SPS MAGAZIN
SONDERAUSGABE 1/2017
www.sps-magazin.de

INDUSTRIAL COMMUNICATION JOURNAL

ETHERNET WIRELESS SECURITY

Bild: Helmholz GmbH & Co. KG

Durchgängige und sichere
Kommunikation vom Feld bis in die Cloud

Intelligente Bausteine für die digitale Fabrik

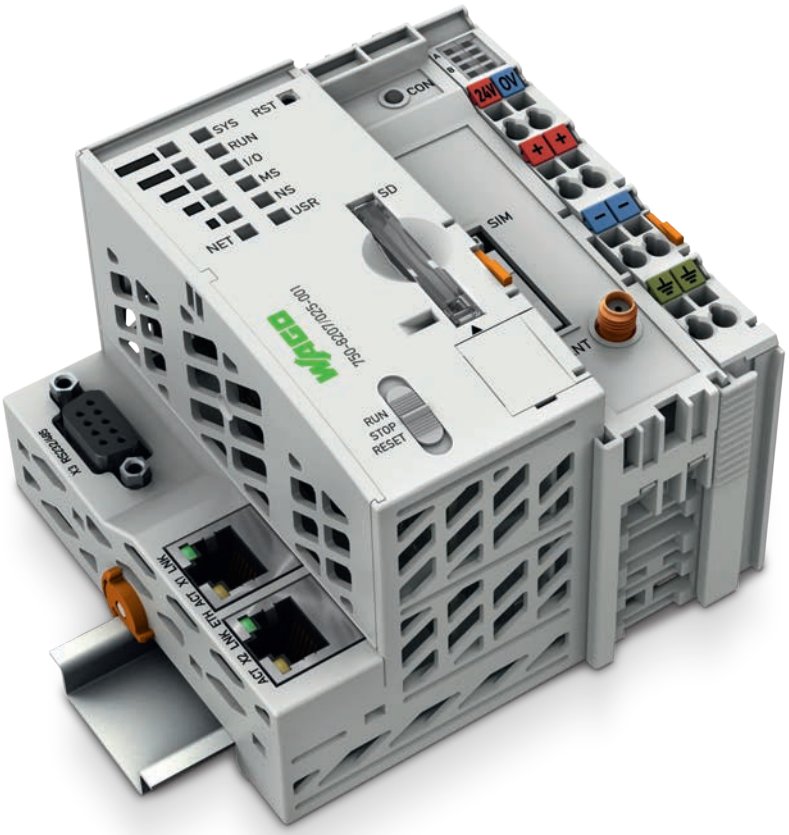
Helmholz®
COMPATIBLE WITH YOU

SCHÖNE NEUE WELT?
Time Sensitive Networking
für den Einsatz in der Industrie
Seite 20

FOKUS PROFINET
Technologie, Anwendungen
und neue Lösungen
ab Seite 25

INDUSTRIAL IOT
Watson als
Maintenance-Berater
Seite 50

VERBINDET DIE WELT DER AUTOMATISIERUNG MIT DEM INTERNET OF THINGS



Der PFC200 von WAGO – Die sichere Basis für den Weg aus der Feldebene

- Frei programmierbares Linux®-Betriebssystem
- Leistungsstarke Steuerung mit integriertem 3G-Modem und Standard-Mini-SIM-Karte
- Drahtlose Datenübertragung über große Distanzen
- GPRS-Verbindung zum Internet und bidirektionale Kommunikation via SMS
- Höchste Sicherheitsstandards dank IPsec und OpenVPN

www.wago.com/pfc200

WE INNOVATE!

WAGO

Rückstand aufgeholt

Mathis Bayerdörfer, Chefredakteur INDUSTRIAL COMMUNICATION JOURNAL

Geht es nach den Anbietern industrieller Kommunikationslösungen, dann hat sich Ethernet in der Fabrik bereits alternativlos durchgesetzt und dann steht jetzt mit OPC UA und TSN die nächste Generation von Standards in den Startlöchern. Aktuelle Marktzahlen sprechen allerdings eine etwas andere Sprache, denn sie zeigen, dass die Geschwindigkeit des Wandels deutlich verhaltener ist. Gleichzeitig unterstreichen sie aber: In der Tat steht Industrial Ethernet als heutiges Kommunikationsmaß in der Fabrik nicht zur Diskussion.

Das SPS-MAGAZIN widmet der Kommunikation mit dem INDUSTRIAL COMMUNICATION JOURNAL viermal jährlich ein eigenes Sonderheft. Schließlich kommt dieser Automatisierungsdisziplin auf dem Weg zu Industrie 4.0 eine besondere Rolle zu. Entsprechend viel Bewegung sollte eigentlich im Markt spürbar sein. Hatten Anfang der 2000er-Jahre industrietauglich modifizierte Ethernet-Standards die Bühne betreten und den Abgesang der klassischen Feldbusse eingeleitet, scheint heute mit neuen Technologien wie OPC UA oder TSN das nächste Kommunikationslevel in greifbarer Nähe zu liegen.

Doch zwischen technologischer Theorie und produktionstechnischer Praxis klafft ein zeitlicher Versatz. Industrial Ethernet gilt zwar längst als etabliert, aber der Einzug in die Produktion ist – wohl auch aufgrund des langen Lebenszyklus von Maschinen und Anlagen – nicht so schnell vonstatten gegangen wie ursprünglich prognostiziert. Erst jetzt ziehen die neu installierten ethernetbasierten Systeme zahlenmäßig in etwa mit den feldbusbasierten Lösungen gleich. Das geht aus Einschätzungen des Kommunikationsspezialisten HMS hervor, der regelmäßig entsprechende Zahlen veröffentlicht.

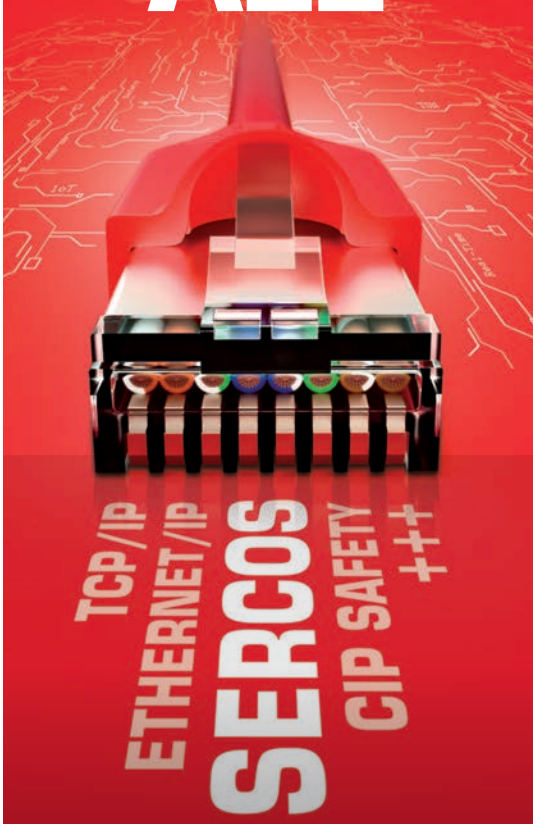
Weil Feldbustechnik ausgereift und nach wie vor sehr beliebt ist, werden in diesem Jahr wohl immer noch rund 48 Prozent der neuen industriellen Netzwerke auf dieser Basis realisiert. Den Ethernet-Marktanteil schätzt HMS für 2017 auf etwa 46 Prozent. Die restlichen Prozentpunkte werden Wireless-Lösungen zugeordnet. Betrachtet man allerdings das Wachstum insgesamt, wird die Ablöse der Feldbusse schnell deutlich: Die Zahl der installierten Feldbusknoten wird im laufenden Jahr nunmehr um vier Prozent zunehmen, wohingegen dem industriellen Ethernet ein Wachstum von rund 22 Prozent zugerechnet wird. Der Siegeszug von Industrial Ethernet ist also nicht zu stoppen.

Mathis Bayerdörfer
mbayerdoerfer@sps-magazin.de

PS: Weil mit Time Sensitive Networking, kurz TSN, wahrlich ein großes Potenzial für die Industrie einhergeht, aber auch viel Diskussionsbedarf, legt das INDUSTRIAL COMMUNICATION JOURNAL ein besonderes Augenmerk in jeder Ausgabe 2017 auf diese Weiterentwicklung des Ethernet-Standards – zu Grundlagen und Eigenschaften, aktuellen Entwicklungen und Trends sowie Expertenmeinungen.

sercos
the automation bus

ONE BUS FITS ALL



Sercos = Real-Time + IoT.

Das ist die Sercos®-Welt.

www.sercos.de

Besuchen Sie uns auf der Hannover Messe 2017, Halle 9, Stand G28

Bild: Helmholz GmbH & Co. KG

08

TITELSTORY

Intelligente Bausteine für die digitale Fabrik

Mit seinem Portfolio an Gateways und Switches, Firewalls und Routern sowie dem IOT-Portal myREX24 V2 präsentiert Helmholz ein breites Spektrum für industrielle Kommunikationslösungen. Auf Basis dieses Angebots kann der Anwender entlang der gesamten Kommunikationskette, vom Feld bis in die Cloud, exakt die Produkte wählen, die er für eine zukunftsfähige Umsetzung seiner Applikation benötigt – inklusive Industrie-4.0-Funktionalität als Basis für die Geschäftsmodelle der Zukunft.

Markt-Trends-Technik

11 Aktuelles aus der Branche

14 Neuheiten und Produktvorstellungen

TSN Faktencheck

20 Quo vadis, TSN?

21 Schöne neue Welt? Experten über TSN

23 TSN und Sercos: Übertragungsprinzip aufgegriffen

Protokolle und Standards

25 Industrie 4.0: Sortieren, bewerten, weiterentwickeln

28 S7-1500 und TIA Portal V14: Neue Funktionen

31 Profibus-FPGAs nach Wahl

32 Sicherheit: Port Stealing bei industriellen Anwendungen

34 Profinet-I/O-Module in der Förderanlage

36 AS-i-Lösung für die Lagerlogistik

Profinet-Nutzerorganisation

Bild: Profibus Nutzerorganisation e.V.

Die Industrie 4.0 Working Group von PI (Profibus & Profinet International) gewährt einen Blick hinter die Kulissen

Seite 25

Profinet-I/O-Module

Bild: Hans Turck GmbH & Co. KG

Hindernisse umgehen und trotzdem direkt ins Ziel kommen

Seite 34

Your Global Automation Partner

TURCK

Steuerparadies!
HMIs und Block-I/Os mit CODESYS-3-SPS

CODESYS

Flexibel einsetzbar als PROFINET Controller, EtherNet/IP Scanner oder Modbus TCP Master – zusätzlich CANopen, Modbus RTU und RS232/485

TX500: Moderne HMI/PLC-Kompaktgeräte zur einfachen Programmierung der Steuerungs- und Visualisierungsfunktionen mit CODESYS 3

TBEN-L-PLC: Robuste IP67-Block-I/Os mit CODESYS-3-SPS für intelligente Steuerungskonzepte ohne Schaltschrank

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

HANNOVER MESSE

www.turck.de/plc

Artikelserie IIoT

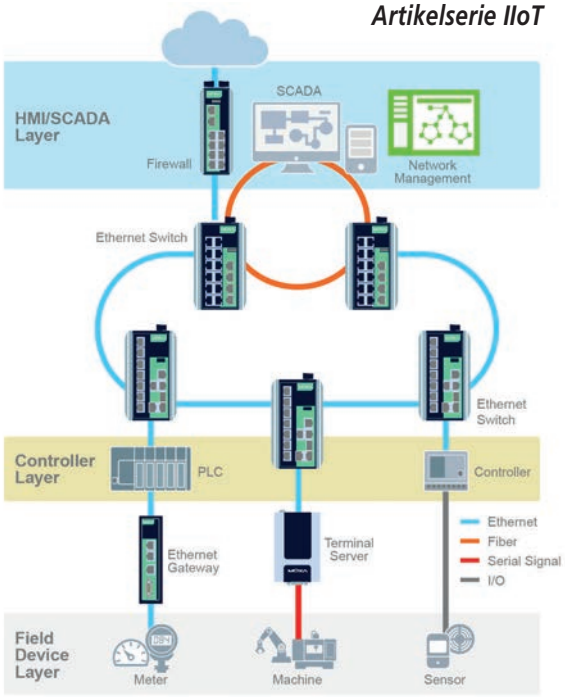


Bild: Moxa Europe GmbH

Antworten auf die fünf meist gestellten Fragen zum Industrial Internet of Things
Seite 51

Komponenten und Lösungen

38 IEC61850: Eine leise Revolution bahnt sich ihren Siegeszug
40 Leistung, Daten und Signale auf einer Leitung übertragen
42 Einkabellösung für die Antriebstechnik

Wireless und Remote

45 Produktübersicht: Wireless-Produkte
46 Predictive Maintenance: Dampfkessel aus der Ferne warten
48 Remote-Lösung für die Glasveredelung
50 Wartung mit dem kognitiven System Watson
51 Artikelserie IIoT: Infrastruktur für smarte Kommunikation
54 Sicherer Remote-Service

Sicherheit

56 Sicherheitsvorfälle schneller erkennen und neutralisieren
58 Key-Management und Datenverschlüsselung

Service

3 Editorial
57 Impressum

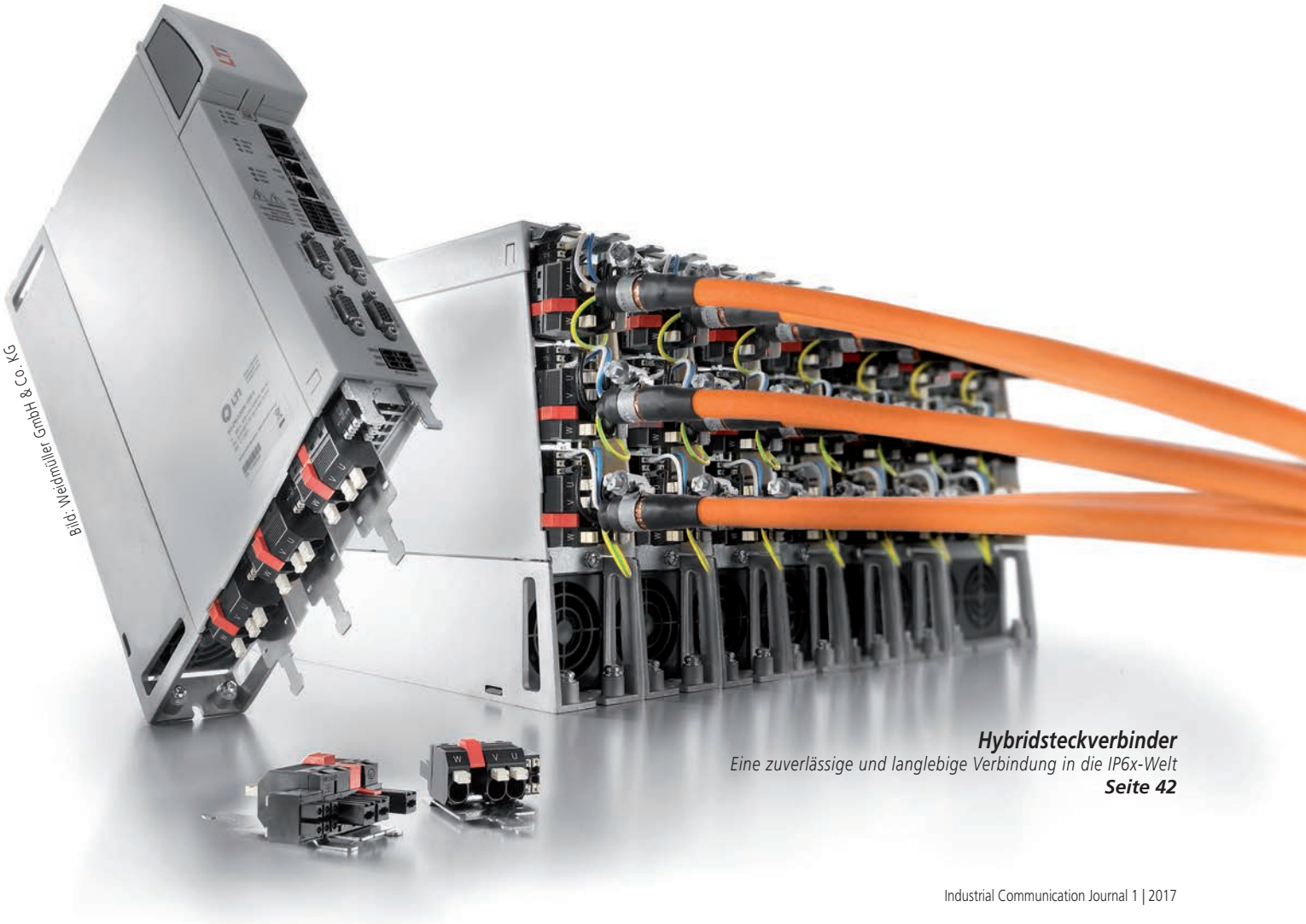


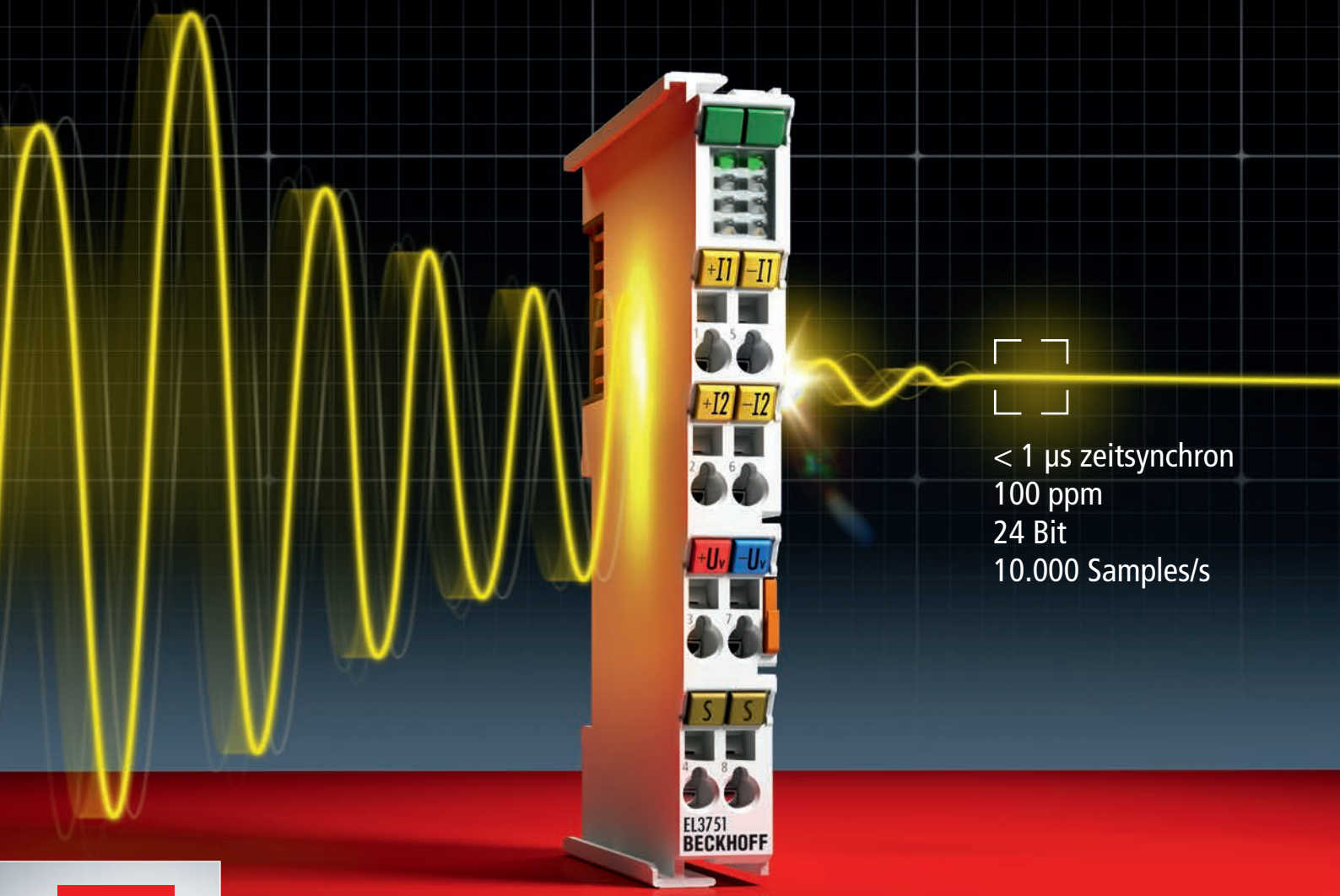
Bild: Weidmüller GmbH & Co. KG

Hybridsteckverbinder
Eine zuverlässige und langlebige Verbindung in die IP6x-Welt
Seite 42

| EK11-14G |

Äußerst präzise. Äußerst schnell.

Die neue Messtechnik-Generation der Beckhoff EtherCAT-Klemmen.



