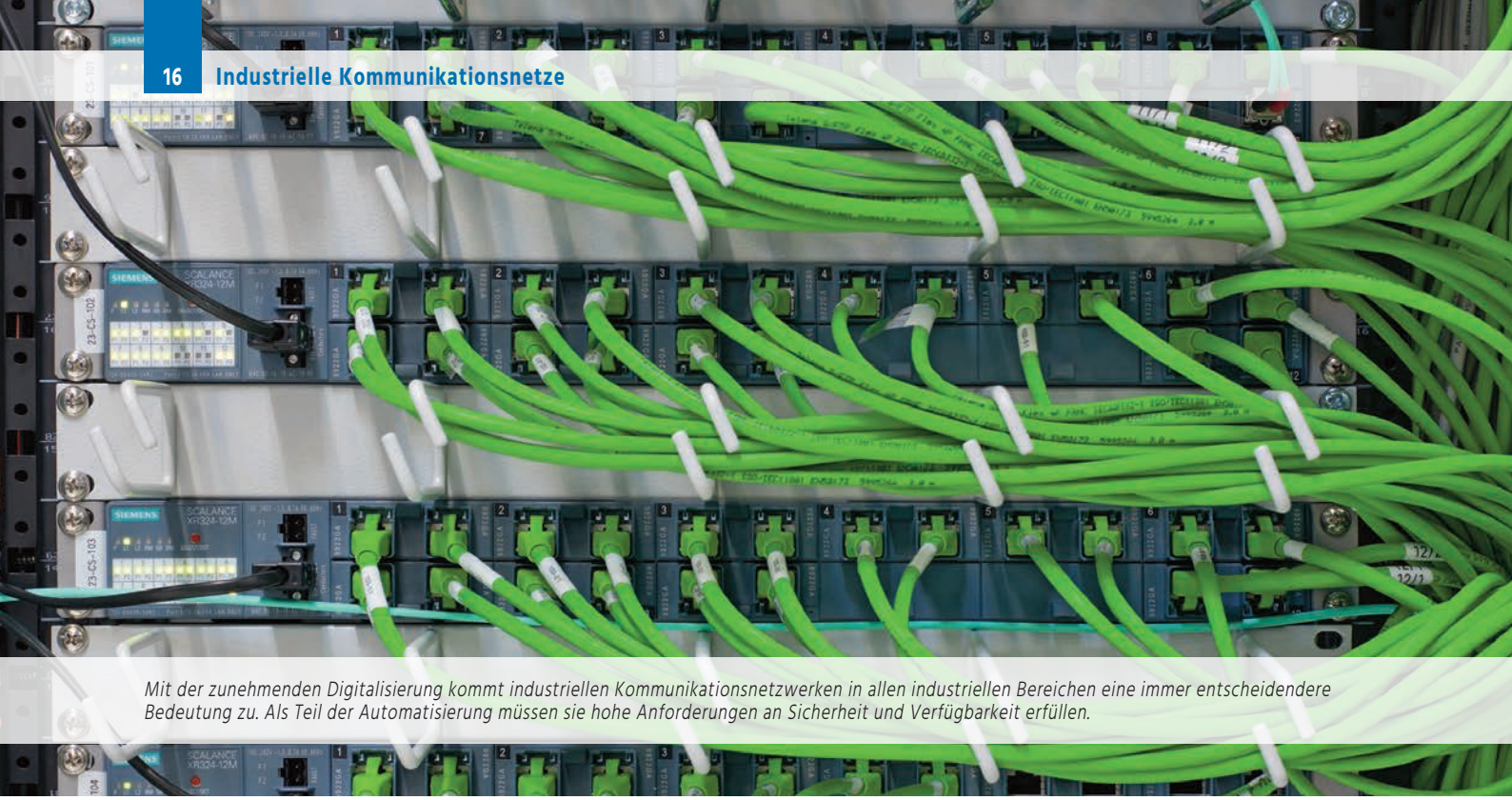
Hilscher Gesellschaft für Systemautomation mbH
www.hilscher.com

Ethercat-Komponenten

Ethercat hat sich als etabliertes Industrial-Ethernet-Derivat einen Namen in der Branche gemacht. Ein Alleinstellungsmerkmal des Standards ist die außergewöhnlich große Anbieterzahl von Ethercat-Komponenten und Lösungen.

Rund 4.400 Mitglieder umfasst die Ethercat-Nutzerorganisation ETG mittlerweile. Darunter sind viele Maschinenbauer sowie Anbieter von Antriebs- und Automatisierungstechnik, die Ethercat aufgrund der hohen möglichen Dynamik in ihren Geräten und Maschinen einsetzen. Aber auch einige andere Branchen und durchaus exotische Applikationen wissen die Eigenschaften von Ethercat zu schätzen. Ein Beispiel: Die Hightech-Katamarane der America's Cup Class benötigen eine sehr schnelle und zuverlässige Buskommunikation für ihr hydraulisches Steuersystem und setzen an dieser Stelle auf Ethercat. So hat das Kommunikationsprotokoll kürzlich auch einen Teil zum Sieg des Teams aus Neuseeland beim America´s Cup 2017 beigetragen. *(mby)*

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



Mit der zunehmenden Digitalisierung kommt industriellen Kommunikationsnetzwerken in allen industriellen Bereichen eine immer entscheidendere Bedeutung zu. Als Teil der Automatisierung müssen sie hohe Anforderungen an Sicherheit und Verfügbarkeit erfüllen.

Bild: Siemens AG

Netzwerke konzipieren, planen und einrichten

Die Basis des Digital Enterprise

Moderne Industrienetze ermöglichen einen durchgehenden vertikalen und horizontalen Informationsaustausch — und dadurch die Anbindung der Fertigungsebene an die Unternehmens-IT oder an Cloud-Plattformen. Damit bilden sie eine wichtige Grundlage für das Digital Enterprise. Dieser Entwicklung folgend, baut Siemens sein Portfolio für die industrielle Kommunikation kontinuierlich aus. Neben Netzwerkkomponenten gehören dazu auch Schulungen und Services, beispielsweise die Planung und Implementierung von Netzwerken.

Als Teil der Automatisierung müssen industrielle Kommunikationsnetzwerke hochverfügbar und robust sein. Netzwerkausfälle sind durch spezielle Redundanzmechanismen zu vermeiden. Zudem ist entscheidend, dass Anwender Geräte schnell und einfach an der Anlage austauschen können. Die Netzwerke müssen darüber hinaus die Anforderungen der zyklisch ablaufenden Steuerungsprozesse erfüllen. So erfordern einige Anwendungen schnelle, deterministische Zykluszeiten, um etwa Maschinen mit einem Notausschalter schnell in einen sicheren Zustand zu bringen. Abgesehen vom Leistungsumfang der eingesetzten Komponenten müssen sich Kommunikationsnetzwerke nahtlos und sicher in die bestehende Netzwerkinfrastruktur integrieren lassen. Industrielle Anlagen haben oft lange Lebenszyklen, insbesondere in der Prozessindustrie (z.B. Chemiebranche). Bei der Planung und Implementierung industrieller Netzwerke gilt es daher, bestehende Systeme zu berücksichtigen und anzuschließen — einschließlich der Anbindung an die Unternehmens-IT. Besondere Bedeutung hat die Datensicherheit. In industriellen Umgebungen sind weder gelegentliche Netzwerkfehler noch längere Zeiträume zur Fehlerbehebung akzeptabel. Die mögliche Fehlertoleranz sowie Ausfallszenarien sind von vorneherein Planungsbestandteile des industriellen Kommunikationsnetzwerkes. Um Industrieanlagen umfassend vor Cyberangriffen von innen und außen zu schützen, muss auf allen Ebenen gleichzeitig angesetzt werden — von der Betriebs- bis zur Feldebene, von der Zutrittskontrolle bis zum Kopierschutz. Zu diesem Zweck setzt Siemens auf eine so genannte tiefengestaffelte Abwehr (Defense in Depth) als übergreifendes Schutzkonzept, nach den Empfehlungen der IEC62443, dem führenden Standard für Security in der industriellen Automatisierung. Datenintegration und ein funktionierendes industrielles Netzwerk vom Sensor/Aktor bis hin zur Unternehmens-IT oder zu Cloudplattformen sind die Basis für die Digitalisierung (Industrie 4.0 bzw. IIoT). Hierfür müssen industrielle Kommunikationsnetzwerke auch den zukünftigen Anforderungen von Digitalisierungslösungen entsprechen. So müssen sie flexibel erweiterbar sein etwa durch einen modularen Aufbau. Dabei ist nicht nur die M2M-Kommunikation sicherzustellen, sondern auch die ortsunabhängige Verfügbarkeit relevanter Daten, etwa für cloudbasierte Services im Bereich vorausschauender Instandhaltung.

Robuste Kommunikation in der Wüste

Im Wüstenstaat Oman herrschen extreme Klimabedingungen: An der Küste sind monsunartige Regenfälle und eine Luftfeuchtigkeit von 90 Prozent möglich, im Landesinnern herrschen Temperaturen von bis zu 50°C. Dies stellt hohe Anforderungen an die Netzwerktechnik der Petroleum Development Oman (PDO), die für 70 Prozent der Öl- und Gasförderung des Landes verantwortlich ist. Da sich die bis dato eingesetzten Netzwerkkomponenten mit klimatisierten Gehäusen als kostspielig und unzuverlässig er-

Bild: Siemens AG

Schnell, zuverlässig, robust: Dies sind die wesentlichen Anforderungen an industrielle Netzwerke und ihre Einzelkomponenten.

wiesen hatten, beauftragte PDO Siemens mit der Erneuerung der Technik, wobei auf die Ruggedcom-Produktlinie gesetzt wurde, die für besonders raue Einsatzbereiche ausgelegt ist, wie zum Beispiel Temperaturbereiche von -40 bis +85°C im lüfterlosen Betrieb. Die Anforderungen sind enorm: Ein Cluster an Ölquellen kann sich über eine Fläche von 30 km² erstrecken. Jedes davon ist mit zahlreichen Sensoren ausgestattet, die an einen kompakten Ruggedcom RS900 Ethernet Switch angeschlossen sind. Die einzelnen Förderstandorte sind über Glasfaserkabel über einen Ruggedcom RSG2100 Switch an einen Knotenpunkt angebunden. Von dort werden die gesammelten Daten per Glasfaserleitung an eine örtliche Leitzentrale geschickt, die mit Ruggedcom RSG2100 oder RSG2200 Switches ausgestattet ist. Mit einer Visualisierungssoftware lässt sich der Förderbetrieb aus sicherer Entfernung beobachten. Gleichzeitig werden die gesammelten Daten an die PDO-Zentrale in der Hauptstadt Muscat geliefert. Zusätzlich profitiert PDO von der Möglichkeit, die Komponenten aus der Ferne zu verwalten und zu überwachen. Dadurch lassen sich die zeitaufwendigen, kostspieligen und darüber hinaus nicht ganz ungefährlichen Einsätze von Service-Technikern in unbemannten, weit abgelegenen Förderstandorten reduzieren. Die Technik ist seit Beginn zuverlässig: „Seit der Installation des ersten Ruggedcom-Switches vor sieben Jahren hatten wir keinen einzigen Ausfall", erklärt Al Kharusi, Projektingenieur bei PDO.

Hohe Verfügbarkeit in der Automobilproduktion

Für eine hohe Produktivität im Presswerk bei Volkswagen in Emden ist es wichtig, dass das Leitsystem nahtlos mit den Pressen, Fördersystemen und Robotern kommuniziert. Siemens konzeptionierte, plante und implementierte eine komplett neue Netzwerkinfrastruktur mit Profinet als Ethernet-Standard für die Automatisierung und seine Netzwerkkomponenten. Die Netzwerkstruktur wurde dabei grundlegend neu aufgebaut. Gab es früher eine einfach ringförmige Topologie, setzt sich das System im Presswerk jetzt aus 14 redundant ausgelegten Netzwerkringen zusammen. Außerdem wurde ein Industrial Backbone auf Basis von Industrial Ethernet Switches Scalance XR-500 eingerichtet, der den gesamten Datenverkehr über mehrere ebenfalls redundant ausgelegte Subnetze mit Routing-Mechanismen steuert. Die uneingeschränkte Echtzeit-Kommunikation über Profinet wird durch ein durchgängig redundant ausgelegtes Netzwerk aus mehreren 100Mbit/s-Subnetzen erreicht. Jörg Lottmann, IT- und Systemadministrator des Werkes: „Seit der Umstellung auf die neue Netzwerkstruktur mit Scalance-Switches gab es noch keinen Ausfall wegen Netzwerkproblemen."

Fazit

„Leistungsstarke Kommunikationsnetzwerke sind eine wichtige Voraussetzung für die Digitalisierung der Industrie. Zugleich sind sie verglichen mit Büronetzwerken deutlich anspruchsvoller, etwa in punkto Zuverlässigkeit, Robustheit und Sicherheit", erklärt Herbert Wegmann, General Manager Industrial Communication and Identification bei Siemens. „Es hat sich in der Praxis gezeigt, dass der One-Size-Fits-All-Ansatz bei industriellen Netzen nicht trägt. Durch unsere Erfahrung in der Automatisierung und in der Kommunikationstechnik können wir spezielle Netzwerkdesigns anbieten, die auf die Applikationen in den unterschiedlichen Branchen zugeschnitten sind." ■

Autor: ***Markus Weinländer,***
Head of Product Management Simatic Ident,
Siemens AG
www.siemens.de

Direkt zur Marktübersicht i-need.de ***www.i-need.de/?f9595***

Leichtere Ethercat-Implementierung mit Mikro-Controllern und Entwicklungs-Kits

Infineon präsentiert neue Kits, die die Entwicklungszeit von Ethercat-Anwendungen auf drei Monate schrumpfen lassen: das XMC4300 Relax Ethercat-Kit und das XMC4800 Ethercat-Automation-Kit. Mögliche Anwendungen der XMC-Mikro-Controller mit integriertem Ethercat-Knoten, XMC4300 und XMC4800 finden sich innerhalb der Fabrikautomatisierung z.B. bei I/O-Modulen oder Robotern. Mit dem neuen Kit lässt sich XMC4300 (auf dem Kit im LQFP-100-Gehäuse) speziell in Ethercat-Slave-Anwendungen evaluieren. Der XMC4300 mit ARM Cortex-M4 läuft mit 144MHz. Er hat bis zu 256KB Embedded-Flashspeicher und 128KB SRAM. Als Stückpreis nennt der Anbieter 50€ je Kit. Der XMC4800 basiert auf einem ARM Cortex-M4-Prozessor. Er bietet eine 144MHz-CPU, bis zu 2MB Embedded-Flashspeicher, 352KB RAM sowie umfangreiche Peripherie- und Schnittstellenfunktionen. Dieses Kit ist laut Anbieter für 200€ erhältlich. Beide Kits werden mit entsprechenden Softwareentwicklungswerkzeugen geliefert.

Infineon Technologies AG
www.infineon.com

Kompakte Fernwirktechnik-Gateways für den dezentralen Einsatz

Mit den kompakten Fernwirktechnik-Gateways der Serie WTG von Wago lassen sich bis zu 16 Unterstationen in einer offenen Struktur an die Leitebene anbinden. Die Geräte eignen sich aufgrund des schlanken Designs für den dezentralen Einsatz und zeichnen sich durch eine hohe Skalierbarkeit aus. Zur seriellen Kommunikation ins Feld lassen sich bis zu sechs RS232-Module anreihen. Das Gateway ist dann hilfreich, wenn Fernwirkunterstationen herstellerunabhängig zu schalten sind oder die Beschränkung der Leittechnik hinsichtlich der Anzahl möglicher Verbindungen aufzuheben ist. Die Anbindung an die Feldebene ist über Standleitung, Wahlverbindung oder transparente TCP/IP-Verbindung und zur Leitebene via Ethernet- oder serieller Kommunikation möglich. Das Gateway kommuniziert die Daten zuverlässig und sicher an die Leitstelle, sodass keine zusätzliche Parametrierung erforderlich ist. Ein optionaler redundanter Aufbau von zwei Gateways über eine TCP/IP-Anbindung ist ebenfalls möglich. Das sorgt gerade in kritischen Infrastrukturen für hohe Sicherheit.

Wago Kontakttechnik GmbH & Co. KG
www.wago.de

Leistungssteller mit Ethercat-Schnittstelle

Die Leistungssteller-Serie Thyristor von Jumo ist nun auch für das Ethercat-Protokoll erhältlich. Über das echtzeitfähige Feldbus-Protokoll haben Anwender Zugriff auf alle Prozessdaten des Stellers. Darüber hinaus lässt sich die Konfiguration über die Twincat-Software vornehmen. Eine zusätzliche Konfiguration über eine Setup-Software entfällt somit, was die Geräteinbetriebnahme vereinfacht. Die Steller sind in Stromstärken von 20 bis 250A für ein- und dreiphasige Anwendungen erhältlich. Durch die neue Schnittstelle lassen sich Prozessdaten wie Laststrom, Lastspannung und Impedanz stetig übermitteln. Aber auch Angaben zum Energieverbrauch sowie Diagnosefunktionen wie Netzspannungsschwankungen, Teillastbruch und Übertemperatur können ausgewertet werden.

Jumo-Thyristor-Leistungssteller sind jetzt auch mit einer Ethercat-Schnittstelle erhältlich.

Bild: Jumo GmbH & Co. KG

Jumo GmbH & Co. KG
www.jumo.de

Ethercat-Medienkonverter für Distanzen bis 25km

Die Medienkonverter der Serie Ecat-2511 von ICPDAS setzen Ethercat-Daten zuverlässig von 100Base-TX auf 100Base-FX um. Im Single-Mode lassen sich so Distanzen bis 25km überbrücken. Um das Troubleshooting zu erleichtern, werden Fehlermeldungen und der Betriebszustand zudem direkt über LEDs am Gerät angezeigt. Die kompakte Bauform und die Möglichkeit zur Hutschienen-Montage erleichtern die Integration in bestehende Ethercat-Netze. Der erweiterte Temperaturbereich von -25 bis +75°C und der redundante Spannungseingang der Medienkonverter bieten zusätzliche Sicherheit im rauen industriellen Umfeld.

Die Medienkonverter setzen Ethercat-Daten zuverlässig von 100Base-TX auf 100Base-FX um.

Bild: ICPDAS-Europe GmbH

ICPDAS-Europe GmbH
www.icpdas-europe.de

Für draußen und für lange Strecken

Neu im Telegärtner-Sortiment ist das Außenkabel A-DQ(ZN)B2Y. Das Kabel mit Nagetierschutz und PE-Mantel ist widerstandsfähig, wetterfest und UV-stabil. Es ist mit Multimode-Fasern der Kategorien OM2 bis OM4 und mit Singlemode-Fasern der Kategorie OS2 und je nach Fasertyp ebenfalls mit vier bis 48 Fasern lieferbar. Die Lieferung erfolgt auf umweltfreundlichen Einweg-Holztrommeln. Unabhängig von Faser- und Kabeltyp beträgt die Liefermenge 2km. Alle Kabel können in den Rangierverteilern der Serien Economy V, Basis V und Profi V sowie in den Spleißmodulen des modularen LWL-Verteilsystems mit 1- und 3-HE-Baugruppenträgern angeschlossen werden. Spleißfertig abgesetzte Pigtails erleichtern dabei die Arbeit und sparen Zeit.

Bild: Telegärtner Karl Gärtner GmbH

Neu im Sortiment von Telegärtner ist das Außenkabel A-DQ(ZN)B2Y, lieferbar mit vier bis 48 Single- oder Multimode-Fasern und auf Kabeltrommel.

Telegärtner Karl Gärtner GmbH
www.telegaertner.de

Powerlink-Schnittstelle für Servoumrichter

Baumüller bietet die Servoumrichter-Familie B Maxx jetzt auch mit Powerlink-Schnittstelle an. Die Umrichterreihen B Maxx 2500, 3300, 4400 und 5000 wurden kürzlich von der Nutzerorganisation EPSG als konform mit den Powerlink-Spezifikationen zertifiziert. Die Umrichterfamilie deckt ein breites Spektrum vom Kleinstumrichter bis hin zu leistungsstarken Geräten mit mehr als 300kW ab. Zentrale Konzepte lassen sich daher ebenso umsetzen wie vollständig dezentrale Ansätze. Vorprogrammierte Funktionen vereinfachen die Inbetriebnahme, verkürzen die Entwicklungszeit und erhöhen die Fehlersicherheit.

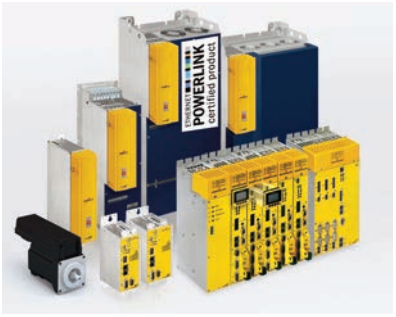


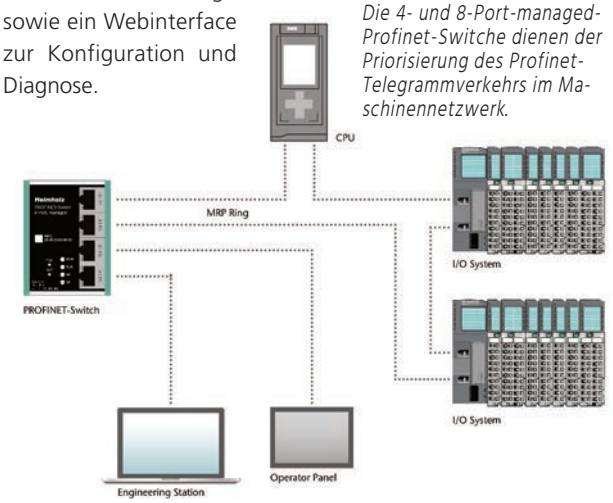
Bild: Ethernet Powerlink Standardization Group

B Maxx, die Servoumrichter-Serie von Baumüller, ist jetzt mit Powerlink-Schnittstelle ausgestattet und von der EPSG zertifiziert.

Ethernet Powerlink Standardization Group
www.ethernet-powerlink.org

Managed-Switche für Profinet

Die 4- und 8-Port-managed-Profinet-Switche von Helmholz dienen der Priorisierung des Profinet-Telegrammverkehrs im Maschinennetzwerk. Der Switch ist dabei in der Lage zu unterscheiden, ob es sich bei dem Telegramm um eine Web-Anfrage, eine FTP-Dateiübertragung, einen Medien-Stream oder ein Profinet-Telegramm handelt. Bei hoher Übertragungslast lassen sich somit die wichtigen Telegramme priorisieren, um zu verhindern, dass es zu Datenverlusten kommt. Mittels GSDML-Datei integrieren Anwender die Switche wie gewohnt in ihre Automatisierungsumgebung. Sie verfügen über eine kompakte, industrietaugliche Bauform zur Hutschienenmontage sowie ein Webinterface zur Konfiguration und Diagnose.



Die 4- und 8-Port-managed-Profinet-Switche dienen der Priorisierung des Profinet-Telegrammverkehrs im Maschinennetzwerk.

Bild: Helmholz GmbH & Co. KG

Helmholz GmbH & Co. KG
www.helmholz.de

WLAN-Modul vereint Access Point und Antenne

Das Funkmodul WLAN 1100 von Phoenix Contact kombiniert Access Point und Antennentechnik in einem Gerät. Darüber hinaus wird es nicht im Schaltschrank, sondern wie eine Antenne direkt auf Maschinen, mobilen Fahrzeugen oder Schaltschränken installiert. Zwei integrierte, leistungsstarke Antennen mit Mimo-Technik sorgen für den Empfang. Das Modul ermöglicht Anwendern eine kostengünstige und einfache WLAN-Anbindung der Maschine. Eine aufwendige WLAN-Planung und Installation der Antennentechnik entfällt somit. Da das Funkmodul keinen Platz im Schaltschrank benötigt, lässt es sich leicht nachrüsten. Es wird mittels Einlochmontage befestigt und wie gewohnt über einen Steckverbinder Combicon und Ethernet-Stecker RJ45 angeschlossen. Auch für raue Industrieumgebungen ist das Funkmodul geeignet. Es ist stoßfest nach IK08 und hält somit auch stärkeren mechanischen Belastungen stand.

Das Modul ermöglicht eine kostengünstige und einfache WLAN-Anbindung der Maschine.

Bild: Phoenix Contact GmbH

Phoenix Contact GmbH
www.phoenixcontact.com

Switches mit Monitoring-Funktion

Beide Modelle können bis zu sechs Ethernet-Geräte miteinander verbinden.

Bild: Insys Microelectronics GmbH

Insys Icom erweitert sein Portfolio um Lite-Managed- und Unmanaged-Switches. Der Lite-Managed-Switch ETSM besitzt eine steuerbare Intelligenz und verfügt über Funktionen wie Monitoring via Modbus TCP oder Port-Priorisierung. Beide sind durch ihr flaches, kompaktes Hutschienengehäuse geeignet für die Installation auf engstem Raum.

Insys Microelectronics GmbH
www.insys-icom.de

Netzwerkbasiertes Remote-I/O-System

Die neu entwickelte Oberfläche schafft die Grundlage dafür, den Funktionsumfang auch zukünftig zu erweitern, ohne dass dies zu Lasten der Bedienbarkeit geht.

Bild: Wiesemann & Theis GmbH

Das Web-IO 4.0 von Wiesemann & Theis ist ein netzwerkbasiertes Remote-I/O-System. Die Benutzeroberfläche trennt die Einrichtung der gewünschten Kommunikationswege und Protokolle von den Aktionen, die das System ausführt, sobald ein Auslöser auftritt. Richtet der Anwender z.B. den Kommunikationsweg E-Mail ein, lässt sich eine Aktion anlegen, die eine E-Mail versendet, wenn einer der Eingänge geschaltet wird.