< 1 µs zeitsynchron
100 ppm
24 Bit
10.000 Samples/s

HANNOVER MESSE

Halle 9, Stand F06

www.beckhoff.de/EL3751

Mit der EtherCAT-Klemme EL3751 präsentiert Beckhoff das erste Mitglied seiner neuen Generation hochpräziser Messtechnik-I/Os. Diese skalierbaren Klemmen integrieren Highend-Messtechnik direkt in das Standard-I/O-System. Maximale Präzision und Abtastraten gewährleisten eine hohe Qualität der erfassten Daten:

- Multifunktionseingang: U, I, R, DMS (Messbrücke), RTD (PT100/1000)
- Zeitpräzise: Exakte Synchronisierung < 1 µs
- Wertpräzise: Messgenauigkeit besser als 100 ppm bei 23 °C
- Schnell: 10.000 Samples/s
- Proaktiv: selbstständige Anschluss- und Funktionsdiagnose
- 24 Bit ΔΣ ADC, Distributed-Clocks integriert, 107 % Extended-Range
- Abgleich höherer Ordnung auch anwenderseitig möglich
- Durch EtherCAT einsetzbar in vielen Messtechnik-Anwendungen

New Automation Technology **BECKHOFF**

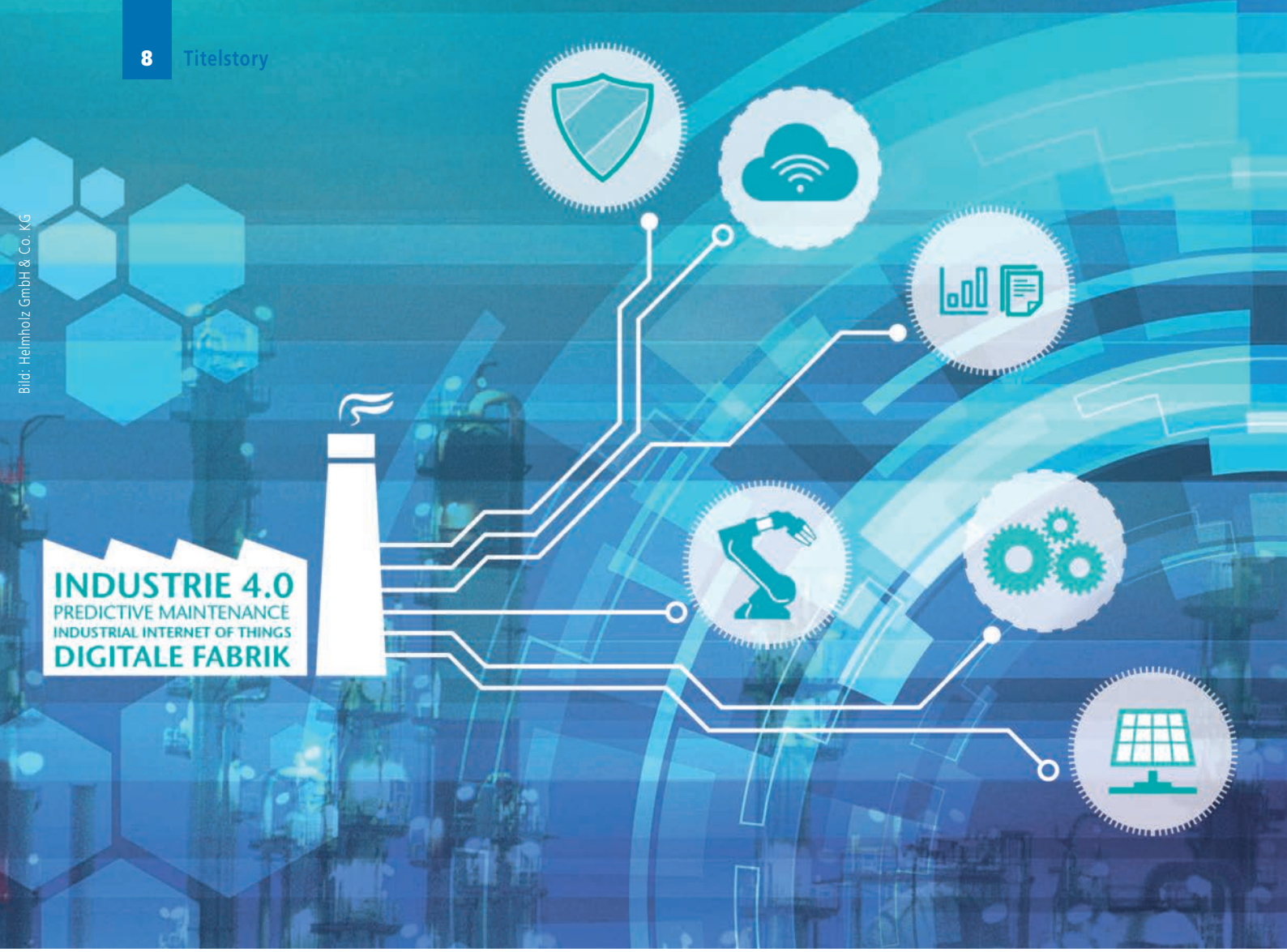


Bild: Helmholz GmbH & Co. KG

Durchgängige und sichere Kommunikation vom Feld bis in die Cloud

Intelligente Bausteine für die digitale Fabrik

Mit seinem Portfolio an Gateways und Switches, Firewalls und Routern sowie dem IOT-Portal myREX24 V2 präsentiert Helmholz ein breites Spektrum für industrielle Kommunikationslösungen. Auf Basis dieses Angebots kann der Anwender entlang der gesamten Kommunikationskette, vom Feld bis in die Cloud, exakt die Produkte wählen, die er für eine zukunftsfähige Umsetzung seiner Applikation benötigt – inklusive Industrie-4.0-Funktionalität als Basis für die Geschäftsmodelle der Zukunft.

„Bei Industrie 4.0 geht es um nichts anderes, als um die Digitalisierung der Fabrik“, bringt es Carsten Bokholt, technischer Geschäftsführer bei Helmholz, auf den Punkt. Im Zuge dieser Entwicklung sei der Anwender darauf angewiesen, möglichst viele Daten aus der Fertigung und dem Prozess zusammenzutragen. „Egal ob aus einer Maschinensteuerung oder aus einem einfachen Sensor im hintersten Winkel der Produktion: All diese Daten müssen übergreifend gesammelt und zentral erfasst werden“, so Bokholt weiter, „und dafür bietet sich nichts besser an, als Online-Plattformen wie unser Portal myREX24 V2.“

Fernwartung und mehr

Das Helmholz-Portal stellt neben klassischen Remote-Service-Funktionen (z.B. Diagnose oder Konfiguration/Programmierung) auch umfangreiche Monitoring- und Alarmfunktionen zur Verfügung. Sie ermöglichen eine schnelle Reaktion auf Probleme in den Anlagen und helfen Maschinenstillstandszeiten zu reduzieren. Von der klassischen Fernwartung bis hin zur Predictive Maintenance hat sich Helmholz über viele Jahre mit allen Facetten des Remote-Zugangs beschäftigt und einen großen Erfahrungsschatz aufgebaut. „Mit dem Portal myREX24 V2 stellen

wir uns auch den im Zuge von Industrie 4.0 vielfach geforderten Funktionen für die Datenerfassung als Basis für Big-Data- und Analytics-Lösungen", geht der Helmholz-Geschäftsführer auf die sich ändernden Anforderungen auf dem Markt ein. „So nimmt das Portal in der Digital Factory eine zentrale Rolle ein." Einerseits bei der Verwaltung von Remote- und Fernwartungskomponenten, die für das Sammeln der Daten zuständig sind. Andererseits als Host für die gesammelten Daten und als Instanz für das Alarm-Management."

Flexible Meldekette

Bei Störungen benachrichtigt myREX24 V2 das Personal per SMS oder E-Mail und löst so eine flexible Meldekette unter Berücksichtigung des verfügbaren Personals, der Tageszeit und des Wochentages aus. Durch den einfachen Zugang zum Portal per Browser kann der Anwender den Zustand der Anlage direkt per Smartphone oder Tablet beobachten. Neben den Helmholz-Routern lassen sich auch andere Standard OpenVPN-Clients zur Fernverbindung in myREX24 V2 V2 einbinden. Es ist auch für große Projekte mit vielen Anlagen, Benutzern und Endkunden konzipiert. Ein flexibles Benutzer-Management mit umfangreichen Zugriffsrechten und Mandantenverwaltung ermöglicht einen kontinuierlichen Überblick und den sicheren Zugriff auf die Anlagen und ihre Daten.

Datenerfassung und -analyse

„Ein großes Thema für unsere Kunden ist die Auswertung von erfassten Daten", schildert Bokholt die aktuelle Situation. „Schließlich gehen mit einer entsprechenden Analyse ganz neue Möglichkeiten einher." Im klassischen Maschinenbau sei man aktuell aber noch oft dabei, entsprechende Businessmodelle zu finden und aufzubauen. „Für unsere Kunden ist es natürlich eine wichtige Frage: Welche Mehrwertdienste kann ich dem Endanwender – über den Fernwartungszugang hinaus – durch die Integration eines Routers und die Nutzung des Online-Portals bieten?" Hier geht es dann nicht mehr nur darum, Daten zu erfassen, sondern diese auch zu protokollieren, zu analysieren oder zu visualisieren. Weil der Umgang mit Produktionsdaten und deren Schutz in der Industrie oft ein sehr sensibles Thema ist, hat der Helmholz-Kunde die Wahl, wo die erfassten Daten abgelegt werden. „Entweder hosten wir die Daten im Rahmen eines Mietmodells bei uns", so Bokholt. „Oder der Kunde bekommt mit myREX24 V2 virtual das entsprechende Werkzeug von uns, um seine Daten komplett unabhängig bei sich selbst oder dem Host seines Vertrauens zu speichern."

Router als Basis für Industrie 4.0

„Die Anwender nutzen unsere REX-Router zwar nach wie vor auch für klassische Ferwartungsapplikationen", sagt Bokholt. „Aber jetzt sind wir schon im nächsten Schritt und bilden mit unseren Geräten auch eine passende Basis für Industrie-4.0-Funktionalität. Entsprechend sind die Modelle der REX-100-Ethernet-Router-Familie bei Helmholz positioniert. Sie sind konsequent auf das Zusammenspiel mit dem VPN-Portal myREX24 V2 ausgelegt und fügen sich nahtlos in das industrielle Umfeld ein. „Router und

Das IoT-Portal myREX24 V2 – Entdecken Sie, wie einfach Fernwartung in Zukunft sein kann!

Portal gehören einfach zusammen", verdeutlicht Bokholt. „Das Zusammenspiel dieser beiden Seiten hat sich für Helmholz zu einer wichtigen strategischen Säule entwickelt." Deshalb baut Helmholz sein REX-100-Produktportfolio kontinuierlich aus und hat kürzlich zwei weitere Varianten vorgestellt:

- Das neue Modell REX 100 LTE ermöglicht eine schnelle Datenübertragung (Upload bis 50MBit/s, Download bis 100MBit/s) und ist für einen erweiterten Temperaturbereich von –40 bis +75°C konzipiert. Des Weiteren ist in der kompakten Bauform ein LAN-Switch mit vier Ports integriert.
- Der neue REX 100 WiFi ermöglicht die drahtlose Anbindung z.B. mobiler Anlagenteile an eine bestehende WLAN-Infrastruktur. Für die Kommunikation im LAN-Netzwerk stehen vier RJ45-Ports zur Verfügung.

Alle REX-100-Router sind mit zwei digitalen Eingängen ausgestattet: Einer dient als Trigger für den Verbindungsaufbau zum Portalserver, der zweite kann mit einer Alarmfunktion belegt werden.

Übergreifende Funktionalität

„Die Funktionalität der Router wird heute steuerungsübergreifend erwartet", erklärt der technische Geschäftsführer. „Unsere Router müssen die Daten also unabhängig vom Hersteller der jeweiligen SPS verarbeiten und weitergeben – egal ob mit Profibus kommuniziert wird, mit Ethernet/IP oder mit Modbus RTU." Dieses Spektrum soll Schritt für Schritt ausgebaut werden. „Eine zukünftig sehr wichtige und für Helmholz strategische Schnittstelle ist OPC UA", verrät Bokholt. Dieser Kommunikationsstandard soll auf beiden Seiten in das Angebot des Unternehmens Einzug halten: „Um die bereits gesammelten Daten aus dem Portal in Datenbanken und andere Systeme zu spielen, werden wir das Portal um eine OPC-UA-Schnittstelle ergänzen", führt Bokholt fort. „Natürlich sollen aber auch die Router selbst über eine OPC-UA-Anbindung Daten von entsprechenden Geräten sammeln können."

REX 100 Ethernet-Router, auch als LTE und WiFi-Variante erhältlich

Zentrales Element Sicherheit

In Ethernet-vernetzten Produktionsumgebungen und gerade im Hinblick auf Industrie 4.0 wird die Sicherheit zu einem immer wichtigeren Thema. Schließlich geht es darum, Maschinen sicher in übergeordnete Produktionsnetze zu integrieren bzw. von diesen abzugrenzen. Deswegen bildet neben der Kombination von Router und Online-Portal die Security ebenfalls eine strategische Säule bei Helmholz. Beide Bereiche seien im Unternehmen eng miteinander verzahnt, weil sie es auch beim Anwender sind: „Von der einen Seite kommend, sind Router heute längst auch Elemente der industriellen Security", so Bokholt weiter, „und umgekehrt kann man sagen: Eine Firewall-Lösung wie unsere WALL IE ist ein kleines spezialisiertes Puzzleteil aus der Welt der Router."

Kombination aus Firewall und Bridge

Mit WALL IE verbindet Helmholz Bridge- und Firewall-Funktionen: Die Komponente schützt vor unerlaubtem Zugriff und fungiert parallel dazu als Bridge. Konkret regelt WALL IE, welcher Teilnehmer mit welchem Gerät Daten austauschen darf, entsprechende Vorgaben können anwenderspezifisch definiert werden. Die Voraussetzung dafür schafft eine Paketfilter-Funktionalität, die den Zugriff zwischen Produktionsnetz und Automatisierungszelle ggf. einschränkt. Beispielsweise kann konfiguriert werden, dass nur bestimmte Teilnehmer aus dem Produktionsnetzwerk mit definierten Teilnehmern aus der Automatisierungszelle Daten austauschen dürfen. Andernfalls wird das Datenpaket zurückgewiesen bzw. verworfen. Als Besonderheit kann WALL IE sowohl im NAT-Betriebsmodus als auch im Bridge-Modus als Layer 2 Switch eingesetzt werden. Auch in dieser Betriebsart ist eine Paketfilterung möglich. Dadurch kann der Zugriff auf einzelne Bereiche eingeschränkt werden, ohne dass es dafür unterschiedlicher Netzwerke bedarf.

WALL IE, die Industrial Ethernet Bridge und Firewall, integriert Maschinennetze auf einfache Weise in das übergeordnete Produktionsnetz.

Reduziert auf das Wesentliche

Die Industrial Ethernet Bridge und Firewall kann speziell auf die Maschine zugeschnitten konfiguriert werden. Sie ist konzipiert für 100MBit Industrial Ethernet. Die zugrundeliegende Software ist Linux-basiert und wurde von Helmholz komplett selbst entwickelt. „Im Rahmen der Firewall setzen wir auf ein speziell angepasstes Linux mit einem außergewöhnlich kleinen Footprint", betont Bokholt. „Es sind wirklich nur die Funktionen integriert, die der Anwender auch wirklich braucht." Auf alles weitere habe man verzichtet, damit sich hier erst gar keine Sicherheitslücken auftun können. Die Hardware ist industrietauglich und geeignet für die Montage auf der Hutschiene. Die Konfiguration erfolgt über ein Webinterface. In die übersichtliche Benutzerführung haben die Helmholz-Entwickler ihre langjährigen Erfahrungen aus der TB20-ToolBox einfließen lassen. Der Online-Zugang ist streng passwortgeschützt und läuft über eine verschlüsselte HTTPS-Verbindung. Aber unabhängig von allen Features und Funktionen unterstreicht Bokholt: „Die Sicherheit ist nur zu einem Teil in Technik und entsprechenden Produkten abbildbar. Es kommt eben auch ganz stark auf den Prozess an." Hier gelte es, Strukturen zu etablieren, ähnlich denen im Qualitätsmanagement.

Auf allen Ebenen der Kommunikation

Zusammenfassend betont Geschäftsführer Bokholt: „Das Helmholz-Portfolio deckt alle verschiedenen Ebenen der Kommunikation ab: Ganz unten im Feld vernetzen unsere Switche als Infrastrukturkomponenten die verschiedenen Geräte und Maschinen, in denen wiederum WALL IE als Firewall integriert ist." Darüber positionieren sich die Router, die über das Internet und myREX24 V2 die Anbindung in alle übergeordneten und räumlich entfernten Systeme bieten. Alle Bestandteile des Helmholz-Portfolios sind aufeinander abgestimmt und einfach zu kombinieren. „Bei uns behält der Kunde aber seine Freiheit und die gesamte Flexibilität", zieht der Helmholz-Geschäftsführer Fazit. „Bei Bedarf bekommt er die gesamte Kommunikationslösung von uns. Andernfalls sucht er sich exakt die Puzzleteile in unserem Kommunikationsportfolio aus, die er benötigt. Egal welche und wie viele Bestandteile das sind: Sie ermöglichen stets eine durchgängige und einfache Nutzung." ■

Autor: ***Carsten Bokholt,***
Managing Director ,
Helmholz GmbH & Co. KG
www.helmholz.de

Direkt zur Marktübersicht i-need.de *www.i-need.de/?f10181*

Bild: ODVA Inc.

In zahlreichen Sessions und Präsentationen ging es auf dem 18. Annual Meeting der ODVA um die Weiterentwicklung der Ethernet/IP-Technologie. Dabei spielen aktuelle IT-Trends wie TSN, Security, Cloud usw. ebenso eine große Rolle wie automatisierungsspezifische Themen wie IO-Link oder Distributed Motion. In der General Session (Bild) skizzierte Catherin Voss die Entwicklung der ODVA-Organisation. Zudem standen Wahlen an.

Zahlreiche technische Weiterentwickelungen von Ethernet/IP

ODVA: Hersteller treffen sich zum 18. Annual Meeting

Vom 21. bis 23. Februar 2017 fand das 18. Annual Meeting der ODVA in Palm Harbor, Florida statt. Die ODVA ist die Herstellervereinigung von Ethernet/IP. Erklärtes Ziel der ODVA ist es, den technischen Fortschritt hin zum industriellen Internet der Dinge mit seinen Kommunikationstechnologien prägend mitzugestalten. Dementsprechend standen viele der Präsentationen und Sessions im Fokus dieses Themenbereichs.

Etwa 125 Teilnehmer aus über 50 Unternehmen nahmen an dem sehr technisch geprägten dreitägigen ODVA-Meeting im warmen Florida teil. Vom schönen Wetter bekommen die Teilnehmer eines ODVA-Annual-Meetings tagsüber allerdings wenig zu spüren, denn die Treffen sind regelmäßig gekennzeichnet von hoher Produktivität und zahlreichen Arbeits-Sessions. Neun Arbeitsgruppen nutzten den ersten Veranstaltungstag für ein Treffen der technischen Arbeitsgruppen, die bei der ODVA Special Interest Group (SIG) heißen.

Weiterentwicklung von Ethernet/IP

Ein ODVA-Roundtable für EtherNet/IP-Hersteller und 15 Präsentationen zu wichtigen Technologieentwicklungen bildeten die inhaltliche Gestaltung des zweiten Veranstaltungstages. Derzeit befassen sich Arbeitsgruppen innerhalb der ODVA mit zahlreichen wichtigen Einflussfaktoren auf die industrielle Kommunikation, darunter beispielsweise Security, IO-Link-Integration, Distributed Motion, TSN oder Cloud-Techniken, um nur einige zu nennen. Unter dem Namen 'Devicenet of Things' ist in einer SIG derzeit eine Technologie in der Diskussion, die die Integration von Geräten in das Netzwerk vorsieht, die bisher üblicherweise parallel verdrahtet werden, beispielsweise Drucktaster, Schaltgeräte usw. Ein ausführlicher Bericht darüber wird in einem der nächsten SPS-MAGAZINe folgen. Der Ausklang des zweiten Tages wurde im Rahmen einer Abendveranstaltung für Networking und soziale Aktivitäten genutzt.

Bild: ODVA Inc.

Die Referenten aus den SIGs stellten die aktuellen Weiterentwicklungen in technischen Session während der ODVA-Konferenz vor.