Wiesemann & Theis GmbH
www.wut.de

Integrierte Lernumgebung rund um Ethernet/IP

Die ODVA hat die Ethernet/IP-Toolbox veröffentlicht, eine integrierte Lernumgebung (ToolBoxILE) für Produktentwickler, die mit der Ethernet/IP-Technologie und diesbezüglichen Standards noch nicht vertraut sind. Die Lernumgebung umfasst eine Gruppe von einfachen integrierten Werkzeugen, die Ingenieuren Grundlagen von Ethernet/IP vermitteln sollen, die benötigt werden, um ein erstes eigenes Ethernet/IP-Projekt zu starten oder um Anforderungen zu definieren, die sich in Kooperation mit einem Technologiepartner ergeben. Eine Benutzerlizenz für die Toolbox kann auf www.odva.org/Submit-Order erworben werden.

ODVA EMEA
www.odva.org

Feldbuskoppler mit CC-Link-Anschluss

Wago hat seinen CC-Link-Koppler zu einer Version mit CC-Link V2.0 weiterentwickelt. Mit dem Feldbuskoppler 750-325 lässt sich ein achtmal größeres Prozessabbild erstellen, als mit der Vorgängerversion. Stationsadresse, Baudrate, belegte Stationen und Umläufe sind über Dreh- und Dip-Schalter konfigurierbar, sodass softwareseitig keine Anpassungen vorzunehmen sind. Anwender können weiterhin die Flexibilität des vorhergehenden I/O-Systems nutzen.

Bild: Wago Kontakttechnik GmbH & Co. KG

Der Koppler eignet sich für den Einsatz in der Prozessindustrie oder im Maschinen- und Anlagenbau.

Wago Kontakttechnik GmbH & Co. KG
www.wago.com

Buskoppler und I/O-Module für CANopen und Ethercat

Zur Einbindung von Sensor- und Aktor-Signalen in CANopen- und Ethercat-Netzwerke erweitert MKT Systemtechnik sein Sortiment an Kleinsteuerungen und Netzwerkkomponenten um die neue Buskoppler- und I/O-Modul-Baureihe IO16. Die Baureihe umfasst die Buskoppler IO16-BCCO und IO16-BCEC für Ethercat bzw. CANopen sowie dazu passende analoge und digitale I/O-Module. Die Komponenten punkten mit kompakten Baubreiten von nur 18,8mm und ihrer werkzeuglosen Montage. Die Kommunikation zwischen Buskopplern und I/O-Modulen erfolgt über einen internen Bus. Über einfach einsteckbare Tragschienen-Busverbinder versorgen die Buskoppler I/O-Module mit einer Gesamtleistung von bis zu 12W, wodurch der Verdrahtungsaufwand reduziert wird. Für erhöhte Betriebssicherheit sind Feldbus-Schnittstellen und I/O-Module von den Buskopplern galvanisch getrennt. Zur Einstellung der Baudrate (CANopen) und der Node-ID dienen Drehkodierschalter an der Gehäusefront. Die auf die Buskoppler abgestimmten I/O-Module sind in analogen oder digitalen Ausführungen erhältlich.

MKT Systemtechnik GmbH & Co. KG
www.mkt-sys.de

Modul für robuste Ethernet-Netzwerkkonnektivität

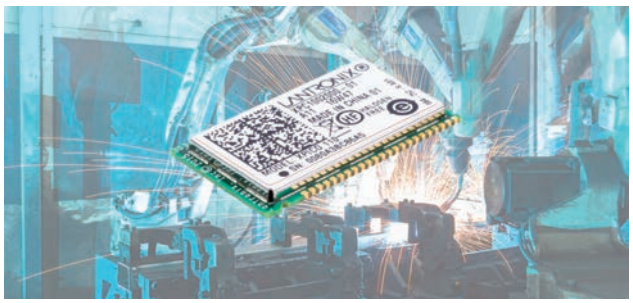


Bild: Atlantik Elektronik GmbH

Das Modul eignet sich für den Einsatz im Bereich erneuerbare Energien und der Gebäudeautomatisierung sowie für Industriemaschinen.

Atlantik Elektronik präsentiert mit dem xPico 110 von Lantronix ein eingebettetes und kabelgebundenes Modul zur Ausstattung von industriellen Geräten mit einer robusten Ethernet-Netzwerkkonnektivität. Der xPico 110 ermöglicht OEMs mit geringem Engineering-Aufwand ihre Industriegeräte zu vernetzen. Durch integrierte Lantronix-TruPort-Serial-Technologie, einem internen Webserver und der Unterstützung für standardmäßige Webdienstprotokolle bietet der xPico 110 OEMs die Möglichkeit, Produkte schnell auf den Markt zu bringen. Ein weiterer Vorteil besteht darin, dass für den xPico keine Software entwickelt werden muss, wodurch sich die Entwicklungskosten und die Markteinführungszeit verringern.

Atlantik Elektronik GmbH
www.atlantikelektronik.de

CAN- und CAN-FD-Busse auf Herz und Nieren prüfen

Bild: Peak-System Technik GmbH

Das PCAN-Diag FD ist eine mobile Alternative zu einem Computer mit CAN-Schnittstelle.

Mit dem neuen PCAN-Diag FD bringt Peak-System Technik eine mobile und preiswerte Lösung für die Analyse und Fehlerdiagnose von CAN- und CAN-FD-Netzwerken auf den Markt. Durch den Handheld gelingt eine Diagnose auf Protokoll- und physikalischer Ebene mit Funktionen wie symbolischer Darstellungen eingehender Nachrichten, Aufzeichnung und Wiedergabe, Messung der Buslast oder Terminierung. Ein speziell für CAN ausgelegtes Oszilloskop erlaubt eine Untersuchung einzelner CAN-Frames. Durch Daten- und Bildspeicherung können nachträglich zusätzliche Auswertungen durchgeführt werden.

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

IoT-Plattform für die holzbearbeitende Industrie

Mit der Internet-of-Things-Plattform 'Tapio' bietet Homag eine Industrie-4.0-Lösung speziell für die holzbearbeitende Industrie. 'Tapio' ist eine offene IoT-Plattform, mit der sich holzbearbeitende Betriebe, Maschinenanbieter und Partnerunternehmen via Cloud-Anbindung digital vernetzen können. Auf dieser Basis lassen sich die individuellen Geschäftsprozesse in der Holzbearbeitung effizienter, schneller und zuverlässiger gestalten. Die von der Dürr-Tochter Homag ins Leben gerufene digitale Plattform stellt alle benötigten Informationen über die Produktion sowie über eingesetzte Maschinen, Werkzeuge und Materialien bereit.

Dürr AG
www.durr.de

IoT-Anwendungen in der Messtechnik

Longlatec ermöglicht es Herstellern von Messtechnik in mobilen Anwendungsfeldern, ihre Geräte in IoT-fähige Produkte zu wandeln. Dazu bietet das Unternehmen mobile Konnektivitätstechnik, die auf Mobilfunkstandards aufbaut und sich direkt in einzelne Messeinheiten integrieren lässt. Die Lösung wurde speziell für mobile Produkte entwickelt und ermöglicht Batterielaufzeiten von mehreren Jahren. Um die Messdaten möglichst energieeffizient in die Web-Anwendungen zu senden, kommt ein Übertragungsprotokoll zum Einsatz. Durch die Reduzierung der Datenpakete lässt sich ein Großteil der Energie für die Übertragung einsparen. Die Weiterleitung der Daten an IoT-Anwendungen findet dann erst in der Cloud statt.

Longlatec
www.longlatec.de

I4.0-Maschinen-Retrofit per Felddaten-Gateway

Bild: SSV Software Systems GmbH

Mit dem I4.0/Senspac sind sowohl Maschinen- und Anlagenüberwachungen als auch intelligente Diagnostikanwendungen – wie Predictive Maintenance – realisierbar.

Das I4.0/Senspac ist ein intelligentes System zur Erfassung und Analyse von Sensor- und Maschinendaten, um bestehende Maschinen und Anlagen nachträglich mit Industrie-4.0-Fähigkeiten auszustatten. Die Lösung besteht aus einem Gateway mit skalier- und konfigurierbaren Felddatenschnittstellen sowie verschiedenen Softwarekomponenten. Dabei werden nicht nur die Daten nachträglich hinzugefügter Sensoren, sondern auch die in den Steuerungen bereits vorhandenen Datenpunkte herangezogen.

SSV Software Systems GmbH
www.ssv-embedded.de

Bild: Coperion GmbH

In Anlagen der Kunststoff- oder Chemieindustrie können Lichtwellenleiter ihren Reichweitenvorteil ausspielen.

Daten-Highways der vernetzten Industrie

Datenkabel sind heimliche Stars. Ohne sie geht nichts, denn sie sind das Netz – nicht im übertragenen Sinn, sondern ganz konkret und physisch. Dennoch fristen sie ein ziemlich unspektakuläres Dasein als typisches C-Teil: kostengünstig im Einkauf, doch mit einem relativ hohen zeitlichen Bereitstellungsaufwand. Wird dies der Schlüsselrolle von Lichtwellenleitern auf dem Weg zur Smart Factory gerecht?

Coperion setzt auf redundante optische Ringnetze, um hohe Anforderungen an die Maschinenverfügbarkeit zu erfüllen. Bei der Auswahl der geeigneten Lichtwellenleiter vertraut der Maschinen- und Anlagenbauer dabei auf das Know-how von Helukabel. Coperion ist Anbieter von Extrusions- und Compoundiersystemen sowie Schüttgutanlagen, die in der Kunststoff-, Chemie-, Nahrungsmittel- und Aluminiumindustrie eingesetzt werden. Hauptprodukte sind Doppelschneckenextruder zur Kunststoffherstellung. Sie erreichen einen Durchsatz von bis zu 100t pro Stunde. Die gleichsinnig drehenden Doppelschneckenextruder ZSK von Coperion finden sich weltweit als eingesetzte Extruder für die Produktion von technischen Kunststoffen. In den Extrudern findet die Compoundierung statt. Darunter versteht man die Aufbereitung des Kunststoffs durch Beimischung von Zuschlagstoffen, um bestimmte Eigenschaften gezielt zu verbessern. Neben dem Extruder als Herzstück umfasst die gesamte Anlage – angefangen beim vorgelagerten Reaktor zur Polymerisation der Kunststoffe bis zu den Silos zur sortenreinen Lagerung der Compounds – ein ganzes Areal mit mehrstöckigen Fabrikhallen. Hier ist es keine Seltenheit, wenn Datenkabel Leitungslängen von 1,5km und mehr erreichen. Das prädestiniert die Anlagen für den Einsatz von Lichtwellenleitern. Je länger die Strecke ist, die ein Datenkabel zu überbrücken hat, desto eher kann ein Lichtwellenleiter (LWL) seinen Reichweiten-Vorteil ausspielen. Bei der Datenübertragung via Kupfer ist bei einer maximalen Segmentlänge von 100m Schluss, danach muss wegen der Dämpfung ein Repeater zwischengeschaltet werden. Allein die räumliche Ausdehnung einer Maschine determiniert somit häufig bereits die Wahl zwischen Kupfer und Glasfaser, besonders dann, wenn weitere Anlagenkomponenten wie Weiterverarbeitungen, Förderung oder Sortierung hinzukommen. Als Grundregel für Datenkabel im Maschinen- und Anlagenbau gilt daher: Dort, wo große Distanzen für die Buskommunikation überbrückt werden


Bild: Coperion GmbH

Arbeitsplatz zum Konfektionieren von LWL-Kabeln

müssen, sind LWL das Medium der Wahl für eine schnelle und störresistente Datenübertragung. Bei LWL spielen auch Potentialunterschiede keine Rolle, was gerade im Anlagenbau von Vorteil ist. Da Coperion mit den Extrudern nur einen Teil der Gesamtanlage liefert, kann es zu Potentialunterschieden mit anderen Teilen der Anlage kommen. Für die Datenkommunikation über LWL stellt dies jedoch kein Hindernis dar.

Glasfaser – Die Diva unter den Datenkabeln

Die Glasfaser besitzt, verglichen mit der elektrischen Übertragung durch Kupfer, das Merkmal einer weitaus höheren Übertragungsrate bei gleichzeitig sehr hoher Reichweite. Zudem findet keine Signalstreuung auf benachbarte Fasern statt. Die Glasfaser wird als optischer Leiter nicht elektromagnetisch beeinflusst und kann elektromagnetisch verträglich (EMV) gemeinsam mit Leistungskabeln verlegt werden, solange der LWL-Leiter ohne metallische Bewährung ausgeführt ist. Das hochreine Glas der Fasern ermöglicht eine klare Signalübertragung. Doch so klar die Übertragung ist, so anspruchsvoll ist die 'Diva' unter den Datenkabeln in der Handhabung: In Abhängigkeit vom Biegeradius entstehen schnell hohe Biegeverluste durch das Abstrahlen von Lichtleistung aus dem Kern in den Mantel, der einen geringeren Brechungsindex aufweist. Speziell die Konfektionierung durch wenig geübtes Personal bezahlt man mit einer starken Zunahme der Signaldämpfung der Glasfasern. Beim Verbinden von Fasern mittels Steck- und Spleißverbindungen können erhebliche Einfüge- bzw. Koppelverluste entstehen. Während Kupferkabel schnell und einfach mit Steckern für die jeweilige Anwendung angepasst werden können, gehört zur Konfektionierung von LWL teures Equipment, Know-how und Erfahrung. Allein Anschaffungskosten von mehreren Zehntausend Euro für das Werkzeug zum Spleißen und Messen macht es attraktiv, bereits fertig konfektionierte LWL vom Spezialisten zu beziehen. Helukabel liefert nach Wunsch LWL 'ready to use' inklusive der Anschlusstechnik. Je nach Anwendung werden die Kabel mit einem passenden Aufteilkörper verbunden, der die Fasern aus dem Bündeladerkabel ohne Spleißungen in einzelne Simplexkabel führt, die wiederum mit werkskonfektionierten Steckern abgeschlossen sind. Zuletzt wird der Übergang vom Kabelmantel zum Aufteilkörper mit Polyamid vergossen, was die typische Kabelschwachstelle deutlich robuster macht als ein ansonsten häufig benutzter Schrumpfschlauch. Das mitgelieferte Messprotokoll gibt Auskunft über die Übergangsdämpfung des fertig konfektionierten Kabels.

Kabel-Know-how direkt vom Hersteller

Martin Wurz, Elektrokonstrukteur Large Extruders bei Coperion, schätzt die direkte Zusammenarbeit mit Helukabel: „Wo bekommen wir eine bessere Beratung als von der Fachabteilung des Kabelherstellers selbst? Natürlich müssen wir unsere Anforderungen an den LWL schon gut definieren können. Dann aber kann ich mich darauf verlassen, dass Helukabel eine geeignete Konfiguration vorschlägt und der Kundenbetreuer sich im Spezialfall direkt bei der eigenen Entwicklungsabteilung erkundigt." Die LWL-Reihe Helucom Connecting Systems besitzt ein breites Produktportfolio, das zwölf Typen von Aufteilkörpern umfasst. „Ich freue mich selbst immer wieder, wenn unser Sortiment auch für ungewöhnliche Fälle etwas bereit hält", berichtet Horst Messerer, Produktmanager der Daten-, Netzwerk- & Bustechnik bei Helukabel: „Vor einiger Zeit benötigte Coperion einen LWL, der durch einen Auslass geführt werden musste mit nur 18mm Durchmesser. Hierfür konnten wir einen schmalen Aufteilkörper anbieten und eine passende Zugentlastung realisieren."

Wissenswert: Redundanter optischer Ring

Ein Doppelring-Netzwerk erhält seine hohe Ausfallsicherheit durch seine physische Architektur als gegenläufiger Doppelring. Neben dem primären Glasfaser-Ring gibt es einen sekundären Glasfaser-Ring, auf dem der Datenverkehr in die entgegengesetzte Richtung zum primären Ring verläuft. Im normalen Betrieb ruht der Datenverkehr auf dem Reservering. Fällt ein Teilnehmer oder sogar ein Abschnitt des LWL aus, läuft der Datenverkehr auch über den Reservering. Vor und hinter dem ausgefallenen Abschnitt werden die Daten zurückgesendet. Aus der Doppelringstruktur entsteht dann ein einfacher Ring, das Netzwerk im Ganzen wird hierdurch aber nicht unterbrochen.

Unverwüstliche Netztopologie des Doppelrings

Zur Anwendung kommen die LWL bei Coperion vorwiegend als Netzwerkkabel für eine möglichst ausfallsichere Rechner-Kommunikation (Visualisierung) innerhalb der Extruder. Von Anfang an war klar, dass sich die Steuerung sowohl über große Entfernungen erstreckt als auch die Netztopologie eine besonders hohe Maschinenverfügbarkeit sicherstellen muss. Die Maschinenkomponenten der Großextruder kommunizieren deswegen in einem redundant ausgelegten optischen Ring. Martin Wurz erläutert: „Wir wollen allen Ausfallszenarien eines Großextruders unbedingt vorbeugen. Gerade in einer Prozessindustrie wie der Petrochemie würde der Stillstand eines Extruders immense Ausfallkosten nach sich ziehen. Alles käme zum Erliegen. Deswegen setzen wir beim Netzwerk auf die Robustheit eines optischen Doppelrings." Zusätzlich zur architekturbedingten Ausfallsicherheit des Doppelrings sind die Netzteilnehmer über gemanagte Switche mit dem Netzwerk verbunden. Falls also ein Teilnehmer ausfällt, kann dieser direkt mit dem Switch überbrückt werden, sodass in diesem Fall noch überhaupt nicht auf den redundanten Reservering zurückgegriffen werden muss. Hierdurch steigt die Fehlertoleranz und das Doppelring-Netzwerk verkraftet mehr als einen Ausfall. Zudem erhält man damit eine Infrastruktur, in der sich alle Netzwerk-Komponenten im laufenden Betrieb warten und austauschen lassen. Wurz erklärt weiter: „Da die gemanagten Switche bereits die Netzwerksicherheit für den Ausfall einzelner Netzteilnehmer regeln, ist der redundante Ring wirklich als letzter Rettungsanker für den Extremfall gedacht. Oder aber für den Fall, dass der LWL des Rings selber gebrochen ist. Das ist mir aber noch bei keinem unserer Großextruder zu Ohren gekommen." Die Großextruder stehen in allen Teilen der Welt, häufig in Schwellenländern mit extrem rauen industriellen Bedingungen. Beispielsweise siedelt sich die Petrochemie oft direkt dort an, wo es entsprechende Vorkommen gibt. Wurz: „Ich habe aber noch von keinem einzigen Alarm gehört, dass der Übertragungspegel eines verbauten LWL sich in einem kritischen Bereich befindet. Das spricht schon sehr für die Robustheit der eingesetzten LWL." ■

Firma: ***Coperion GmbH***
www.coperion.com

Firma: ***Helukabel GmbH***
www.helukabel.com

Bus-Extender für erweiterte Kabellänge

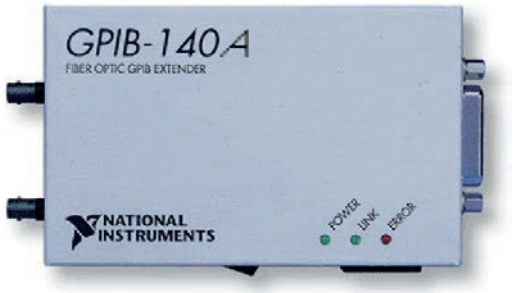


Bild: AMC Analytik & Messtechnik GmbH

Die General-Purpose-Interface-Bus (GPIB)-Bus-Extender der GPIB-140A-Serie von AMC-Systeme heben die durch den IEEE488-Standard vorgegebenen Beschränkungen bei der Kabellänge und/oder Gerätezahl auf. Der IEEE488-Standard legt fest, dass die komplette Kabellänge für ein GPIB-System 20m nicht überschreiten darf. Weiterhin ist es maximal erlaubt, 15 Geräte anzuschließen. Der GPIB-Bus ist ein Industriestandard, der vom Institute of Electrical and Electronic Engineers (IEEE) als ANSI/IEEE-Standard 488 veröffentlicht wurde. Mittels IEEE488/GPIB werden hauptsächlich programmierbare Messgeräte wie Oszilloskope, Funktionsgeneratoren, Digitalmultimeter u.a. mit Büro-PCs, Notebooks oder Industrie-PCs verbunden, um leistungsfähige Mess- und Prüfplätze in Industrie, Forschung, Entwicklung und Ausbildung bereitzustellen, zu steuern und Mess- und Steuerungsdaten zu übertragen. Mithilfe von je zwei Extendern des Typs NI GPIB-140A oder NI GPIB-140A-2 lässt sich die Kabellänge auf bis zu 2km erhöhen, ohne dass die GPIB-Funktionalität beeinträchtigt wird bzw. Programmänderungen notwendig werden. Die Extender erweitern die Kabellänge auf bis zu 1km und erhöhen die Anzahl der angeschlossenen Geräte von 15 auf 26. Sie nutzen eine gepufferte Übertragungstechnik, um Daten so schnell wie möglich zu übertragen und Kabelkosten gering zu halten. Gleichzeitig gewährleisten die kompakten Extender dabei einen geringen zusätzlichen Platzverbrauch. Sie verwenden einen Standard-Glasfaseranschluss als Übertragungsmedium. Das Glasfaserkabel isoliert den Fernbus vom lokalen Bus. Die Signale im Lichtwellenleiter sind gegen äußere elektromagnetische Störungen geschützt. Jeder Extender hat ein Fehlerprüfverfahren, um eine fehlerfreien Verbindung zu sichern. Die maximale Datenübertragungsrate der Extender beträgt mehr als 2,8MByte/s. Jeder GPIB-Extender überwacht die GPIB-Aktivität und übersetzt GPIB-Nachrichten in serielle oder parallele Signale zur Übertragung zu einem Matching. Der empfangende Extender wandelt die Signale wieder in IEEE488-Signale zurück. Zur Verfügung stehen die zwei Datenübertragungsbetriebsarten gepuffert und ungepuffert. Im gepufferten Modus verwenden die Extender einen FIFO-Puffer, um die Datenübertragungsraten zu erhöhen. Alle HS488-High-Speed-Datenübertragungen, die von den Extendern behandelt werden, verwenden den gepufferten Modus. Die Pufferung, die durch die Hardware vollständig automatisch verwaltet wird, erfordert keine Änderung ihrer Anwendungssoftware. Es gibt zwei wählbare Modi, um parallele Umfragen zu behandeln: sofort und verriegelt. Die Bus-Extender eignen sich für den Ausbau des GPIB-Busses zu längeren Entfernungen. Sie nutzen Fehlerprüf- und Wiederherstellungsalgorithmen, um eine fehlerfreie Datenübertragung zu sichern, und überwinden einige der Einschränkungen des IEEE488-Standards.

AMC – Analytik & Messtechnik GmbH
www.amc-systeme.de

Interview mit Diamond-Geschäftsführer Andreas Kohl

„Auf Nummer sicher gehen“

Geht es um lange Übertragungsstrecken und hohe Bandbreite, dann sind auch im industriellen Umfeld Lichtwellenleiter die bessere Alternative zu Kupfer. Doch wie in vielen anderen Fällen auch, stellt die Industrie dabei besondere Ansprüche. Wie die Firma Diamond an dieser Stelle ihre Kompetenz aus dem Telekommunikationsbereich auf die Industrie überträgt und welche Vorteile den Anwender dadurch erwarten, das erklärt Andreas Kohl, Geschäftsführer der deutschen Tochter des LWL-Anbieters Diamond, im Gespräch mit dem INDUSTRIAL COMMUNICATION JOURNAL.

Herr Kohl, das Unternehmen Diamond hat ursprünglich Industriediamanten hergestellt. Wie kommt es, dass Sie heute auf Lichtwellenleiter spezialisiert sind?

Andreas Kohl: *Diamond wurde 1958 in der Schweiz gegründet und hat in der Tat zunächst Industriediamanten für Tonabnehmersysteme von Plattenspielern hergestellt, insgesamt 1,5 Milliarden. 1979 begann der Siegeszug des CD-Players und wir mussten uns nach neuen Betätigungsfeldern umschauen. Mehr oder weniger zufällig rückte dann die optische Verbindungstechnik ins Zentrum unserer Aktivitäten. Am Anfang stand der weltweit erste gefederte Stecker für den Anschluss von Glasfasern, den wir entwickelt haben. Mittlerweile setzen nahezu alle großen Telekommunikationsunternehmen unsere optische Verbindungstechnik ein.*

Welche strategische Bedeutung hat das Industriegeschäft für das Unternehmen?

Kohl: *Natürlich ruhen wir uns auf dem Erfolg in der TK-Branche nicht aus, sondern suchen ständig nach neuen Einsatzgebieten für die optische Datenübertragung. Dabei sind wir auf den Industriebereich gestoßen und haben dort bereits erste Projekte im Bergbau sowie zur Anbindung von Messtechnik realisiert. Denn Glasfasern ermöglichen im Vergleich zu Kupferkabeln ein deutlich besseres Bandbreiten/Längen-Produkt, das ist die Relation zwischen maximaler Datenrate und Übertragungsentfernung, und sind zudem immun gegenüber elektromagnetischen Störungen wie auch Potentialunterschieden. Insofern sehen wir gute Chancen, dass unsere neu entwickelte Verbindungstechnik für raue industrielle Umgebungen zu einem weiteren Standbein von Diamond wird.*

Bild: Diamond GmbH

> *„Durch Industrie 4.0 und Co. werden Anlagenbetreiber, die ausschließlich auf kupferbasierte Infrastrukturen setzen, über kurz oder lang Probleme bekommen.“*
>
> *Andreas Kohl*

Welche Kernkompetenzen bringt das Unternehmen dabei mit?

Kohl: *Zunächst einmal beherrschen wir die Bearbeitung ultraharter Materialien aus dem Effeff, was eine wichtige Voraussetzung ist, um optische Stecker herzustellen. Im Grunde bestehen diese aus zwei Stiften, die die Glasfasern halten, und einer Führungshülse, mit der sie exakt zusammengebracht werden. Die Leistungsfähigkeit der Stecker hängt maßgeblich davon ab, dass die Stirnflächen der Fasern möglichst ballig poliert sind und deren Kerne nur einen sehr geringen lateralen Versatz aufweisen. Das erfordert große feinmechanische Fertigkeit. Mit anderen Worten: Wir sind in der Lage, den Außen- wie auch den Innendurchmesser der Stifte unabhängig voneinander auf 0,1µm genau zu bearbeiten – sogenanntes Lappen und Hohnen – und eine Balligkeit der Stirnfläche mit einem Radius von 15mm zu erreichen. Um zu gewährleisten, dass alle Stecker von uns diese Parameter einhalten, haben wir schon 1979 die Kern-Kern-Zentrierung entwickelt. Dabei handelt es sich um ein spezielles Verfahren, mit dem die Kerne von Singlemode-Fasern mit einer Restexzentrizität von 0,125µm positioniert werden können. Dadurch beträgt die Einfügedämpfung max. 0,1dB, was derzeit am Markt einzigartig ist.*

Welche Branchen und Anwendungen adressiert Diamond im Industriebereich?

Kohl: *Wir sind weder auf bestimmte Industriebranchen noch Automatisierungsszenarien festgelegt. Vielmehr wollen wir überall dort Alternativen anbieten, wo die Datenübertragung via Kupferkabel an Grenzen stößt. Grundsätzlich sind Glasfasern für alle Anwendungen geeignet, in denen große Datenmengen mit geringer Latenz über Entfernungen von mehr als 100m schnell übertragen werden müssen. Nach meiner Überzeugung werden Anlagenbetreiber, die ausschließlich auf kupferbasierte Infrastrukturen setzen, aufgrund von Entwicklungen wie Industrie 4.0 und Co. über kurz oder lang Probleme bekommen. Abgesehen davon würde ich jedem, der heute eine neue Fabrik errichtet, empfehlen, auf Nummer sicher zu gehen und von vornherein Glasfasern zu verlegen. Denn niemand kann heute mit Sicherheit sagen, welche Anforderungen die Datenübertragung in fünf Jahren erfüllen muss. Und angesichts von Abschreibungszeiten von 15 bis 20 Jahren würde man sicherlich am falschen Ende sparen.*

HE-2000: feldkonfektionierbarer LWL-Stecker in Schutzart IP67

Bild: Diamond GmbH

Welches Produktspektrum bietet Diamond für die Fabrik an?

Kohl: *Wir waren uns von Anfang an im Klaren darüber, dass Stecker alleine für eine flexible optische Verkabelung in rauen Industrieumgebungen nicht ausreichen. Deshalb haben wir mit FlexMile ein System entwickelt, das zudem einen kompakten Ethernet-Medienkonverter, hutschienenmontierbare Patch- und Spleißmodule sowie ein portables Fusionsspleißgeräte-Set umfasst. Alle unsere Komponenten für Single- und Multimode-Fasern sind aufeinander abgestimmt und haben Schutzart IP65 oder IP67. Da wir damit aber natürlich nicht alle Anforderungen abdecken können, bieten wir zudem kundenspezifische Lösungen an, bei denen wir – nach einer vorherigen Machbarkeitsstudie – entsprechende Anpassungen vornehmen. Schließlich stellen wir einen kompletten Service für optische Infrastrukturen bereit, der von der Planung über die Installation und Wartung bis hin zu Schulungen reicht.*

Welche Vorteile bietet die Technik von Diamond dem Anwender?

Kohl: *Zu den USPs zählt sicherlich, dass alle Singlemode-Stecker von uns eine Einfügedämpfung von max. 0,1dB haben. Dadurch lassen sich mit ihnen leistungsfähige Infrastrukturen realisieren, die zugleich mehr als genug Reserve für künftige Anwendungen bieten. Zudem ist auch die Kombination von Steckern in hoher Schutzart, selbstschließender Schutzkappe und Feldkonfektionierbarkeit einzigartig am Markt. Der Anschluss vor Ort ist möglich, da es sich bei unseren Steckern um sogenannte Splice-on Connectors, kurz SOC, handelt. Das sind Stecker mit einem integrierten Mini-Pigtail, die sich ohne zusätzlichen Spleißschutz konfektionieren lassen. Außerdem sind Mehrkanalstecker verfügbar, die variabel mit optischen und elektrischen Kontakten bestückt werden können, etwa für eine Spannungsversorgung von Endgeräten via PoE+. Ein weiterer Vorteil unseres Verkabelungssystems liegt darin, dass sich der Medienkonverter anders als klassische Varianten nicht nur im Schaltschrank einsetzen lässt, sondern auch dezentral, wodurch etwa Maschinen flexibel an das Netzwerk angebunden werden können.*

> *„Da unser Standardprogramm nicht alle Anforderungen abdecken kann, bieten wir auch kundenspezifische Lösungen und entsprechende Anpassungen an.“*
>
> *Andreas Kohl*

Bild: Diamond GmbH

Sie sprachen bereits das Thema IoT bzw. Industrie 4.0 an: Inwieweit wirken sich diese Trends auf den LWL-Bereich aus? Welchen neuen Anforderungen begegnen Sie hier, Herr Kohl?

Kohl: *Der gemeinsame Nenner dieser Trends ist die Digitalisierung. Denn nur so lassen sich vielfältige Informationen direkt an den Maschinen erfassen und entweder vor Ort oder in der Cloud mittels IT-Systemen auswerten. Ein zentraler Baustein, um dies zu erreichen, ist eine leistungsfähige Infrastruktur in der Feldebene, die eigentlich nur auf Glasfasern beruhen kann. Das war einer der Gründe, weswegen wir unser optisches Verkabelungssystem für raue Umgebungen entwickelt haben. Dabei konnten wir auf unsere langjährige Erfahrung aus dem Telekommunikationsbereich zurückgreifen, die wir um ein fundiertes Know-how auf dem Gebiet des IP-Schutzes erweitert haben. Das Ergebnis sind IP67-bzw. IP65-Stecker, die sich mit einer Hand bedienen lassen und auch im nicht verbundenen Zustand die empfindlichen Stirnflächen sicher vor Staub, Schmutzpartikel und Feuchtigkeit schützen.*

Besten Dank für das Gespräch, Herr Kohl.

Firma: ***Diamond GmbH***
www.diamond.de

Direkt zur Marktübersicht i-need.de ***ineed: www.i-need.de/?f2669***

Optische IP65-Anschlusstechnik: Ethernet-Medienkonverter (links) mit LWL-Stecker

Bild: Diamond GmbH

AS-i/FSoE-Gateway für sicherheitsgerichtete Kommunikation

Das Nächste, bitte

Bild: Bihl+Wiedemann GmbH

Sichere Bewegungsüberwachung spielt eine immer größere Rolle in der modernen Fabrik- und Prozessautomation. Doch die Safety stellt besondere Anforderungen an die Kommunikation. Mit einem neuen AS-i/Ethercat-Gateway, Safety over Ethercat (FSoE), lassen sich Antriebe ohne zusätzliche Sicherheits-SPS auf direktem Weg sicher steuern und überwachen.

Das neue AS-i/FSoE-Gateway ist ausgestattet mit zwei AS-i-Mastern, drei zweikanaligen sicheren Eingängen, sechs unabhängigen sicheren Ausgängen im Gerät. Es ist erweiterbar um fast 2.000 sichere I/Os über Safe Link.

In den vergangenen Jahren ist Bewegung in den Bereich der sicheren Bewegungsüberwachung gekommen. Das liegt z.B. an den höheren Sicherheitsanforderungen der seit Mai 2015 verbindlichen Norm für Schutztüren EN ISO14119, aber auch am zunehmenden Kostendruck in den Produktionsbetrieben, der in logischer Konsequenz auch den Zeitdruck immer weiter steigen lässt. Eine Maschine zu Wartungszwecken vollständig herunterzufahren, kann oder will sich heute kaum mehr jemand leisten. Einen Ausweg aus diesem Dilemma eröffnet die sichere Bewegungssteuerung: Sie ermöglicht einerseits manuelle Eingriffe im laufenden Betrieb und damit die Verbesserung der Produktionsabläufe zum Beispiel durch Minimierung der Stillstandszeiten. Andererseits gewährleistet sie größtmöglichen Schutz für Mensch und Maschine. „Wir haben deshalb bereits vor Jahren damit begonnen, leistungsfähige und flexible Lösungen für das Thema zu entwickeln“, sagt Jochen Bihl, Geschäftsführer von Bihl+Wiedemann. „Inzwischen ist unser Sortiment für die sichere Bewegungsüberwachung so facettenreich wie die unterschiedlichen Anforderungen in den jeweiligen Anlagen.“

Die Vorteile von Safety over Ethercat

„Nach dem AS-i-Safety-Gateway zu CIP Safety über Sercos und dem AS-i-Safety/Profisafe-Gateway war die Frage, welches System wir uns als Nächstes vornehmen, nicht schwer zu beantworten”, verrät Jochen Bihl. „Mit unserem neuen AS-i/Ethercat-Gateway, Safety over Ethercat, stoßen wir in eine Lücke: Es gibt sehr viele Antriebshersteller, die genau dieses System favorisieren, aber keine eigene sichere Steuerung dafür haben. Bisher mussten diese Firmen ihre Kunden wohl oder übel auf die sicheren Steuerungslösungen ihrer Wettbewerber verweisen. Wir dagegen sind als Partner ungefährlich, weil wir selbst keine Antriebe anbieten.“ Dass Safety over Ethercat (FSoE) in der Antriebstechnik so weit verbreitet ist, hat viel mit Geschwindigkeit

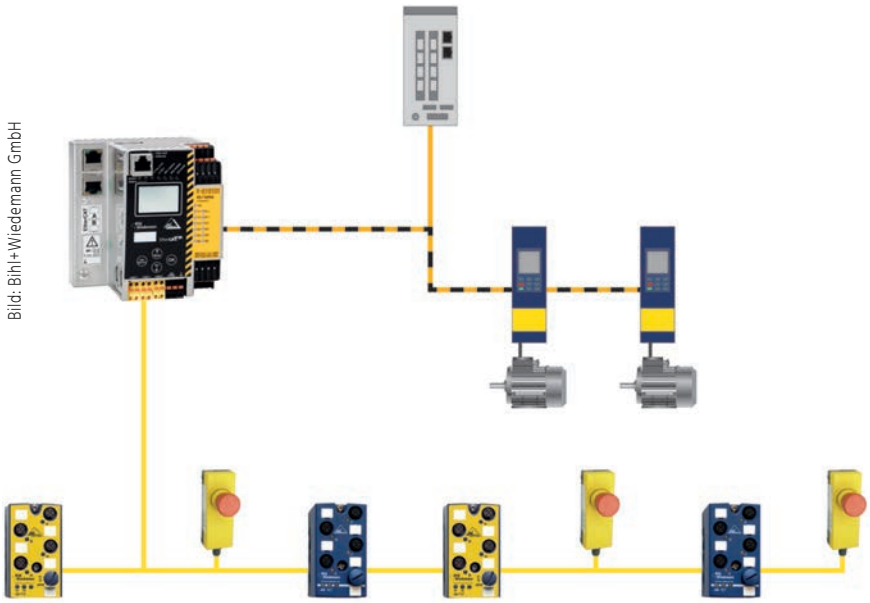


Bild: Bihl+Wiedemann GmbH

Das AS-i/FSoE-Gateway agiert als Safety Master im FSoE-Netz und kann ohne zusätzliche sichere Steuerung sämtliche Safety-Aufgaben übernehmen.

AS-i/Ethercat-Gateway, Safety over Ethercat (FSoE), mit Safe Link (BWU3418)

- Safety over Ethercat (FSoE), Safe Link und AS-i Safety in einem Gerät
- Ethercat-Gateway mit zwei AS-i Mastern, drei zweikanaligen sicheren Eingängen und sechs unabhängigen sicheren Ausgängen im Gerät, erweiterbar um fast 2.000 sichere I/Os über Safe Link
- Sichere Überwachung und Steuerung von Antrieben, die über FSoE kommunizieren, ohne zusätzliche Sicherheits-SPS

zu tun. Zum einen gilt Ethercat als schnellster Industrial-Ethernet-Standard, zum anderen sorgen die kurzen Zykluszeiten von maximal 100µs und der geringe Jitter von höchstens 1µs für eine exakte Synchronisation. FSoE erfüllt die Anforderungen nach SIL3 und eignet sich für zentrale Safety-Steuerungen ebenso wie für dezentrale. Das AS-i/FSoE-Gateway agiert als Safety Master im Netzwerk und kann ohne zusätzliche sichere Steuerung sämtliche sicherheitstechnischen Aufgaben übernehmen. Dazu gehört auch die sichere Steuerung der Antriebe, die über FSoE mit dem Gateway kommunizieren. Für die standardmäßige Steuerung der Antriebe kann weiterhin die gewohnte SPS genutzt werden. Das AS-i/Ethercat-Gateway mit Safe Link (BWU3418) vereint zwei AS-i-Master für zwei AS-i-Kreise und bietet damit bis zu 62 zweikanalige sichere Eingänge, drei zusätzliche sind bereits integriert. Mit seinen sechs schnellen elektronischen sicheren Ausgängen kann das Gateway das Tempo problemlos mitgehen, das von der modernen Antriebstechnik vorgegeben wird. Über Safe Link, eine sichere Kopplung von Bihl+Wiedemann, lässt sich das Gerät ganz ohne Aufpreis noch um fast 2.000 sichere Einund Ausgänge erweitern. „Für uns ist das neue Gateway die logische Fortsetzung unseres Angebots im Bereich der sicheren Bewegungsüberwachung“, resümiert Jochen Bihl. ■

Autor: *Thomas Rönitzsch, Unternehmenskommunikation/Verbandsarbeit, Bihl+Wiedemann GmbH*
www.bihl-wiedemann.de

i-need.de *www.i-need.de/?f1323*

Monitoring-Software für Automatisierungssysteme im Online-Versand

Komplexe Netzwerke zentral überwachen

Mit den Möglichkeiten des Online Shoppings – heute bestellt, morgen da – erhöhen sich auf Seiten der Logistik die Anforderungen an kurze Lieferzyklen und Zustellzeiten. Beim Baur Versand transportiert ein insgesamt 13km langes Labyrinth aus Förderbändern und Sortieranlagen auf einer Fläche von rund 125.000m² durchschnittlich etwa 200.000 Artikel pro Tag zum Versand. Um reibungslose Abläufe sicherzustellen, setzt man auf eine zentrale Überwachung der Systeme durch eine Monitoring-Software.

Im Jahr 1925 gründete Friedrich Baur den ersten Schuhversandhandel Deutschlands. Heute hat sich nicht nur das Portfolio unter anderem um Schmuck, Möbel oder Mode erweitert. Baur ist inzwischen Teil der Otto-Gruppe. Das Wachstum des Konzerns ist auch mit Blick auf die Standorte unübersehbar: Inzwischen befindet sich in Altenkunstadt ein Hochregallager, das vorwiegend häufig nachgefragte Artikel, sogenannte Schnelldreher, enthält. Seit 2002 ist hier zudem eine Hauptumschlagsbasis (HUB), eine Art LKW-Bahnhof, angeschlossen, die die zügige Auslieferung an den Bestimmungsort gewährleistet. Zusammen mit den Mehrflächenlagern, die sich aus Kapazitätsgründen in Burgkunstadt und Weismain befinden, sind so insgesamt eine halbe Million Normkartonplätze zu verwalten. Durch die kontinuierliche bauliche Erweiterung des Standortes sind zudem unterschiedliche Technologien parallel im Einsatz, bei deren Betrieb und Wartung individuelle Besonderheiten zu berücksichtigen sind. Setzte man in den 1990er Jahren und Anfang der 2000er noch stark auf die Feldbustechnologie (Profibus und CAN), ist bei Baur für Neuanlagen seit 2010 der Einsatz von Profinet vorgeschrieben. Damals wie heute findet zudem der ASi-Bus Anwendung.

Nutzen eines Monitoring-Systems

Aus der Praxis heraus ergab sich früh die Notwendigkeit eines Monitoring-Systems. So berichtet Harald Fiedler, der gemeinsam mit seinen 25 Kollegen im Dreischichtbetrieb bei Baur dafür verantwortlich ist, dass alle Artikel und Pakete zur richtigen Zeit das Depot verlassen: „2001 haben wir den Verladesorter in Betrieb genommen. Dieser hat Priorität 1 – wenn der steht, steht in absehbarer Zeit die ganze Firma“. 2008 hat man sich entschieden, das dort installierte Profibus-Netzwerk von Indu-Sol messtechnisch überprüfen zu lassen. Das Unternehmen verfügt über eine mehr als 15-jährige Erfahrung in der qualitativen Bewertung industrieller Datenkommunikation. Von den Analysemöglichkeiten bei der Messung sei man so begeistert gewesen, dass man sich den Profibus-Inspektor als Analyse-Tool zugelegt habe. Dieser

Bild: Indu-Sol GmbH

Stiller Wächter im Schaltschrank: Der Profinet-Inspektor NT zeigt bereits auf dem Display den aktuellen Netzwerkgesamtzustand an und liefert erste Diagnosehinweise.

Promanage NT liefert dem Anwender alle wichtigen Informationen auf einen Blick, z.B. den Netzgesamtzustand im Zeitverlauf mit grafischer Untermalung nach dem Ampelfarbenprinzip.

Bild: Indu-Sol GmbH

überwacht permanent und passiv den logischen Datenverkehr im Profibus und alarmiert den Betreiber bei ersten Auffälligkeiten, bevor es sicht- und spürbare Beeinträchtigungen der Arbeitsabläufe gibt.

Stille Wächter analysieren das Netzwerk permanent

Ausgehend von diesen Erfahrungen wurden die übrigen Systeme ebenfalls nach und nach mit dem für das jeweilige Netzwerk passenden Inspektor von Indu-Sol ausgerüstet. Insgesamt sind heute 33 dieser Mess- und Analysegeräte für Profibus, Profinet und ASi als 'stille Wächter' in den Schaltschränken verbaut. Sie überwachen das Netzwerk auf Qualitätsparameter wie Telegrammwiederholungen und Buszykluszeiten (Profibus) bzw. Netzwerklast, Aktualisierungszeiten oder verspätete bzw. verloren gegangene Telegramme (Profinet). Das Team von der Anlagentechnik stand dabei vor der Herausforderung, die Diagnoseinformationen der Einzelgeräte zu vereinen, um den Überblick zu behalten und den Gesamtzustand aller Netzwerke einschätzen zu können. Hier kommt die zentrale Netzwerkmanagement-Software Promanage NT ins Spiel. Sie führt die Ereignisse aller Feldbusse und Netzwerke zentral auf einem Server zusammen, visualisiert das Ergebnis und bietet zahlreiche Analysemöglichkeiten. So können die für die Anlagentechnik zuständigen Mitarbeiter beispielsweise über den Netzwerkzustandsgraph jederzeit und netzwerkübergreifend den historischen und aktuellen Zustand des Gesamtsystems einsehen. Über- oder unterschreiten die von den Inspektoren überwachten Qualitätsparameter definierbare Schwellwerte, werden diese Ereignisse mit Zeitstempel abgespeichert und können auch später noch bei der Ursachenforschung herangezogen werden. Ein Klick auf den jeweiligen Datenpunkt des historischen Verlaufs offenbart tiefergehende Informationen zum Ereignis (Qualitätsparameter, siehe oben). Gerade im Schichtbetrieb und für die rückblickende Analyse aufgetretener Störungen ist nach Fiedlers Ansicht die Fähigkeit von Promanage NT, Daten bis zu einem Jahr in die Vergangenheit minutengenau verfügbar zu halten, entscheidend: „Zur Überwachung eines aktuellen Fehlers ist der Inspektor wichtig, aber für die Historie brauchen wir Promanage NT – die Fehler, die es erkennt, sind für einen Außenstehenden nicht sichtbar." So führten 2012 bei mehreren sporadischen Fehlern und Ausfällen eines Anlagenteils die Fehlerinformationen aus der SPS allein nicht zur Ursache. Die externe Errichterfirma des Anlagenteils änderte zunächst die Erdung. Kurzzeitig schien der Fehler behoben, trat im weiteren Betrieb aber wieder auf – die historischen Zustandsdaten von Promanage (damals noch die Vorgängerversion) waren hier wertvolle Unterstützung und Nachweis zugleich. Auch beim Profibus-Retrofit des Verladesorters an der HUB im Jahr 2016 wurde die Kommunikation im Netzwerk regelmäßig im laufenden Betrieb überprüft, um den erfolgreichen Tausch der Komponenten und Teilnehmer kontrollieren zu können.

Qualitätsveränderungen stets im Blick

Auch wenn keine Umbaumaßnahmen anstehen, überwacht man im Logistikzentrum Altenkunstadt permanent den Datenverkehr im Netzwerk, um über eventuelle Qualitätsveränderungen sofort informiert zu werden. „Besonders komfortabel ist hier die Alarmfunktion per E-Mail, sobald ein Ereignis auftritt. Wir können ja keinen Mitarbeiter abstellen, der permanent die Web-Oberflächen aller 33 Inspektoren im Blick behält", unterstreicht Fiedler die Erleichterung der Instandhaltung durch die zentrale Software. Ein weiterer Vorzug von Promanage NT ist, dass der Anwender sofort sehen kann, welcher der verbauten Inspektoren einen Alarm abgesetzt hat. So kann das technische Personal schnell und zielgerichtet reagieren. Auch hier skizziert Fiedler die Notwendigkeit im Fehlerfall: Die Kommissionierer packen die Artikel nicht kundenbezogen, sondern nach gleichartigen Artikeln aus mehreren Bestellungen in wannenähnliche Transportbehältnisse. An speziellen Packstationen werden dann von Menschenhand die einzelnen Komponenten zur individuellen Bestellung des Kunden aus verschiedenen Wannen zusammengefügt und um Beilagen und Dokumente ergänzt. „Wenn der Wannenzufluss einmal steht, können 50 Leute auf einen Schlag nicht mehr arbeiten." Dies wäre nur durch Mehr-

Bild: Baur Versand GmbH & Co. KG

Die Kombination aus Hauptumschlagsbasis und Lager an einem Standort wie in Altenkunstadt sichert bei Baur eine schnelle Bestellabwicklung.

Bild: Indu-Sol GmbH

Um bei der Fehlersuche oder bei Umbaumaßnahmen eine schnelle Eingrenzung vornehmen zu können, wurden die einzelnen Bereiche mit unterschiedlichen Farben versehen.

arbeit auszugleichen. Durch das Alarmmanagement können die Benachrichtigungsparameter individuell angepasst werden und alle erforderlichen Mitarbeiter sind sofort informiert, um auf Vorboten von Qualitätsverschlechterungen reagieren zu können, bevor diese sichtbar werden. Mit Blick auf die Zukunft steht vor allem die Fördertechnik im Fokus, bei der Teile bereits älter als 25 Jahre seien – hier wird bei neuen Anlagen dann direkt auf die neue Technologie Profinet gesetzt. Außerdem möchte man bei den eigenen Analysewerkzeugen auf dem aktuellen Stand bleiben, da sich die Herausforderungen an die Instandhaltung angesichts immer weiter steigender Vernetzung – Stichwort Industrie 4.0 – stetig erhöhen. Deshalb lösen aktuell die Profinet-Inspektoren NT schrittweise ihre Vorgängermodelle ab, da sie mit einigen Neuerungen die Überwachung des Netzwerks weiter vereinfachen und zu einer erhöhten Sicherheit beitragen. Beispielsweise ermöglicht es ein Display, erste Diagnoseinformationen direkt am Gerät anzusehen und Hinweise zum Netzwerkzustand zu erhalten – der Laptop muss also nicht permanent dabei sein. Auch die Anwesenheit unbekannter Teilnehmer wird sofort gemeldet und von Promanage NT ebenfalls erkannt und dokumentiert. Mit einer solchen permanenten Netzwerküberwachung (PNÜ) sollte es Baur gelingen, die Empfänger der etwa 50 Millionen jährlich versendeten Artikel durch einen reibungslosen Betrieb pünktlich glücklich zu machen – egal ob während des Sommerlochs oder zu Spitzenzeiten wie den Weihnachtstagen. ■

Firma ***Indu-Sol GmbH***
www.indu-sol.com

Direkt zur Marktübersicht i-need.de ***www.i-need.de/?f15249***

Interface erfasst Daten in Produktions- und Montagelinien

Mit dem Interface MG70 von Magnescale lassen sich Messdaten von inkrementellen Messtastern in Produktions- und Montagelinien über Profinet RT an Siemens-Steuerungen oder über Ethernet/IP an Rockwell- bzw. Allen-Bradley-Steuerungen übertragen. Das Interface arbeitet mit einer Baudrate von 100MBit/s. Dadurch lassen sich die Messwerte von bis zu 250 inkrementellen Messtastern gleichzeitig mit einer Zykluszeit von 1ms übertragen. Somit lassen sich große Messdatenmengen schnell an übergeordnete Steuerungen oder Messrechner weiterleiten und auswerten. Das Interface besteht aus den Buscontrollern MG70-PN für Profinet RT bzw. MG70-EI für Ethernet/IP sowie den Zählermodulen MG71-CM für inkrementelle Messtaster der DK- und DT-Serie. Durch den modularen Aufbau und die einfache Inbetriebnahme lassen sich die Interface-Module flexibel einsetzen. Die Konfiguration des modularen Systems wird von Profinet bzw. Ethernet/IP unterstützt.