Präsentation der ODVA und Vorstandswahlen

Am dritten Tag standen neben der Plenumveranstaltung (General Session) auch Vorstandswahlen an. ODVA-Präsidentin Catherin Voss skizzierte die Entwicklung der Organisation, der Technologie sowie der zukünftigen technischen Anforderungen. Aus diesen Anforderungen ergeben sich die technischen Weiterentwicklungen und die Arbeiten der SIGs an der Spezifikation. Voss präsentierte zahlreiche internationale Aktivitäten in Europa, Japan, Asien usw. um die weltweite Verbreitung des Ethernet/IP-Standards weiter zu steigern. Bei den Vorstandswahlen wurde David Lagerstrom von Turck als neues Mitglied in den Vorstand gewählt. Dieser besteht nun aus den Unternehmen Weidmüller, Schneider Electric, Rockwell Automation, Omron, Bosch Rexroth, Endress+Hauser und Turck. Das nächste Annual Meeting wird im Oktober 2018 stattfinden. Ausgewählte Präsentationen und Unterlagen stehen auf der Website der ODVA zum Download bereit. *(kbn)* ■

News-Ticker

Prozessabsicherung mittels Asset-Management

Nach einer Konzeptphase hat die Nutzerorganisation PI die Profinet-Spezifikation um die Funktion Asset Management Record erweitert. Zusammen mit den Identifikation&Maintenance-Daten ist damit eine Erfassung von Geräten und Maschinen möglich, die nicht im Profinet-Umfeld projektiert werden.
www.sps-magazin.de/?19138

Neue Bluetooth-Spezifikation

Mit Bluetooth 5 ist die neue Kernspezifikation für Bluetooth verfügbar. Neben höherer Reichweite und Geschwindigkeit gehört auch eine höhere Übertragungskapazität sowie eine verbesserte Interoperabilität und störungsfreie Nutzung mit anderen drahtlosen Technologien zu den Neuerungen.
www.sps-magazin.de/?19139

Sigfox strebt 80% Netzabdeckung an

Der Funknetzanbieter Sigfox will bis Ende 2017 bis zu 80% der Fläche Deutschlands versorgen. Aktuell sind rund 35% der Bevölkerung abgedeckt – inklusive großer Städte wie Berlin, Hamburg, München oder Köln.
www.sps-magazin.de/?19140

Ethercat: 500 Mitglieder in China

Die ETG hat kürzlich die 500-Mitgliedermarke in China geknackt. Insgesamt hat die Nutzerorganisation aktuell knapp 4.200 Mitglieder. Mit der wachsenden Verbreitung des Standards sollen auch entsprechende Informationsveranstaltungen zunehmen.
www.sps-magazin.de/?19141

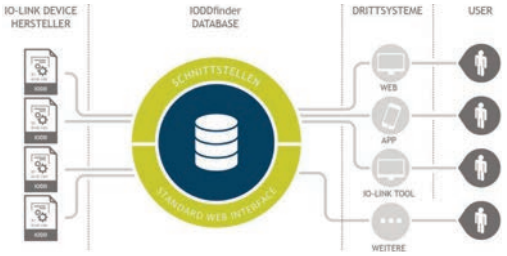
Neuer Standard: OPC UA für Spritzgießmaschinen

Euromap 77 heißt der neue OPC-UA-basierte Standard für den Datenaustausch zwischen Spritzgießmaschinen und Leitrechnern oder MES. Er wurde von dem Unternehmen Arburg, Engel, Ferromatik Milacron, KraussMaffei, Netstal, Negri Bossi, Sumitomo (SHI) Demag und Wittmann Battenfeld entwickelt – mit Untertützung durch die OPC Foundation und Ascolab sowie verschiedenen MES-Anbietern. Die Spezifikation ist als Release Candidate unter www.sps-magazin.de/?19154 veröffentlicht.

Euromap
www.euromap.org

Herstellerübergreifende Datenplattform für IO-Link-Geräte

Die IO-Link-Firmengemeinschaft stellt den IODDfinder vor, eine zentrale Datenbank für IO-Link-Gerätebeschreibungen. Der Service bietet für Hersteller einen konsistenten und aktuellen Daten-Pool. Anwender profitieren von einer zentralen, herstellerübergreifenden Datenbank für alle verfügbaren IODDs. Im Portal sind mehr als 3.500 IO-Link-Geräte von 38 Herstellern gelistet, versehen mit Zusatz- und Hintergrundinformationen. Damit soll die oftmals mühsame Suche von IODDs unterschiedlicher Hersteller im Internet der Vergangenheit angehören. Die Nutzung des Online-Service ist für Anwender und Mitglieder kostenlos. IO-Link-Mitglieder erhalten ein Nutzerkonto für die Datenbank, indem sie sich per E-Mail registrieren. Die IO-Link Community baut zudem ihr Qualitätswesen aus: Zusätzlich zu den fünf Competence-Centern gibt es ab sofort auch drei akkreditierte Test-Center, die IO-Link-Geräte auf normkonformes Verhalten testen. Eine neue IO-Link-Planungsrichtlinie bietet interessierten Anwendern Unterstützung bei der Planung von Automatisierungsanlagen mit IO-Link Devices. In einer handlungsorientierten Form werden erforderlichen Tätigkeiten Schritt für Schritt beschrieben. Als Grundlage dient die Spezifikationsversion 1.1.2.



Funktion der herstellerübergreifenden, zentralen Datenbank der IO-Link Community für IO-Device Descriptions.

Bild: Profibus Nutzerorganisation e.V.

Profibus Nutzerorganisation e.V.
www.profibus.com

CC-Link IE kompatibel zu 100Mbit-Ethernet-Geräten

Jedes Produkt mit einem 100Mbit-Ethernet-Port kann zukünftig einfach mit CC-Link-IE-Kompatibilität ausgestattet werden. Allein durch die Software kann CC-Link IE Field Network Basic in Geräte oder Master Controller implementiert werden. Auf diese Weise erreichen vorhandene Produkte entsprechende Kompatibilität ohne Hardware-Modifikation. CC-Link IE ist für Datenraten im Gbit-Bereich ausgelegt. Es gibt jedoch auch Produkte und Anwendungen auf niedrigerer Ebene, die ebenfalls von Gigabit-Performance profitieren. Darauf hat die Nutzerorganisation CLPA mit dem Basic Mode reagiert. Da der Basic-Mode-Protokoll-Stack kompatibel zu TCP/IP und UDP/IP ist, lässt er sich gut in andere ethernetbasierte Umgebungen einfügen. Um die Implementierung zu vereinfachen, bietet die CLPA ihren Mitgliedern kostenlosen Mustercode an.

CLPA Europe
www.clpa-europe.com

Offizielle Spezifikationsdokumente zu Ethercat P

Die Ethercat-Nutzerorganiation ETG hat den ersten Entwurf der offiziellen Technologiespezifikation zu Ethercat P sowie die Erweiterung aller zugehörigen Dokumente veröffentlicht. Das Dokument 'ETG.1030 Ethercat P Specification' definiert die Basics des Standards als Erweiterung der physikalischen Ethercat-Schicht. Als solche wurden auch alle anderen Dokumente zu den Standards, in die sich Ethercat P integriert, entsprechend erweitert. Um Entwicklern bereits jetzt

Jürgen Welker, Bereichsleiter Automatisierung und Service bei der KOCH Pac-Systeme GmbH, und Martin Rostan, Executive Director der EtherCAT Technology Group

die Implementierung zu ermöglichen wurde als Richtlinie zur Implementierung von Ethercat P Slaves zeitgleich auch eine entsprechende Application Note fertiggestellt. Sie befasst sich mit der entsprechenden Erweiterung inklusive Verbindern, elektrischer Spezifikation sowie Empfehlungen für den EMV-gerechten Aufbau. Darüber hinaus informiert sie über verschiedene Design-Vorgaben – insbesondere in Bezug auf die Nutzung und Verbindung von Versorgungsspannungen – und beschreibt die Berechnungsgrundlagen der Ströme und Spannungen im Netzwerk.

Ethercat Technology Group
www.ethercat.org

VDMA Robotik und OPC Foundation unterzeichnen Memorandum of Understanding

Die VDMA-Fachabteilung Robotik und die OPC Foundation haben ein Memorandum of Understanding zur Erarbeitung einer OPC UA Robotics Companion Specification unterzeichnet. Dem Entschluss zugrunde lag die Erkenntnis, dass die M2M-Kommunikation gut auf Basis von OPC UA gestaltet werden kann. Erste Diskussionen darüber, welche Informationen, Daten, Funktionen und Dienste in ein Produktionsnetzwerk zu integrieren sind und in OPC UA abgebildet werden sollen, wurden schon geführt. Ein Arbeitskreis zur Entwicklung der Companion Specification formierte sich ebenfalls bereits mit einer Kick-off-Veranstaltung im VDMA. Innerhalb des Verbands befassen sich mehr und mehr Bereiche mit OPC UA. Ein Leitfaden zu Industrie-4.0-Kommunikation mit OPC UA ist in Arbeit. Er soll den Maschinen- und Anlagenbau bei der Einführung unterstützen und Handlungsempfehlungen geben.

VDMA e.V.
www.vdma.org

AutomationML Teil 3 ist internationaler Standard

Teil 3 des AutomationML-Standards spezifiziert die Integration von Geometrie- und Kinematikinformationen, wie sie für den Datenaustausch zwischen Entwurfswerkzeugen in der Anlagenplanung erfolgen soll. Neben Teil 1 und Teil 2 hat nun auch Teil 3 den Status des internationalen Standards erreicht. Teil 1 spezifiziert die generelle Architektur des Formates und Teil 2 definiert grundlegende Rollenklassenbibliotheken. Teil 4 ist als neues Projekt in der IEC gestartet und soll zukünftig die Modellierung von Verhaltensbeschreibungen beschreiben.

AutomationML e.V. c/o IAF
www.automationml.org

Fachkonferenz Maschinensteuerung aus der Cloud

Längst ist auch dem letzten Automatisierungstechniker bewusst geworden, dass IT und Steuerungstechnik unumkehrbar zusammenwachsen. Anbieter wie Beckhoff, Bosch Rexroth und Phoenix Contact realisieren eigene Cloud-Lösungen, um die vertikale Vernetzung von der Klemme bis zur Datenwolke Realität werden zu lassen. Auch klassische Maschinenbauer wie die Firma Trumpf gründen Start-ups wie Axoom, um an den Geschäften mit Produktionsdaten teilhaben zu können. Offen bleibt dabei die Frage, was das für die Steuerungstechnik an sich bedeutet. Die Veranstaltung 'Maschinensteuerung aus der Cloud' am 20. und 21. Juni 2017 in Stuttgart widmet sich genau diesem Thema und zeigt die aktuellen Entwicklungen. Details und Anmeldung über die u.g. Internet-Adresse.

Süddeutscher Verlag Veranstaltungen GmbH
www.sv-veranstaltungen.de/maschinensteuerung

IXXAT®

Multi-Protokoll PC-Interface

IXXAT INpact

Eine Karte, alle Protokolle!

- Ideal für PC-basierte Mess-, Visualisierungs- und Service-Anwendungen
- Einheitliches API für alle unterstützten Protokolle – einfacher Wechsel ohne Softwareanpassung!
- Als PCIe-Mini- oder PCIe-Variante (Standard-/Low-Profile)
- Für alle gängigen Industrial Ethernet und Feldbus-Standards
- Umfangreiches Windows- und Linux-Treiberpaket im Lieferumfang

NEU

IXXAT INpact PCIe Mini für PROFIBUS und PROFINET IRT Fiber Optic.

HMS Industrial Networks GmbH
Emmy-Noether-Str. 17 · 76131 Karlsruhe
+49 721 989777-000 · info@hms-networks.de
www.anybus.de · www.ixxat.de · www.ewon.biz

Industrie-Apps mit Verbindung in die Cloud

Mit den Apps für die Siemens-Cloud MindSphere von Accenture sind Maschinenbauer und Industrieausrüster in der Lage, ihr Geschäft auszuweiten, die Kundenzufriedenheit zu erhöhen sowie die Kosten für Reklamationen und Garantiefälle zu senken. Endkunden profitieren wiederum von kürzeren Stillstandszeiten, geringeren Instandhaltungs- und Energiekosten sowie einer längeren Maschinenlebensdauer. OEMs erhalten mit den Apps einen aktuellen und kontinuierlichen Einblick in ihre Maschinen und Anlagen. Grundlage dafür ist die Verbindung von Operational Technology (OT) und Information Technology (IT) mit dem Produktionsmanagement, der Produktion, der Logistik und ERP-Systemen. OEMs können so Produktionsengpässe erkennen und verhindern. Zudem lassen sich faktenbasierte Entscheidungen treffen, um den Betrieb, den Einsatz von Mitarbeitern, die Zulieferprozesse und das Produktdesign zu verbessern.

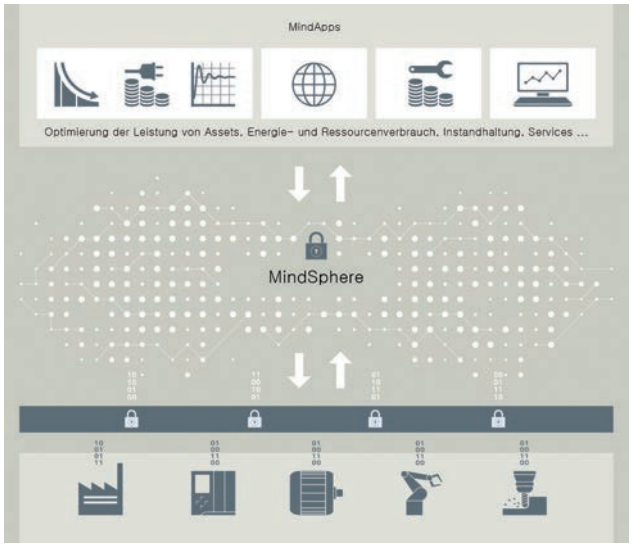


Bild: Accenture Dienstleistungen GmbH

Mit den Apps für die Siemens-Cloud MindSphere von Accenture entsteht eine Verbindung von OT und IT.

Accenture Dienstleistungen GmbH
www.accenture.com

Ethercat-I/O-System zur dezentralen Sensor-/Aktorsteuerung

Das Adam-5000/ECAT-AE von AMC ist ein Vier-Slot-Remote-I/O-System zur dezentralen Erfassung und Steuerung von Sensoren und Aktoren mittels der dazugehörenden I/O-Module via Ethercat. Damit ergänzt das Unternehmen sein Produktportfolio um ein flexibles I/O-System zur Erweiterung von Ethercat-Datenerfasungssystemen in der Automatisierungstechnik. Das System verfügt über vier I/O-Steckplätze für bis zu 64 Punkte der Datenüberwachung und -steuerung sowie eine ARM-32-Bit-Risc-CPU. Es unterstützt den Ethercat Distributed Clock (DC) Mode und den SyncManager Mode sowie das Modular Device Profile (MDP), wenn alle Module eine reine I/O-Konfiguration besitzen. Die Konfiguration und Einstellung der I/O-Module erfolgt über die Utility. Knotenadressen lassen sich durch Drehschalter festlegen oder per Software einstellen. Das I/O-System ist kompatibel mit Advantech Common Motion SDK oder anderen Ethercat Mastern mithilfe von ENI-Dateien. Darüber hinaus besitzt es einen 8-Bit-DIP-Schalter zum Einstellen des Modus sowie drei Rotationsschalter für bis zu 4.096 Slave-IDs.

Bild: AMC Analytik & Messtechnik GmbH

Das Adam-5000/ECAT-AE von AMC ist ein flexibles I/O-System zur Erweiterung von Ethercat-Datenerfasungssystemen.

AMC Analytik und Messtechnik GmbH
www.amc-systeme.de

IO-Link-Master für intelligente Diagnosen in rauen Industrieumgebungen

Der IP67-klassifizierte Allen-Bradley-ArmorBlock-IO-Link-Master der Serie Slim Line von Rockwell Automation eignet sich für raue Industrieumgebungen. Hersteller und industrielle Anwender greifen mit dem Master auf detaillierte Sensordiagnosen zu. Das Gerät bietet zudem Ereignis- und Prozess-Zeitstempelfunktionen für On-Machine-Anwendungen. Der IO-Link-Master speichert auf jedem Kanal bis zu 40 Zeitstempel von Sensorereignissen. Mithilfe dieser Ereignishistorie lassen sich Änderungen nachverfolgen und Probleme diagnostizieren. Es ist ebenfalls möglich, Eingangszeitstempel aller Sensordaten bei einer Statusänderung an die Steuerung zu senden. Durch diese und weitere Diagnosen, die das Gerät zur Verfügung stellt, lässt sich die Fehlerbehebungszeit um bis zu 90% verkürzen sowie die vorbeugende Wartung und die allgemeine Systemleistung verbessern. So unterstützt der IO-Link-Master in Verbindung mit IO-Link-fähigen Sensoren herstellende Unternehmen dabei, intelligente Abläufe zu entwickeln, ohne dass dafür eine Komplettüberholung erforderlich ist.

Bild: Rockwell Automation GmbH

Der IP67-klassifizierte IO-Link-Master von Rockwell Automation eignet sich auch für raue Industrieumgebungen.

Rockwell Automation GmbH
www.rockwellautomation.de

Industrie-PC mit Ethercat-Konnektivität

Bild: Harting Deutschland GmbH & Co. KG

Die ersten Ethercat-Serienmodelle der Mica werden Anfang 2017 erhältlich sein.

Mit den Ethercat-Serienmodellen des Industrie-PCs Mica von Harting lassen sich Daten über zwei M8-Steckverbinder direkt aus industriellen Produktionsnetzwerken abgreifen, vorverarbeiten und über verschiedene Standardprotokolle wie OPC-UA oder MQTT an übergeordnete Systeme oder Cloud-Anwendungen weiterleiten. Aufgrund der modularen Open-Source-Software-Architektur eignet sich der Industrie-PC, um Edge- und Cloud-Anwendungen in der Produktion zu realisieren. Durch das Ethercat-fähige interne Funktionsmodul bleiben die übrigen Eigenschaften, wie Schutzart IP67, industrietaugliche Steckverbinder und das Erfüllen der Industrienormen, erhalten.

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

Dezentrales I/O-System mit Kommunikationsmodul

Mit dem dezentralen I/O-System PSSUniversal 2 bringt Pilz eine weitere Gerätegeneration für die Feldebene auf den Markt. Es besteht aus einem Profinet-Kommunikationsmodul und mehreren I/O-Modulen. Mit dem dreiteiligen Systemaufbau reduzieren sich die Aufwendungen für Service und Wartung, denn die Diagnose lässt sich im Remote-I/O-System sehr genau vornehmen. Das erlaubt eine schnelle Fehlerlokalisierung und -behebung. Der Modultausch ist im laufenden Betrieb möglich. Dabei ist es möglich, den Tausch des Kopfmoduls ohne Neukonfiguration vorzunehmen. Für den Tausch der Backplane ist zudem keine vollständige Demontage notwendig. Anwender stellen den Systemaufbau schnell und einfach per Drag&Drop am Bildschirm zusammen. Hierfür steht das Konfigurationstool PASConfig zur Verfügung. Der logische Aufbau führt den Anwender Schritt für Schritt durch die manuelle Installation. ➡

- Anzeige -

HANNOVER MESSE
Halle 9,
Stand H10
24. – 28. April 2017

IBHsoftec

NEU!

IBH OPC UA IoT2040

Siemens Gateway IoT2040 goes OPC UA

Ab sofort ist eine microSD Karte mit dem OPC UA Server/Client mit Firewall von IBHsoftec für das Siemens Gateway IoT2040 verfügbar. Diese Lösung erweitert SIMATIC S5, S7-200, S7-300, S7-400, S7-1200, S7-1500 und Logo! (Ethernet Versionen) Steuerungen um OPC UA.

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

OPC UA

SIMATIC, STEP, LOGO! und TIA sind eingetragene Marken der Siemens Aktiengesellschaft Berlin und München.

Turmstraße 77 | D-64743 Beerfelden | Hotline +49 6068 3001 | Verkauf +49 6068 3002 | Fax +49 6068 3074 | info@IBHsoftec.com | www.IBHsoftec.com

Dabei hilft die intuitive Handhabung, Fehler zu vermeiden. Das System verarbeitet sowohl sichere als auch nicht sichere Steuerungssignale. Sicherheit und Automation sind physikalisch gemischt, aber logisch voneinander getrennt und somit rückwirkungsfrei. Das Kopfmodul kommuniziert in der Grundfunktion mit Profinet/Profisafe. In der nächsten Stufe wird das System um ein Kommunikationsmodul mit Ethernet-IP/CIP-Safety-Schnittstelle und weitere I/O-Module erweitert.

Bild: Pilz GmbH & Co. KG

Die Grundfunktion des PSSUniversal 2 von Pilz umfasst ein Kopfmodul mit Profinet/Profisafe-Kommunikationsfunktion.

Pilz GmbH & Co. KG
www.pilz.com/de

Sichere Fernwartungslösung für Maschinen und Anlagen

Baumüller bietet mit Ubiquity eine sichere Lösung für die Fernwartung von Maschinen und Anlagen. Das System ist nach IEC62443-3-3 zertifiziert und entspricht den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es besteht aus drei verschiedenen Komponenten: dem Control Center, einer Bediensoftware, die Fernwartungssysteme verwaltet, beobachtet und aktualisiert, der Laufzeitumgebung, die auf den Bediengeräten des Herstellers installiert ist und ohne zusätzliche Hardware auskommt, sowie einer Server- und Infrastruktur, über die der Austausch von Daten, Zertifikaten und Schlüsseln stattfindet. Eine Fernwartung ist möglich, wenn die Laufzeitumgebung mit dem Control Center verbunden ist. Dazu kommen Zertifikate und eine Zweifaktorauthentifizierung zum Einsatz. Eine separate Verbindung ist hierfür nicht nötig, die bestehende Internetverbindung lässt sich verwenden.

Bild: © Alex – fotolia.com

Für die Fernwartung von Maschinen und Anlagen bietet Baumüller Ubiquity als Sicherheitslösung an.