Magnescale Europe GmbH
www.magnescale.com

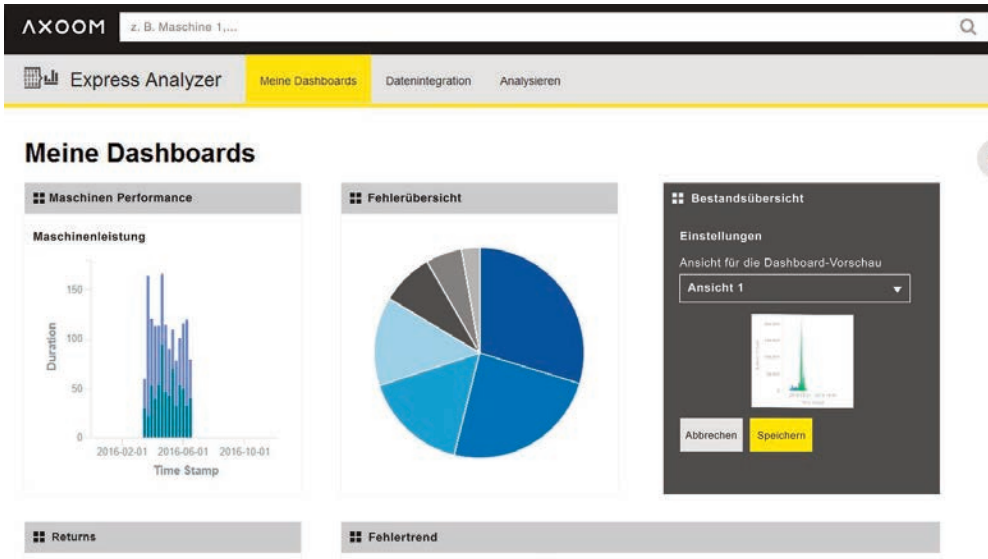
Bild: Magnescale Europe GmbH

Vertikale Vernetzung vom Sensor bis in die Cloud

Übersetzer zwischen den Maschinen

Das vom Maschinenbauer Trumpf gegründete Unternehmen Axoom erweitert sein Produktspektrum in Richtung Maschinen- und Komponentenhersteller. Das Angebot der horizontalen Vernetzung aller Prozessschritte vom Auftragseingang bis zur Auslieferung, das bei Axoom Smart Enterprise heißt, wird ergänzt um die vertikale Vernetzung vom Sensor bis in die Cloud.

Bild: Axoom GmbH



Mit dem Express Analyzer lassen sich Sensor- und Maschinendaten schnell analysieren und verstehen.

Der neue Produktbereich Axoom IoT bietet in vier Bereichen Mehrwerte: Das IoT Management mit dem Connection Center hilft Maschinenherstellern ihre Geräte im Feld anzubinden und zu verwalten, um die Verfügbarkeit und den Service zu verbessern. Der Baustein Condition Monitoring überwacht das Verhalten von Maschinen und Komponenten und macht deren Zustand transparent. Mit Remote Services werden drittens Konfigurationen, Software-Updates und Fehlerbehebungen aus der Ferne möglich, der Instandhaltungsaufwand sinkt. Der vierte Bereich Analytics schließlich analysiert Daten mit Blick auf Verbesserungspotenziale, um die Produktivität zu steigern.

Vernetzte Messtechnik

Die Möglichkeiten des erweiterten Portfolios macht sich beispielsweise das Unternehmen Zeiss zunutze. Der weltweit tätige Konzern hatte bereits auf dem Axxom-Stand der Hannover Messe eine vernetzte Lösung für die mehrdimensionale Messtechnik gezeigt. Das Fertigungsmessgerät DuraMax misst in diesem Fall die Präzision von Blechteilen, die zuvor auf einem Lasersystem von Trumpf geschnitten worden sind. Die Daten werden direkt in einem Analyse-Dashboard sichtbar. In Kooperation mit Trumpf und Axoom zeigt Zeiss so, wie Messgeräte in übergeordnete Systeme – etwa die Fertigungsfeinplanung oder automatisierte Qualitätsmeldungen – eingebunden und damit Teil einer Smart Factory werden können.

Fertigungsfeinplanung

Das Thema Fertigungsfeinplanung ist die Kernkompetenz des Axoom-Partners Xetics. Dessen Manufacturing Execution System (MES) Xetics Lean erfasst kontinuierlich alle relevanten Produktionsdaten und sorgt dadurch für hohe Transparenz. So lässt sich das MES auf Basis schlanker Prozesse sowohl die Feinplanung der Fertigung als auch die Interaktion zwischen Maschinen, Werkern und Produktionsplanung vereinfachen. Mit Hilfe weiterer Apps, die auf der Axoom-Plattform zur Verfügung stehen, können dann zusätzliche Optimierungspotenziale für die Fertigung gehoben werden.

Datenanalyse

Wie die Produktion anhand von Datenanalysen sicherer gemacht werden kann, zeigt der Maschinenbauer Felss anhand einer Rundknetanlage. Mit Hilfe digitaler Services lassen sich die Produktqualität verbessern und der Ausschuss reduzieren. Bei der Bearbeitung der Bauteile werden Prozessparameter wie etwa Drehzahlen aufgenommen und im Hintergrund analysiert. Anhand dieser Parameter erkennt die über Axoom angebundene Anlage selbstständig, ob das gefertigte Bauteil in Ordnung oder ein Eingriff des Maschinenbedieners vonnöten ist. Diese Information erscheint in Echtzeit zusammen mit diversen Kennzahlen auf dem Monitor und wird Kunden des Maschinenbauers künftig als Smart Correction zur Verfügung stehen. ■

Firma: ***Axoom GmbH***
www.axoom.de

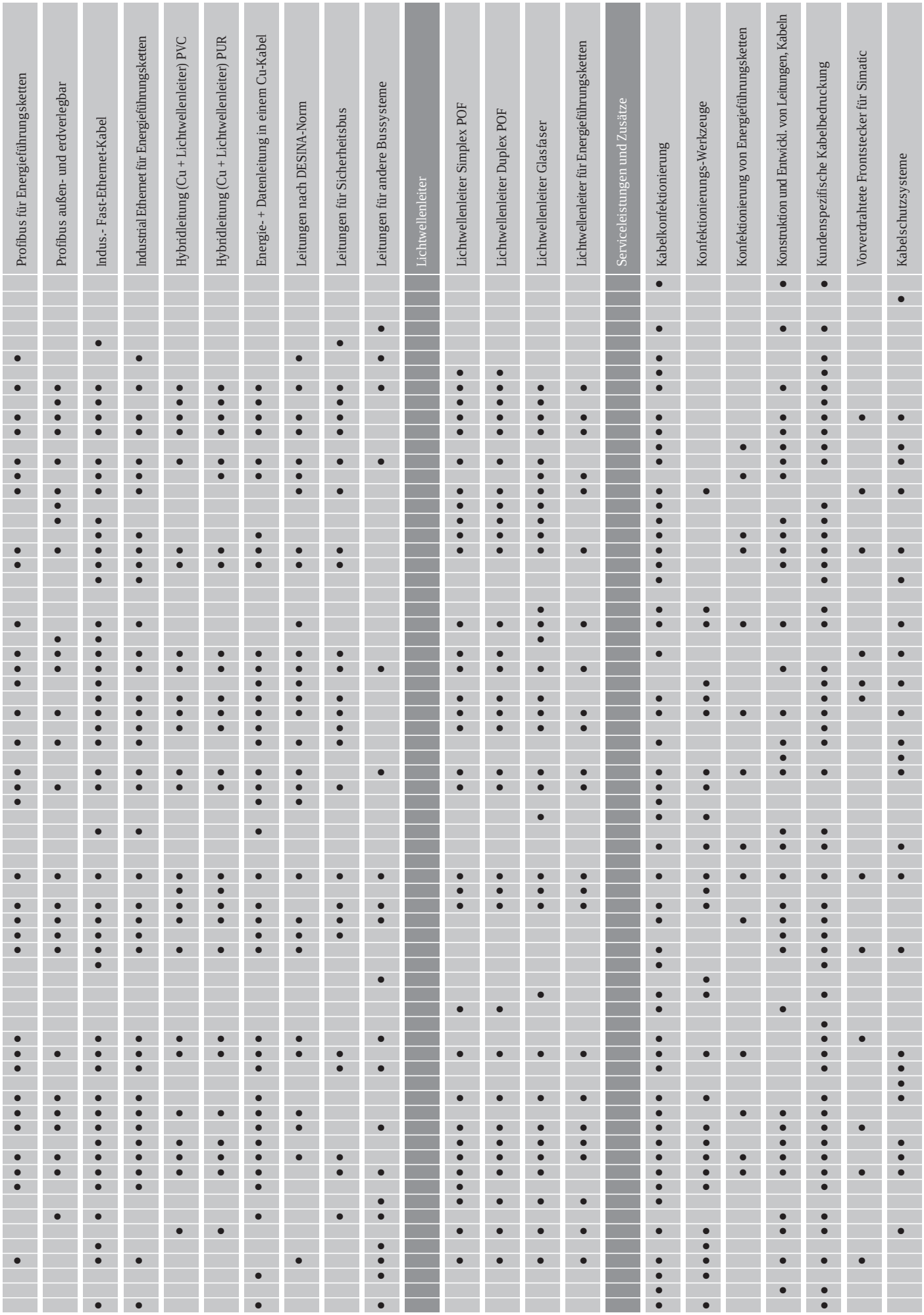
Marktspiegel Kabel und Leitungen

Der Hochhausbrand am Grenfell Tower zeigt eindringlich, welche Gefahren entstehen, wenn billiges aber hoch brennbares Material für die Außenfassade verbaut wird. Bereits im Inneren eines Gebäudes lauern Gefahren: Schadhafte elektrische Geräte sowie überlastete Kabel und Leitungen können zu Bränden führen, wobei brennende Leitungen den Brand fortsetzen.

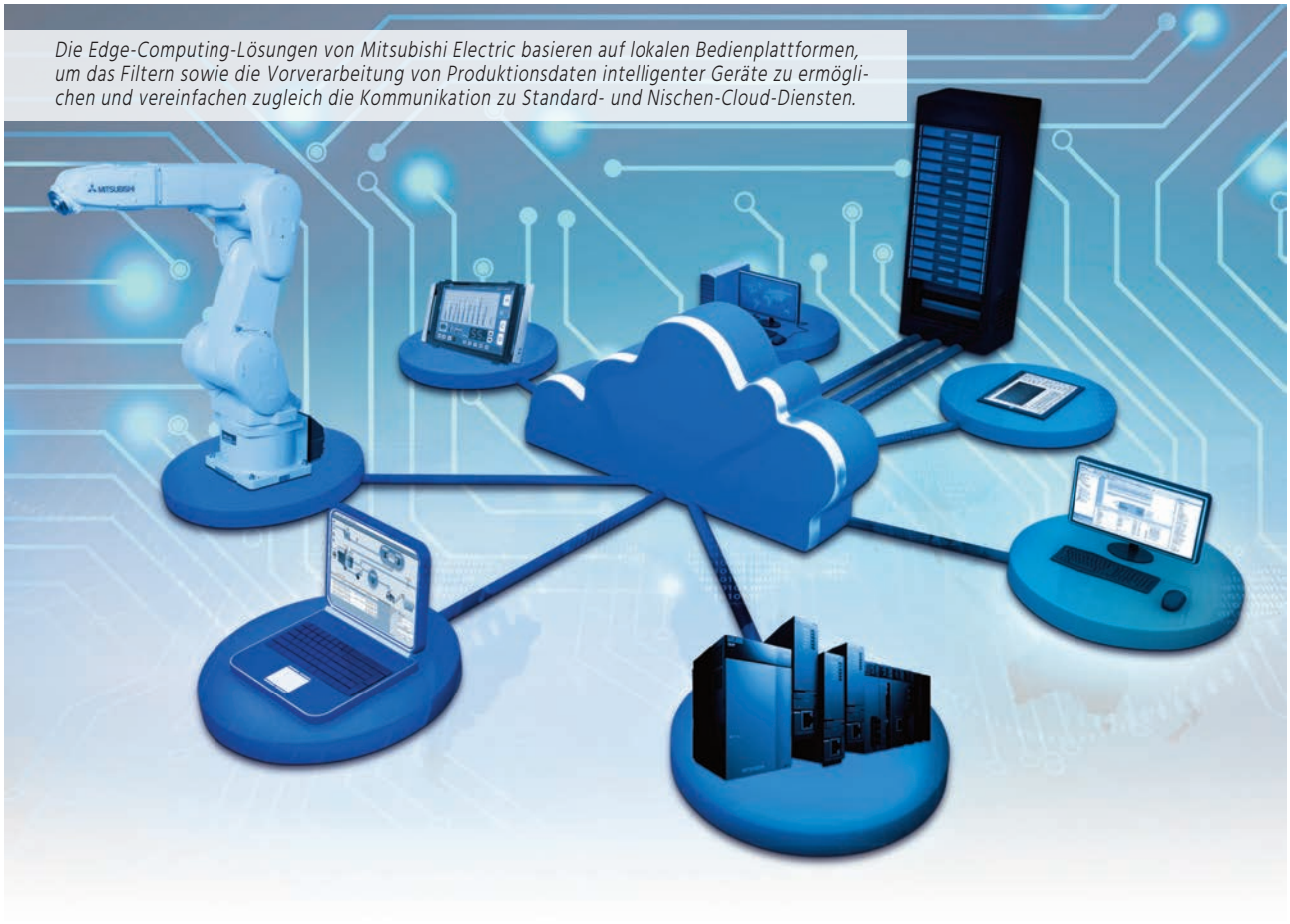
Unvergessen ist der Kabelbrand des Düsseldorfer Flughafens 1996, bei dem die Gefährdung von Menschen, neben den Sachschäden, deutlich wurden. In der Konsequenz war klar, dass auch Kabel und Leitungen einen Beitrag zum Brandschutz in Gebäuden leisten müssen. Spezielle Brandschutzkabel, deren Aufbau aus selbstverlöschenden, flammenhemmenden und halogenfreien Verbundwerkstoffen bestehen, helfen dabei. Mit der neuen Europäischen Norm 50575 gibt es ab 1. Juli 2017 eine einheitliche Klassifizierung von Brandeigenschaften. Sie betrifft Starkstromkabel und -leitungen sowie Kommunikations- und Steuerleitungen für die dauerhafte Installation in Bauwerken. Voraussetzung für eine CE-Kennzeichnung sind eine Prüfung und eine Leistungserklärung für neu in den Verkehr gebrachte Produkte. *(ghl)* ■

Bild: Belden Wire & Cable

Anbieter	Internet-Adresse	Feldbusleitungen	Sensor-/Aktor-Leitung	ASI-Sensor-/Aktor-Leitung	CAN / DeviceNet	DeviceNet für Energieführungsketten	Interbus	Profibus	Profibus PA
Adapt Elektronik	www.adapt.de		●						
Agro	www.agro.ch								
Automation24	www.automation24.de		●						
Axon Kabel	www.axon-cable.com								
B&R Industrie-Elektronik	www.br-automation.com		●		●			●	
Balluff	www.balluff.de		●		●	●		●	
Beck Kabel- u. Gehäusetechnik	www.beck-kabelkonfektion.de						●	●	
Bedea Berkenhoff & Drebes	www.bedea.com		●	●	●	●	●	●	●
Belden Wire & Cable	www.beldencables-emea.com		●	●	●		●	●	●
Thorsten Beulecke Kabelvertrieb	www.beulecke.de		●	●	●	●	●	●	●
Böhm Kabel	www.boehm-kabel.de		●	●	●	●	●	●	●
Codico	www.codico.com								
ConCab kabel	www.concab.de		●	●	●	●	●	●	●
Conductix-Wampfler	www.conductix.de				●	●	●	●	
Conrad Electronic	www.conrad.biz		●	●	●	●	●	●	
Contrinex Sensor	www.contrinex.de		●					●	●
DigiComm	www.digicomm.de				●		●	●	●
Elektrosil	www.elektrosil.com		●	●	●	●	●	●	●
Eltec Technology	www.eltec-gmbh.de		●	●	●	●	●	●	
Ernst & Engbring	www.eue-kabel.de		●	●	●	●	●	●	●
Escha Bauelemente	www.escha.de		●		●	●		●	
Esd Electronic System Design	www.esd.eu				●			●	
EVE	www.eve.de								
EVG Martens	www.evg.de		●	●	●	●		●	●
Klaus Faber	www.faberkabel.de		●	●			●	●	●
Fct Electronic	www.fct-electronic.de		●		●		●	●	●
Gebauer & Griller Kabelwerke	www.griller.at		●	●	●	●	●	●	●
Gogatec	www.gogatec.com		●		●	●		●	●
Harting Deutschland	www.harting.de		●		●			●	
Helukabel	www.helukabel.de		●	●	●	●	●	●	●
Hradil Spezialkabel	www.hradil.de				●				
Hummel	www.hummel.com		●	●	●	●	●	●	●
IBH Elektrotechnik	www.ibh-elektrotechnik.de								
Igus	www.chainflex.de		●	●	●	●	●	●	●
Indu-Sol	www.indu-sol.com		●	●	●	●	●	●	●
Industrieservice Hoppe	www.ish-industrieservice.de						●	●	●
Ipf Electronic	www.ipf.de		●						
Kabeltronik Arthur Volland	www.kabeltronik.de		●	●					
Kemmler Electronic	www.kemmler-electronic.de								
Kübler Gruppe, Fritz Kübler	www.kuebler.com				●			●	
U.I.Lapp	www.lappkabel.de		●	●	●	●	●	●	●
Laser 2000	www.laser2000.de								
Leoni Kerpen	www.leoni-industrial-projects.com				●		●	●	●
Leoni Special Cables	www.leoni-industrial-solutions.com		●	●	●	●	●	●	●
Letronic	www.letronic.de		●	●	●	●	●	●	●
Friedrich Lütze	www.luetze.com		●	●	●	●	●	●	●
Lumberg Automation, (Belden)	www.lumberg-automation.com		●	●	●		●	●	
Meilhaus Electronic	www.meilhaus.de								
Metz Connect	www.metz-connect.com								
MKU Metrofunk Kabel-Union	www.metrofunk.de							●	
Muckenhaupt & Nusselt - Kabelwerk	www.munu-kabel.de								
Murrelektronik	www.murrelektronik.com		●	●	●		●	●	
Mütron Müller	www.muetron.de		●	●	●	●	●	●	●
Pepperl+Fuchs	www.pepperl-fuchs.com		●	●	●	●	●	●	●
Pflitsch	www.pflitsch.de								
Phoenix Contact Deutschland	www.phoenixcontact.com		●		●		●	●	●
SAB Bröckskes	www.sab-kabel.de		●		●	●	●	●	●
Siemens	www.siemens.com/simatic-net			●				●	●
Sommer cable	www.sommercable.com							●	
TE Connectivity	www.te.com		●	●	●	●	●	●	●
TKD Kabel	www.tkd-kabel.de			●	●	●	●	●	●
Turck	www.turck.com		●	●	●	●		●	●
UBF EDV Handel und Beratung	www.ubf.de/shop/lwl-kabel.shtml								
Vogtländisches Kabelwerk (VOKA)	www.voka.de		●		●		●	●	●
W+P Products	www.wppro.com								
Wago Kontakttechnik	www.wago.com		●		●			●	
Weidmüller	www.weidmueller.de		●	●	●	●		●	●
Wieland Electric	www.wieland-electric.com		●	●				●	
XBK-Kabel Xaver Bechthold	www.xbk-kabel.de								
Yamaichi Electronics Deutschland	www.yamaichi.eu								



Alle Einträge basieren auf Angaben der jeweiligen Firmen.



Die Edge-Computing-Lösungen von Mitsubishi Electric basieren auf lokalen Bedienplattformen, um das Filtern sowie die Vorverarbeitung von Produktionsdaten intelligenter Geräte zu ermöglichen und vereinfachen zugleich die Kommunikation zu Standard- und Nischen-Cloud-Diensten.

Bild: © bluebay2014 / thinkstock.de; © stockchairatgfx / thinkstock.de

Steigende Datenmengen verarbeiten

Echtzeitproduktion und Enterprise-Welt verbinden

Als Anbieter moderner Automatisierungstechnik legt Mitsubishi Electric auch einen Fokus auf Edge Computing und die Unterstützung von Cloud Computing. Die Edge-Computing-Lösungen basieren auf lokalen Steuerungsplattformen, um das Filtern und die Vorverarbeitung von Produktionsdaten intelligenter Geräte zu ermöglichen. Zugleich vereinfachen sie die Kommunikation zu einer breiten Palette an Standard- und Nischen-Cloud-Diensten.

Über alle Industriesektoren hinweg fördert eine aussagekräftige Datenbasis eine verbesserte Produktivität und erhöhte Produktqualität. Sie ermöglicht präventive Zustandsüberwachung und Fernwartung. Fundierte Geschäftsentscheidungen können nur mithilfe von aussagekräftigen Daten getroffen werden. Aus diesen Gründen wurden Daten zunehmend aus einem immer größeren Spektrum von Steuerungskomponenten und Feldgeräten integriert. Die Integration kann über Ethernet geschehen. Immer mehr intelligente Geräte verfügen über eine eigene IP-Adresse. Die Integration kann aber auch drahtlos per GSM-Standard oder über die Verknüpfung bestehender RS232 Geräte über ein Netzwerk-Gateway erfolgen. Geräte generieren eine riesige Informationsmenge und sind über die offenen Standardprotokolle miteinander verbunden. Die daraus entstehende weit vernetzte Intelligenz wird als Schlüsselelement betrachtet, um eine digitale Umgebung innerhalb von Unternehmen zu schaffen. Die Kombination digitaler Daten in vernetzen Systemen dient der schnelleren und besseren Entscheidungsfindung.

IT-Infrastrukturen anpassen

Aktuellen Schätzungen zufolge sind bereits über 5 Milliarden Geräte durch das IIoT miteinander verbunden. Diese Zahl wird in den nächsten Jahren massiv ansteigen. Da die Datenmenge

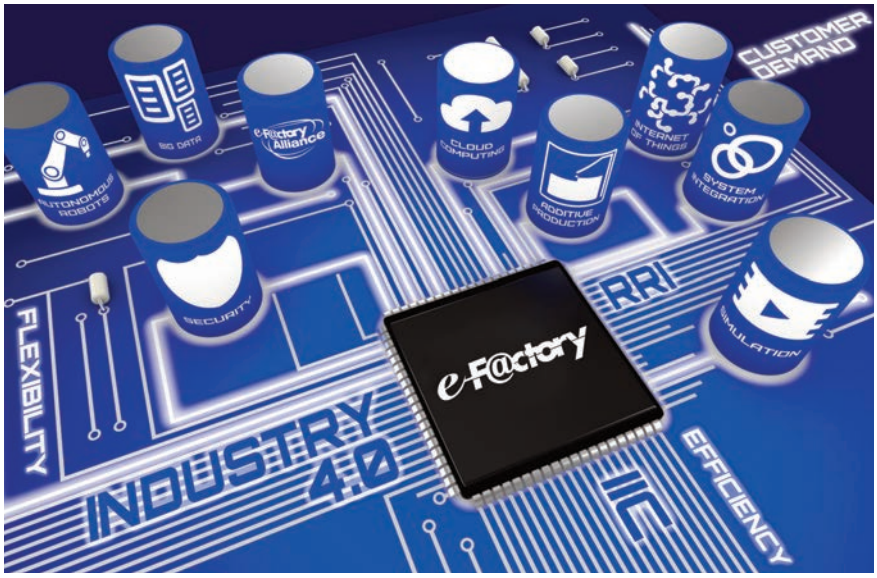


Bild: Mitsubishi Electric Europe B.V.

Mitsubishi Electric bietet mit seinen e-F@ctory Alliance Partnern IoT Connectoren für eine nahtlose Cloud-Konnektivität.

dadurch in Zukunft deutlich zunehmen wird, wird es signifikante Änderungen in der IT-Infrastruktur geben müssen. Damit steigt auch der Wert von cloudbasierter Datenspeicherung und -verarbeitung. Diese ermöglicht eine sicherere, zuverlässigere, skalierbarere und kostengünstigere Datensammlung und -verteilung als die bestehenden IT-Infrastrukturen. Daher nutzen immer mehr Unternehmen Cloud-Dienste. Diese ermöglichen nicht nur das problemlose Speichern großer Datenmengen, sondern bieten auch die Möglichkeit, Daten zu analysieren. Daraus können einfach individuelle Trends und Dashboards abgeleitet werden. Die Gesamtleistung der Anlage und die Anlagenverwaltung können somit verbessert werden.

Edge Computing als Bindeglied

Einige Anforderungen bedingen, auf Echtzeitdaten zu reagieren. Teilweise kann dies nicht mit Cloud-Diensten gewährleitest werden. Daten müssen direkt vor Ort erfasst, gesammelt und analysiert werden, damit sie in Echtzeit in den Prozess und die Maschinen zurück gespiegelt werden können. Das ist die Aufgabe von Edge Computing. Es ist das Bindeglied zwischen der Enterprise Welt und der Echtzeitproduktion. Es bringt die Intelligenz, Rechenleistung und Kommunikationsfähigkeiten eines Edge Gateways oder intelligenten Gerätes direkt in Verbindung mit lokalen und leistungsstarken PAC-Systemen (Programmable Automation Controllers). Edge Computing arbeitet in Ergänzung zu Cloud Computing und Unternehmen merken nach und nach, dass sie das Potenzial beider Möglichkeiten benötigen. Die Cloud bildet das umfassendere Bild des Industriellen Internets der Dinge, während Edge Computing das IIoT zum Leben erweckt, indem es Anwendungen unterstützt, die Echtzeit-Reaktionen erfordern. Mitsubishi Electric hat Lösungen entwickelt, die Edge- und Cloud-Computing ergänzen. Sie bieten einfachen und sicheren Zugang zu einer Reihe an unterschiedlichen Cloud-Diensten und ermöglichen gleichzeitig Edge Computing. Diese Lösungen basieren auf Technologien wie dem Mitsubishi Electric C-Controller, MES Interface-Modul und der Scada-Plattform MAPS .

C-Controller und MES Interfaces

Der C-Controller von Mitsubishi Electric ist ein Open Platform Controller, der auf der Programmiersprache C basiert. Er ermöglicht eine effiziente Edge Computing Plattform. Außerdem können Datenbanken von Partnern der Mitsubishi Electric e-F@ctory Alliance direkt in Steuerungen von Mitsubishi Electric eingebunden werden. Das sorgt für größere Transparenz und eine Verbesserung der Leistung sensibler Produktionsabläufe. Produktionsdaten von Sensoren, Antrieben, SPSen, Aktoren und Robotern werden innerhalb des C-Controllers und den MES Interface-Lösungen (wie dem C Application Server oder dem MES IT-Modul) gefiltert und vorverarbeitet. Die lokale Verarbeitung der Daten und eine bessere Datenverfügbarkeit sorgen für direkte Vorteile im Hinblick auf Leistung und Schnelligkeit. Die C Applikation kann die Daten vorverarbeiten oder direkt in unterschiedliche Cloud Dienste übertragen. Nicht nur die bekanntesten und größten Cloud-Dienste werden unterstützt – wie SAP Hana, Microsoft Azure und Amazon – sondern auch spezielle Cloud-Lösungen, Nischen-Cloud-Anwendungen und cloudbasierte Analysedienstleistungen können integriert werden.

Lösungen für Cloud-Konnektivität

Zur Anbindung an diese Cloud-Systeme steht ebenfalls eine OPC UA Schnittstelle zur Verfügung (MX OPC UA). Zusätzlich bietet Mitsubishi Electric mit seinen e-F@ctory-Alliance-Partnern IoT Connectoren für eine nahtlose Cloud-Konnektivität. Zu diesen Partnern gehören u.a. eWon, Secomea oder Iconics. Außerdem können mit dem C-Applications Server Informationen aus den unterschiedlichen Cloud-Diensten genutzt werden. In prozessorientierteren Bereichen und Branchen unterstützt die MAPS-Scada-Plattform die gesamte Palette an Microsoft-Verbindungstechnologien sowie Virtual Basic Scripts und OPC UA Strukturen. Cloud Computing ist bereits zu einem unentbehrlichen Tool für viele Unternehmen geworden, deren IT-Strukturen durch stetig steigende Datenmengen und den Zugriff auf diese Daten auf vielfältigen Geräten, lokal und per Fernzugriff, immer stärker strapaziert werden. Zugleich wachsen die Anforderungen an Edge Computing rapide, und die Verbreitung von vorverarbeiteten Daten, in Anwendungen, die geringe Latenzzeiten erfordern, steigt. ■

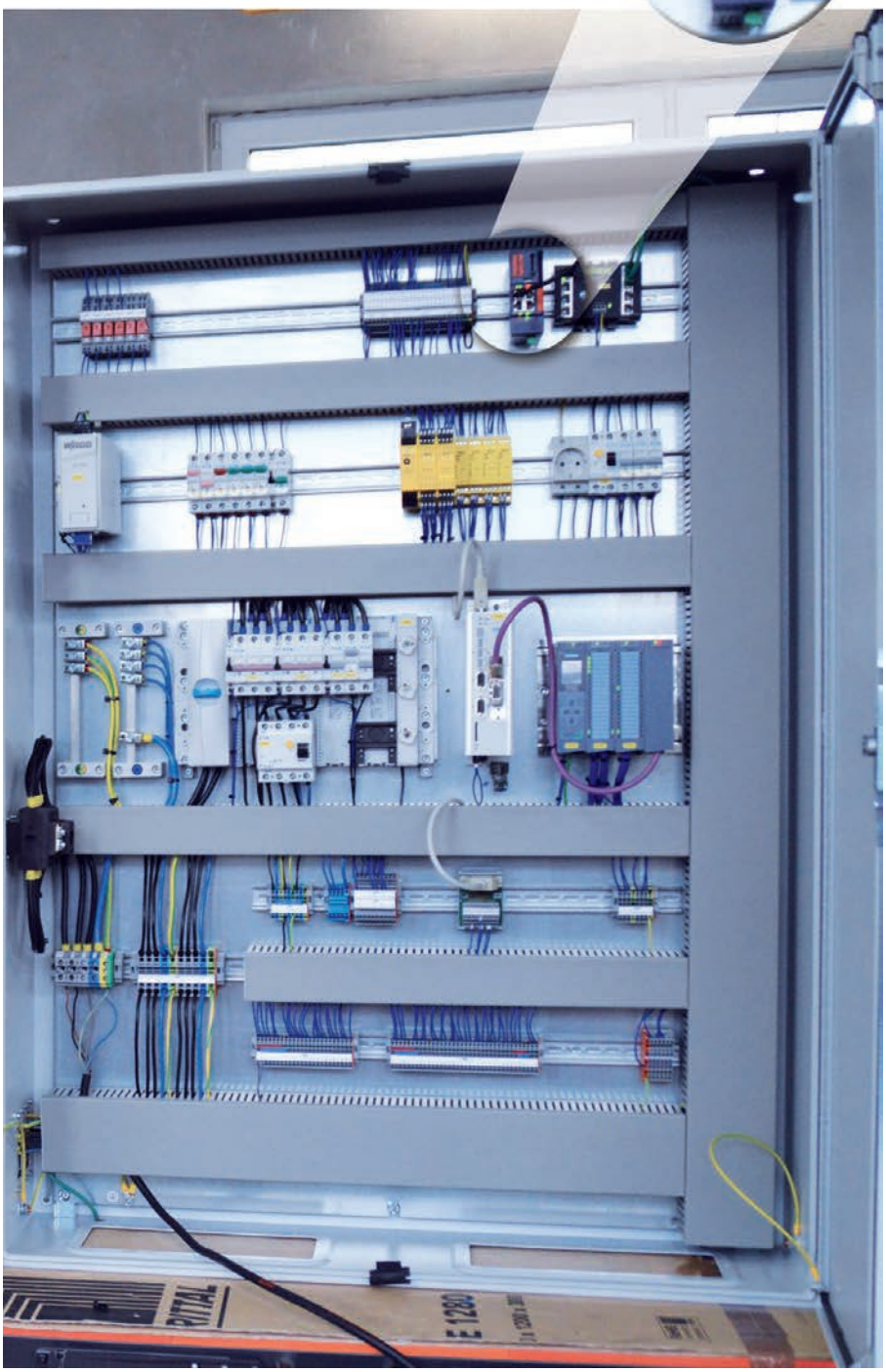
Autor: ***Thomas Lantermann***
Senior Solution Consultant Factory Automation EMEA
Mitsubishi Electric Europe B.V.
www.mitsubishielectric.com

Fernwartungsrouter für hohe Anlagenverfügbarkeit

Als wäre man vor Ort

Nicht erst seit Industrie 4.0 in aller Munde ist, steht in der Fertigung auch das Thema Fernwartung im Raum. Ziel sind transparente und effiziente Prozesse sowie eine hohe Verfügbarkeit von Maschinen und Anlagen. Mit flexiblen Fernwartungsroutern und einem Serviceportal auf Cloudbasis lassen sich diese Anforderungen auch nachträglich realisieren.

Die Versorgung von Maschinen und Anlagen mit Strom reicht schon lange nicht mehr aus. Auch an übergeordneter Stelle ist es wichtig, alle Daten im Blick zu behalten, um die Effizienz von Prozessen zu steigern, Störmeldungen sofort zu erkennen oder Softwareänderungen schnell und unkompliziert umzusetzen. Themen wie Industrie 4.0, IIoT, Smart Factory oder auch die Energiewende haben diesen Trend noch befeuert. So gibt es immer mehr kleinere, dezentrale Energieerzeuger wie Windräder, Biogasanlagen oder Wasserkraftwerke. Sie haben eins gemeinsam: Oft werden sie an abgelegenen Standorten errichtet, wobei es aber nicht ausreicht, einfach nur Strom in das Netz einzuspeisen. Daten müssen ebenfalls aus unterschiedlichen Gründen ausgetauscht werden. „Zum Einen geht es natürlich um die Überwachung der Anlage und die Anzeige von Störmeldungen“, erklärt Dominic Schott, der in seiner Eigenschaft als Systemintegrator häufig mit der Errichtung von Kleinwasserkraftwerken zu tun hat. „Andererseits wollen die Betreiber aber auch wissen, wieviel Energie hier erzeugt wird“, erklärt der Elektroingenieur. Für solche Anwendungsfälle eignen sich Fernwartungslösungen.



Schlüsselfertige Schaltschränke von Schodo kommen in der Automobilindustrie zum Einsatz und übernehmen dort z.B. die Steuerung einer Schweißanlage.

Bild: Wachendorff Prozesstechnik GmbH & Co. KG

Fernwartung in der Produktion

Und auch in der Produktion geht heute ohne Fernwartung kaum noch etwas. „Unsere Kunden fragen solche Systeme vor allem nach, um die Verfügbarkeit ihrer Anlagen zu erhöhen“, erklärt Schott, dessen Firma Schodo nicht nur komplette Automationslösungen projektiert, sondern auch schlüsselfertige Schaltschränke baut. Damit erhalten seine Kunden bei Bedarf vom Engineering bis zur Hardware alles aus einer Hand. Zu den Kunden gehören Anlagenbauer vieler Branchen. Sie liefern ihre Lösungen z.B. an die Automobilindustrie. Auch wenn das Unternehmen eigentlich nur Zulieferer ist, verbleibt die Verantwortung für die Steuerung und Software häufig auch nach der Projektierung in den Händen von Schodo. „Oft kommt es im laufenden Betrieb zu Änderungen von Taktzeiten oder Produkteigenschaften“, erklärt Schott. Um solche Anpassungen schnell und kostensparend vorzunehmen, kommen wir heute um Fernwartung eigentlich nicht mehr herum“, ergänzt er. Schott registriert seit etwa zehn Jahren eine immer größer werdende Nachfrage nach Möglichkeiten des Fernzugriffs. „Wir haben uns damals auf der Nürnberger Messe nach Lösungen umgesehen und sind bei Wachendorff fündig geworden“, berichtet er. Denn der Anbieter hat in seinem Portfolio eine Vielzahl an Fernwartungsroutern mit unterschiedlichen Bauformen und Funktionen, die für unterschiedliche Branchen die passende Funktionalität umfassen. Auf diese Weise wird verhindert, dass der Kunde für Leistungen zahlen muss, die er gar nicht benötigt. Er kann exakt das wählen, was für die jeweilige Anforderung das Richtige ist und bleibt so auch preislich im Rahmen.

Fernwartungsrouter der Serie eWon kommunizieren mit allen marktgängigen Steuerungen namhafter Hersteller.

Bild: Wachendorff Prozesstechnik GmbH & Co. KG

Flexible Fernwartungsrouter

Die VPN-Router der Serie eWon Cosy sind kostengünstige und effiziente Werkzeuge, um Anlagendaten aus der Ferne einzusehen oder Parameter zu ändern. „Schon beim ersten eingesparten Kundenbesuch hat sich die Investition in ein solches Gerät amortisiert“, bringt Schott die Vorteile auf den Punkt. Werden mehr Möglichkeiten benötigt, wie z. B. Alarmmangement und/oder umfassendes Daten-Logging, so wird einfach auf die Serien eWon Flexy und eWon CD zurückgegriffen, um die passende Lösung zu realisieren. Sicherheitsbedenken gibt es dabei von Kundenseite nur wenig. „Spätestens, wenn wir erklären, dass wir uns nicht von außen in das Firmennetzwerk einwählen, sondern per GSM, LAN oder WLAN den Zugriff herstellen und die IT-Abteilung keine besonderen Änderungen in den unternehmensspezifischen Sicherheitsrichtlinien und -maßnahmen für uns vornehmen muss, sind alle Hürden schnell überwunden“, erklärt Schott. Hilfreich dabei ist sicherlich das zwischengeschaltete Online-Serviceportal Talk2M. Es bietet einen komfortablen Zugriff auf viele Anlagen in der ganzen Welt und für die Kunden hohe Sicherheit.

Online-Serviceportal auf Cloudbasis

Die industrielle, Cloudbasierte Lösung stellt mit derzeit 25 weltweit verteilten Servern nicht nur die Zuverlässigkeit der VPN-gesicherten Kommunikation sicher, sondern protokolliert auch alle Verbindungen. So lässt sich jeder Zugriff auch nachträglich nachvollziehen und einfach in Reports ausleiten. Die Kommunikation erfolgt über einen SSL-basierten OpenVPN-Tunnel. Die ausgetauschten Informationen werden verschlüsselt übertragen (SSL, 2048Bit-Schlüssel) und ausschließlich authentifizierte Benutzer können sich mit dem Router verbinden. Der Anwender hat zudem die volle Zugriffskontrolle: Er definiert, welche Benutzer auf welche Geräte zugreifen, denn das Portal Talk2M Pro erlaubt die Deklaration von Benutzer- und Gerätegruppen. Der Administrator ist so in der Lage, differenziert die verschiedenen Zugriffsrechte und Ansichten zuzuweisen.

Sicherheit durch reglementierte Benutzeranmeldung

Eine streng reglementierbare Benutzeranmeldung sorgt für weitere Sicherheit. Die Passwörter müssen bestimmten Regeln entsprechen (Mindestlänge, Kombination aus Buchstaben, Zahlen und Sonderzeichen erforderlich, begrenzte Gültigkeitsdauer, Benutzung alter Passwörter nicht erlaubt). Hinzu kommt eine Zweifaktorauthentifizierung, bestehend aus dem Password und einem zusätzlichen SMS-Schlüssel. Die Lösung ist außerdem offen für Steuerungen aller namhaften Hersteller. ■

Autor: **Helmut Halmburger,**
Produktmanager Industrielle Kommunikation,
Wachendorff Prozesstechnik GmbH & Co. KG
www.wachendorff-prozesstechnik.de/fernwartung

Im Rahmen des Steuernetzmanagements sind vollständige Transparenz der Kommunikation und Anomalieerkennung in Echtzeit die treibenden Faktoren einer effektiven Produktionssteuerung.

Für eine effektive Produktionssteuerung

Anomalieerkennung für Ausfallsicherheit

Das Industrielle Internet der Dinge bedeutet für Industrieunternehmen neue Herausforderungen in Bezug auf Steuernetzstabilität und Anlagenverfügbarkeit. Die Netzwerke benötigen ein kontinuierliches Monitoring, um sowohl Transparenz über die Kommunikation als auch eine Anomalieerkennung in Echtzeit zu gewährleisten.

Die Umstellung industrieller Steuernetze bedeutet, sich vom alten Industriestandard der Punkt-zu-Punkt-Verbindungen zu verabschieden. Anstelle eindeutig zugewiesener Kommunikations-Infrastrukturen treten mit Systemen wie Ethernet/IP und Ethercat dezentrale, virtuelle Netzwerke, die zudem an externe Backend-Systeme wie MES, SAP oder Browserlösungen angebunden werden. Diese Umstrukturierung der Produktionssteuerung stellt mit einer Zunahme der Zugangspunkte ins Steuernetz auch neue Anforderungen an das grundlegende Netzwerkmanagement in Bezug auf Kommunikationssteuerung und Sicherstellung der Anlagenverfügbarkeit. Steuernetze in automatisierten Produktionen werden zusehends komplexer und anfälliger für Störungen. Eine Mikrosekunde Verzögerung kann in eng getakteten Fertigungslinien bereits zu Produktfehlern und Anlagenausfällen führen. Zusätzlich entstehen im Zuge von Industrial Big Data neue Anforderungen an die Datennutzung seitens präventiver Instandhaltung, aber auch Prozessoptimierung und Qualitätssicherung. Unternehmen müssen deshalb in ihrem Steuernetz vollständige Transparenz herstellen und Werkzeuge einsetzen, die eine Anomalieerkennung in Echtzeit ermöglichen.

Kommunikation im Steuernetz lenken

Die Grundbedingung, um sowohl redundante Kommunikation als auch Kommunikations- und Netzwerkfehler zu vermeiden, ist vollständige Transparenz. Viele Unternehmen haben nach wie vor nur bedingt Einblick, welche Komponenten in ihr Steuernetz eingebunden sind. Noch unschärfer ist das Wissen, welche Komponenten in welcher Form miteinander kommunizieren: Welche Komponente darf Befehle erteilen? Welche Protokolle dürfen verwendet werden? Gibt es eine zeitliche Taktung, wann bestimmte Komponenten kommunizieren dürfen? Viele Steuernetze funktionieren noch nach dem Prinzip der Netzneutralität. Die Komponenten kommunizieren je nach Bedarf miteinander. Im schlimmsten Fall kommunizieren alle Komponenten ungehindert und unter voller Auslastung des Netzwerks. Bei der Vielzahl der Sensoren, kann es schnell zu Kapazitätsengpässen oder sich blockierenden Datenpaketen kommen. Das kann zu Störungen durch verloren gegangene, doppelt oder verzögert gesendete Kommunikationspakete führen. Ein weiterer Aspekt der Transparenz ist die Informationstiefe der Monitoringlösung. Die meis-

ten Technologien beschränken sich auf die Standarddaten wie Absender und Empfänger. Die relevante Information findet sich jedoch in den Datenpaketen - auf Inhaltsebene. Diese muss in das Monitoring und die Echtzeitanalyse eingebunden werden. Wer seine Steuernetzkommunikation effektiv lenken möchte, benötigt ein Monitoring, das:

• alle Komponenten im Steuernetz und deren Verlinkungen und Kommunikationsstrukturen zuverlässig erkennt (siehe Abb. 1);
• mit Hilfe industrieller Deep-Packet-Inspection-Technologien die Kommunikation im Steuernetz auf Inhaltsebene ausliest und auswertet. Die Informationen zu Störungen, Anomalien oder unbekannter Kommunikation werden detailliert gespeichert und können als PCAP / Trace bei der Fehlersuche gezielt ausgewertet werden.

Bild: Rhebo GmbH

Die Monitoring-Lösungen der industriellen Deep-Packet-Inspection-Technologie erlauben einen detaillierten Einblick in die Steuernetzkommunikation.

Anomalien in Echtzeit erkennen

Die Anomalieerkennung in industriellen Netzwerken wird häufig zweifach eingeschränkt eingesetzt:

• räumlich: Das Monitoring (insbesondere unter dem Sicherheitsaspekt) beschränkt sich auf die Peripherie, also dem Übergangsbereich zu anderen Netzen (z. B. per Firewall);
• zeitlich: Netzwerkanalyse-Werkzeuge kommen ausschließlich bei schon vorgefallenen Störungen für die Fehlersuche zum Einsatz.

Die meisten Störungen entstehen jedoch innerhalb des Netzwerkes und in der Regel schleichend oder nicht vorhersehbar. Um die störungsfreie Produktion zu gewährleisten, muss eine Anomalieerkennung flächendeckend und in Echtzeit erfolgen. Gerade in Fertigungslinien herrschen sich wiederholende Kommunikationsmuster vor, die eine Standardkommunikation darstellen. Spezielle industrielle Deep-Packet-Inspection-Technologien erlernen deshalb mittels maschinellen Lernens binnen weniger Minuten die Standardkommunikation und melden nachfolgend in Echtzeit alle Abweichungen von diesem Standard. So werden auch unbekannte, erstmals auftretende und schleichende Veränderungen im Steuernetz sichtbar. Kommunikationseingriffe wie z. B. durch versteckte Schadprogramme, wie WannaCry oder Industroyer, können so frühzeitig erkannt und gestoppt werden. Das kontinuierliche Netzwerk-Monitoring sollte dabei rückwirkungsfrei arbeiten, um nicht selbst zur Fehlerquelle zu werden. Gerade in komplexen Netzwerken, in denen eine gewisse Datendynamik vorherrscht, ist das Risiko von 'false-positive'-Befunden verhältnismäßig hoch. Würde das Monitoringwerkzeug automatisch alle unbekannten Aktionen im Steuernetz blockieren, sind wiederholte, ungewollte Stillstände sehr wahrscheinlich. Eine Alternative dazu sind Monitoringwerkzeuge, die zwar alle abweichenden Operationen zuverlässig und in Echtzeit melden, aber dem Netzwerkadministrator vollständige Hoheit über die Entscheidung geben.

Industrial Big Data nutzen

Mit einem Monitoringwerkzeug, das flächendeckend, kontinuierlich und detailliert die gesamte Steuernetzkommunikation überwacht, werden auch weitere Anwendungen im Unternehmen möglich. Kommunikationsdaten und Veränderungen innerhalb dieser können:

• für die Planung präventiver Instandhaltungsmaßnahmen genutzt werden;
• die Prozessoptimierung durch detaillierte Einblicke in Netzwerkstruktur und -dynamik unterstützen und
• eine ganzheitliche Qualitätssicherung unter Einbeziehung von Anlagen-, Performance- und Kommunikationsdaten etablieren.

Dafür sollten die Ergebnisse des Netzwerkmonitorings übersichtlich auf einem Dashboard dargestellt und in bestehende Backend-Strukturen wie MES oder SAP integriert werden. Um den verschiedenen Akteuren aus Netzwerksicherheit, Instandhaltung, Produktionssteuerung, Qualitätssicherung und Prozessoptimierung den einfachen Zugriff auf die Daten zu ermöglichen, sollte das Dashboard z. B. über verschiedenen Filterfunktionen frei konfigurierbar sein. Die einfache Weiterverarbeitung der Daten in anderen Systemen muss über sinnvolle, universelle Austauschformate sichergestellt werden.

Fazit

Industrieunternehmen müssen sich den operativen Herausforderungen IIoT-fähiger Steuernetze stellen. Im Rahmen des Steuernetzmanagements sind dabei vollständige Transparenz der Kommunikation und Anomalieerkennung in Echtzeit die treibenden Faktoren einer effektiven Produktionssteuerung. Industrielle Deep Packet Inspection bietet Administratoren einen detaillierten Einblick in die Steuernetzkommunikation sowie eine lückenlose Meldung aller Veränderungen innerhalb dieser. Durch die gründliche, flächendeckende und kontinuierliche Datenbereitstellung können sowohl präventive Instandhaltung und Netzwerksicherheit als auch Qualitätssicherung und Produktionssteuerung effektiv und ganzheitlich im Unternehmen umgesetzt werden. ■

Autor: ***Martin Menschner,***
CTO,
Rhebo GmbH
www.rhebo.com

Bild: Endian S.r.l.

Das Lösungspaket von Endian ermöglicht sicheren und skalierbaren Zugriff auf Endpunkte.

Sicherer Fernzugriff auf Medizintechnikanlagen

Ein Tool für alle Fälle

Die einst so aufwendige Wartung von Maschinen und Anlagen lässt sich heute über das Internet erledigen. Dabei steht die Sicherheit der Maschinen und Kundennetzwerke an oberster Stelle. Dass Fernwartung auch in einer Branche mit besonders sensiblen Daten erfolgreich ist, zeigt der Medizintechnikhersteller Werfen. Mit einem Lösungspaket wartet und sichert das Unternehmen seine In-vitro-Diagnostika. Die gewonnenen Daten werden gleichzeitig für Predictive Maintenance genutzt.

Werfen entwickelt In-Vitro-Diagnostika (IVD). Weltweit nutzen Krankenhäuser und Laboratorien diese Geräte für die Analyse von Blut- und Gewebeproben. Das Unternehmen übernimmt auch die Wartung und Überwachung der Geräte. Um einen reibungslosen und durchgängigen Betrieb der IVDs zu sichern, wurden bisher Techniker zu den Kunden entsandt. In den zeitintensiven Vororteinsätzen führte das technische Personal dann verschiedene Maßnahmen durch, wie Log-Sammlung, Maschinenüberwachung und Wartung. Schon früh erkannte Werfen das Potential der Digitalisierung und suchte nach einer einheitlichen und sicheren Möglichkeit zu Fernwartung für seine Geräte über das Internet. Die Lösung sollte einen zentralen Zugriff auf alle Maschinen erlauben, auch wenn diese beim Endkunden in unterschiedliche Netzwerkumgebungen eingebunden sind. Die Lösung fand Werfen beim Security-Anbieter Endian. Das Unternehmen bietet mit Endian Connect einen Schutz der gesamten Kommunikations- und Informationsstruktur eines Unternehmens. Das zentrale Element der Lösung ist das Endian Switchboard. Dieses Management-Tool ermöglicht die Verwaltung aller Anwender, Geräte und Berechtigungen über eine einzige Plattform. Dabei zeichnet sich die Lösung durch eine hohe Skalierbarkeit aus: Unbegrenzt viele Endpunkte können über sichere VPN-Verbindungen angesteuert werden. „Die VPN-Verbindung ist stabil und auf zwei Richtungen ausgelegt“, erklärt Raphael Vallazza, CEO von Endian. „Damit kann man aus den Maschinen Daten auslesen, die als Basis für Predictive Maintenance dienen. Gleichzeitig ist die Verbindung für die Fernwartung einsetzbar.“ Die Mandantenfähigkeit ist ein wichtiger Bestandteil der Lösung, denn damit können granulare Nutzungsrechte erteilt werden.

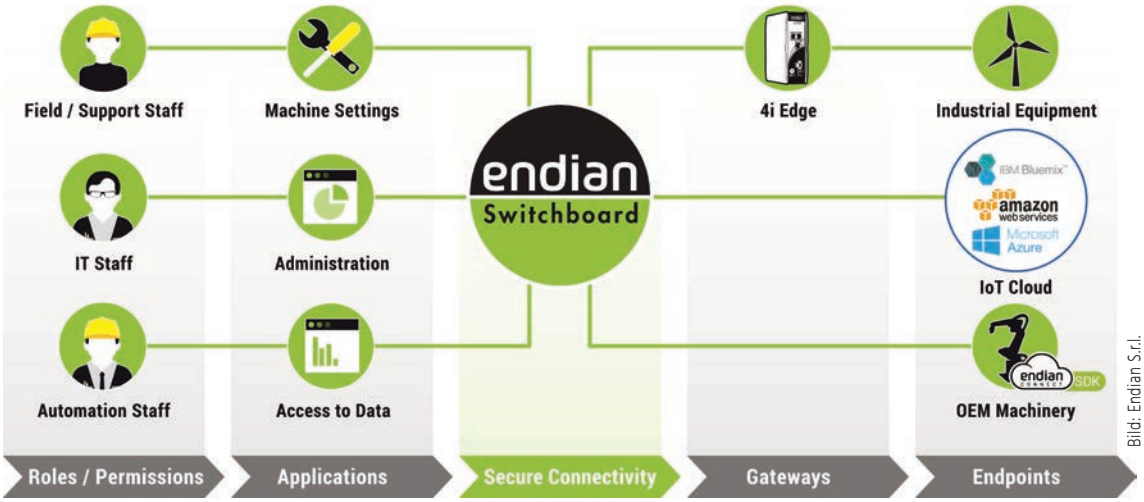


Bild: Endian S.r.l.