Baumüller Holding GmbH & Co. KG
www.baumueller.de

Stellantriebe mit Powerlink-Schnittstelle

Die Stellantriebe AG25 und AG26 von Siko stehen jetzt mit Powerlink-Schnittstellen zur Verfügung. Die Stellantriebe werden mit umfangreichen PLCopen-Motion-Bibliotheken geliefert und lassen sich an Powerlink-Steuerungen einfach in Betrieb nehmen. Aufgrund der kompakten Abmessungen lassen sich Positionieraufgaben dezentral und auch bei beengten Platzverhältnissen vollautomatisch ausführen. Die Stellantriebe AG25 haben einen Durchmesser von 80mm. Der Antrieb AG26 ist etwas größer und bietet bis zu 13Nm Drehmoment. Die Antriebe verfügen über eine Hohlwelle mit Klemmring für eine einfache Montage. Motor, Getriebe, Leistungs- und Steuerelektronik sowie Buskommunikation und Positionsregler sind in den Stellantrieben integriert, sodass es im Feld nur erforderlich ist, den Busanschluss und eine 24V-Gleichspannungsversorgung zuzuführen. Dadurch lassen sich die Gesamtsystemkosten für die Integration in die Maschine gegenüber einem diskreten Aufbau reduzieren. Zudem ist ein hochpräziser Multiturn-Absolutwertgeber integriert, der die Position der Antriebswelle auch beim Verdrehen der Welle im stromlosen Zustand des Stellantriebs erfasst.

Bild: Ethernet Powerlink Standardization Group (EPSG)

Die kompakten Stellantriebe AG25 und AG26 stehen ab sofort mit Powerlink-Schnittstelle zur Verfügung.

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

Robuste Mobilfunk-RTUs für IVS-Umgebungen

Red Lion Controls gab kürzlich bekannt, dass die 4G-LTE-Sixnet-Serien RAM 6000 und 9000 seiner industriellen Mobilfunk-RTUs jetzt mit NEMA TS2 Abschnitt 2 konform sind. Ein Einsatz in intelligenten Verkehrssystemen ist dadurch bestätigt. Die einfache Erweiterung für IVS-Umgebungen ohne Kommunikations- oder Überlandleitung bietet Systemintegratoren, Gemeinden, Ingenieurbüros und Netzwerkintegratoren eine einfach einzurichtende Verbindung per Mobilfunknetz. Die hohe Bandbreite und industrielle Härtung der RAM-RTUs unterstützt eine zuverlässige Kommunikation mit entfernten Standorten und solchen, die ihre Position verändern, wie Anhänger zur mobilen Verkehrsregelung. Die Überwachung von Mehrdienstanwendungen wie Videokameras und Verkehrs-überwachungssystemen ist ebenfalls vorgesehen. Zusätzlich verfügen die robusten Mobilfunk-RTUs über große Temperaturbereiche und eine hohe Erschütterungs- sowie Vibrationstoleranz.

Bild: Red Lion Controls Inc.

Die 4G-LTE-Sixnet-Serien RAM 6000 und 9000 von Red Lion Controls sind jetzt mit NEMA TS2 Abschnitt 2 konform.

Red Lion Controls Inc.
www.redlion.net

Cloud-Dienst für das sichere Verbinden von Feldgeräten

Deltas Smart-Factory- und Cloud-Lösung bietet eine Fernsteuerungs- und Überwachungsplattform für das Echtzeitmanagement von Produktionsstätten. Die Lösung beinhaltet die Industrie-3G-Cloud-Router der DX-2100-Serie, um Betriebsdaten der Produktionsstätten von SPSen und industriellen Steuergeräten in Fabriken zu sammeln und sie auf dem Internet-Cloud-Dienst DIACloud zum Management hochzuladen. Sie erlaubt es Anwendern, Produktionsstätten- und Produktionsmanagementinformationen von weltweiten Fabriken in Echtzeit zu sammeln. Der Cloud-Dienst stellt Datensicherheit für alle Benutzer sicher. Derzeit betreibt das Unternehmen Cloud-Server an weltweit sieben Standorten. Bei dem Cloud-Dienst handelt es sich um eine Cloud-basierende IoT-Plattform. Mit dieser und den korrespondierenden Netzübergängen haben Anwender von Feldgeräten die Möglichkeit, zu kommunizieren, Daten zu sammeln, diese auf ein Cloud-Webportal hochzuladen und die Steuerbefehle oder Einstellungen für Feldgeräte jederzeit und überall einzugeben. Die mobile Plattform zeigt Gerätestatus, Alarme und Felddaten an und versendet Steuerbefehle. Die Cloud-Router aktivieren hierfür einen eingebauten sicheren Tunnel zwischen dem Cloud-Dienst und einer Reihe von industriellen Geräten wie SPSen, HMIs, Wechselstrommotorantrieben, Wechselstromservosystemen oder Sensoren.

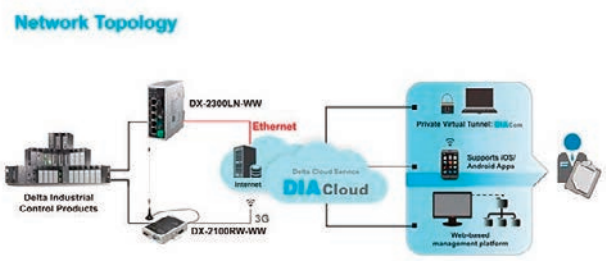


Bild: Delta EMEA

Deltas Smart-Factory- und Cloud-Lösung beinhaltet Industrie-3G-Cloud-Router der DX-2100-Serie, um Betriebsdaten auf dem Internet-Cloud-Dienst DIACloud hochzuladen.

Delta EMEA
www.delta-europe.com

IO-Link-Module für Profinet-Netze in Schutzart IP67

Die Brad-HarshIO-Module von Molex kommunizieren mithilfe des offenen Standardprotokolls IO-Link. Die für Maschinenbauer im Bereich der industriellen Automatisierung konzipierten Module bieten dabei schnelle und zuverlässige Lösungen für den Anschluss industrieller Steuerungen an I/O-Module in rauen Umgebungen. Mit einem in IP67 ausgelegten Gehäuse zum Schutz vor Staub, Flüssigkeiten und Schwingungen lässt sich das kompakte Ethernet-Modul direkt auf der Maschine montieren. Das Push-to-Lock-Verbindungssystem sorgt unabhängig vom jeweiligen Anwender für einen schnellen und sicheren IP67-konformen ➡

- Anzeige -

Wir zeigen den Wert von Industrie 4.0

Smartes System für Predictive Maintenance und Produktionsoptimierung

BAUDIS IoT

◎ IoT-Nachrüstung von Bestands- und Neumaschinen
◎ Planbare Instandhaltung reduziert Servicekosten
◎ Hersteller- und baujahrunabhängig einsetzbar

HANNOVER MESSE

Besuchen Sie uns auf der Hannover Messe 2017:
24.–28. April 2017
Halle 14, Stand H12

BAUMÜLLER

be in motion

www.baumueller.de

Anschluss von Verbindungskabeln. Die Produktfamilie umfasst Profinet-IO-Link-Master-Module im 60mm-Format sowie digitale Hubs. Die Module verfügen über acht M12-Ports, wobei jeder Port einen IO-Link-Masterkanal und einen konfigurierten digitalen I/O-Kanal umfasst. Die digitalen Hubs besitzen insgesamt 16 Eingänge oder 12 Eingänge und vier Ausgänge. Aufgrund der Daisy-Chain-Verdrahtung und einem integrierten 2-Port-Switch mit Vollduplex-Datenübertragung mit einer Geschwindigkeit von 100MB/s lassen sich Anwendungen komplett ohne Switches zu niedrigeren Kosten verdrahten. Besondere Merkmale der Module wie Kurzschlussschutz, Media Redundancy Protocol (MRP), Webserver und gut sichtbare Diagnose-LEDs sorgen für eine hohe Anwenderfreundlichkeit und eine einfache Bedienbarkeit.

Bild: Molex Deutschland GmbH

Die Brad-HarshIO-Module von Molex kommunizieren mithilfe des offenen Standardprotokolls IO-Link.

Molex Deutschland GmbH
www.molex.com

IEC-62439-3-konformes HSR/PRP-Erweiterungsmodul

Advantechs Erweiterungsmodul ECU-P1524PE ist konform mit den Protokollen der IEC-62439. Damit bietet es einen einfachen Zugang zu den Standards HSR und PRP, ohne dabei die CPU-Last zu erhöhen oder die Installation zusätzlicher Geräte in der Schaltanlage erforderlich zu machen. Auf diese Weise verhilft das Modul dem Netzwerk sowohl zur Zero-loss-Redundanz als auch zur Zero-time Recovery und damit zu höherer Kommunikationssicherheit und Applikationsleistung. Mit einer typischen Ringtopologie ermöglicht es HSR den Quellknoten, alle Datenpakete zu verdoppeln und sie in jeweils eine der beiden Richtungen zu schicken. Dadurch wird eine Redundanz erreicht, ohne dass Kabel oder Switche verdoppelt werden müssen.

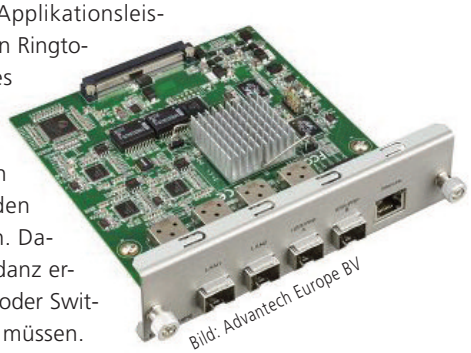


Bild: Advantech Europe BV

Beim ECU-P1524PE von Advantech handelt es sich um ein IEC-62439-3-konformes Erweiterungsmodul.

Advantech Europe B.V.
www.advantech.eu

Softwaregestütztes Verfahren zur Datenkommunikation per App

Bild: © ClarkandCompany/iStock.com und IVG Göhringer

Mit der IVGNetApp erfolgt die Profinet-Abnahme anhand einer Tablet-gestützten Sichtprüfung.

IVG Göhringer hat für die anlagenweite Datenkommunikation ein softwaregestütztes Verfahren konzipiert. Die darauf basierende IVGNetApp gibt dem Anwender einen strukturierten und fundierten Prozess vor und unterstützt damit eine systematische Vorgehensweise. Die App ist neben Profinet auch für Profibus, Interbus, CAN und AS-Interface verfügbar und berücksichtigt die Besonderheiten der einzelnen Netzwerk- und Bussysteme. Per Tablet und App ist das Anlagenpersonal in der Lage, die geführte Sichtprüfung selbst zu erledigen und die erkannten Fehler zu beheben. Werden bestimmte Fragen mit nein beantwortet, so gilt es, mithilfe geeigneter Messtechnik zu entscheiden, ob es erforderlich ist, korrigierend einzugreifen.

I-V-G Göhringer
www.i-v-g.de

Melde- und Befehlsgeräte via Profinet mit der Steuerung verbinden

Siemens bietet für seine Befehls- und Meldegeräte eine neue Kommunikationsanbindung an. Mit Sirius ACT lassen sich die Geräte direkt mit der Steuerung über Profinet verbinden. Zudem lassen sich auch Sicherheitslösungen schnell realisieren. Die flexible Kommunikationslösung reduziert den Verdrahtungsaufwand sowie die Fehlerquellen und erleichtert die Anpassung bei Änderungen. Dazu werden die Befehlsstellen mit den aufgeschnappten Terminalmodulen einfach per Flachbandleitung mit dem Interface-Modul verbunden. Über das Interface-Modul erfolgt dann die Profinet-Kommunikation und der Austausch mit der Steuerung. Für Sicherheitslösungen wie den Nothalt schnappen Anwender diesen einfach auf das fehlersichere Interface-Modul auf. Die Geräte sind für den einfachen Aufbau von Bedienpanels ausgelegt und lassen sich einfach über Profinet an z.B. eine HMI-Schnittstelle anschließen und im TIA Portal projektieren sowie parametrieren.

Bild: Siemens AG

Die flexible Kommunikationslösung Sirius ACT verbindet Befehls- und Meldegeräte über Profinet direkt mit der Steuerung.

Siemens AG
www.siemens.de

Gateway verbindet Maschinen und Anlagen mit der Feldbusebene

Bild: Eaton Industries GmbH

Das Gateway EU5C-SWD-Sercos dient der Kommunikation innerhalb von Maschinen und Anlagen.

Eaton bietet Maschinen- und Anlagenbauern eine Möglichkeit, das intelligente Verdrahtungs- und Kommunikationssystem SmartWire-DT an den Feldbus Sercos III anzubinden. Das Gateway EU5C-SWD-Sercos ist aus einer Kooperation mit Hilscher hervorgegangen und unterstützt die Feldbusprotokolle Profibus-DP, CANopen, Modbus-TCP, Ethernet/IP, Profinet, Powerlink und Ethercat sowie das Sercos-Protokoll. Das Kommunikationssystem sorgt mithilfe des Moduls für eine einfache Planung, Projektierung, Verdrahtung, Inbetriebnahme und Wartung. Das Modul eignet sich für Befehls- und Meldegeräte, Schütze und Motorschutzschalter, Module zur Sicherungsüberwachung, Softstarter, Drehzahlstarter, Frequenzumrichter und Leistungsschalter.

Eaton Industries GmbH
www.eaton.de

Ethernet Switch für den industriellen Einsatz

Bild: Spectra GmbH & Co. KG

Der Ethernet Switch IGPS-9080-24V von Spectra verfügt über acht Ports.

Spectra bietet mit dem IGPS-9080-24V einen kompakten 8-Port-Ethernet-Switch mit PoE, 30W Leistung je Port und Gigabit-Ethernet für den industriellen Einsatz an. Ein robustes Metallgehäuse, die Möglichkeit zur DIN-Schienen-Montage und ein Temperaturbereich von –40 bis +70°C zeichnen den industriellen Switch aus. Er verfügt zudem über zwei redundante Spannungseingänge von 12 bis 57VDC. Für redundante Datenströme sorgt die Administrierbarkeit, die den Aufbau einer Ringstruktur mit <30ms Recovery-Time ermöglicht. Darüber hinaus stehen Funktionen wie Jumbo Frame, PoE Auto-Ping Check und IP-based Bandwith Management zur Auswahl.

Spectra GmbH & Co. KG
www.spectra.de

Industrie-Router mit weitem Temperaturbereich

Die Router der Serie Wienet v3 von Wieland Electric verfügen über eine hohe Leistung und zahlreiche Einsatzmöglichkeiten. Der weite Temperaturbereich von –40 bis +75°C erlaubt den Einsatz unter harten Umweltbedingungen und der Eingangsspannungsbereich von 10 bis 60VDC ermöglicht optional PoE. Die Router eignen sich für die Branchen Maschinenbau, Logistik, Energietechnik und Energieerzeugung. Die Verbindung ins Internet erfolgt über LAN, WLAN oder Mobilfunk. Der LTE-Chipsatz sorgt im Mobilfunkbetrieb für eine hohe Bandbreite. Verschlüsselte VPN-Verbindungen sorgen für große Sicherheit der zu übertragenden Daten und automatische Backup-Verbindungen ins Internet sichern den störungsfreien Arbeitsablauf.

Bild: Wieland Electric GmbH

Der Temperaturbereich der Wienet-v3-Router reicht von –40 bis +75°C.

Wieland Electric GmbH
www.wieland-electric.com

MURR ELEKTRONIK
stay connected

24 V STROM-ÜBERWACHUNG
MAXIMAL MODULARISIERT!

JETZT NEU!

Mico Pro®

HANNOVER MESSE
Besuchen Sie uns:
Halle 9, Stand D27
24. bis 28. April 2017

murrelektronik.de

Standard-Ethernet für die Automatisierung

Quo vadis, TSN?

In der Branche ist Time Sensitive Networking als Weiterentwicklung des Ethernet-Standards in aller Munde. Bislang ist Standard-Ethernet für Anwendungen in der Automatisierung nicht geeignet, weil es weder deterministisch noch echtzeitfähig ist. Und dennoch hat sich Ethernet in speziellen Ausprägungen durchgesetzt. Was macht TSN eigentlich so interessant für die Branche? Kann TSN im Kontext von Industrie 4.0 einen offenen Kommunikationskanal zwischen verschiedenen Systemen liefern?

Damit industrielle Steuerungssysteme sicher und effizient arbeiten können, ist deterministische und echtzeitfähige Kommunikation eine Voraussetzung. Anders ist es bei IT-Systemen, bei denen eher der offene Datenzugang im Vordergrund steht. Diese Ambivalenz der Bedürfnisse gilt es in Zeiten von Industrie 4.0 auszuloten, denn es werden einerseits sichere Maschinen, andererseits freier Zugang, Analyse und Nutzung der Daten gefordert. Es braucht also eine offene und herstellerunabhängige Kommunikationsplattform, die beiden Seiten gerecht wird.

Bild: Bosch Rexroth AG

ABB, Bosch Rexroth, B&R, Cisco, General Electric, Kuka, National Instruments, Parker Hannifin, Schneider Electric, SEW-Eurodrive und TTTech wollen gemeinsam OPC UA TSN als einheitliche Kommunikationslösung zwischen industrieller Steuerung und der Cloud vorantreiben. Die Gruppe von Automatisierungs- und Informationstechnologieherstellern gab auf der SPS IPC Drives 2016 bekannt, OPC UA TSN als einheitliches Protokoll für die Kommunikation im Industrial Internet of Things bis zur Steuerungsebene zu forcieren. Erste Prototypen werden bereits in ein Testbed des IIC integriert. 2017 sollen erste Produkte am Markt verfügbar sein.

Treiber Automobilindustrie

Ursprünglicher Initiator von TSN ist der Broadcasting-Bereich, der heutige große Treiber ist allerdings die Automobilbranche. Denn nicht nur in der Industrie, auch in Kraftfahrzeugen ist die Datenmenge gestiegen, so dass die Bandbreite bisheriger Bussysteme zukünftig nicht mehr ausreicht. Die Automobilbranche setzt auf den Standard, weil er ein synchronisiertes und priorisiertes Streaming von Audio- und Videodateien ermöglicht. Die IEEE TSN Task Group hat sich Ende 2012 aus der AVB-Arbeitsgruppe entwickelt. Oberstes Ziel ist es, industrielle Systeme mit ihren verschiedenen Netzwerken zu verschlanken und zueinander inkompatible Protokolle zu entfernen. Denn diese überlaufenen Systeme sind einerseits nicht flexibel, andererseits können sie nicht ihr volles Leistungspotential entfalten. Konkrete Themen der Arbeitsgruppe sind z.B. Zeitsynchronisierung im Netz, zeitliches Scheduling von über das Netzwerk versendeten Datenpaketen für garantierte Latenzzeiten oder Netzwerkredundanz. Weil TSN-Mechanismen in großem Umfang in der Automobiltechnik implementiert werden sollen, können industrielle Anwender deshalb davon ausgehen, dass die TSN-Basistechnologie in Form von Prozessoren und Halbleiterlösungen zu sehr attraktiven Preisen auf den Markt kommt.

TSN plus OPC UA

Da es sich bei TSN nicht um einen einzelnen Standard, sondern vielmehr um eine Gruppe von Standards handelt, decken diese verschiedene Aspekte der Echtzeitkommunikation und Zuverlässigkeit ab. TSN stellt Mechanismen bereit, mit denen sich über Standard-Ethernet-Verbindungen verteilte, synchronisierte Systeme mit harten Echtzeitanforderungen erstellen lassen. Diese Systeme nutzen sowohl für die Echtzeitsteuerung als auch für die Übertragung von IT-Daten dieselbe Infrastruktur, darum werden Steuerung, Regelung, Messungen, Konfiguration, Benutzeroberflächen und Dateiaustausch in einem Netzwerk zusammengeführt. Je nach Anwendung ist es ausreichend, Geräte einzusetzen, die nur einen Teil der TSN-Standards realisieren. Die Kombination von OPC UA Publisher/Subscriber und TSN ermöglicht eine offene und vor allem nicht-herstellerspezifische Technologie. Sowohl Anbieter, als auch Anwender und Nutzerorganisationen sehen in dieser Kombination eine zukunftstaugliche Alternative bzw. Erweiterung zu den bisher eingesetzten industriellen Ethernet-Protokollen. *(clj)* ■

Time Sensitive Networking

Schöne neue Welt?

Mit Time Sensitive Networking (TSN) als Weiterentwicklung des Ethernet-Standards eröffnet sich der industriellen Kommunikation eine große Chance. Es besteht aber noch großer Informationsbedarf in der Branche: Wo liegt das größte Potenzial von TSN für den Maschinen- und Anlagenbau und die industrielle Automatisierung? Welche neuen Möglichkeiten werden entstehen? Das INDUSTRIAL COMMUNICATION JOURNAL hat bei verschiedenen Experten nachgefragt.