Endian Connect Platform Architektur

Einzelne Anwender oder Anwendergruppen erhalten in Abhängigkeit von ihren Zuständigkeiten Zugang zu bestimmten Endgeräten. Gleichzeitig wird festgelegt, für welche Anwendungen auf dem jeweiligen Gerät die Benutzer eine Berechtigung erhalten. Das Interface ist intuitiv zu bedienen.

Integration in bestehende Umgebungen

Wer Endian Connect einsetzen möchte, kann zwischen verschiedenen Möglichkeiten der Installation wählen: Die Lösung ist als Hardware, Software, Cloud und On-Premise verfügbar. Endian bietet die Lösung auch als OEM an. Über eine API-Softwareschnittstelle ist das Switchboard deshalb in bereits bestehende Kundenumgebungen integrierbar. Das technische Personal kann damit auf bereits bekannten Oberflächen arbeiten, aufwendige Schulungen sind nicht nötig. Über die Endian Connect App haben Benutzer von jedem Endgerät aus Zugriff auf die Anwendungen, für die sie zuvor eine Berechtigung bekommen haben. Die App ist für die Windows-, Mac- und Linux-Betriebssysteme verfügbar, ebenso für mobile Endgeräte über iOS und Android. Eine VPN-Anbindung wird standardmäßig bei jeder Anmeldung aufgebaut und sichert damit den Zugriff ab.

> *„Mit unserer VPN-Verbindung kann man Daten als Basis für Predictive Maintenance auslesen, gleichzeitig ist die Verbindung für die Fernwartung einsetzbar.“*
> *Raphael Vallazza, CEO Endian*

Bild: Endian S.r.l.

Sicherheit für industrielle Einsätze

Für die Sicherung der einzelnen Geräte kommen die Security Gateways Endian 4i Edge zum Einsatz. Jedes Werfen-Gerät wird mit einem Gateway ausgestattet, das für Sicherheit und Verschlüsselung in Industrieumgebungen sorgt. Dazu gehört die Ausstattung mit Firewall, VPN und IPS (Intrusion Prevention System). Mit der VPN-Technik von Endian können sich die 4i-Geräte aber auch hinter bestehenden Firewalls verbinden. Die Endian-Serie 4i Edge unterstützt so gut wie jede Art der Internetanbindung und beinhaltet auch wahlweise 3G- und 4G-Mobilfunk. Die verschiedenen Verbindungsoptionen sorgen für eine maximale Verfügbarkeit der Remote-Endpunkte und Netzwerke und garantieren einen reibungsfreien Betrieb. Über einen Digital Input/Output lässt sich die VPN-Verbindung zu- oder abschalten. Falls an dem Gerät vor Ort Maßnahmen durchgeführt werden, wird eine gleichzeitige Fernwartung damit unterbunden.

Einfacher Launch per USB-Stick

Damit die Anwendungen beim Endkunden schnell einsatzbereit sind, entwickelte Endian das USB Provisioning Tool. Alle notwendigen Konfigurationen werden dabei auf einem USB-Stick gespeichert, der an die verschiedenen Standorte der Geräte geschickt wird. Vor Ort können Techniker oder auch ungeschultes Personal das Gateway damit einfach mit dem zentralen Management-Tool und vorkonfigurierten Einstellungen verbinden. Insgesamt hat Werfen mit dem Einsatz von Endian Connect zwei wichtige Ziele erreicht: Bei gleichbleibend hoher Servicequalität wurde die Produktivität der Belegschaft gesteigert und die Response-Zeiten verringert. Seit dem Start des Projekts sind tausende IVDs mit Endian Connect ausgestattet worden. Es ist geplant, in Zukunft noch viele weitere Geräte anzubinden. ■

Autor: *Raphael Vallazza,*
CEO,
Endian
www.endian.com

Fernzugriff auf Industriemaschinen via Router und Gateway

Schritt für Schritt zur Remote-Access-Lösung

Bild: HMS Industrial Networks

Die Ewon-Remote-Data-Lösung verbindet Remote Access mit Datendiensten via IIoT-Router und Daten-Gateway der Serie Ewon Flexy.

Maschinenbauer wissen heutzutage, wie wichtig der Fernzugriff auf Maschinen und Anlagen ist. Remote Access kann in der Tat die Wettbewerbsfähigkeit der Hersteller wahren. Denn der Zugriff auf Industriemaschinen über die Kombination aus IIoT-Router und Daten-Gateway hilft, Wartungskosten zu reduzieren, die Betriebszeiten der Maschinen zu verbessern oder einen guten Kundenservice bereitzustellen.

HMS Industrial Networks verzeichnet regelmäßige Statistiken über seine IIoT-Cloud-Plattform Talk2M. Hier sind 120.000 Ewon-VPN-Router registriert, die insgesamt bereits 9Mio. VPN-Verbindungen hergestellt haben. „Innerhalb von vier Jahren hat sich die Anzahl der Verbindungen verzehnfacht", erklärt Serge Wautier, R&D Software Manager, Business Unit Ewon. Die Ewon-Remote-Data-Lösung verbindet Remote Access mit Datendiensten via IIoT-Router und Daten-Gateway der Serie Ewon Flexy. So verfügen Maschinenbauer jederzeit über die nötigen Datendienste für ihre zukünftigen oder laufenden IIoT-Projekte.

IIoT-Router und Daten-Gateway

Das Ewon Flexy, IIoT-Router und Daten-Gateway in einem, wurde speziell für Fernwartungstechniker entwickelt, die das Gerät für ihre betrieblichen Anwendungen nutzen. Es funktioniert unabhängig von jedem anderen angeschlossenen Gerät. Der Hauptzweck des Produkts besteht im Fernzugriff auf Industriemaschinen über das Internet. Dieses Konzept ermöglicht die Fehlersuche und Prüfung von Variablen sowie die Reprogrammierung der SPS, die Anzeige und Steuerung der Maschinen-HMIs über den Fernzugriff oder den Zugriff auf eine IP-Kamera zur ortsnahen Unterstützung. Darüber hinaus ermöglicht das Produkt das Erfassen von Daten der SPS. Das dient dazu, Übersichten aus den Daten zu erstellen, die entweder lokal auf dem Flexy gespeichert sind oder, bei Daten von mehreren Geräten, über eine Webportal-Plattform bereitgestellt werden. Die Daten lassen sich darüber hinaus in Edge-Computing-Anwendungen wie die Leistungsüberwachung und vorausschauende Wartung durch Drittanbieter-Produkte einspeisen.

Flexibles Gerät

Ewon Flexy ist ein modularer IIoT-Router und Daten-Gateway, der eine Vielzahl unterschiedlicher Feldschnittstellen (Ethernet, Seriell, I/O oder USB) und WAN-Konnektivität (WLAN, Mobilgeräte) über Erweiterungskarten bietet. Diese Flexibilität ermöglicht es, entfernte Geräte in einer Umgebung mit sich permanent verändernder Kommunikationstechnik zu verbinden und gleichzeitig universell mit unterschiedlichen Feldgeräten ungeachtet des verwendeten Protokolls zu kommunizieren. Das Ewon Flexy lässt sich

neben dem Fernzugriff auch zur Erfassung und Zusammenstellung von Felddaten nutzen.

Schritt 1: Verbinden mit Feldgeräten

Das Daten-Gateway ist in der Lage, sich mit einer Vielzahl unterschiedlicher Industriegeräte zu verbinden: hauptsächlich SPSen, aber auch Fern-I/Os, Messsysteme und Sensoren. Auch wenn hauptsächlich der Ethernet-Port zur Verbindung mit der SPS zum Einsatz kommt, steht für ältere SPSen ebenfalls ein serieller Anschluss zur Verfügung. Das Flexy umfasst die Kommunikationsprotokolle aller großen SPS-Marken, um die SPS-Register zu pollen. Anwender müssen lediglich das richtige SPS-Protokoll auswählen, angeben, wie Sie vorhaben, Daten in dem Gerät zu sammeln (Register, Datenblock), und die Verbindung herstellen.

Bild: HMS Industrial Networks

Das viewON-Dashboard ist über jeden Web-Browser durch das M2Web-Portal zugänglich.

Schritt 2: Daten in Tags speichern

Ein Tag ist eine Variable oder ein Register, das einen von der SPS übermittelten numerischen Wert enthält. Es wird verwendet, um die Herkunft der Daten anzugeben (Beispiele für Tag-Bezeichnungen sind 'Tankfüllstand', 'Ewon-Speicher1' oder 'Siemens_MW100'). Sobald die Felddaten in den Tags gespeichert wurden, lassen sie sich verwenden, um:

- Alarmfunktionen zu verwalten (Alarmauslösung und Alarmmitteilungen),
- Ein eigenes benutzerdefiniertes Fern-Web-Dashboard zu erstellen,
- Daten zu protokollieren (historisches Protokollieren=1.000.000 Datensätze mit Zeitstempel),
- Echtzeit- oder historische Daten auf einen zentralen Server zu übertragen (über FTP oder HTTP(S) oder über die Talk2M Data-MailBox),
- Die Tags im Modbus-TCP oder OPCUA für den lokalen SCADA-Zugriff zu veröffentlichen.

Direkt einsetzbare Monitoring-Anwendungen

Die Alarmverwaltung ist ein wesentlicher Aspekt für Maschinenbauer und Endanwender, da sie die Möglichkeit bietet, Maschinenausfallzeiten durch Verbesserung der Reaktionszeit zu reduzieren. Darüber hinaus vermeiden Alarmmitteilungen den unnötigen Zeitaufwand der Überwachung des Maschinenzustands durch die unmittelbare Übermittlung der richtigen Informationen. Die Anwendung ist unkompliziert. Für jedes erstellte Tag lassen sich Alarmmeldungen durch die Definition von Schwellenwerten oder Aktivierungsverzögerungen auslösen. Wenn der Tag-Wert einen Schwellenwert überschreitet, löst das Ewon Flexy einen Alarm aus. Es ist in der Lage, für jeden definierten Alarm Mitteilungen in Form einer E-Mail, SMS oder Datei an einen FTP-Server oder Daten über HTTP(S) zu verschicken. Mitteilungen lassen sich bei unterschiedlichen Alarmzuständen versenden: wenn jemand einen Alarm quittiert, wenn der normale Zustand wiederhergestellt wird oder wenn der Alarm endet. Um sicherzustellen, dass die versendete Mitteilung für jeden Benutzer relevant ist, ist es möglich, sie benutzerdefiniert anzupassen. Das umfasst dynamische Inhalte wie Tag-Name, Alarmzustand und Alarmstufe, Tag-Beschreibung, Zeitstempel und Wert zu diesem Zeitpunkt, Alarmmaßnahmen und Geräteinformationen.

Bild: HMS Industrial Networks

Das Ewon Flexy, IIoT-Router und Daten-Gateway in einem, wurde speziell für Fernwartungstechniker entwickelt, die das Gerät für ihre betrieblichen Anwendungen nutzen.

Software-Editor für Web-Dashboards

Das Flexy ist darüber hinaus in der Lage, Webseiten zu speichern. Auf diese Weise erhält jeder Benutzer Fernzugriff auf sein eigenes personalisiertes Web-Dashboard, das auf dem Flexy gespeichert ist und spezifische Informationen über die Maschine enthält. Das setzt allerdings die Gestaltung von Web-Dashboards voraus. Ewon hat zu diesem Zweck die kostenlose Software viewON entwickelt. Hierbei handelt es sich um einen Web-HMI-Editor, der es ermöglicht, animierte Web-Dashboards wie Produktionsübersichten, Leistungsindikatoren, Produktionszähler, Datentrenddiagramme oder Alarmanzeigen zu gestalten. Die kostenlose Software lädt die Dashboards anschließend als HTML5.0-Seiten in das Ewon Flexy hoch, sodass sie über jeden Web-Browser zugänglich sind. Darüber hinaus gibt es die Möglichkeit, das M2Web-Portal zu personalisieren, sodass Marketer die Möglichkeit haben, es an ihre Markenidentität anzupassen.

Fazit

Unkomplizierte, direkt anwendbare Lösungen, wie der Fernzugriff mit Alarmverwaltung und Web-HMI, ermöglichen Kosteneinsparungen, Reduzierungen der Maschinenausfallzeiten und bieten Endanwendern gleichzeitig nützliche Mehrwertdienste. Doch IIoT-Anwendungen wie Datentrends- oder Leistungsüberwachungs-Dashboards lassen sich ebenso einfach einrichten. ■

Autor: ***Romain Borremans,***
eWON Business Unit,
HMS Industrial Networks AB
www.hms-networks.de

Eine informationsfähige Fertigungsumgebung planen

Im Netzwerk-Fabric-Reifegradmodell werden die vier Stufen einer Netzwerk-Fabric aufgezeigt. Anhand des Modells können Hersteller sehen, wo sie heute stehen und was sie bei der Durchschreitung der verschiedenen Stufen bis zum Erreichen des Endziels noch vor sich haben.

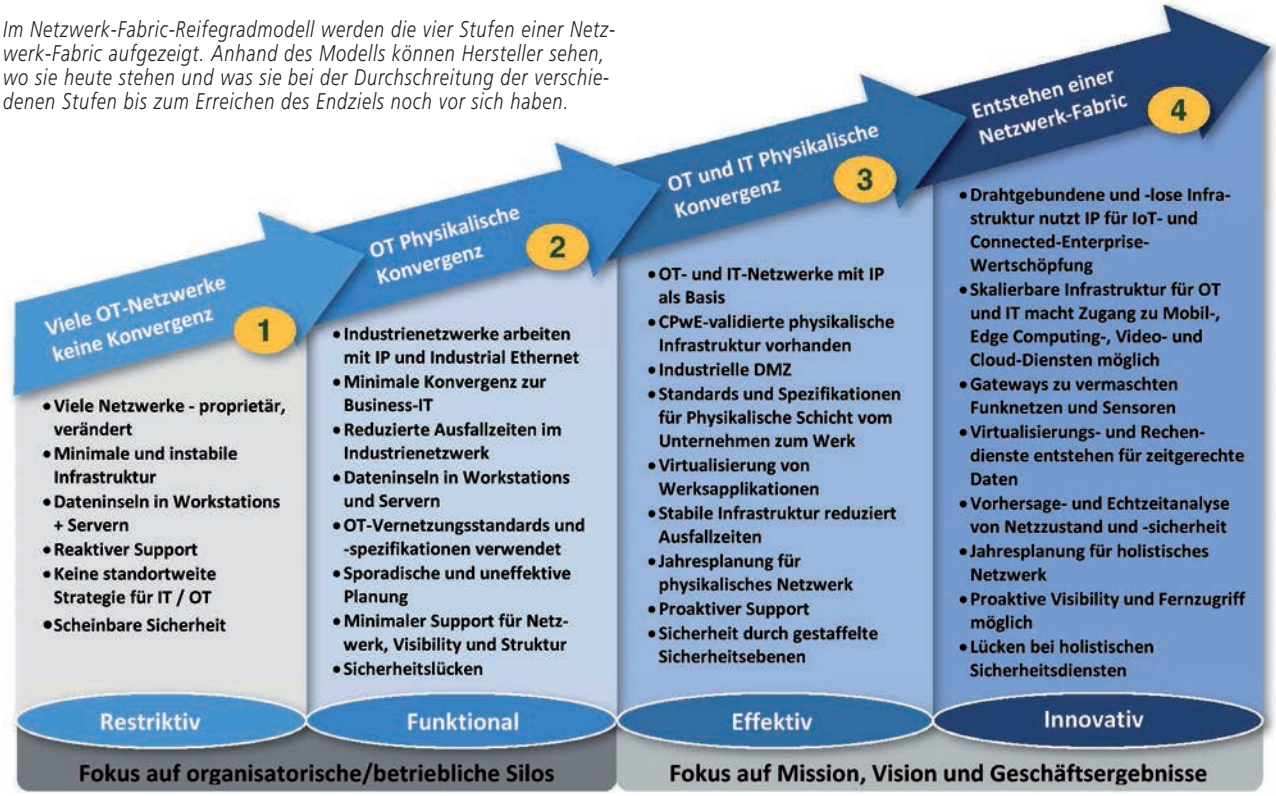


Bild: Panduit Ltd.

Das Internet der Dinge und Industrie 4.0 gestalten die Fertigungshalle neu. Durch den Einzug intelligenter Ausrüstung und vernetzter Geräte, die über ein industrielles Ethernet-Netzwerk kommunizieren können, können Hersteller die Leistungsfähigkeit ihrer Maschinen und Verfahren besser als je zuvor verstehen und nutzen. Aber bei der Vernetzung geht es nicht nur um das 'Was', sondern auch um das 'Wie'.

Durch innovative Technologien können Hersteller auf neue Art und Weise ihre Infrastruktur managen, Geräte einsetzen und Informationen teilen. Zunächst einige Beispiele :

- Mithilfe von Cloud Computing können Geräte, die auf mehrere Standorte verteilt sind, in Echtzeit und von einer zentralen Position aus fernüberwacht werden, und es können je nach betrieblichen Erfordernissen mehr Rechenleistung und Speicherplatz zur Verfügung gestellt werden.
- Durch die Virtualisierung werden Software und Hardware voneinander getrennt bzw. entkoppelt, was erhöhte Betriebszeiten der Applikation, mehr Flexibilität beim Einsatz und schnellere Upgrades ermöglicht.
- Funktechnik sorgt für mehr Flexibilität und ermöglicht das unkomplizierte Teilen von Daten, wie bei Mobilgeräten in der Werkshalle.

Unter dem Strich resultiert diese Fülle an Informationen und nahtloser Vernetzung in der Fähigkeit, Entscheidungen schneller und präziser zu fällen, was sich wiederum in verbesserter Zusammenarbeit und in neuen Möglichkeiten für die Verbesserung der Produktivität äußert. Der traditionelle Ansatz, separate Netzwerke für die Informations- und die Betriebstechnik (IT und OT) zu nutzen, behindert die nahtlose Vernetzung und ist zu einschränkend und unsicher, um eine wirkliche Option zu sein. Stattdessen fordern Hersteller eine einzelne und vereinheitlichte Netzwerkinfrastruktur, die auf eine einzige physikalische Netzwerk-Fabric aufbaut und die ganze Stärke des Internetprotokolles und Sicherheitsabwehr in der Tiefe nutzt.

Die einheitliche Netzwerk-Fabric

Eine vereinheitlichte Netzwerk-Fabric dient als physikalische Basis, auf der die vernetzten Betriebsabläufe eines Herstellers bestehen

und laufen können. Zur Fabric gehören alle Verkabelungs-, Funk-, Switching-, Rechner- und Speichersysteme und sie nutzt eine standardmäßige und unveränderte Internetprotokoll(IP)-Anbindung, um zu einem sicheren und offenen Datenaustausch beizutragen. Netzwerk-Fabric ist ein branchentypischer Begriff, der eine Netzwerktopologie beschreibt, in der Geräte Daten über verbindende Switches austauschen. Systeme für die Automatisierung von industriellen Werken entwickeln sich weg von der dedizierten Punkt-zu-Punkt-Verbindung und hin zu einer mehr Switch-basierten Auslegung. Durch die Switches und einer konvergenten Werksarchitektur können Daten jetzt nicht nur sicher durch das gesamte Werksautomationssystem geswitcht und geroutet werden, sondern auch nach 'oben' für die Schaffung von Mehrwert. Die Netzwerk-Fabric kann nicht nur als notwendiges Backbone für die Informationsarchitektur eines Herstellers dienen, sondern auch der entscheidende Faktor für den Erfolg des Herstellers sein. Gar keine oder schlechte Planung und eine reaktive Entscheidungsfindung können dazu führen, dass ein Netzwerk zu einem riesigem Wust aus Verbindungen und Switches verkommt, der für Produktionsausfälle und Sicherheitsverstöße verantwortlich ist. Daher entwerfen führende Hersteller zielgerichtet und proaktiv ihre Netzwerk-Fabric und sorgen so für mehr Betriebszeit, und letztendlich für die Erfüllung ihrer Leistungsvorgaben. Für das beste Ergebnis sollten Systemintegratoren beim Entwurf und bei der Realisierung einer Netzwerk-Fabric die fünf folgenden Schlüsselfaktoren beachten

- Skalierbarkeit: Das Wachstum der Fabrikanlagen, die Einführung neuer Techniken und die wechselnden Anforderungen an die Bandbreite in den kommenden Jahren sind schwer vorherzusagen. Die Sicherung einer wachsenden Infrastruktur und einer zukünftigen Skalierbarkeit trägt dazu bei, komplett ersetzende (Rip-and-Replace)-Upgrades zu verhindern, die Verfügbarkeit zu erhöhen und die Installationszeiten zu verkürzen.
- Zuverlässigkeit: Netzwerkausfallzeiten sind immer häufiger gleichbedeutend mit Maschinenausfallzeiten, weil immer mehr der automatisierten Produktionsprozesse auf dem Netzwerk laufen. Weil es in der Fertigungshalle auf jede Mikrosekunde ankommt, ist es wichtig, die Netzwerk-Fabric auf einer robusten Architektur aufzubauen, die Industriestandards zu befolgen und die IT/OT-Zusammenarbeit zu nutzen und zu fördern, um eine möglichst hohe Zuverlässigkeit im gesamten Werk zu erreichen.
- Sicherheit: Zu einer größeren Netzwerktransformation gehören zwangsläufig Sicherheitsbedenken. Eine Strategie der gestaffelten Sicherheitsebenen (Defence-in-Depth) ist der empfohlene Quasi-Standard der Branche, bei dem mehrere Sicherheitsmechanismen auf physikalischen, Netzwerk-, Computer-, Anwendungs- und Geräteebenen eingesetzt werden, um mehrere Abwehrfronten gegen die immer größer werdende Bedrohungslandschaft aufzubauen.
- Unkomplizierte Umsetzung: Ein gut geplanter und durchdachter Ansatz für die Netzwerk-Fabric trägt dazu bei, den Entwurf und die Realisierung zu vereinfachen, und reduziert die Wahrscheinlichkeit von Problemen bei der Inbetriebnahme oder im Betrieb. Standards und Normen wie z.B. IEC62443 und TIA-1005 und validierte Architekturen wie Converged Plantwide Ethernet (CPwE) können eingesetzt bzw. herangezogen werden, um die Netzwerk-Fabric mit größerer Sicherheit zu entwerfen. Anerkannte Verfahren und Praktiken bei der strukturierten Verkabelung und validierte integrierte Lösungen reduzieren Installationszeiten und Risiken bei der Inbetriebnahme.
- Innovation: Die Netzwerk-Fabric bietet eine Plattform für die Nutzung der neuesten Innovationen. So wird beim Power-over-Ethernet (PoE) zum Beispiel dasselbe Kabel für die Stromversorgung und Datenübertragung verwendet, was die Verdrahtungskomplexität sowie die Installations- und Wartungskosten reduziert. Ein strukturiertes Netzwerk aus drahtloser und drahtgebundener Vernetzung schafft Möglichkeiten für den Einsatz neuer Dienste, wie der Fernüberwachung und der Edge Intelligence (Rechnerkapazität auf Geräteebene) für die Zustandsüberwachung und die vorhersagende Analyse.

Ein Maturity Model für die Bewertung der Netzwerk-Fabric

Panduit hat ein Netzwerk-Fabric-Reifegradmodell (Abbildung 1) entwickelt, um Hersteller dabei zu unterstützen, den Weg zur einheitlichen Netzwerk-Fabric zu begehen. In diesem Modell werden die vier Stufen einer Netzwerk-Fabric aufgezeigt – von vielen nicht gemanagten Werksnetzwerken bis zu einer vollständig vereinheitlichten Netzwerk-Fabric. Anhand dieses Modells können Hersteller sehen, wo sie heute stehen und was sie bei der Durchschreitung der verschiedenen Stufen bis zum Erreichen des Endziels noch vor sich haben. Bei diesem Modell geht es um die Verschiebung bei industriellen Netzwerken weg vom alleinigen Fokussieren auf die betrieblichen/organisatorischen Silos der Werksautomationssysteme und hin zu einem mehr ganzheitlichen Fokus auf Mission, Vision und das gesamtheitliche Unternehmensergebnis. Auf dem Weg zu einer vollständig vereinheitlichten Stufe-4-Netzwerk-Fabric muss ein Unternehmen zuerst den Ist-Reifegrad des Netzwerks bestimmen.

Aufstieg von Restrictive (Stufe 1) auf Functional (Stufe 2)

Um die Netzwerkinfrastruktur auf die Stufe Functional zu erheben, ist ein geplanter und auf Standards/Normen aufbauender Ansatz für die Migration in den wichtigsten Bereichen erforderlich. Zuerst muss die Werkshallenumgebung erfasst und verstanden werden. Danach müssen die Übertragungsmedien, Erdungs- und Vernetzungslösungen im Hinblick auf die Anforderungen in der Fertigung spezifiziert werden. Schließlich gilt es, Sicherheitslöcher, die häufig in Netzwerkarchitekturen der Stufe Restriktive gefunden werden, zu schließen, was die Implementierung einer physikalischen Sicherheitsbasis erfordert.