Einheitliches Protokoll für die Kommunikation im IIoT

In Kombination mit OPC UA wird TSN eine große Auswirkung auf die industrielle Produktion haben. Wir sehen in OPC UA TSN das einheitliche Protokoll für die Kommunikation im Industrial IoT bis zur Steuerungsebene. Gemeinsam mit Partnerunternehmen haben wir bereits in der Praxis bewiesen, dass OPC UA TSN alle Anforderungen für die Kommunikation von der Linien- bis zur ERP-Ebene erfüllt. Für die Produktivität vernetzter Maschinen und Anlagen ist eine reibungslose Kommunikation zwischen den einzelnen Teilsystemen und Komponenten entscheidend. Dabei ist es Maschinen- und Anlagenbauern sehr wichtig, dass ihre Möglichkeiten beim Umsetzen eines Prozesses in eine Maschine oder Anlage nicht durch proprietäre Lösungen eingeschränkt werden. Der offene Standard OPC UA setzt sich daher zunehmend als Kommunikationsprotokoll von der Steuerungsebene bis zu ERP-Systemen durch. Ethernet TSN ist die ideale Ergänzung zu OPC UA auf Linienebene, wo Zykluszeiten von bis zu zwei Millisekunden benötigt werden. Ein großer Vorteil von TSN ist zudem, dass auch die Automobilbranche auf diesen Standard setzt. Damit werden die nötigen Halbleiter-Baugruppen sehr schnell und vergleichsweise kostengünstig verfügbar sein

> *„Ethernet TSN ist die ideale Ergänzung zu OPC UA auf Linienebene, wo Zykluszeiten von bis zu zwei Millisekunden benötigt werden.“*
>
> *Sebastian Sachse, Technology Manager Open Automation, B&R*

Bild: B&R Industrie-Elektronik GmbH

TSN ist kein Feldbus

TSN wird hilfreiche Erweiterungen für Ethernet bereitstellen. Allerdings: Über TSN sind aktuell mehr Mythen als Fakten im Umlauf. Zu den Mythen gehört, dass TSN die Sauce ist, die man einfach über ein Ethernet-Gericht gießt, um es echtzeitschmackhaft zu machen. Zu den Fakten gehört, dass TSN ein Bündel von Protokollen und Technologien in unterschiedlichsten Entwicklungsstadien umfasst, von denen viele (aber nicht alle) die Verbesserung der Echtzeiteigenschaften von Ethernet zum Ziel haben. TSN ist also ein Werkzeugkasten, aus dem man sich je nach Bedarf bedienen kann. Die Werkzeuge sind vergleichbar mit früheren Ethernet-Entwicklungen wie „Switche statt Hubs“ – irgendwann waren Switche durchgängig vorhanden, und dann konnte man ihre Eigenschaften nutzen. Ein weiterer Fakt: Ethernet mit TSN-Eigenschaften wird zwar weitgehend deterministisch werden, aber auch bei weitem nicht so schnell und effizient, wie es die Mythen suggerieren. Und: TSN ist kein Feldbus und wird auch keiner werden. TSN wird auch aus OPC UA Pub/Sub keinen Feldbus machen. TSN-Features werden aber helfen, die Echtzeiteigenschaften der Kommunikation zwischen Steuerungen zu verbessern – mit dem Ethercat Automation Protocol oder OPC UA. Unterstützt durch TSN werden Steuerungen über die beim Anwender vorhandene Ethernet-Infrastruktur auf ein Netzwerk aus Ethercat-Slaves zugreifen können. TSN wird auch dazu beitragen, die Cloud-Kommunikation deterministischer zu machen. TSN wird also bei einigen Industrial-Ethernet-Technologien genutzt werden, diese aber nicht ersetzen. Die Ethercat Technology Group trägt zur TSN-Entwicklung bereits seit dem ersten Tag bei – schon als TSN noch als AVB be-

kannt war – und ist in der entsprechenden Arbeitsgruppe innerhalb der IEEE 802.1 aktiv. So wird sichergestellt, dass Ethercat in den genannten Anwendungsfällen von TSN profitieren kann und wird.

> *„TSN wird bei einigen Industrial-Ethernet-Technologien genutzt werden, diese aber nicht ersetzen.*
> *Martin Rostan, Executive Director, Ethercat Technology Group*

Bild: Ethercat Technology Group

Einmalige Chance für die Feldebene

Für die Technologien von Profibus und Profinet sehen wir großes Potential in TSN. Die Mechanismen, die in der IEEE entwickelt werden, versprechen Synchronität und Robustheit in der industriellen Kommunikation. Und das ist auch wichtig, da die Datenmenge, die künftig über die Netze transportiert werden, mit Industrie 4.0 noch weiter ansteigen werden. Hier ist es wichtig, über alle Ebenen eine stabile Kommunikation zu ermöglichen. Dies haben wir heute schon durch Mechanismen wie IRT (Isochronous Realtime) bei Profinet in der Feldebene erreicht, aber mit TSN ergibt sich die Möglichkeit, dieses Verfahren auf das gesamte Netz in der Anlage auszudehnen. Auf der anderen Seite bietet die Technologie die Chance, auch in der Feldebene auf Standard-Ethernet-Controller zu setzen und so noch schneller von den Entwicklungen im IT-Bereich zu profitieren, wie z. B. der höheren Bandbreite durch Gigabit Ethernet. Das ist also auch eine einmalige Chance für die Feldebene. Mit Profinet und IRT haben wir bereits bewiesen, dass diese Mechanismen funktionieren. Daher werden wir TSN auch für Profinet nutzbar machen. Bis es aber soweit ist, sind noch einige Hürden zu überwinden. Insbesondere das Thema Konfiguration muss einfacher werden als dies heutige Lösungen sind, damit die neue Technologie im Markt angenommen wird. Daran arbeiten wir in unserem Industrie 4.0 Arbeitskreis. Unser Ziel ist es, ein konvergentes Netzwerk zu erreichen, in dem unterschiedliche Protokolle genutzt werden können, ohne dass es zu Beeinträchtigungen kommt. Ein echter Mehrwert für die Anlagenbetreiber.

> *„Die Konfiguration muss einfacher als bei heutigen Lösungen werden, damit die neue Technologie im Markt angenommen wird.*
> *Karsten Schneider, Chairman, Profibus & Profinet International*

Bild: Profibus Nutzerorganisation e.V.

- Anzeige -

EMBEDDED DESIGN
Smarte Systeme für das Internet of Things

Mit dem **EMBEDDED DESIGN Fachmagazin**, dem **Newsletter** und der **Website** haben Sie alle relevanten Medien für **Embedded-Systeme** und das **Internet der Dinge** aus einer Hand.

embedded-design.net

Bild: ©sdecoret-FOTOLIA.com

TSN und Sercos

Übertragungsprinzip aufgegriffen

Time-Sensitive Networking soll eine zeitgesteuerte und deterministische Übertragung von echtzeitkritischen Nachrichten über Standard-Ethernet-Hardware möglich machen. Dabei nutzt Ethernet TSN das Prinzip eines Zeitschlitzverfahrens, das Sercos bereits seit über 25 Jahren für die Echtzeitkommunikation verwendet. Zunächst für die Antriebskommunikation mit Sercos I und II auf LWL-Basis, später mit Sercos III auf Basis von Fast Ethernet.

Die Vorteile einer Verwendung von Ethernet TSN liegen auf der Hand. Es kann eine Standard-Ethernet-Hardware mit integrierter Echtzeitfähigkeit eingesetzt werden, was in einem breiten Hersteller- und Produktangebot und niedrigen Kosten resultiert. Gleichzeitig profitieren Hersteller und Anwender von den technischen Weiterentwicklungen von Ethernet wie z.B. höhere Übertragungsraten, Redundanzverfahren oder Funkübertragung. Der TSN-Standard ermöglicht die Konvergenz von Produktions- und IT-Netzen, d.h. Echtzeitkommunikation und normale Ethernet-Kommunikation können über einen einheitlichen Standard übertragen werden.

Sercos und Ethernet TSN im Vergleich

Das Übertragungsverfahren von Sercos ist im Standard IEC61784/61158 beschrieben. Unter anderem werden dort das Zeitschlitzverfahren, die zyklische Übertragung der Echtzeittelegramme im Echtzeitkanal und die Übertragung beliebiger anderer Ethernet-Protokolle im sogenannten UC-Kanal spezifiziert. Die Basis von Ethernet TSN ist hingegen der Standard IEEE802.1Q, welcher die Aufteilung physikalischer Netzwerke in mehrere logisch getrennte, priorisierte virtuelle Netze spezifiziert. Mit verschiedenen Substandards werden darauf aufbauend ergänzende Features spezifiziert, die im Folgenden erläutert werden und in den Kontext des Übertragungsverfahrens von Sercos gebracht werden.

Zeitsynchronisation

Alle Netzwerkteilnehmer haben ein gemeinsames Verständnis der Zeit.

- Bei Sercos leiten alle Netzwerkteilnehmern ihre Synchronisation (Zeit) aus dem zyklisch übertragenen MST im ersten Sercos Frame ab, welches der Master generiert und von allen Netzwerkteilnehmern empfangen wird. Die Gleichzeitigkeit unter allen Sercos Geräten wird dadurch erreicht, dass die Laufzeiten im Netzwerk kompensiert werden.
- Um eine einheitliche Zeitbasis im gesamten Netz zu schaffen nutzt Ethernet TSN Mechanismen aus IEEE802.1ASrev bzw. IEEE1588. Das darin beschriebene Protokoll zur Zeitsynchronisation (PTP=Precision Time Protocol) definiert, wie räumlich verteilte Echtzeituhren untereinander synchronisiert werden.

Zeitschlitzverfahren

Synchrone Zeitschlitze erlauben die Übertragung verschiedener Traffic-Klassen und eine zeitgesteuerte Datenübertragung.

- Bei Sercos werden das Zeitraster und die Zeitschlitze (Kanäle) während des Hochlaufs durch den Sercos Master festgelegt.
- Ethernet TSN nutzt dafür den IEEE-Substandard IEEE802.1Qbv (Zeitmultiplexverfahren).

- Anzeige -

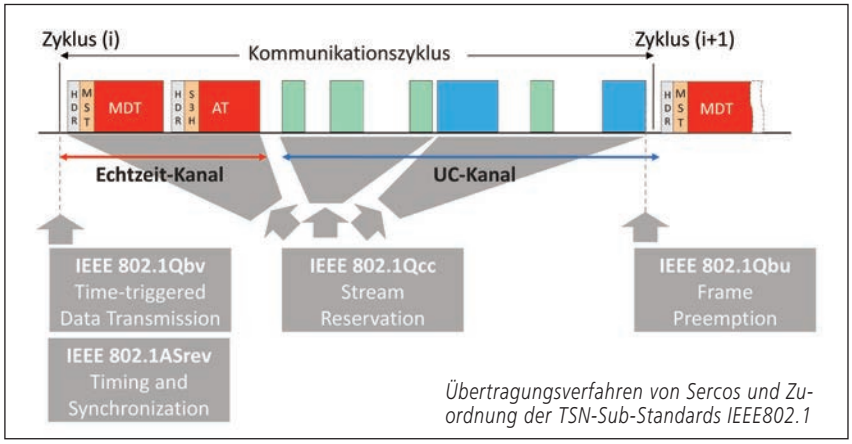


Bild: Sercos International e.V.

Übertragungsverfahren von Sercos und Zuordnung der TSN-Sub-Standards IEEE802.1

Scheduling und Traffic Shaping

Alle teilnehmenden Geräte arbeiten bei der Bearbeitung und Weiterleitung von Netzwerkpaketen nach den gleichen Regeln.

- Bei Sercos werden alle Echtzeit-Telegramme während des Knotendurchlaufs bearbeitet und sofort weitergeleitet ('On-the-fly'). Weitere Ethernet-Telegramme im UC-Kanal werden im Cut-Through oder Store-and-Forward-Verfahren empfangen bzw. weitergeleitet. Ohne laufendes Sercos Protokoll steht die komplette Bandbreite für beliebige Ethernet-Protokolle zur Verfügung.
- Ethernet TSN nutzt dafür den IEEE-Substandard IEEE802.1Qcc (Stream Reservation).

Frame Preemption

Telegramme können unterbrochen und später fortgesetzt werden.

- Bei Sercos werden Telegramme im UC-Kanal, die aufgrund ihrer Länge mit dem Beginn des nächsten Kommunikationszyklus kollidieren würden, zwischengepuffert und im nächsten Zyklus übertragen oder bei Überlast ggfs. auch verworfen.
- Ethernet nutzt dafür den IEEE-Substandard IEEE802.1Qbu (Frame Preemption).

Zusammenfassend besitzt Ethernet TSN alle Eigenschaften und Mechanismen, um das Sercos-Übertragungsverfahren mit Standard-Ethernet-Hardware nachzubilden. Zudem ergibt sich ein interessanter Ansatz daraus, Sercos-III-Geräte in einer TSN-Netzwerkinfrastruktur gemeinsam mit anderen Ethernet- und TSN-Geräten zu betreiben. Dies war der Ausgangspunkt für einen Sercos-TSN-Demonstrator, der als Proof of Concept dienen sollte und auf der SPS IPC Drives 2016 Premiere feierte.

Proof of Concept für Sercos über TSN

Der Sercos TSN Demonstrator wurde vom ISW der Universität Stuttgart mit Unterstützung von mehreren Industriepartnern realisiert. Er zeigt die Möglichkeiten auf, eine echtzeit- und multiprotokollfähige Netzwerkinfrastruktur auf Basis von TSN für die Automatisierungstechnik und darüber hinaus bereitzustellen. Zum Einsatz kommt dabei ein TSN-basierter Sercos III SoftMaster mit einer Soft-CNC des Anbieters ISG. In diesen Master wurde das Precision Time Protocol nach IEEE1588 integriert, so dass sämtliche Netzteilnehmer, die über TSN-Switche der Firma Hirschmann kommunizieren, eine einheitliche Zeitbasis verwenden. Parallel zur Sercos-Echtzeitkommunikation über TSN werden Videostreams einer Webcam zu einem Remote-Display übertragen, ohne jedoch die Charakteristik und Funktionalität der Echtzeitübertragung zu beeinträchtigen. Die Untersuchung des Echtzeitverhaltens zeigte, dass sich die Fehler in der Zeitsynchronisation auf einen zweistelligen Nanosekundenbereich beschränken.

Integration ohne Abstriche

„Mit dem Sercos TSN Demonstrator ist der praktische Nachweis erbracht, dass Sercos-III-Geräte unverändert in ein TSN-Netzwerk integriert werden und über TSN miteinander kommunizieren können. Dabei werden weder Funktionalität noch Echtzeitcharakteristik eingeschränkt. Auch können bestehende Tools, wie beispielsweise der Sercos Monitor als Diagnose- und Analysewerkzeug, weiterhin vollumfänglich verwendet werden", so Peter Zahn, Projektleiter für den Sercos TSN Demonstrator am ISW. „Die Umsetzung von TSN in Produkten setzt eine solide technische Plattform in der Zeitsynchronisation voraus", ergänzt Dr. Oliver Kleineberg, zuständig für den Bereich Advance Development bei Hirschmann. „Somit waren die Switche vom Typ RSP35 mit ihren FPGAs und der umfassenden Unterstützung für das IEEE1588-Protokoll der geeignete Träger für eine prototypische Entwicklung, die aller Voraussicht nach bis zur Serienreife weitergehen wird. 2017 erwarten wir die ersten Ergebnisse aus unserer TSN-Entwicklungsarbeit." Der kurze Zeithorizont und der Optimismus begründe sich aus der bereits jetzt hohen Stabilität der TSN-Prototypen und der Erfolge in der Entwicklung. Auf Basis der IEEE-TSN-Standards sei eine effiziente und zielgerichtete Entwicklung bereits heute möglich. „Der Sercos TSN Demonstrator zeigt eindrucksvoll auf, dass TSN die Konvergenz von herkömmlichen Echtzeit-Ethernet-Lösungen zu einer einheitlichen, standardisierten und durchgängigen Netzwerkinfrastruktur ermöglicht", fügt Peter Lutz, Geschäftsführer von Sercos International, hinzu. „Sercos profitiert von TSN gleich in mehrfacher Hinsicht. Zum einen können Standard-Ethernet-Komponenten mit integrierter Echtzeitfähigkeit eingesetzt und damit flexible Netzwerktopologien realisiert werden. Zum anderen stehen mit Ethernet TSN auch höhere Übertragungsbandbreiten zur Verfügung." ■

Sercos-over-TSN-Demonstrator auf der SPS IPC Drives 2016

Bild: Sercos International e.V.

Firma: ***Sercos International e.V.***
www.sercos.de

Industrie 4.0: Sortieren, bewerten, weiterentwickeln

Details für die Zukunft

Bei der aktuellen Vielfalt an Meinungen und Diskussionen rund um Industrie 4.0 steht meist der theoretische Ansatz im Vordergrund. Dabei ist für entsprechende Konzepte und Lösungen, die in der Praxis funktionieren sollen, sehr viel Detailarbeit nötig. Das zeigt ein Blick hinter die Kulissen der Industrie 4.0 Working Group von PI (Profibus & Profinet International).

Von UseCases zu realer Technologie

Bild: Profibus Nutzerorganisation e.V.

Tatsache ist, dass viele der Themen, die mit IoT und Industrie 4.0 in Verbindung gebracht werden, wie IPv6 oder TSN, nicht von der Automatisierungsindustrie, sondern von der IT- und Kommunikationsseite getrieben werden. „Die Herausforderung ist es, zu beurteilen, welche von diesen vielen Detailfunktionen denn eigentlich benötigt werden", beschreibt Xaver Schmidt, Leiter der Working Group 'Industrie 4.0' von PI (Profinet & Profibus International) die derzeitige Situation. Und dies ist angesichts der unterschiedlichen Anwendungen, Branchen und Interessen gar nicht so einfach. Die Arbeitsgruppe ist daher international (Mitglieder aus China, Japan, USA und Europa) aufgestellt, besetzt unterschiedliche Branchen und steht in Kontakt mit Anwenderverbänden wie Aida und Namur. In der Gruppe sind auch System- und Gerätehersteller sowie Anbieter von Basistechnologien vertreten. „Wir müssen abstrakte Theorien in eine begreifbare und anwendbare Technik umwandeln", führt Schmidt aus und nennt als Beispiel: „Der Zugriff auf die Daten, die für Instandhaltungsaufgaben im Sinne von Industrie 4.0 nötig sind, muss einfach sein, sonst hat er in der Praxis keine Chance. Einfachheit ist in der Regel jedoch mit standardisierten Mechanismen gleich zu setzen. Das heißt, jemand muss sich mit Standards, Normen und Richtlinien beschäftigen und sie mit den bisherigen und neuen Technologien abgleichen. Das ist sehr zeitaufwändig, aber es lohnt sich." Der Arbeitskreis habe daher seine Schwerpunkte auf die Anwendbarkeit (also Use Cases), Technologie und Standardisierung gelegt. „Aus Sicht von Profinet haben sich dann aus der Kombination von Anforderungen und technischen Möglichkeiten die Themenschwerpunkte IPv6, OPC UA, Security, Semantik und TSN herauskristallisiert. Sie werden aktuell in den eigens geformten Teams diskutiert", so Schmidt.

Autoadressierung als Thema der Zukunft

IPv6 wird vor allem durch die IT-Branche getrieben. Die Automatisierungstechnik wird trotzdem davon profitieren, so sind in puncto Kommunikation die Autoadressierung und neue Namenskonzepte interessant. „In Zukunft werden nicht mehr einfach IP-Adressen vergeben, wie wir sie kennen, sondern sie werden viel länger und schwieriger. Diese manuell nachzutragen oder zu verwalten, ist schlicht nicht mehr möglich, da viel zu viele Fehler passieren würden. Hier benötigen wir intelligente Mechanismen der Autoadressierung", erklärt Schmidt. Ähnliches gilt für die Namensauflösung.

	Status Technik	Vorgehen	Ziel
IPv6	Viele Detailfunktionen im Standard	Erarbeiten Konzept Abstimmung mit Kunden incl. IT	Autoadressierung Namenskonzept
OPC UA	Parallele Kommunikation Integrierte Lösungen verfügbar	Klärung Marktbedarf	Zusammenarbeit mit OPC
Security	Diverse Anforderungen Verschiedene Lösungen	Auswahl anhand von Anforderungen / Usecases	Integration der benötigten Security-Features
Semantics	eClass, Automation ML,...	Auswahl der wichtigsten Definitionen	Integration der bestehenden Features in Standard
TSN	Viele Detailfunktionen im Standard	Abbildung von PN auf TSN	Partizipieren vom technischen Fortschritt der Standard-Ethernet-Technologie

Bild: Profibus Nutzerorganisation e.V.

Technologien, die den Schwerpunkt der Weiterarbeit bilden

OPC UA – Parallele Kommunikation

Es zeichnet sich heute ab, dass die serviceorientierte Architektur von OPC UA ein Baustein für die Entwicklung von Industrie 4.0 sein wird, insbesondere wenn es z.B. um die Kommunikation mit Geräten wie Bedienerstationen über der Controller-Ebene oder um Produktionsdaten von den Geräten zur Unternehmens-IT oder in die Cloud geht, vor allem in einer Umgebung mit unterschiedlichen Anbietern. Während Profinet in Automatisierungssystemen die Übertragung von deterministischen Real-Time-Daten und steuerungsrelevanten azyklischen Daten übernimmt, wird OPC UA zum Bindeglied für die nicht deterministische Kommunikation zwischen Geräten und überlagerten Servicediensten und zwischen den Controller-Ebenen. „Hier ergänzen sich Profinet und OPC UA perfekt, da Profinet eine offene Kommunikation auf Basis von TCP/IP ohne zusätzlichen Aufwand parallel erlaubt“, so Schmidt. Es sei bereits heute Praxis, dass eine Steuerung in Echtzeit über Profinet automatisiert wird, aber Qualitäts- und Servicedaten per OPC UA übertragen werden und zwar über ein- und dasselbe Kabel. Seit zwei Jahren arbeitet die Nutzerorganisation eng mit der OPC Foundation zusammen – mit dem Fokus auf Industrie-4.0-Anwendungen. In weiteren Schritten sollen die Beschreibungsmöglichkeiten von OPC UA genutzt werden, um z.B. Diagnosedaten oder Profinet-Geräte abzubilden. Mit der kürzlich definierten Pub/Sub-Spezifikation für OPC UA wird die heutige im Prinzip auf Punkt-zu-Punkt-Kommunikation ausgerichtete Client/Server-Architektur von OPC UA durch einen Publish/Subscribe-Mechanismus erweitert, der dann auch eine One-to-Many- bzw. Many-to-One-Kommunikation erlaubt. In Kombination mit TSN kann dieser Mechanismus sogar echtzeitfähig gemacht werden, was z.B. interessant für die deterministische M2M-Kommunikation bei Industrie 4.0 ist.