Aufstieg von Functional (Stufe 2) zu Effective (Stufe 3)

Um die Netzwerkarchitektur-Stufe Effective zu erreichen, sind Referenzarchitekturen und Best Practices unerlässlich. Hier sollten Referenzarchitekturen wie CPwE von Cisco und Rockwell Automation und der Physical Infrastructure Reference Architecture Guide von Panduit genutzt werden, um ein robusteres und auf Industriestandards aufbauendes Netzwerk aufzubauen. Die Übertragungsmedien müssen so spezifiziert werden, dass sie auch für steigende Daten- und Vernetzungsanforderungen ausgelegt sind. Billige Unmanaged Switches in Plug-and-Play-Technik sind durch

Das Mikro-Rechenzentrum (MDC) dient als Verbindungsstelle zwischen Unternehmensnetzen und industriellen Netzwerken und besitzt folgende Aufgaben: Hohe Netzwerklaufzeiten gewährleisten, Trennung von Netzwerken ermöglichen, Netzwerksicherheit überwachen, Systemänderungen sowie Fehlersuche- und -behebung beschleunigen und eine einfache Installation gewährleisten.

Bild: Panduit Ltd.

Managed Switches zu ersetzen, um die Netzwerküberwachung und das Traffic Management zu verbessern. LWL- und 10GB-Kupferkabel bieten hohe Leistung und hoch verfügbare Vernetzung, wobei deutlich gekennzeichnete und farblich oder mechanisch codierte Stecker dazu beitragen, Fehlsteckungen und -anbindungen zu vermeiden. Hier sollten vorkonfigurierte und auf Industriestandards aufsetzende Netzwerkbausteine verwendet werden, um Risiken und Installationszeiten zu reduzieren.

Mögliche Lösungen:

- Das vorkonfigurierte Micro Data Center (MDC) von Panduit kann eine vollständige Datenzentruminfrastruktur in einem einzigen Rack aufnehmen.
- Durch vereinte Technik von Panduit, Cisco und Rockwell Automation wird das Industrial Data Center (IDC) zu einer Virtualisierungsinfrastruktur, in der Hardware, Software und Dokumentation in einer vormontierten, vorkonfigurierten und gebündelten Lösung kombiniert sind.
- Mithilfe der Panduit Network Zone Systems kann ein IP-Netzwerk in der Fertigungshalle über einen zuverlässigen und strukturierten Ansatz in kürzester Zeit aufgebaut werden, der Installationszeiten und Lebenszykluskosten reduziert. Um den Netzwerkaufbau zu beschleunigen und gefährliche Spannungen zu isolieren, gehören zu allen Systemen die Anbindung über Kupfer oder Glasfaser, das Kabelmanagement, die Erdung und ein patentierter Überspannungsschutz.
- Mit dem vorkonfigurierten Industrial Distribution Frame (IDF) von Panduit lassen sich industrielle rackmontierte Ethernet-Switches um 25 Prozent schneller als nicht vorkonfigurierte IDFs installieren, wodurch die Gefahr von Ausfallzeiten durch Überhitzung des Switches reduziert wird.

Entwicklung von Effective zu Innovative – Stufe 3 auf Stufe 4

Eine Netzwerkarchitektur der Stufe Innovative zeichnet sich durch ein konvergiertes IT/OT-Netzwerk aus, das neue Möglichkeiten für die Erfassung und Nutzung von Daten im gesamten Fertigungsunternehmen bietet. Wenn die Infrastruktur für den Fernzugriff ausgelegt wird, können Fachtechniker die Geräte von überall aus überwachen und auf diese zugreifen. Durch Mobiltechnik können die Vorgänge in der Werkshalle überall sichtbar gemacht werden, sei es auf dem Werksgelände oder an anderen Standorten weltweit. So können Zusammenhänge schneller erkannt, Entscheidungen schneller getroffen und Abhilfemaßnahmen schneller durchgeführt werden. Modernere Ansätze arbeiten mit Dashboards und vorhersagenden Analysen, die dazu beitragen, Netzwerkprobleme bereits in der Entstehung zu vermeiden, bevor sie zu Ausfallzeiten führen. Hier können Cloud Computing, Fog Computing, Gateways und vermaschte Funknetze eingesetzt werden.

Zusammenfassung

Die zukünftige Wettbewerbsfähigkeit fast aller fertigenden Unternehmen hängt davon ab, wie schnell sie das Konvergenzkonzept und die entsprechenden IP-Technologien für sich umsetzen können. Eine vereinheitlichte und auf den IP-Standard aufbauende Netzwerk-Fabric mit starker physikalischer Infrastruktur wird als Basis der Informations- und Vernetzungsanforderungen von morgen dienen und es ermöglichen, konvergierende Netzwerke robuster, transparenter und zuverlässiger auszulegen. Der Einsatz von Reifegradmodellen kann sowohl die OT- als auch IT-Abteilung dabei unterstützen, den Fortschritt in Richtung effektiverer und innovativerer Netzwerke zu beschleunigen, mit denen die vielversprechenden Möglichkeiten des Internets der Dinge und Industrie 4.0 realisiert werden können. ■

Autor: ***Dan McGrath,***
Product Line Manager,
Panduit Ltd.
www.panduit.com

Drahtlos Daten-Inseln erobern

Mit Funkmodulen die Herausforderungen des IIoT meistern, blinde Flecke beseitigen und Inbetriebnahmezeit einsparen

Bild: Advantech Europe BV

Das Industrial Internet of Things (IIoT) ist die Zukunft der Produktion und steht vor einem enormen Wachstum. Bis ins Jahr 2020 steigt laut seriösen Prognosen die Anzahl der weltweiten Smart Objects von 6 Milliarden auf 50 Milliarden Objekte. Diese Entwicklung stellt die Industrie vor große Herausforderungen, um das Ziel des IIoT – effektive, schnelle und sichere Prozesse in der Fertigung aber auch im Warenfluss – zu erreichen. Drahtlose I/O-Module sind eine zuverlässige Möglichkeit, Daten auf der Feldebene zu erfassen.

Smart Objects sind nichts anderes als vernetzte Maschinen oder Sensoren. Auf dem Weg zu effektiven Prozessen in der Fertigung ist es unabdingbar, die klassische Automatisierungspyramide zu durchbrechen. Diese besteht üblicherweise aus verschiedenen und voneinander getrennten Ebenen: der Feldebene (I/O-Module), der Steuerung (SPS), der Prozessleitebene (SCADA), der Betriebsebene (MES) und der Unternehmensleitebene (ERP). Grundvoraussetzung für IIoT ist ein Datenfluss durch und zwischen allen Ebenen der Automatisierungspyramide anstatt eines Datenflusses in nur einer Ebene. Prozessdaten, wie beispielsweise Mess- oder Positionierungsdaten werden heute schon erfasst und direkt an der Maschine in Form von Displays oder Warnleuchten ausgegeben. Durch die Vernetzung der Maschinen werden diese ermittelten Daten zusätzlich durch die Automatisierungspyramide hindurch verarbeitet und final im ERP-System oder in der Cloud zugänglich gemacht. Aufgrund des zu erwartenden Wachstums besteht die Herausforderung in der Schaffung skalierbarer und ökonomischer Systeme, um die vorhandenen Maschinen und Sensoren zu vernetzen. Besonders drahtlose I/O-Module bieten hier große Vorteile durch verkürzte Inbetriebnahme, geringere Kosten und hohe Flexibilität.

Verkürzte Inbetriebnahme

Hauptargument für eine verkürzte Inbetriebnahme ist die stark reduzierte Infrastruktur. Eine Verlegung von Datenkabeln ist nicht nötig. Alleine dieser Aspekt reduziert die Inbetriebnahme enorm. Selbstverständlich sind drahtlose I/O-Module nicht komplett kabellos. Die Energieversorgung des I/O-Modules erfolgt in der Regel über ein Netzkabel. Da es sich bei der Anbindung in der Regel um Maschinen oder Sensoren handelt, die ebenfalls Energie über Stromnetze beziehen, ist lokal die Energieversorgung bereits vorhanden. Gemäß dem Fall, dass für spezielle Anwendungen keine Energieversorgung über ein Stromnetz vorliegt oder eine Verlegung zu kostenintensiv ist, bietet das Wise-4050 I/O-Modul von Advantech eine Micro-USB-Schnittstelle zur Leistungsaufnahme an. Zusätzlich ist eine Versorgung über Akku möglich, da drahtlose I/O-Module für einen geringen Leistungsverbrauch konzipiert sind.

Plug&Acquire

Die Unabhängigkeit von Datenkabeln und Power Supply ermöglicht dem Anwender eine flexible Konzeption. Diese Flexibilität fügt sich in das modulare Industrie-Anlagenkonzept Plug & Produce ein. Plug & Produce basiert auf verkürzter Inbetriebnahme, Kostenvorteilen und mehr Flexibilität durch höhere Kompetenz der eingesetzten Komponenten. Module werden nach benötigter Produktionskapazität eingebunden oder entfernt – sinngemäß ein Plug & Acquire. Drahtlose I/O-Module zur Datenerfassung sind wie gemacht für dieses Anlagenkonzept.

Drahtlos die Daten-Inseln erobern

Die Vernetzung von 50 Milliarden Smart Objects in kurzer Zeit ist eine immense Aufgabe. Viele bestehende Maschinen und Sys-

teme in der Industrie sind als 'Daten-Insellösungen' konzipiert. Die Herausforderung bei der Vernetzung besteht in der Vermeidung von Störungen bei den Datenerfassungen durch I/O-Module. In der Praxis können beispielsweise Stromtransmitter zur Übermittlung des Energieverbrauchs der Maschine hinzugefügt werden. Bei analogen Signalen bestehender Daten-Insellösungen wie beispielsweise Temperatursendern hilft die Installation von Signal-Isolatoren zur Digitalisierung und schlussendlich Übertragung der Daten mittels I/O-Module ohne Beeinträchtigungen des Systems bzw. der Maschine.

Akzeptanz und Verbreitung drahtloser Netzwerke

Die allgemeine Verbreitung und Akzeptanz von drahtlosen Technologien durch beispielsweise Smartphones oder Tablets hilft unterstützend bei der Implementierung drahtloser I/O-Module. Protokolle wie WiFi und Bluetooth sind weit verbreitet, aber auch industriespezifische Protokolle wie beispielsweise WirelessHart, ISA100.11a, Zigbee und Z-Wave sind einem weiten Anwenderkreis bekannt. Viele drahtlose IIoT-Protokolle basieren auf WiFi-Technologien oder weisen große Ähnlichkeiten zu kommerziellen drahtlosen Systemen auf.

Überwachung mit und ohne Kontrolle

Zum gegenwärtigen Zeitpunkt liegt der Fokus von drahtlosen I/O-Modulen mehr auf der Datenerfassung sowie -übertragung, nicht auf der Steuerung der jeweiligen Maschinen sowie Sensoren. Dabei ist dies technisch durchaus möglich, jedoch gibt es berechtigte Zweifel, ob drahtlose Technologien dafür zum jetzigen Zeitpunkt die geeignete Wahl sind. Im Gegensatz zu kabelgebundenen Systemen sind sie störungsanfälliger. Der Verlust von Statusinformationen der Maschine aufgrund von Verbindungsstörungen ist kalkulierbar und akzeptabel, der totale Kontrollverlust über die Maschine hingegen nicht!

Verringerte Risiken

Die Flexibilität, verkürzte Inbetriebnahme und Usability ändern die Voraussetzungen bei der Datenerfassung enorm. Die Zeit vom Konzept bis hin zur finalen Realisierung von Projekten mit drahtlosen I/O-Modulen verkürzt sich signifikant. Anwender können schnell und einfach auf der Feldebene Daten erfassen und zur Analyse übertragen. Zusätzlich reduzieren sich die Auswirkungen für falsche Entscheidungen. Anpassungen oder auch Erweiterungen sind mit geringem Aufwand möglich. Fehler fallen nicht schwer ins Gewicht und lassen sich leichter und unkomplizierter beheben als mit kabelgebundenen Systemen.

Bild: Advantech Europe BV

Drahtlose I/O-Module können verschiedene Input-Signale erkennen und diese in drahtlose Ausgangssignale umwandeln.

Bild: Advantech Europe BV

Maschinen lassen sich nachträglich mit drahtlosen I/O-Modulen ausstatten, um sie in die IoT-Welt zu bringen. Dies ermöglicht die schnelle und einfache Überwachung über jedes mobile Web-gebundene Gerät.

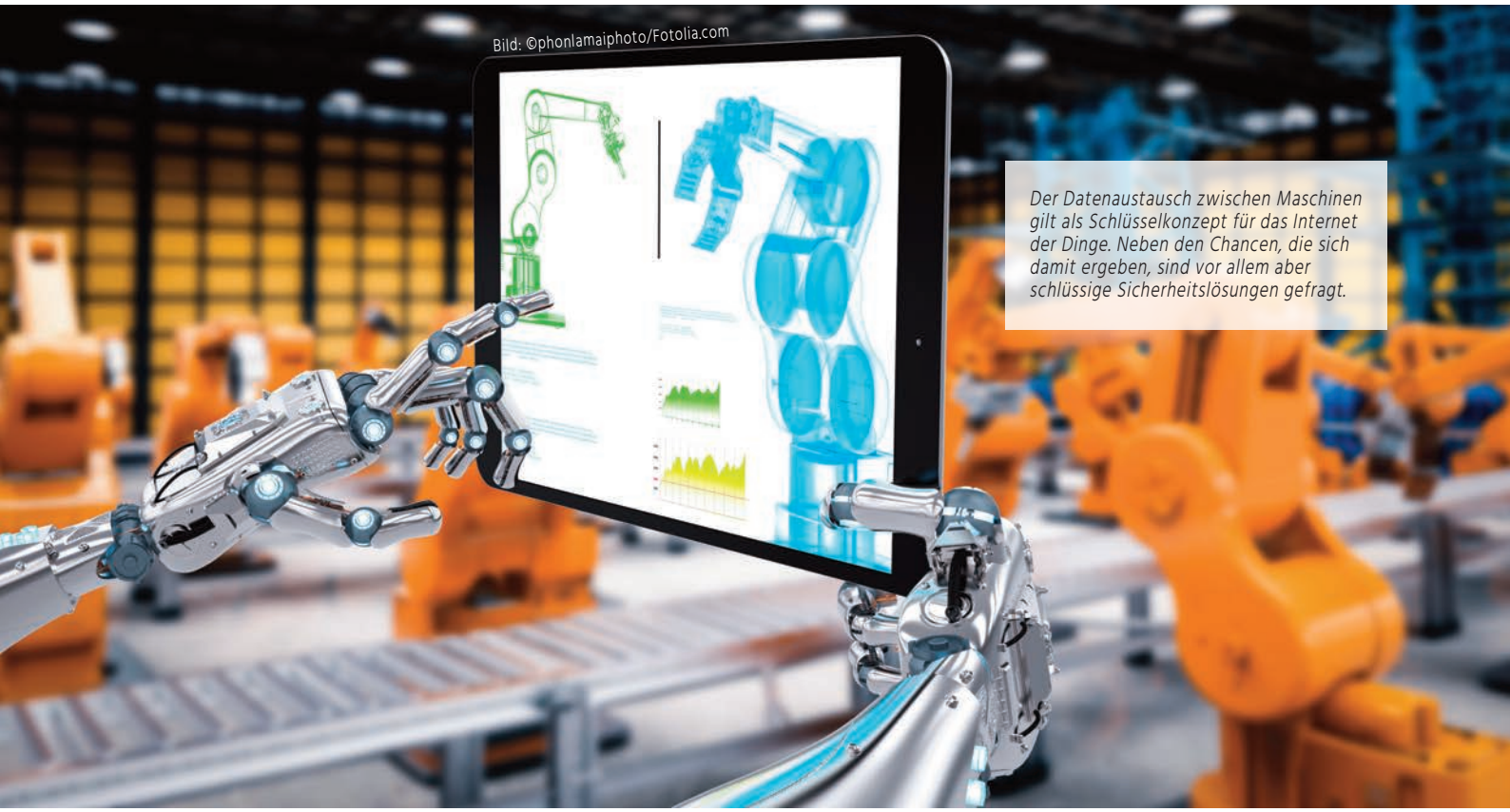
Browserbasierte Darstellung

Nicht nur die Datenerfassung, sondern auch das Auslesen der Daten ist aufgrund der drahtlosen Technologie vorteilhaft. Im Unterschied zu kabelgebundenen Strukturen ermöglichen drahtlose Architekturen einfachere Darstellungsmethoden der erworbenen Daten. Die Kommunikation der I/O-Module mit HMI aber auch mit Smartphones, Tablets oder anderen browserfähigen Devices wird durch WiFi oder Bluetooth unterstützt. Software wie beispielsweise WebAccess HMI bereiten Daten in Grafiken auf. Dabei ist es möglich, Daten von unterschiedlichen Quellen einzubeziehen.

Drahtloser Game Changer

Bedienbarkeit, Flexibilität und eine kurze sowie einfache Inbetriebnahme machen drahtlose I/O-Module zu einem Game Changer in der Datenerfassung der Feldebene. Verringerte Risiken sowie Plug&Acquire ermutigen Datenarchitekten, neue Wege zu gehen. ■

Autor: **Stephan Kopka,**
Industrial IoT Marketing DACH,
Advantech Europe B.V.
www.advantech.de



Der Datenaustausch zwischen Maschinen gilt als Schlüsselkonzept für das Internet der Dinge. Neben den Chancen, die sich damit ergeben, sind vor allem aber schlüssige Sicherheitslösungen gefragt.

Gefahren, Lösungen, Visionen

Die Identität für ein sicheres IoT

Der Datenaustausch zwischen Maschinen (M2M) ist ein Schlüsselkonzept für das Industrielle Internet der Dinge. Wesentlich für die erfolgreiche und vor allem sichere Vernetzung weltweit verteilter Systeme sind die Etablierung und Nutzung von geeigneten Standards sowie der Aufbau eines gemeinsam nutzbaren Vertrauensankers.

Sobald ein Unternehmen die Sprünge von der Mechanisierung, Elektrifizierung und Digitalisierung geschafft hat, steht mit dem nächsten Schritt der industriellen Revolution die Internetanbindung und Hochkonnektivität der cyber-physischen Systeme an. Dabei entsteht für Unternehmen die Herausforderung, ihre vormals gekapselten Systeme hin zu einem offenen System weiterzuentwickeln und abzusichern. Hierfür ist eine grundlegende Auseinandersetzung mit dem Thema IT-Sicherheit notwendig, die Antworten auf folgende Fragen geben muss:

- Darf Maschine MA von Unternehmen A Ware bei Maschine MB im Unternehmen B auf der anderen Seite der Welt rechtskräftig bestellen?
- Wie kann sichergestellt werden, dass Maschine MA mit Maschine MB von Unternehmen B kommuniziert und nicht jemand anders?
- Wie stelle ich eindeutige Maschinenidentitäten her und wie sichert man diese ab?
- Wie stellt man Vertrauenswürdigkeit her und welches Vertrauensniveau wird benötig? (LoA – Level of Assurance)
- Wie kann ich die Integrität der Daten während der Übertragung sicherstellen?
- Wie können die unterschiedlichen Architekturen in den Unternehmen, Maschinenparks (Technologien, Software und Hardware) und unterschiedlicher Performance-Kriterien (Limitierungen) umsetzen?

Sicherheit mittels Identität

Um die Sicherheitsherausforderungen des IoT und von Industrie 4.0 zu meistern, ist der Einsatz von eindeutigen Identitäten und Kryptographie unabdingbar. Damit Maschine MA von Unterneh-

Bild: ©vectorfusionart/Fotolia.com

Ein erster Ansatz zur vertrauenswürdigen Einbindung der IoT-Geräte und -Maschinen in das Netzwerk ist es, standardisiert Identitäten an die Devices zu vergeben.

men A neue Rohware bei Maschine MB im Unternehmen B bestellen darf oder andere Aktionen anfordern kann, bedarf es zunächst der Schaffung von Rahmenbedingungen. So ist beispielsweise sicherzustellen, dass eine vertrauenswürdige Einbindung der IoT-Geräte beziehungsweise der Maschinen in das jeweilige Unternehmensnetzwerk vorhanden ist – was nur mittels einer eindeutigen Identität möglich ist. Ein praktikabler Ansatz zur Realisierung dieser Grundvoraussetzung entsteht aus der standardisierten Vergabe von Identitäten an alle IoT-Geräte und -Maschinen – ähnlich den Standardprozessen zur Zuordnung digitaler Identitäten bei der Einstellung neuer Mitarbeiter. Erst die Vergabe eindeutiger Identitäten stellt beispielsweise sicher, dass nur bekannte (Maschinen-)Identitäten aus Unternehmen A überhaupt Anfragen beim Unternehmen B stellen. B muss sich dann auf die sichere Identitätsprüfung innerhalb der Domäne von A verlassen – eine klassische Vertrauensbeziehung wie sie in der IT seit Jahren erfolgreich mit Hilfe des Protokolls SAML 2.0 (Security Assertion Markup Language) etabliert wurde. Hierfür muss der bevorzugte Identitätsanbieter – in diesem Fall das Maschinenverzeichnis bei A – eine Vertrauensbeziehung zum Service-Provider aufbauen und nutzen.

Unternehmensübergreifende Sicherheit

Für den sicheren, auch über die Grenzen unterschiedlicher, teils stark beschränkter Architekturen hinausgehenden Datenaustausch, bedarf es eines ganzheitlichen Lösungsansatzes. Zwischen den Beteiligten sollte darum eine Einigung über die zu verwendenden Schnittstellen (API – Application Programming Interfaces) erzielt werden, damit Anpassungen schnell und praktikabel umsetzbar bleiben. Die Komplexität der bisherigen Schnittstellen für den Elektronischen Datenaustausch (EDI) und deren langwierige Versionsplanung sind den Anforderungen des IoT schlicht weg nicht gewachsen. Da die Verwendung der gemeinsamen Sprache für IoT-Devices und Maschinen aus Sicherheitsaspekten zudem häufig nicht ausreicht, müssen die Geräte auch in der Lage sein, mit cryptografischen Credentials umzugehen und eine verschlüsselte Kommunikation aufzubauen. Hierfür raten Experten, etwa die Firma Accessec, zum Einsatz von Prüfsummen und Zertifikaten. Hierbei sind etablierte Standards und Protokolle für die Authentifizierung der Teilnehmer sowie die Verschlüsselung und Signatur von Daten anzuwenden, da diese bereits von Experten geprüft und validiert wurden. Der Einsatz von fortschrittlichen Algorithmen und sicherem Schlüsselmaterial in Applikationen, Apps und IoT-Geräten ist in der Praxis jedoch nicht unproblematisch, insbesondere unter dem Gesichtspunkt der limitierten Geräte (Constrained Devices), die nur bedingt CPU-Leistung, Speicher und Batterie bieten. Für den sicheren Einsatz von IoT-Geräten muss über die zuvor beschriebene Prozedur die Zugehörigkeit des Endgerätes bestimmt werden (ist das Gerät im entsprechenden Kontext zugelassen), um eine Sicherheitseinstufung für die entstehende Verbindung zu ermöglichen und die jeweils erlaubten Aktionen zu bestimmen. Die Informationen können dabei über die physikalische Schicht, über die Transportschicht mit Meldungsprotokollen MQTT oder CoAP und schließlich über die Applikationsschicht ausgeliefert werden, wo schließlich auch digitale Signaturen, Message-Authentication-Codes, Sicherheitszertifikate, et cetera anwendbar sind. Dabei weisen die Protokolle MQTT oder CoAP für die M2M-Kommunikation jeweils Vor- und Nachteile auf, die abhängig vom Einsatz der jeweiligen Geräte und Applikatonen abgewägt werden müssen.

Zuverlässige Sicherheitsinfrastruktur

Die Kommunikation zwischen Maschinen wird in Zukunft eine große Rolle spielen. Eine wirksame Absicherung einer weltweiten Kommunikation im Unternehmensnetzwerk kann nur über eine eindeutige Identität der Geräte, einer Authentifizierung und Autorisierung über den Einsatz von Algorithmen und einer gemeinsamen Sprache erfolgen. Dabei ist die Einbettung der Geräteidentitäten in das Unternehmensnetzwerk, die Vergabe entsprechender Zertifikate, so wie der einhergehende Aufbau einer entsprechenden Sicherheitsinfrastruktur notwendig, um im IoT-Umfeld Einfluss auf die (externen) IoT-Geräte zu haben und die notwendige Kontrolle auf diese ausüben zu können. ■

Autor: ***Sebastian Rohr,***
Technischer Geschäftsführer,
Accessec GmbH
www.accessec.com

Autor: ***Markus Soppa,***
Research Consultant,
Accessec GmbH
www.accessec.com

- Anzeige -

Einblick ins Microsoft Cybercrime Center, Redmond (USA)

Bild: Microsoft

Unternehmenskritische Sicherheitsvorfälle schneller erkennen und neutralisieren

Der Wächter vor dem Tor genügt nicht mehr

Cyberattacken richten sich immer öfter auch an Industrieunternehmen. Doch obwohl ein erfolgreicher Angriff oft nur wenige Minuten dauert, benötigt der Betreiber hingegen meist viele Monate, um den Einbruch zu erkennen und das Problem zu lösen. Entsprechend bedarf es mehr Augenmerk auf wirkungsvolle Maßnahmen und Strategien für die Zeit unmittelbar nach dem Angriff. Nachdem der erste Teil des Artikels im INDUSTRIAL COMMUNICATION JOURNAL 1/2017 die industriellen Voraussetzungen und Anforderungen beleuchtet hat, geht der folgende Teil 2 konkret auf Post-Breach-Möglichkeiten und entsprechende Sicherheitsstrategien ein.