Ohne Security ist kein Industrie 4.0 möglich

Security hat bei PI einen hohen Stellenwert. „Bei aller Dringlichkeit: Gerade bei diesem Thema ist es wichtig, sich auch einmal zurück zu lehnen und gut zu analysieren. Das Konzept muss schlag-

Konsequente Weiterentwicklung auf Basis bewährter Standards

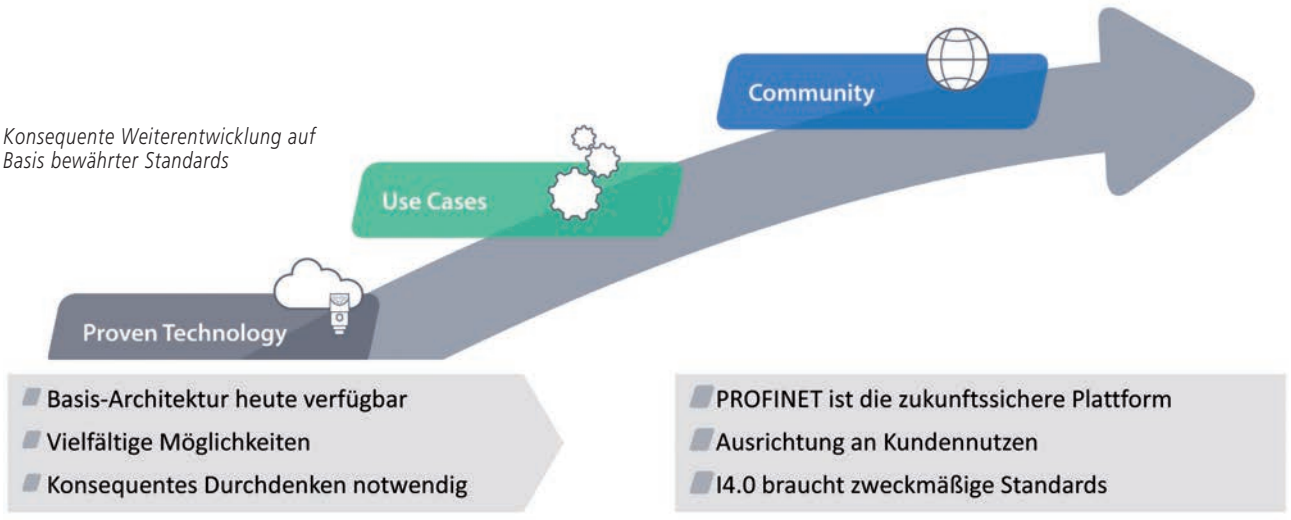


Bild: Profibus Nutzerorganisation e.V.

kräftig, aber auch zukunftsgerichtet sein und darf die Funktion der Anlagen nicht gefährden", bringt es Schmidt auf den Punkt. Authentizität und Integrität sind Anforderungen, die immer stärker beachtet werden müssen, wenn im Zuge von Industrie 4.0 Geräte aus der Controller- oder Geräteebene direkt an überlagerte Servicedienste angeschlossen werden. „Die besondere Herausforderung ist State-of-the-Art-Security-Mechanismen für die Automatisierungstechnik im gesamten Life-Cycle anwendbar zu machen. So ist es einfach nicht möglich, z.B. Schlüssel per SmartCard in sämtlichen Geräten zu hinterlegen", erklärt Schmidt. „Gleichzeitig muss auch hier das entsprechende Normenumfeld beachtet werden, bei Security entsprechend die IEC62443."

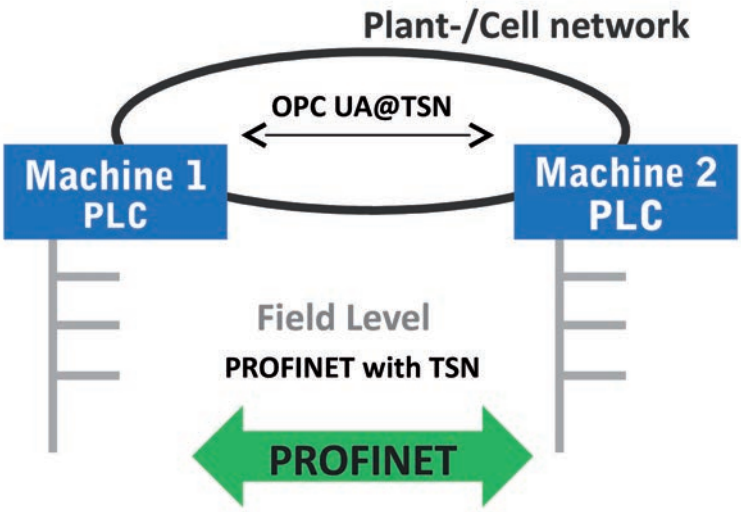
Semantik – Daten als wertvoller Rohstoff

Das Team Semantik hat sich zum Ziel gesetzt, bestehende Profinet-Features im Standard zu integrieren, wobei die wichtigsten Definitionen bei den zugrunde gelegten Standards eCl@ss und Automation ML auszuwählen sind. „Das Problem hierbei ist, dass die Daten maschinenlesbar sein müssen. Und es gibt noch Auswahllisten, wo Profinet nicht ausreichend auftaucht, weil es schlicht vergessen oder die Details übersehen wurden. Hier müssen Schritt für Schritt Erweiterungen eingebracht werden", beschreibt Schmidt die Situation. Das Ziel muss es sein, die Bedeutung von Daten und Funktionen eines Feldgerätes eindeutig und vor allem herstellerübergreifend zu beschreiben. Nur so ist eine bessere Unterstützung im Engineering, im Betrieb und in der Instandhaltung möglich. Doch häufig existiert die Beschreibung nur in den Köpfen der Anwender und lässt sich somit nicht verarbeiten. Letztendlich ist es mit dem Erzeugen von Daten allein nicht getan, sondern die Informationen müssen aufbereitet und bewertet sowie zu der entsprechenden Steuerungs- oder Verwaltungsebene transportiert werden. So kann 42 erst einmal alles bedeuten, mit der Einheit Grad bekommt die Zahl einen Sinn, aber erst mit einer Semantik, dass diese Temperatur einen Grenzwert überschreitet, werden die Daten zu einer Information, die sich für die Anlagensteuerung verwerten lässt. Nichts anderes machen im Übrigen Profile wie PA, Profidrive, Profisafe oder Profienergy. Sie ordnen die Daten ein, so dass z.B. Condition Monitoring, Asset- oder auch Energiemanagement möglich ist.

TSN – Fundament für Industrie 4.0?

IT- und Produktionsnetze verschmelzen zunehmend. In der Vergangenheit waren sie allerdings stets durch unterschiedliche Charakteristika gekennzeichnet. So bedienen IT-Netze vor allem große Bandbreiten und verbinden verschiedene Standorte miteinander, während Produktionsnetze sich vor allem durch hohe Leistung und kurze Latenzzeiten auszeichnen. TSN soll nun die Bandbreite der IT-Seite mit der kurzen Latenz der Produktion verbinden. Generell stellt die Nutzung der neuen TSN-fähigen Standard-Ethernet-Bausteine für Hersteller von Profinet-Geräten kein Problem dar. Im Gegenteil: PI sieht in TSN eine große Chance, die Stärken von Profinet und TSN miteinander zu kombinieren, Mehrwerte für den Anwender zu generieren und damit Profinet auf ein zukunftsfähiges Fundament zu setzen. Allerdings funktioniert das nicht von alleine. Denn auch TSN ist

Bild: Profibus Nutzerorganisation e.V.



TSN wird auf verschiedenen Ebenen eine Rolle spielen.

nicht von den Automatisierern getrieben, sondern stammt ursprünglich aus der Audio- und Videoübertragung. So liegt eine Herausforderung etwa darin, dass TSN verschiedene IEEE-Standards enthält, z.B. Enhanced synchronization behavior (IEEE802.1ASbt), Suspending (Preemption) of long frames (IEEE802.1Qbu), Enhancements for scheduled traffic (IEEE802.1Qbv), Path control and bandwidth reservation (IEEE802.1Qca), Seamless redundancy (IEEE802.1CB), Stream reservation (IEEE802.1Qcc) und noch einige weitere. Doch welche davon sind für die industrielle Kommunikation entscheidend? „Auch hier ist viel Detailarbeit nötig", sagt Schmidt, und führt weiter aus: „TSN kann keinen Feldbus ersetzen, da diese Technologie lediglich Basismechanismen auf der Data-Link-Ebene (Layer 2) bereitstellt. Die echten Mehrwertfunktionen und Feldbusdienste wie z.B. Diagnose werden dagegen auf den höheren Ebenen definiert. Diese Dienste machen den Feldbus erst zu einem leistungsfähigen Kommunikationssystem." Für den Anwender sollen daher Profinet-Dienste, Profile und Anwenderschnittstellen (z.B. Diagnose, Alarme, Profisafe sowie Profidrive) bestehen bleiben. Generell würden Anwender aber profitieren, bestätigt Schmidt. „Mit TSN ist eine höhere Bandbreite möglich, die Synchronisation zwischen anderen echtzeitfähigen Anwendungen wird ermöglicht, die Bausteine werden leistungsfähiger und vor allem können Standard-Ethernet-Controller auch für isochrone Echtzeitanwendungen eingesetzt werden." Für die Working Group geht es jetzt darum, den nahtlosen Übergang zu heutigen Installationen zu gestalten und den Anwendern einen einfachen Weg zu TSN-basierten Netzen aufzuzeigen. Das gilt übrigens nicht nur für TSN, bei der Einführung von neuen Technologien ist immer ein sinnvoller und auch machbarer Migrationsweg mit zu entwickeln. „Ich bin überzeugt, dass die heute verfügbaren PI-Technologien eine solide Basis bilden, aber die weiteren Schritte werden nicht von alleine geschehen", resümiert Schmidt. ■

Autorin: ***Sabine Mühlenkamp,***
freie Redakteurin,
Profibus Nutzerorganisation e.V.
www.profibus.com

S7-1500 und TIA Portal V14

Neue Funktionen vereinfachen Vernetzung

Aufgaben wie die Profinet-Konfiguration und Inbetriebnahme von Antrieben und dezentraler Peripherie, bis hin zur Vernetzung der Maschinen mit Echtzeit-Datenaustausch können nun durch zahlreiche Neuerungen bei S7-1500 und TIA Portal V14 effizienter erledigt werden.

Zur Realisierung von weltweit wettbewerbsfähigen Maschinen und Anlagen ist ein durchgängiges System, das eine performante und präzise Echtzeit-Kommunikation zwischen Steuerungen, Antrieben und dezentraler Peripherie, sowie hohe Anpassungsfähigkeit an die Anforderungen der jeweiligen Automatisierungsaufgabe bietet, von großer Bedeutung. Dabei ist eine leistungsfähige Diagnose und Offenheit, z.B. für Cloud-Dienste, ein weiterer wichtiger Faktor für effizienten Service und Zusatzgeschäfte für die eigenen Lösungen.

Performante und präzise Automatisierung

Profinet hat sich in vielen Anwendungsfeldern bewährt und bietet ausreichend Performance für heutige Automatisierungsanwendungen. Mit der Integration von Realtime-Kommunikation (RT) und Isochronous-Realtime-Kommunikation (IRT) in Profinet lassen sich mit der Simatic leistungsstarke Automatisierungsanwendungen für die Aufgaben der Fabrikautomation bis hin zu präzisen hoch dynamischen Regelungen realisieren. Darüber hinaus gibt es spezifische Anwendungen, die heute oder zukünftig eine höhere Kommunikationsleistung erfordern. Daher wurden nun bei der S7-1500, die mit der Profinet Spezifikation V2.3 definierten Mechanismen eingeführt, die die Kommunikation mit Profinet noch einmal beschleunigen. Mit diesen neuen Mechanismen, auch bezeichnet als Performance Upgrade, bietet Profinet hohe Leistungsreserven mit Zykluszeiten bis minimal 31,25µs. Mit der neuen Funktionsstufe bei Simatic S7-1500 lassen sich nun Anwendungen mit einem Buszyklus bis minimal 125µs bei gleichzeitiger Taktsynchronität realisieren. Die taktsynchrone Kommunikation stellt eine präzise, zeitgleiche Erfassung und Ausgabe der Signale über verteilte I/O-Stationen sicher. Dazu ist neben den genauen Übertragungszeitpunkten von Ethernet-Frames auch die eigentliche Signalerfassung bis hin zur Baugruppe mit deren Wandlungszeit / Ausgabezeit einbezogen. Daher können Aufgaben wie z.B. ein Gleichlauf von mehreren Achsen mit hoher Qualität realisiert werden. Neben den kürzeren Zykluszeiten beim Profinet Performance Upgrade bewirken die Verbesserungen hinsichtlich einer schnellen Weiterleitung der Ethernet-Frames und das dynamische Zusammenfassen der I/O-Daten in einen oder wenigen Frames eine weitere Leistungssteigerung – so profitieren auch Konfigurationen mit großer Anzahl an dezentralen I/O-Stationen und mit wenigen I/O-Daten zusätzlich von einem erhöhten Gesamt-

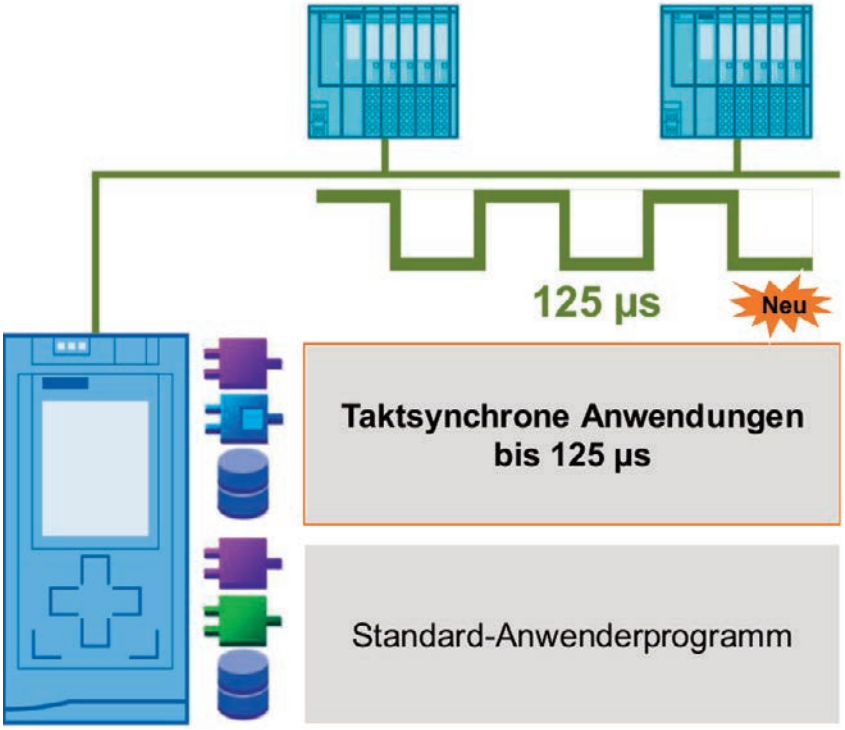


Bild: Siemens AG

Profinet bietet mit dem IRT Performance Upgrade eine Leistungssteigerung für eine taktsynchrone Bearbeitung bis 125µs.

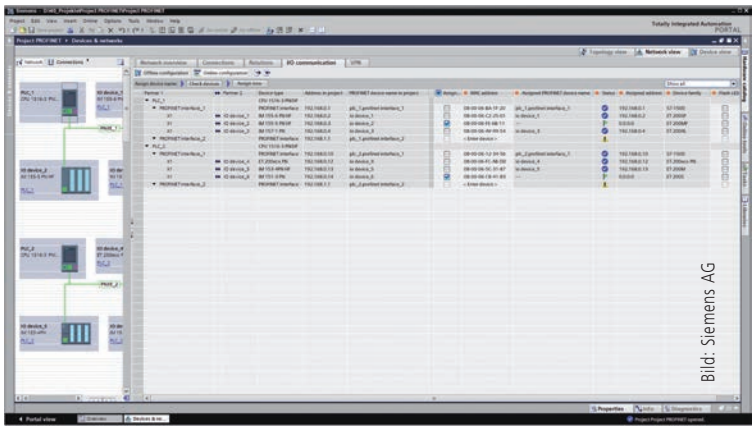
mengengerüst. Einen großen Vorteil stellt auch die gleichzeitige Offenheit für Standard-TCP/IP-Kommunikation dar – so kann bei paralleler Echtzeitkommunikation in µs-Genauigkeit ohne zusätzliche Vernetzung ein paralleler Datenaustausch mit dem optionalen OPC UA Server der Simatic S7-1500 erfolgen.

Einfacher Echtzeit-Datenaustausch zwischen Maschinen

Auch der Echtzeit-Datenaustausch zwischen einzelnen Maschinen oder Anlagenteilen gewinnt zunehmend an Bedeutung. Profinet bietet mit der Unterstützung mehrerer I/O-Controller in einem Netzwerk dazu eine Voraussetzung – der I/O-Controller kann in der Rolle eines intelligenten I/O-Device über eine flexibel definierbare Datenaustausch-Schnittstelle Hersteller-übergreifend Daten zwischen einen oder mehreren I/O-Controllern über die gleiche Schnittstelle austauschen. Mit der zweiten integrierten Profinet-Schnittstelle bei S7-1500 ist eine zusätzliche Vereinfachung möglich. Sollen Maschinen aus organisatorischen Gründen über getrennte Netze miteinander gekoppelt werden ist das über ein steckbares Kommunikationsmodul wie z.B. CM1542-1 oder bei S7-1500 mit zwei Profinet-Schnittstellen ohne Zusatzhardware möglich. Bei Simatic-Failsafe-Controllern erlaubt das zweite Interface eine weitere Schnittstelle für die Profisafe-Kommunikation – damit sind die Voraussetzungen auch für einen sicheren Datenaustausch auf der Maschinenebene gegeben.

Erhöhte Verfügbarkeit mit stoßfreier Umschaltung

Für einen wirtschaftlichen Betrieb von Maschinen und Anlagen ist eine hohe Verfügbarkeit ein wichtiger Faktor. Zur Erhöhung der Netzverfügbarkeit bietet das Profinet Media Redundancy Protocol (MRP) eine kostengünstige Möglichkeit: Einerseits kann die Verkabelung ohne zusätzliche Switches linienförmig dem physikalischen Layout der Maschine bzw. Anlage folgen und



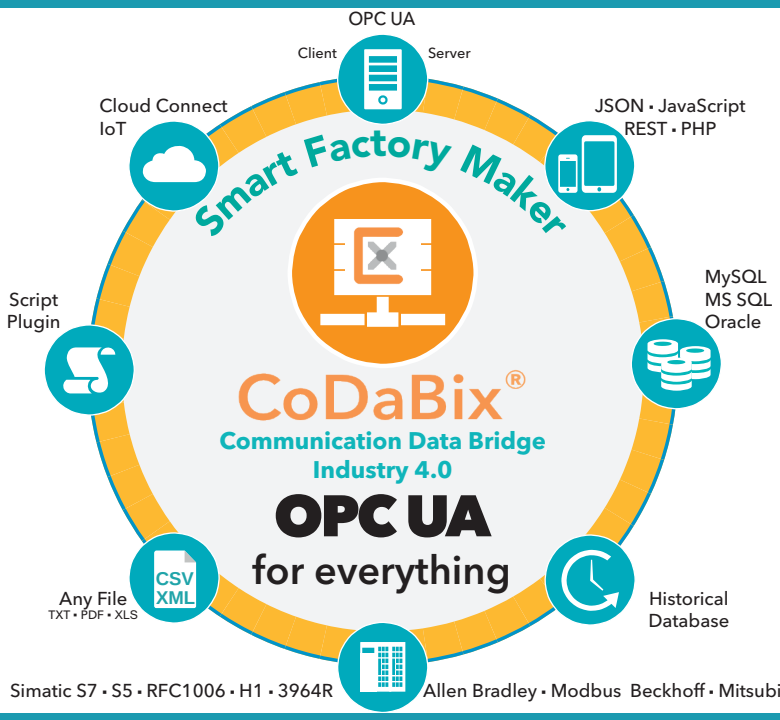
Mit der zweiten bei S7-1500 integrierten Profinet-Schnittstelle ist eine einfache und flexible Vernetzung von Maschinen für den Echtzeitdatenaustausch möglich.

dabei die Verfügbarkeit des Netzes durch einfaches Schließen der Linie zu einem Ring mit MRP erhöht werden. Ein Profinet Switch übernimmt dabei die Rolle des sogenannten MRP Managers, der im Falle einer Störung innerhalb des Rings, den alternativen Netzwerkpfad aktiv schaltet. So steht nach einer kurzen Umschaltzeit von typischerweise 200ms das Netzwerk wieder zur Verfügung. Mit den neuen Funktionserweiterungen bei Simatic S7-1500 steht nun auch Profinet Media Redundancy for Planned Duplication (MRPD) bei Simatic zur Verfügung. Dieses Protokoll versendet, in Verbindung mit Profinet IRT, die Profinet-Daten gleichzeitig auf beiden Netzwerkpfaden im Ring. Jedes MRPD-fähige Profinet Device erhält dadurch seine Echtzeitdaten über zwei Wege und kann bei Ausfall eines Pfades den Prozess ungestört bedienen. So lassen sich nun Applikationen mit hoher Präzision realisieren, die auch bei Netzstörungen einen unterbrechungsfreien I/O-Datenaustausch benötigen.

- Anzeige -

TRAEGER.DE
INDUSTRY COMPONENTS

Communication Data Bridge
CoDaBix®
Industrie 4.0
www.codabix.com
OPC-UA Server und Client
Windows 7/8/10
universelle Schnittstellen
flexibel
innovativ ▪ ausgereift ▪ praxisorientiert
www.traeger.de



Traeger Industry Components GmbH ▪ Söllnerstraße 9
92637 Weiden i.d.Opf. ▪ Tel.: +49 961 48230-0 ▪ info@traeger.de
CoDaBix ist ein eingetragenes Markenzeichen der Traeger Industry Components GmbH

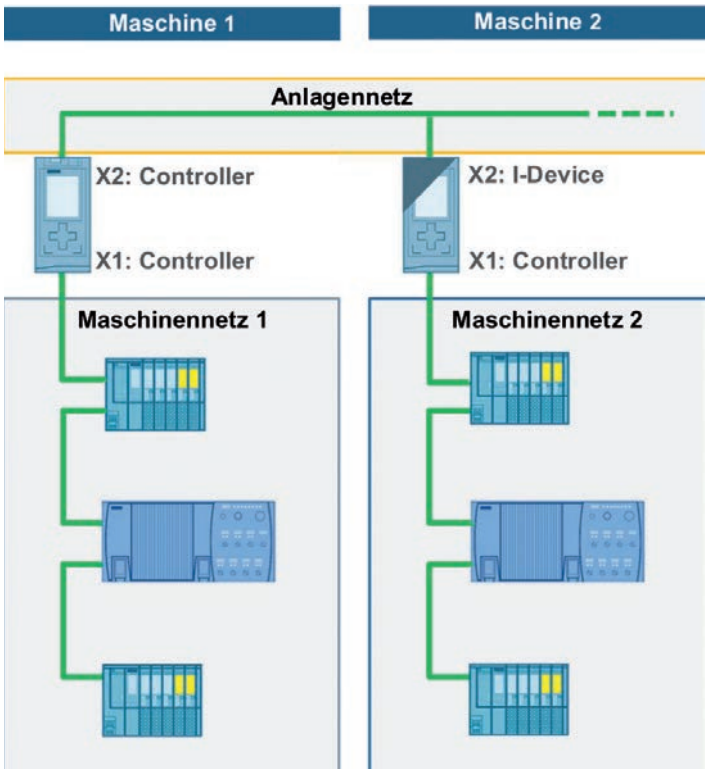


Bild: Siemens AG

Mit den neuen Sammeloperationen wie der Gerätenamenvergabe im TIA Portal lassen sich Profinet-Konfigurationen effizient realisieren.

- Anzeige -

SPS MAGAZIN

Mit der Fachzeitschrift **SPS-MAGAZIN**, dem **Automation Newsletter**, dem **Produkt Newsletter** und der **Website** finden Sie alle relevanten Informationsmedien für die Automatisierungstechnik übersichtlich aus einer Hand.

sps-magazin.de

Bild: ©sdecoret-FOTOLIA.com

Hilfreiche Funktionen im Engineering

Für den Maschinen- und Anlagenbau sind niedrige Engineering- und Herstellungskosten sowie ein durchgängig anwendbares Automatisierungskonzept wichtig. Das Engineering Framework TIA Portal von Siemens unterstützt Maschinenhersteller wie Endanwender dabei, durch eine intuitive Bedienung und ein leistungsfähiges Bibliothekskonzept die Softwareentwicklungszeiten zu reduzieren. Neue Funktionen helfen auch dabei Profinet-Konfigurationen noch einfacher zu realisieren und einen schnellen Überblick zu erhalten. Z.B. ermöglicht die neue Sammeloperation zur Vergabe der Gerätenamen die Gerätetaufe der kompletten Profinet-Konfiguration in einem Zug. Hierbei werden durch eine geführte Bedienung die Online erkannten Geräte den im Projekt konfigurierten Geräten zugeordnet und hinsichtlich bestimmter Kriterien auf z.B. den passenden Online erkannten Gerätetyp überprüft. Nach erfolgter Zuordnung kann der Anwender den Taufvorgang für alle I/O-Devices anstoßen. Auch eine Export- und Importfunktion steht dabei optional zur Verfügung. Durch diese Neuerung lassen sich Konfigurationsfehler im Vorfeld noch besser vermeiden und die Geräte schneller in Betrieb nehmen. Weitere Funktionen wie das einfache Synchronisieren der grafischen Netz- und Topologiesicht, sowie die Gruppierung von Geräten in der Projektnavigation vereinfachen Konfiguration und Diagnose: Sofern vom Anwender erwünscht kann mit einem Klick ein schneller Abgleich der grafischen Topologiesicht mit der Netzsicht erfolgen. Die Gruppierung in der sogenannten Projektnavigation erlaubt eine flexible Zusammenfassung der Geräte in kompakte Gruppen und Untergruppen. Dadurch lassen sich einerseits auch bei sehr hohen Teilnehmerzahlen im Projekt die Geräte zur Konfiguration oder Parametrierung schnell anwählen, aber auch im Diagnosefall schnell auffinden. Jede Gruppe besitzt dazu in der Online-Sicht ihren eigenen Diagnose-Sammelstatus. Sammeloperationen für das Zuweisen von I/O-Devices oder der Profinet-Aktualisierungszeit und die Edit-in-Place-Funktionen für IP-Adresse und Gerätenamen sind weitere Neuerungen für effizientes Arbeiten im TIA Portal.

Nützliche Funktionen

Neben neuen Vernetzungsmöglichkeiten für den Echtzeitdatenaustausch zwischen Maschinen oder Anlagenteilen, sowie stoßfreier Medienredundanz bieten zahlreiche Engineering-Erweiterungen nützliche Funktionen von einer schnellen Inbetriebnahme bis hin zur effizienten Wartung und Diagnose. Zusammen mit der Leistungsfähigkeit der in Simatic integrierten Profinet-Funktionen gepaart mit dem TIA Portal kann der Maschinen- und Anlagenbau in allen Phasen des Engineerings, bei der Konstruktion, beim Aufbau sowie bei der Integration von Maschinen und Anlagenteilen Kosten reduzieren und damit seine Wettbewerbsfähigkeit steigern. ■

Autor: *Joachim Ohlmann,*
System Manager Simatic-Hardware,
Siemens AG Factory Automation
www.siemens.de/profinet

Direkt zur Marktübersicht i-need.de *www.i-need.de/?Produkt=22602*

Profibus-FPGAs nach Wahl

Mit dem Profibus DP Master für Xilinx FPGAs erweitert Softing sein Angebot an ladbarer Logik mit integrierter Protokollsoftware für industrielle Kommunikationsprotokolle.

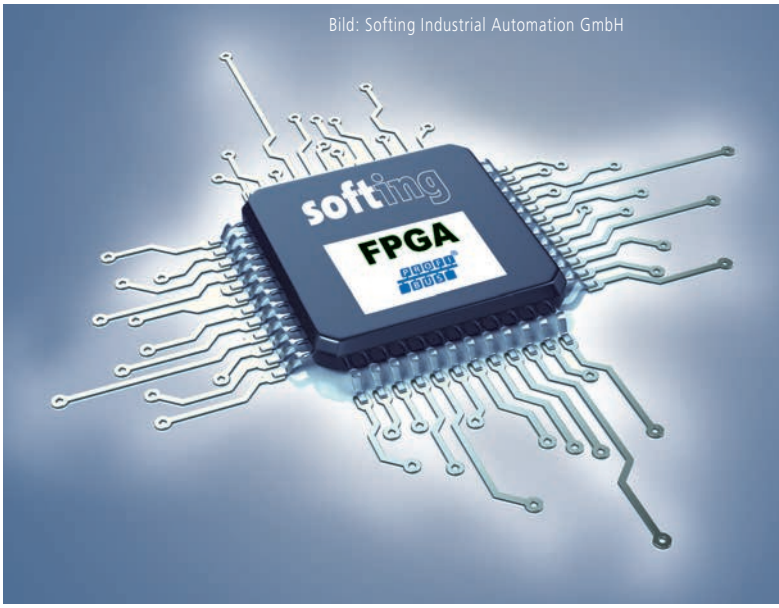


Bild: Softing Industrial Automation GmbH

Das neue Angebot ergänzt die Familie FPGA-basierter Feldbus- und Industrial-Ethernet-Implementierungen für Feldgeräte und Controller-Anwendungen. Der Profibus-Master steht nun neben der bekannten Lösung für Altera-FPGAs auch für Xilinx-FPGAs zur Verfügung. Anwender haben somit die Möglichkeit, den FPGA-Anbieter nach ihren Anforderungen zu wählen und die ihnen vertraute Entwicklungsumgebung zu nutzen. Die komplette Protokollsoftware liegt auf dem im IP-Core enthaltenen Prozessor bereits lauffähig vor. Der Anwender muss also keine Portierung durchführen, sondern kann sich direkt auf die Applikationsentwicklung konzentrieren, die durch Beispielprojekte auf gängiger Evaluierungs-Hardware unterstützt wird.

Der Anwender hat die Wahl

Durch die Realisierung im FPGA entfällt die Abhängigkeit von der Verfügbarkeit klassischer Kommunikationsbausteine. Stattdessen wählt der Anwender die für sein Produkt am besten passende FPGA-Familie und -Größe, in der das Kommunikationssubsystem dann unverändert eingesetzt werden kann. Die große Auswahl an passenden FPGAs und deren hohe Verfügbarkeit über lange Zeit empfehlen die Kommunikationslösungen nicht nur für Neuentwicklungen. Sie können auch bei der Überarbeitung erfolgreicher Bestandsprodukte eingesetzt werden, um das Risiko von Abkündigungen und Preiserhöhungen älterer Bauteile zu vermeiden. ■

Autorin: Stephanie Widder,
Marketing Communications Specialist - Industrial,
Softing Industrial Automation GmbH
www.softing.de

Direkt zur Marktübersicht i-need.de *www.i-need.de/?f9751*

Vortex Report 2017

Fit für mehr Daten?

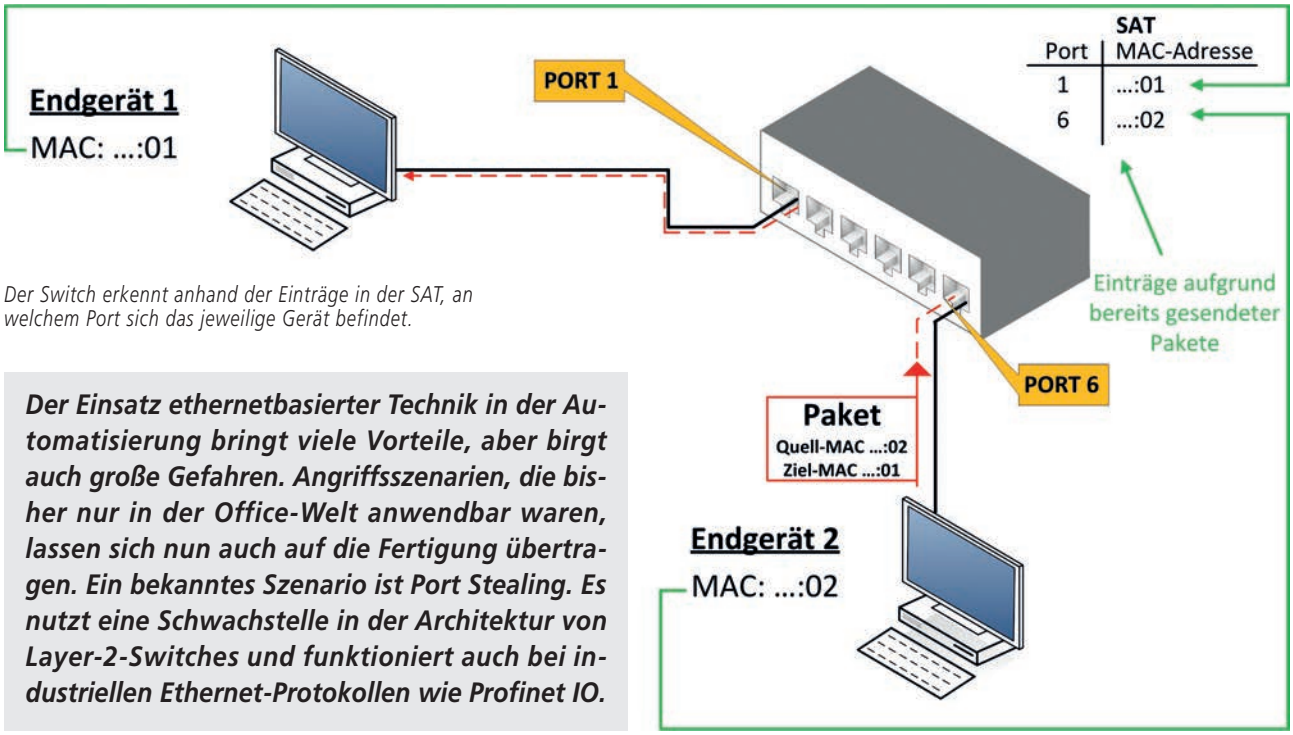
Der gestiegene Datenbedarf erfordert eine ständige technologische Anpassung: Bot der Interbus-Standard Ende der 1980er Jahre eine Übertragungsrate von 500kBit/s, überschritt Profibus in den 1990ern bereits die 1Mbit/s-Grenze. Die 100Mbit/s von Profinet wirken da schon wie ein Quantensprung, doch soll TSN in absehbarer Zeit mehrere Gbit/s in Echtzeit übertragen. So verlockend die Vorteile, die hohe Kapazität belastet in zunehmendem Maße die Physik. Der Frage, inwieweit industrielle Netzwerke weltweit bereits fit für moderne Datenraten sind, widmet sich der Vortex-Report 2017.

Die Erkenntnisse aus dem Report stammen aus 646 Messeinsätzen, die von den Technikern der Firma Indu-Sol zur Bestimmung der Kommunikationsqualität in industriellen Netzwerken durchgeführt wurden. Technologieübergreifend zeigt sich, dass aktuelle Potentialausgleichssysteme den Bedingungen einer vernetzten Industrie und dem steigenden Einsatz hochfrequenter Leistungselektronik nicht mehr gerecht werden. 2016 musste etwa jeder zehnte Messeinsatz, der ursprünglich als Einmessung beauftragt wurde, aufgrund der gefunden Mängel im Nachhinein als Fehlersuche deklariert werden. Bestehende Normen und Handlungsempfehlungen sind weder zeitgemäß noch passen sie zur Realität vieler Instandhaltungsbereiche. Eine Arbeitsgruppe der Profibus/Profinet-Nutzerorganisation will deshalb noch in diesem Jahr eine zeitgemäße Handlungsempfehlung zum Thema EMV & Potentialausgleich herausgeben. Schließlich gilt es, Lösungen für neue Standards wie TSN in der Automatisierung zu finden, Security auch im Umfeld einer vernetzten Industrie 4.0 zu gewährleisten und zeitgemäße Potentialausgleichssysteme zu entwickeln. Dafür soll der Vortex Report als aktueller Zustandsbericht eine passende Basis liefern. ■

Firma: Indu-Sol GmbH
www.indu-sol.com/?id=477#VORTEX

Port Stealing bei industriellen Anwendungen

Sicherheitsrisiko Layer-2-Switch



Der Switch erkennt anhand der Einträge in der SAT, an welchem Port sich das jeweilige Gerät befindet.

Bild: THD-Technische Hochschule Deggendorf

Der Einsatz ethernetbasierter Technik in der Automatisierung bringt viele Vorteile, aber birgt auch große Gefahren. Angriffsszenarien, die bisher nur in der Office-Welt anwendbar waren, lassen sich nun auch auf die Fertigung übertragen. Ein bekanntes Szenario ist Port Stealing. Es nutzt eine Schwachstelle in der Architektur von Layer-2-Switches und funktioniert auch bei industriellen Ethernet-Protokollen wie Profinet IO.

Switches verbinden als Kopplungselemente die Teilnehmer eines Netzwerks miteinander und leiten Pakete anhand von Informationen der Sicherungsschicht (Schicht 2 des ISO/OSI-Modells) weiter. Jeder Teilnehmer eines Netzwerks besitzt eine Hardware-Adresse (MAC-Adresse). Um einem Gerät einen (physikalischen) Port zuzuordnen, analysiert der Switch die auf einem Port empfangenen Pakete und liest die Quell-MAC-Adresse aus. Er speichert diese in einer Tabelle, der Source-Address-Table (SAT) ab. Empfängt der Switch ein Paket von Endgerät 2 mit der Quelladresse ...:02, welches die Zieladresse ...:01 enthält, kann er anhand der Einträge in der SAT feststellen, hinter welchem Port der Empfänger (Endgerät 1) zu finden ist (Port 1) und leitet es dorthin weiter.

Datenpakete stehlen

Wechselt ein Gerät den Port, muss der Switch diesen Vorgang erkennen, um eine Weiterleitung von Paketen an diesen Teilnehmer sicherzustellen. Der Switch handelt dynamisch und schreibt die SAT entsprechend um. Allerdings kann ein Angreifer diesen Mechanismus nutzen und Pakete stehlen (daher Port Stealing). Hierzu muss dieser einen physikalischen Zugang zum Switch besitzen (Port 3). Sendet er ein (manipuliertes) Paket mit der MAC-Adresse von Endgerät 1 als Quelle und einer beliebigen als Ziel (im Beispiel seine eigene), wird die SAT aktualisiert und der Angreifer erhält das an Endgerät 1 adressierte Paket.

Mögliche Angriffsszenarien

Werden kontinuierlich derartige Pakete versandt, gelangen die an das Opfer adressierten Daten nicht mehr an ihr eigentliches Ziel – die klassische Denial-of-Service-Attacke. In industriellen Netzen können damit wichtige Komponenten vom Netzwerk getrennt werden, was schwerwiegende Folgen haben kann. Doch in der Regel werden Systeme, die über Profinet IO kommunizieren, so projektiert, dass bei einer vorbestimmten Zeitspanne ohne Paketeingang eine Alarmmeldung gegeben wird. Das betroffene Gerät wird in einen sicheren Zustand versetzt und der Operator beginnt mit der Fehlersuche. Ein gefährlicheres Szenario ist der Man-in-the-Middle-Angriff (MITM-Angriff). Dabei positioniert sich der Angreifer zwischen zwei Netzteilnehmern und kann dadurch übertragene Daten mitlesen oder manipulieren. Dies stellt sowohl aus datenschutzrechtlicher Sicht, als auch aus Gründen der Betriebssicherheit ein hohes Risiko dar.

Datenübertragung bei Profinet IO

Bei Profinet IO werden die Prozessdaten zwischen der Baugruppe, in der das Automatisierungsprogramm abläuft (I/O-Controller) und dem Feldgerät (I/O-Device) zyklisch übertragen. Der Datenaustausch erfolgt in einem parametrisierbaren Takt (abhängig von Gerät und Anlagengröße). Die Zykluszeit liegt im ms-Bereich, typischerweise bei 4ms. Beim Prozessdatenaustausch wird zur Identifizierung der

Teilnehmer nur die MAC-Adresse verwendet. Konfigurations- und Diagnoseinformationen werden azyklisch über einen separaten Kanal versandt. Hierzu benötigt jeder Teilnehmer eine IP-Adresse.

MITM bei Profinet IO

Ein Angreifer gelangt an die für ihn relevanten Informationen (MAC-/IP-Adressen, Geräterolle, d.h. Controller oder Device) über das Discovery and Configuration Protocol (DCP). Dabei schickt dieser einen DCP-Identify-Request an alle Teilnehmer eines Netzsegments (Broadcast) und erhält von jedem eine DCP-Identify-Response-Nachricht mit den benötigten Informationen. Anschließend kann er einen MITM-Port-Stealing-Algorithmus ausführen und besitzt die volle Kontrolle über den Datenverkehr.

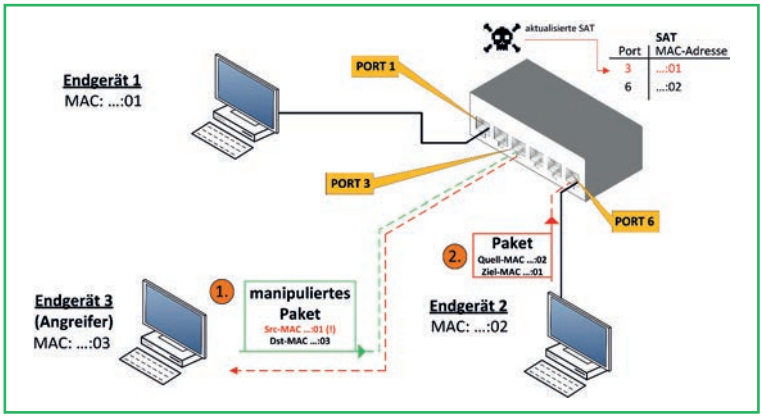


Bild: THD-Technische Hochschule Deggendorf

Der Angreifer schickt ein gefälschtes Paket, überschreibt die SAT und erhält damit die für Endgerät 1 bestimmten Daten.