Neue Formen der Bedrohung erfordern eine neue Art der Verteidigung. Bis dato setzen Unternehmen in allen Branchen vorrangig auf Schutzmechanismen wie Firewalls und Anti-Viren- bzw. Malware-Lösungen zum Schutz vor Angriffen. Diese agieren als Wächter; sie prüfen eingehende Dateien und den Arbeitsspeicher auf schädliche Inhalte und blockieren sie. Aber egal, wie gut die Verteidigungsstrategie auch aufgebaut ist: Da Hacker heute häufig über umfangreiche Finanzmittel sowie Spezialwissen verfügen, finden sie früher oder später einen Weg. So nahmen zum Beispiel Attacken auf große Unternehmen von 2014 auf 2015 um 40 Prozent zu. Kundendaten und geistiges Eigentum sind dabei die vorrangigen Ziele der Angreifer, die oft gar keine Malware benutzen, sondern sich über Social-Engineering-Verfahren (wie beispielsweise Phishing) Zugriff und Berechtigungen über die ahnungslosen Nutzer verschaffen. War ein Hacker erfolgreich und hat sich Zugang zum System verschafft, muss er zunächst verschiedene, zeitintensive Aktivitäten durchführen: Das Netzwerk erkunden und nach wertvollen Elementen durchsuchen, Informationen abgreifen und Maßnahmen zur Verschleierung treffen. Damit das System in der Lage ist, einen solch versteckten Überfall schnell zu registrieren, muss die Abwehr tief in der Infrastruktur selbst – in Prozessen und Endpunkten – verankert sein. Dieser Denkansatz hat die Entwicklung von Windows 10 geprägt und zahlreiche Pre- und Post-Breach-Features hervorgebracht. Dazu zählen Windows Device Guard, Credential Guard, Windows Information Protection und Windows Defender Advanced Threat Protection.

Analyseschlagkraft gegen Cybereindringlinge

Seit dem Anniversary Update von Windows 10 im August 2016 steht Unternehmenskunden der Service Defender Advan-

Im Cyber Crime Center auf dem Campus des Firmengeländes in Redmond (USA) laufen die Fäden der weltweit agierenden Digital Crimes Unit (DCU) zusammen, bestehend aus weit über 100 IT-Experten, Kriminalbeamten und Anwälten in 30 verschiedenen Ländern. Sie alle gehen gemeinsam mithilfe modernster Technologien und in Kooperation mit Hochschulen, Industriepartnern, NGOs sowie Strafverfolgungsbehörden wie der Polizei und dem FBI gegen organisierte Online-Kriminalität vor.

Bild: Microsoft

Kampfplatz gegen Eindringlinge: Microsoft Malware Labor

ced Threat Protection (Defender ATP) zur Verfügung. Dabei handelt es sich um ein integriertes cloudbasiertes Analyse-Tool, das auf Basis von Machine-Learning-Prozessen Bedrohungen aufspürt, die bereits andere Sicherheitsmaßnahmen durchbrochen haben. Mit Hilfe sensibler Analysen ermöglicht es der Service, komplexe Cyberangriffe im Netz schneller zu erkennen, zu untersuchen und zu beseitigen. Die Lösung setzt sich aus drei Elementen zusammen: Erstens aus sensiblen Endpunkt-Sensoren, die tief in das Betriebssystem eingebettet detailliert protokollieren, was auf dem Computer passiert und Metadaten dieser Informationen an den kundeneigenen, isolierten Cloudspeicherplatz senden. Zweitens, einem cloudbasierten Sicherheitsanalyse-Tool, das die Signale mit Hilfe von Big Data, selbstlernenden Algorithmen sowie einer ganzen Reihe Windows-eigener Anti-Malware-Tools auf auffällige Verhaltensmuster hin auswertet. Hat das Tool eine Bedrohung aufgespürt, löst es Alarm aus und gibt Handlungsempfehlungen für die konkrete Reaktion auf die potentiell bestehende Bedrohung. Und drittens, umfassendem Cyber-Defense-Fachwissen der Microsoft-Experten wie z.B. der Digital Crime Unit oder der Enterprise Cybersecurity Group. Dazu kommen Erkenntnisse aus täglich rund 1Mio. identifizierter Schaddokumenten sowie die Analyse von rund 600.000 Microsoft-eigenen Endpunkten und fortlaufende Informationen aus Cloud-Services wie Office 365, Azure oder Bing. Windows Defender ATP profitiert von diesem geballten Informations-Pool über Cyberangriffe und kann diese dadurch sehr schnell identifizieren und Alarm auslösen, sobald entsprechende Muster im System auftreten.

Mit Virtualisierungstechnik Schadsoftware isolieren

Die meisten Cyberangriffe – 90 Prozent – nutzen mittlerweile Hyperlinks, um sich Zugang zu Unternehmensnetzen zu verschaffen. Eine beliebte Vorgehensweise sind E-Mails, die aussehen, als kämen sie von Mitarbeitern und per Hyperlink auf ein wichtiges Dokument hinweisen. Hinter dem Link steckt allerdings eine Website, über die sich die Schadsoftware auf dem jeweiligen lokalen PC installiert und von dort aus das gesamte Netzwerk ins Visier nimmt. Mithilfe ausgeklügelter Virtualisierungstechnik hindert Windows Defender Application Guard in Kombination mit dem Browser Microsoft Edge Angreifer daran, sich auf einem Endpunkt festzusetzen und von dort aus das Netzwerk zu infiltrieren. Surft ein Mitarbeiter auf einer als unbekannt eingestuften Website bzw. klickt auf einen Link dorthin, dann isoliert Windows Defender Application Guard die Website in einem temporären, komplett isolierten Container auf der Hardwareebene – inklusive einer Kopie des Betriebssystemkernels sowie aller Services, die für die Nutzung des Browsers nötig sind. Im Vergleich zu reinen Software-Containerboxen sorgt der hardwarebasierte Ansatz für einen noch höheren Isolierungsgrad. Die Kopie erhält keinerlei Zugang zu Anwendungen, Datenspeichern oder Zugangsdaten, ist dabei aber vollständig funktionsfähig. Der User kann also ungestört weiterarbeiten, egal ob beim Surf-Vorgang ein Sicherheitsfall vorliegt oder nicht. Der virtuelle Container wird nach jedem Surf-Vorgang entsorgt und für den nächsten Klick auf eine unbekannte Website wird ein neuer erstellt. Im Fall eines tatsächlichen Angriffs befindet sich im Container eine Umgebung ohne interessante Daten oder Zugänge – die Schadsoftware kann kein Unheil anrichten. Ist der Surf-Vorgang beendet, wird sie mit dem isolierten Container entsorgt und hat somit keine Chance, sich auf dem lokalen Endpunkt festzusetzen oder sich von dort aus ins Netzwerk zu verbreiten.

Folgekosten eines Angriffs reduzieren

Wie wichtig schnelle, leistungsstarke Post-Breach-Funktionen sind, zeigen folgende Zahlen: Im Schnitt benötigt ein Unternehmen derzeit noch mehr als 200 Tage, um einen Sicherheitsvorfall zu entdecken. Danach dauert es oft nochmals bis zu 80 Tagen, bis der Schaden vollständig behoben ist. Viel Zeit also, um Daten zu entwenden und im Unternehmensnetzwerk großen Schaden anzurichten. In der Folge sind diese Angriffe sehr kostenintensiv und haben oft weitreichende negative Folgen – auch für das Image eines Unternehmens. Der Verlust an Reputation in Folge eines derartigen Einbruchs kann sich als größter finanzieller Posten im Nachgang erweisen und sogar die Unternehmensexistenz bedrohen. Die internationale Risk-Value-Studie von NTT Com Security beziffert die Kosten zur

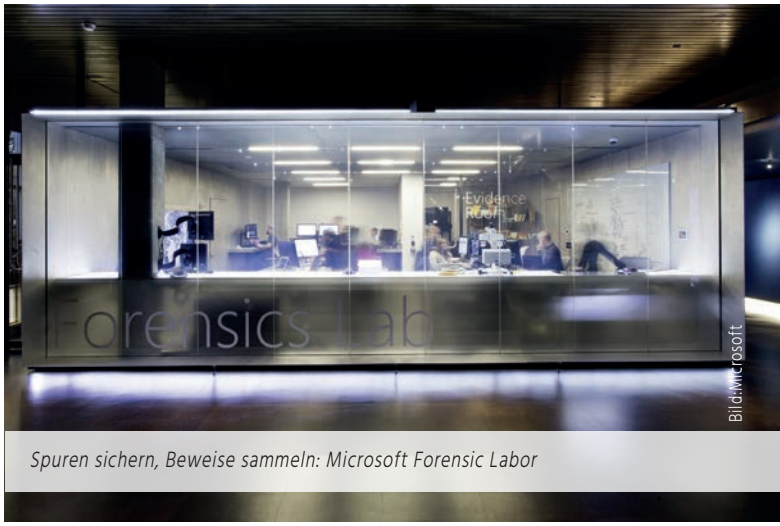


Bild: Microsoft

Spuren sichern, Beweise sammeln: Microsoft Forensic Labor

Bild: Microsoft

Zum Anniversary gab es zahlreiche Updates, die mehr Sicherheit versprechen.

Behebung der Schäden bei großen Konzernen im Jahr 2015 durchschnittlich auf über 800.000€. Laut einer SANS-Studie aus dem gleichen Jahr zeigen sich die finanziellen Auswirkungen eines erfolgreichen Angriffs oft erst Monate bis Jahre danach. 40 Prozent der betroffenen Unternehmen verzeichneten die spürbarsten finanziellen Auswirkungen zwölf Monate später – vor allem anhand von ungeplanten Kosten für Datenrückgewinnung und Forensik (57 Prozent). Dennoch haben nach aktuellem Stand nicht einmal fünfzig Prozent aller Unternehmen Versicherungen für IT-Security und Cyber-Risks abgeschlossen. Derzeit bewegt sich das Segment in Deutschland mit rund 10Mio€. Prämienvolumen pro Jahr auf äußerst niedrigem Niveau. Weltweit wird der Cyberpolicen-Markt auf 3Mrd.US$ geschätzt, wovon die USA alleine zwei Drittel der Summe auf sich vereinen.

Schaden vom Unternehmen abwenden

Waren noch vor wenigen Jahren ausschließlich Großkonzerne und nur bestimmte Industrien im Visier von Hackern und Datendieben, kann es mittlerweile jede Unternehmensgröße in jeder Branche treffen. Der Global Threat Intelligence Report (GTIR) von 2016 verzeichnet für das Jahr 2015 beachtliche 6,2Mrd. Sicherheitsangriffe gegen Firmen und staatliche Institutionen. Während die Wahrnehmung für dieses Thema in den Unternehmen und der allgemeinen Öffentlichkeit deutlich gestiegen ist, sind laut GTIR allerdings 77 Prozent aller Unternehmen noch immer nicht ausreichend auf derartige Angriffe vorbereitet. Gerade in der Fertigungsindustrie und besonders bei mittelständischen Unternehmen ist es heute eine Überlebensnotwendigkeit, Security als ein umfassendes Konzept zu planen, umzusetzen, zu monitoren und immer wieder auf den aktuellsten Stand zu bringen. ■

Autor: ***Milad Aslaner,***
Senior Product Manager,
Microsoft Deutschland
www.microsoft.de

Praxisbericht: Umsetzung der Kritis-Verordnung

Noch ausbaufähig

Das IT-SiG (IT-Sicherheitsgesetz) ist weitestgehend definiert. Im Mai 2016 ist der erste Teil der Verordnung für kritische Infrastrukturen (KRITIS) in Kraft getreten. Betroffen sind Unternehmen aus Energie, Informationstechnik, Telekommunikation, Wasser sowie Ernährung. Der zweite Teil — für die Sektoren Finanzen, Transport, Verkehr und Gesundheit — wird in Kürze erwartet. Mit der Umsetzung wurde bereits begonnen. Wie die ersten Praxisberichte zeigen, geht das kleinen wie großen Betrieben nicht allzu leicht von der Hand.


Bild: Data Center Group

DNA der Gesellschaft: Im Rahmen des IT-Sicherheitsgesetzes werden Betreiber sogenannter kritischer Infrastrukturen wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet, ihre Netze vor Hacker-Angriffen zu schützen.

Denn eine zentrale Forderung ist es, ein ISMS (Informationssicherheits-Managementsystem) umzusetzen und nachzuweisen. Über alle Sicherheitsbereiche hinweg wird dabei eines deutlich: Die Sicherheit in der Gebäudetechnik, also der Teil des Anforderungskatalogs, der sowohl vergleichs-

weise klein in der ISO27001 als auch ausgiebig in der EN50600 behandelt wird, wurde von den meisten RZ-Betreibern unterschätzt. Spätestens bei der Zertifizierung durch den TÜV oder andere Prüfinstitute nimmt dieser Teil dann eine wichtige Rolle ein. Ganz nach dem Motto 'die beste Sicherung nützt nichts, wenn die Türe offen steht'. Zusätzlich wird die Umsetzung der ISMS durch eine verbesserungsfähige Kommunikation zwischen Facility-Managern und IT-Managern erschwert. Insgesamt ergeben sich in der Praxis daher Herausforderungen, bei denen Unternehmen auf Unterstützung angewiesen sind.

Die Standzeitkosten sind nur eine grobe Schätzung

So ist für Kritis die Gesamtrisikoanalyse für Rechenzentren eine ernstzunehmende Aufgabe. Sie gliedert sich in die Ereignisrisikoanalyse und die Geschäftsrisikoanalyse. Erstere deckt Themen wie externe Bedrohungen durch beispielsweise Brand, Flugzeugabsturz, Bombenanschlag oder Einbruch ab und zählt heute eigentlich zum Standard in der Umsetzung. Oft fällt RZ-Betreibern bei der Geschäftsrisikoanalyse allerdings zum ersten Mal auf, dass sie sich zu wenige Gedanken über die wirtschaftlichen Folgen eines IT-Ausfalls gemacht haben. Bei einem Stromausfall schalten auch die Server ab. Hier entsteht im Rahmen der Geschäftsrisikoanalyse die erste Schnittstelle zwischen IT-Hardware, IT-Software, der Gebäudetechnik und dem Umsatz. Schließlich müssen Datacenter-Verantwortliche bei der Zertifizierung nach ISO27001 auch die Standzeitkosten zumindest ansatzweise definieren können. Relativ einfach ist das, wenn die gesamte IT ausfällt: Dann sind entsprechend alle Geschäftsprozesse nicht mehr verfügbar und Unternehmen können gut abschätzen, wann sie zahlungsunfähig sind bzw. wann es zu ernsthaften Konsequenzen für die Gesellschaft kommt. Für den Ausfall von einzelnen IT-Systemen, beispielsweise wenn die Stromverteilung für nur zehn Server unterbrochen ist, ist diese Analyse dann schon deutlich schwieriger. Aber die Norm fordert genau das: Unternehmen müssen die Standzeitkosten ursachengerecht berechnen. Mit anderen Worten, welcher Schaden entsteht für das Geschäft im Falle eines Einzelausfalls. Diese Kalkulation erweist sich in der Praxis als nahezu unmöglich. In einer virtualisierten Umgebung wissen die Wenigsten, welcher virtuelle IT-Dienst auf welchem physischen Server läuft, geschweige denn, können sie die Standzeitkosten ermitteln. Um die Zertifizierung nach ISO27001 zu erhalten, wird daher die €-Zahl zum Geschäftsrisiko grob geschätzt. Seit der EN50600 existiert eine einheitliche Kategorisierung für die Verfügbarkeits- und Schutzklassen von Datacentern, so gesehen für den Ausfall des RZ respektive dessen Schutz vor externer Bedrohung. Sie regelt damit auch die Gebäudetechnik, inklusive der Stromversorgung. Diese Teile sind gemäß Norm ebenfalls einer Risikoanalyse zu unterziehen. RZ-Betreiber nehmen dies jedoch selten zum Anlass, um die Analyse mit der für die ISO27001 zusammenzulegen. Zudem sind sie hier nicht selten durch die Schnittstellen zwischen Facility-Technik und IT überfordert. Organisatorisch sind diese beiden Welten seit jeher getrennt. Zu einer Kernaufgabe für die Umsetzung der Kritis-Verordnung kristallisiert sich daher heraus, 'einen Dolmetscher zu finden'. Dabei bilden gerade die ISO27001 aus dem IT-Bereich und die EN50600 aus dem Gebäudetechnikbereich sehr gute Möglichkeiten, die beiden Organisationseinheiten strukturiert aneinander zu führen.

Zwischen Praxis und Theorie

Allgemein wird in der Praxis die potenzielle Nichtverfügbarkeit von Strom sträflich vernachlässigt. Zwar stellen sich professionelle Betreiber gerade in diesem Bereich überdimensioniert auf. Allerdings sind viele Bestands-RZ mit dem eigentlichen Betrieb der redundanten Stromversorgung überfordert. Zudem sehen sich bestehende Rechenzentren auch mit anderen Herausforderungen konfrontiert. So hadern viele beispielsweise bei der Umsetzung des Sicherheitszonenkonzepts, das ebenfalls durch die Norm EN50600 definiert ist. Während ein neues Rechenzentrum entsprechend geplant werden kann, ist es denkbar schwierig im bestehenden Gebäude eine Wand zu versetzen oder sie hinsichtlich der Brandschutzwerte aufzurüsten. Im besonderen Fall der Pflegeeinrichtungen entstehen dagegen eigene Probleme. So ist auch die Infrastruktur außerhalb des Datacenters, mit allen Knotenpunkten und Verteilern, Teil der KRITIS-Verordnung. Gerade aber diese Netzverteilerpunkte sind in Form von einzelnen kleinen Racks auf nicht selten 40 bis 50 verschiedene, kleine Räume verteilt. Sie sind wichtige Knotenpunkte für viele Endgeräte z.B. auch in OP-Sälen. Allerdings sind sie meist weder gesichert, gekühlt oder mit einer USV-Anlage versehen. Fremdzugriffen sind diese Räume oft schutzlos ausgeliefert. Das öffnet Tür und Tor für Datendiebstahl, Datenmanipulation oder einfach nur Datenbeschädigung. Die größten Unsicherheiten bestehen jedoch im Notfall- respektive Betriebsmanagement. Vor allem mittelständische Betriebe, die ihre RZ noch selber betreiben, haben selten einen konkreten Plan für Notfälle. Die KRITIS-Verordnung wurde jedoch gerade für den Ausnahmefall geschaffen. Hier suchen Unternehmen derzeit sehr häufig die Hilfe von Beratern. Nicht umsonst werden als Hilfsmittel Notfall-Handbücher für die Gebäudestruktur von Rechenzentren beauftragt. Solche Handbücher sind keine Standards, sondern werden individuell erstellt. Denn: Noch zu selten sind die Abhängigkeiten der Gerätschaften bzw. der gebäudetechnischen Anlagen im Datacenter dokumentiert. So müssen beispielsweise Alarme definiert, Kommunikationswege detailliert aufgeschrieben und konkrete Maßnahmen festgehalten werden. In einem nächsten, großen Schritt folgen Workshops mit den Angestellten, in denen auch herausgefunden werden soll, wer für welche Aufgaben zuständig ist. Neukunden, die ein Rechenzentrum bauen lassen, bestellen dieses Notfall-Handbuch daher oft mit. Sie nutzen die Tatsache, dass die Arbeitsschritte und der Aufbau dem Dienstleister im Detail bekannt sind und die Erstellung der Handbücher entsprechend leichter und schneller geht. ■

Autor: ***Marc Wilkens,***
Senior Consultant,
SecuRisk
www.securisk.de

Vorschau

Ausgabe 3/2017 erscheint am 06.10.2017

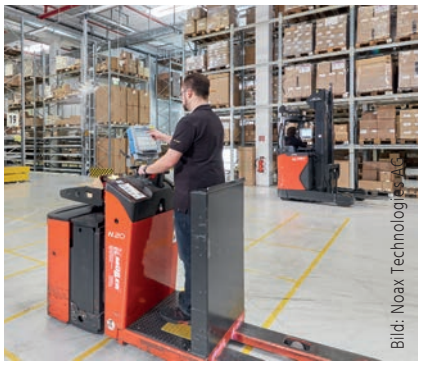


Bild: Noax Technologies AG

IPCs können die logistischen Prozesse in einem Lager für Formulare und Marketing-Artikel verbessern. Stabiles WLAN sorgt für beständigen Datenstrom, eine eingebaute USV verhindert Spannungsschwankungen.

Bild: © Alex/Fotolia.com

Für die Fernwartung von Maschinen und Anlagen ist Security essentiell. Eine neue Fernwartungslösung kann weltweit den Maschinenzustand überwachen und Fehler schnell diagnostizieren und beheben.

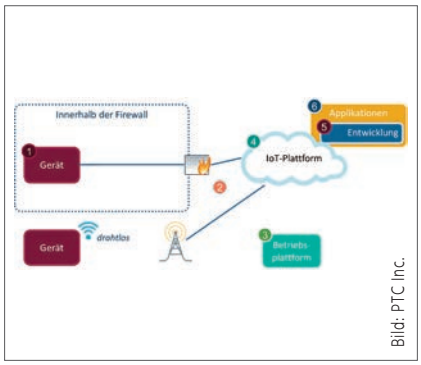


Bild: PTC Inc.

Das IoT bringt Sicherheitsrisiken mit sich, es gilt bestehende Geräte zu administrieren und zu sichern. Eine gemeinsame IoT-Sicherheitsarchitektur zwischen den Beteiligten kann typische Gefahren ausmerzen.

Inserentenverzeichnis

Impressum

VERLAG/POSTANSCHRIFT:
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:
Anja Giesen, Frauke Itzerott,
Pascal Jenke Victoria Kraft,
Kristine Meier, Melanie Novak,
Kristina Sirjanow, Marco Steber,
Florian Streitenberger,
Natalie Weigel

ANZEIGEN:
Heiko Hartmann, Christina Worm,
Daniel Katzer, Markus Lehnert,
Thomas Möller

ANZEIGENDISPOSITION:
Michaela Preiß
Tel. 06421/3086-0

Es gilt die Preisliste der Mediadaten 2017.

GRAFIK & SATZ:
Anja Beyer, Tobias Götze,
Melissa Hoffmann, Moritz Klös,
Timo Lange, Ann-Christin Lölkes,
Nadin Rühl, Verena Vornam,
Laura Jasmin Weber

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

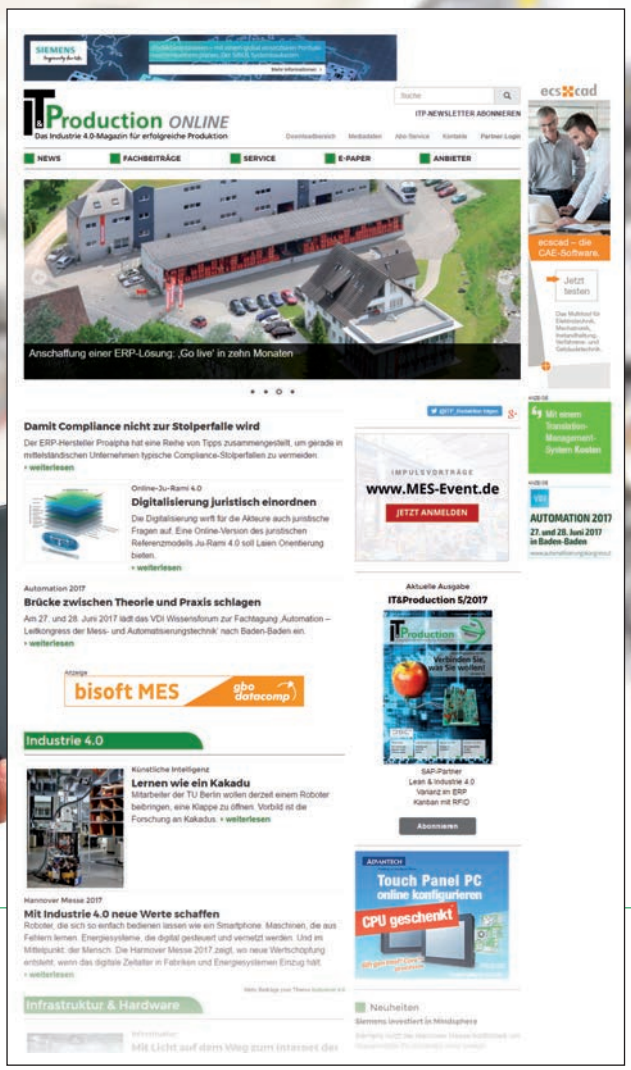
ISSN 0935-0187
Vertriebskennzeichen G30449

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

IT&Production ONLINE

Das Industrie 4.0-Magazin für erfolgreiche Produktion

Bilder: © industrieblick/Fotolia.com; © Jochen Schweizer



Jetzt im neuen Design!

Erleben Sie das neue IT&Production Online-Magazin:
Das Wissensportal rund um die Themen Industrie 4.0
und industrielle IT- und Softwarelösungen.

it-production.com

TeDo Verlag GmbH • Zu den Sandbeeten 2 • 35043 Marburg • Postanschrift: Postfach 2140 • 35009 Marburg
Tel.: 06421 3086-0 • Fax 06421 3086-280 • info@tedo-verlag.de • www.tedo-verlag.de

AUTOMATISIERUNG INNOVATIV VERNETZEN

mit den 4/8-Port managed PROFINET-Switches

Verbinden Sie bis zu acht Netzwerkteilnehmer zeit- und kostensparend mit dem neuen 4/8-Port PROFINET-Switches. Die managed realtime Switches unterstützten PROFINET nach Conformance Class B und bieteten Übertragungssicherheit durch Ringredundanz als MRP-Client.

- Priorisierung von PROFINET-Telegrammen
- Integration in das Automatisierungsnetzwerk mittels GSDML-Datei
- Schnelle, einfache Konfiguration und Diagnose über PROFINET und Webinterface
- Medienredundanz mit MRP
- Port-Mirroring und Diagnose-Alarme zur Netzwerkanalyse

www.helmholz.de

Helmholz®
COMPATIBLE WITH YOU