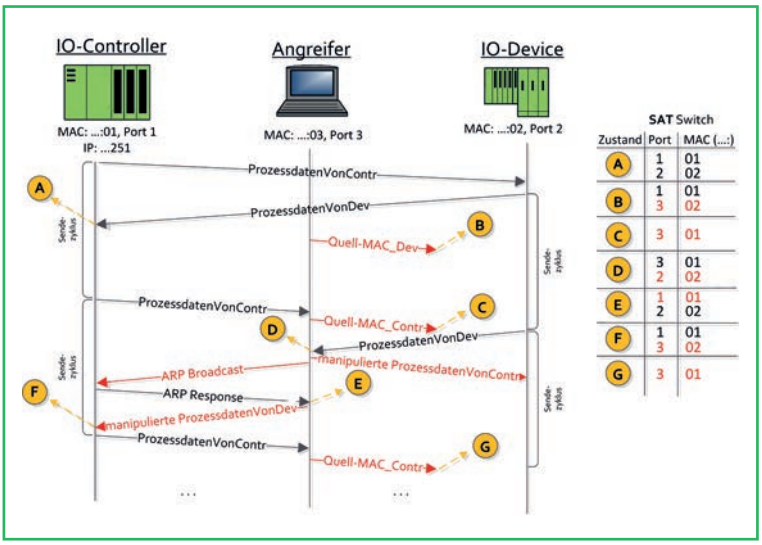


Bild: THD-Technische Hochschule Deggendorf

MITM-Port-Stealing-Algorithmus bei Profinet IO

Auswahl an Schutzmaßnahmen

Um einen effektiven Schutz zu gewährleisten, sollte ein mehrstufiges Sicherheitskonzept implementiert werden. Basis dieses Konzepts ist ein wirksamer Zugriffsschutz. Mit Hilfe von Zutrittskontrollen muss Unbefugten der unmittelbare, physische Zugang zu Steuerungskomponenten und Netzwerkhardware verwehrt bzw. erschwert werden. Moderne Switches bieten zudem ein Sicherheitsfeature (MAC-Locking), dass es ermöglicht, die SAT statisch zu schalten und an eine MAC-Adresse zu binden. Meist erlauben es diese auch, ungenutzte Ports zu deaktivieren. Sollte ein Angreifer trotz Zutrittskontrollen sich physischen Zugang zum System verschaffen, müsste dieser ein angeschlossenes Gerät vom Netz trennen und mit dessen MAC-Adresse das Angriffsszenario ausführen. Im Regelfall wird das (wenn auch nur kurzzeitige) Entfernen eines Geräts protokolliert. Damit lässt sich ein Angriff zwar nicht verhindern, aber besser zurückverfolgen.

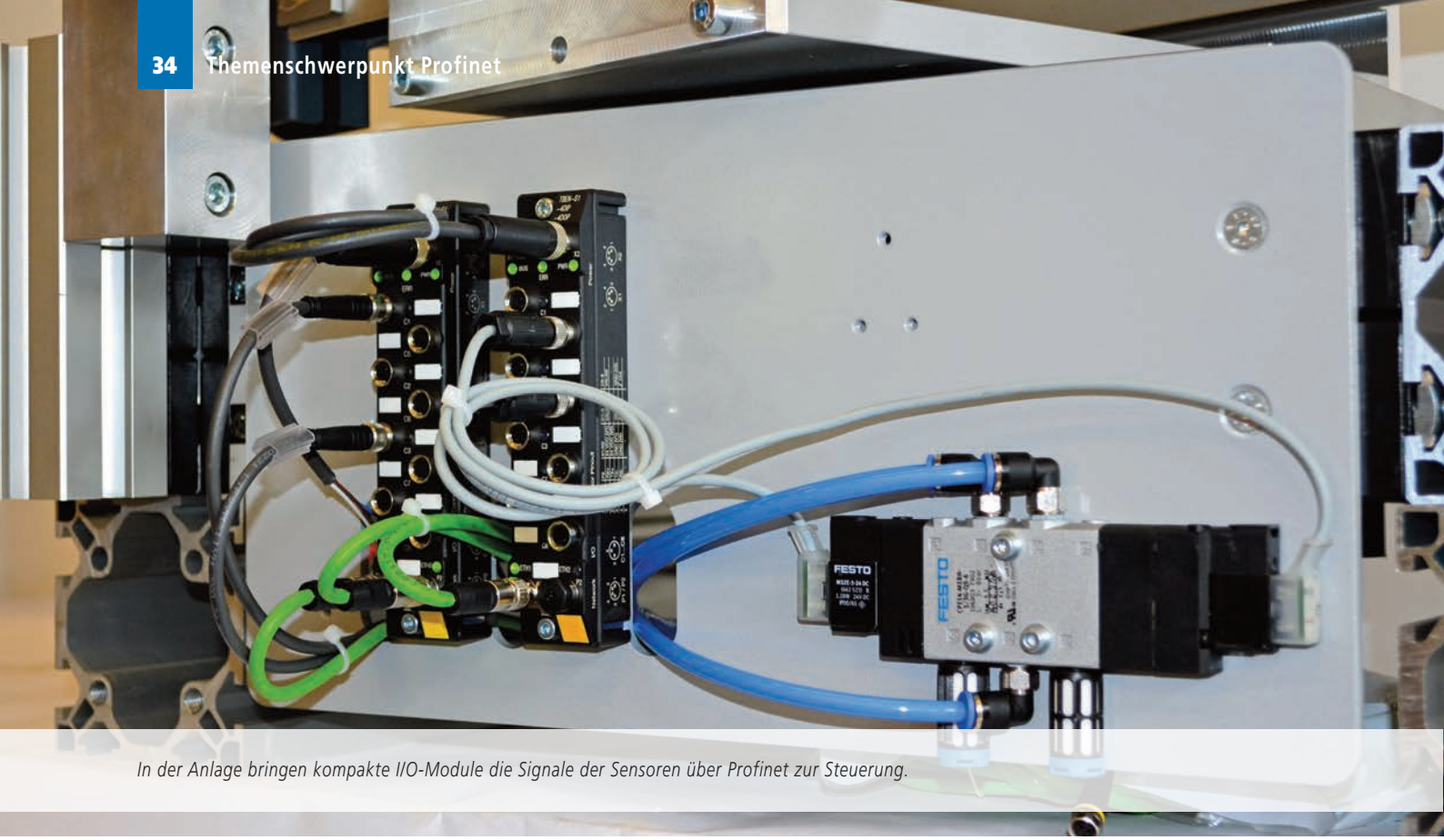
Hürden für Angreifer

Ist zusätzlich portbasierte Authentifizierung nach IEEE 802.1X konfiguriert, setzt man eine hohe Hürde für den Angreifer. Mit Hilfe dieser Technologie wird ein Port vom Switch erst dann für die Kommunikation freigegeben, nachdem sich das angeschlossene Gerät authentisiert hat. Hierzu übermittelt das Gerät vor dem Verbindungsaufbau vorher festgelegte Authentisierungsdaten an ein zentrale Instanz, die diese Informationen überprüft. Ist die Verifizierung nicht erfolgreich, verwehrt der Switch den Zugriff zum Netzwerk. Gelangt ein Angreifer nicht an die Authentisierungsdaten, erhält er keinen Zugang und kann damit das Port-Stealing-Szenario nicht ausführen. Eine Möglichkeit Angriffe zu erkennen, ist der Einsatz eines Intrusion Detection Systems (IDS). Es wird mittels Sensoren in das industrielle Netz integriert und überwacht kontinuierlich den Datenverkehr. Dabei nimmt ein Sensor einzelne Pakete im Netzwerkfluss auf und untersucht diese mit geeigneten Algorithmen auf Abweichungen. Im beschriebenen MITM-Szenario werden fortlaufend ARP-Pakete verschickt. Sie stellen eine Anomalie dar und sind ein Angriffsindikator. Tritt eine derartige Abweichung im System auf, wird dies dem Operator gemeldet und er kann entsprechenden Gegenmaßnahmen einleiten.

Absicherung der Kommunikation

Eine weitere Schutzmöglichkeit ist die Absicherung der Kommunikationswege. Hierzu wird das im IEEE802.1AE-Standard beschriebene MACsec-Verfahren angewandt. Es bietet neben erweiterten Integritätsschutzmechanismen auch die Möglichkeit den Datenverkehr auf Layer 2 zu verschlüsseln. Wird ein Automatisierungssystem mit den erläuterten Methoden abgesichert, bietet es einem potentiellen Angreifer eine recht geringe Angriffsfläche. Port-Stealing-Szenarien werden damit deutlich erschwert. ■

Autor: *Peter Semmelbauer,*
Projektingenieur, Technische Hochschule Deggendorf,
Institut ProtectIT – Protection for Industrial Technologies
www.th-deg.de/protectit



In der Anlage bringen kompakte I/O-Module die Signale der Sensoren über Profinet zur Steuerung.

Bild: Hans Turck GmbH & Co. KG

Profinet-I/O-Module in der Förderanlage

Fertigungslinie für High-End-Küchenhelfer

Hindernisse umgehen und trotzdem auf direktem Weg ans Ziel kommen – das sind die Anforderungen einer neuen Förderlinie, auf der Vorwerk die Küchenmaschine Thermomix produziert. Die Sensor- und Aktor-Signale gelangen darin über Profinet-I/O-Module zur Steuerung. Um die Flexibilität der gesamten Anlage sicherzustellen, kommt es bei den Modulen auf Baugröße, Flexibilität und Unabhängigkeit an.

Der Küchenhelfer Thermomix TM5 von Vorwerk soll mit seinem Design, seiner Guided-Cooking-Funktion und seinen Rezept-Chips das digitale Zeitalter des Kochens einleiten. Für dieses Produkt eine effiziente Fertigungslinie aufzubauen, war eine Herausforderung. Vorwerk vertraute hier auf den Böma, einen österreichischen Anbieter von Fördertechnik. Das Unternehmen plante, konstruierte und baute die Förderlinien für die wesentlichen Bauteile des smarten Küchenhelfers zwischen Kunststoffspritzerei und Gerätemontage. Die Aufgabe ist schnell erklärt: Das zu befördernde Produkt muss in der richtigen Zeit materialschonend und auf die Mitarbeiter abgestimmt von A nach B transportiert werden. Ein Roboter entnimmt dazu die Spritzgussteile aus der Maschine und legt sie auf das Förderband. Diese Teile müssen dann über die einzelnen Linien an bestimmte Positionen in einer anderen Halle gebracht werden. Dabei war die Taktzeit vorgegeben, in der ein Teil von den Werkern in der Montagelinie entnommen werden kann. Auf die gesamte Länge der Förderbänder, jeweils rund 50m, musste also auch ein Zeitpuffer eingeplant werden.

Hindernislauf

Die erste Herausforderung war die bestehende Raumaufteilung in der Produktionshalle. Punkt A war klar, Punkt B auch, dazwischen ergaben sich aber Hindernisse, die es zu überwinden galt. Die Böma-Konstrukteure haben zunächst damit begonnen, die Förderlinien genau in die bestehende Halle einzupassen. Manche Hindernisse wie Mauern wurden umgangen, andere auch durchdrungen, um den Platz bestmöglich auszunutzen. Teilweise konnten auch bestehende Öffnungen verwendet werden. Die theoretische Konstruktion der Förderbänder musste genau in die Planung der Halle eingepasst werden. Dies geschah über

Um Überraschungen vorzubeugen wurden wesentliche Teile der Thermomix-Förderanlage bereits vorab aufgebaut und getestet.

Bild: Hans Turck GmbH & Co. KG

mehrere Linien und auf mehreren Ebenen. Um vertikal zu fahren, wurden Hubwerke eingesetzt. Um die Spritzgussteile nach links oder rechts zu bewegen, verwendete man pneumatische Dreheinheiten und je nach den Gegebenheiten vor Ort elektrische oder pneumatische Querverschubachsen. Die Produkte selbst werden über Flachgurtbänder transportiert. Für ein Produkt musste Böma jedoch seinen selbst entwickelten Zahnriemenförderer einsetzen. Das variable System ist genau auf die Form dieses Produkts angepasst und ermöglicht so einen störungsfreien Transport vom Spritzguss zum Werker.

Kompakte I/O-Module überzeugen

Auch die Steuerung der kompletten Anlage übernahm Böma. Die Signale der Sensoren bringen kompakte I/O-Module TBEN-S von Turck über Profinet zur Steuerung. An die Module sind auch die Aktoren der Anlage angebunden. Die Konfiguration der TBEN-S-Variante mit vier digitalen Ausgängen und vier digitalen Eingängen entsprach dem Signalbedarf an etlichen Stellen der Förderstrecke. „Ein Teil der Anlage wurde nicht neu gebaut, sondern in bestehende Anlagen integriert. Da war zunächst unklar, wie viele Ein- und Ausgangssignale wir zur Steuerung bringen müssen. An diesen Stellen haben wir die frei konfigurierbaren TBEN-S-DXP eingesetzt. So konnten wir die Konfiguration auch noch im Nachhinein dem konkreten Bedarf anpassen. Geräte mit frei konfigurierbaren Ein- und Ausgängen haben wir bei anderen Herstellern nicht gefunden“, erklärt Helmut Sutterlüty, Konstruktionsleiter bei Böma und ergänzt: „Andere Systeme in dieser Bauform benötigen zusätzliche Kopplermodule zum Profinet-Strang und müssen wiederum untereinander gekoppelt werden.“ Außerdem war die Baugröße ausschlaggebend: Mit 32mm Breite passen sie auf die schmalen Aluprofile der Förderanlage. Alle Sensoren im Projekt stammen aus dem Turck-Portfolio. Zur Erfassung der Teile auf dem Band wurden hauptsächlich QS-18-Einweglichtschranken vom Turck-Partner Banner Engineering eingesetzt. Neben der Reichweite von 7,5m, zeichnen sie sich mit einem kleinen Lichtpunkt, der eine hohe Genauigkeit liefert, aus. Um die Position der Pneumatikzylinder zu erfassen, setzte Böma magnetinduktive BIM-UNT-Schalter ein, die direkt in die Nut der Aluzuylinder gesetzt werden können und dort die Position des Kolbens erfassen. Auch die Anschlusstechnik, insbesondere die M8-Sensor/Aktor-Leitungen zur Anbindung an die TBEN-Module und M8-Power-Leitungen lieferte Turck. Für die Positionsabfrage und Endschalter der Hubwerke wurden Sensoren vom Typ Bi4-M12-VP6X verwendet. Wer Projekte dieser Größenordnung kennt, weiß, dass zwischen Planung und Konstruktion auf der einen und der Umsetzung in der Praxis auf der andern Seite Welten liegen können. Durch die enge Abstimmung der Konstruktionsabteilung mit dem Kunden und den Monteuren war hier gewährleistet, dass auch der Aufbau der Anlage passend realisiert wurde. Wesentliche Teile der Anlage wurden zuerst bei Böma aufgebaut, um erste Testläufe durchzuführen und dem Kunden eine Abnahme bzw. ein erstes Bild der Anlage zu ermöglichen. Das ersparte Überraschungen beim Aufbau beim Kunden. Auch durch die I/O-Module von Turck ging der Aufbau recht zügig voran, da viele Elemente bereits bei Böma vorverdrahtet werden konnten. Bei der eigentlichen Inbetriebnahme der Anlage in der Produktionshalle konnte Böma die Stärke seines selbst entwickelten Baukastensystems ausspielen, denn die Monteure können damit auch in letzter Minute noch Anpassungen vornehmen. Die unterschiedlichen Profile haben alle dieselbe Nut, egal wie breit sie sind. Zur Verbindung der einzelnen Elemente muss nicht gebohrt werden. Die Förderanlage konnte schließlich alle Ansprüche erfüllen. Die unterschiedlichen Linien sind in die Produktionshalle integriert. Zusätzlich wurden noch Portale unter den Linien eingerichtet, um leichtere Zugänge für die Mitarbeiter zu schaffen. Die einzelnen Komponenten des Thermomix laufen in der richtigen Zeit von A nach B, werden an keiner Stelle des Prozesses beschädigt und der Werker kann im vorgegebenen Takt direkt an der Förderlinie die Produkte entnehmen. ■

Autor: ***Florian Fink,***
Technischer Vertrieb für Tirol Vorarlberg,
Hans Turck GmbH & Co. KG
www.turck.com

Direkt zur Marktübersicht i-need.de *www.i-need.de/?Produkt=24307*

AS-i-Lösung für die Lagerlogistik

Passend gemacht

Wenn es bei Unternehmen darum geht die Fertigungslogistik zu modernisieren, sind die Anforderungen an die neue Technik im Regelfall sehr hoch – hinsichtlich Effizienz- oder Produktivitätssteigerung genauso wie bei verkürzten Montagezeiten oder der einfachen Integration und Installation. Die Firma Knapp, Lösungsanbieter im Bereich Lagerlogistik, hat sich in diesem Rahmen für eine AS-Interface-Basis entschieden. Die entsprechenden Vorteile spielen sich jetzt u.a. in der Logistik des Herrenausstatters Hugo Boss aus.

Knapp setzt als Anbieter im Bereich der Lagerlogistik auf maßgeschneiderte Lösungen. Es gibt nichts von der Stange. Das Unternehmen setzt auf eine Verknüpfung von Branchenkenntnis sowie technologischem Wissen und schreckt auch vor neuen Wegen nicht zurück, wenn es darum geht, wesentliche Verbesserungen zu erzielen.

Modulare Förderanlage

Diese Ausrichtung war der Start in die Neuentwicklung eines modular installierbaren Anlagenkonzepts: eine komplette Förderanlage, aus Modulen aufgebaut, die im eigenen Haus vollständig vormontiert, konfiguriert und geprüft werden, und sich vor Ort beim Kunden in kurzer Zeit zur Gesamtanlage installieren und in Betrieb nehmen lassen. Gemeinsam mit dem Automatisierungsanbieter Pepperl+Fuchs wurde die Idee eines kompakten und intelligenten Motormoduls entwickelt, das sich einfach in profilierte Tragschienen der Transportbänder montieren lässt. Aus der anfänglichen Idee entstand in enger Abstimmung zwischen den beiden Partnern schließlich die G20-Baureihe der AS-Interface-Module: Dabei handelt es sich um ein Motorrollenmodul und ein Digitalmodul, die sich beide in das neue, kompakte Tragschienendesign integrieren lassen. Die AS-i-typische Installation mit Direktanschluss der Sensoren und Aktoren über profilierte Flachkabel mit 2,5mm² bringt dabei wichtige Vorteile. AS-Interface ist zwar für die Sensor/Aktor-Ebene entwickelt, eignet sich aber nicht nur für einfache Aufgaben. „Am Anfang hätten wir nicht gedacht, dass mit wenigen Bits zwei Motoren mit acht Geschwindigkeiten und acht Anfahrts- und Bremsrampen gesteuert werden können – und sich auch noch eine Motordiagnose sowie die Sensorsignale mit übertragen lassen“, sagt Claus Blödorn von Knapp. „Das ermöglicht uns die komplette Vormontage eines Fördertechnikelements.“ Knapp nutzt ein Planungs-Tool, mit dem nicht nur die Anlage konzipiert wird, sondern das auch gleich die Fertigungsplanung der Segmente liefert. Selbst die Adressierung der G20-Module zur Anbindung der Sensoren und Aktuatoren erfolgt dabei halbautomatisch über einen Barcode. Nichts bleibt dem Zufall überlassen und alle Segmente verlassen das Werk komplett vorgetestet, ohne dass dies Zusatzkosten verursacht.

Bild: AS-International Association e.V.

Vormontiert, geprüft und versandbereit: Die Idee eines modularen Fertigungskonzepts ist aufgegangen.

Wettbewerbsvorteil durch Flexibilität

„Für unsere Kunden bedeutet das mehr Flexibilität, schnellere Inbetriebnahme der Anlage und kürzere Projektzeiten“, so Blödorn weiter. Es sei wichtig, dass die Fördertechnik flexibel und mit der Flachkabelinstallation vor Ort schnell aufgebaut werden kann. Weiterhin seien auch externe Sensoren, Aktoren und Nothalttaster mit anzubinden. „Hierfür gab es mit der bereits am Markt verfügbaren Baureihe G10 bereits eine passende Lösung für Passivverteiler, Digitalmodul und Safety-Modul mit direkter Flachkabelanbindung auf 30x40mm Grundfläche.“ Inzwischen hat sich das AS-i-System in Logistiklösungen fest etabliert und bietet zusätzliche Diagnoseoptionen für die Inbetriebnahme und den laufenden Betrieb. Sollte einmal eine Motorrolle ausfallen oder zu viel Strom ziehen, wird dies dediziert gemeldet und der betroffene Ausgang sicher abgeschaltet.

Vereinfachte Fertigung

Die Fördertechnikteilelemente werden bei Knapp im Haus komplett montiert. Die Sensoren und Aktoren werden am vormontierten AS-i-G20-Motormodul angeschlossen, das auch bereits richtig voradressiert ist. Vor Ort müssen die Fördertechnikelemente nur noch mechanisch miteinander verbunden und im letzten Schritt

AS-i-Kommunikation bei Hugo Boss

Für sein 35.000m² großes Distributionszentrum in Filderstadt setzt Hugo Boss auf Automatisierungstechnik von Knapp. Im Einsatz ist ein OSR Shuttle mit 440.000 Stellplätzen in Kombination mit ergonomischen Arbeitsplätzen, an denen effizient und ressourcenschonend im Ware-zur-Person-Prinzip kommissioniert wird. Mit den Shuttles hat das Unternehmen jederzeit Zugriff auf jeden Artikel im System. Weitere Vorteile sind die Einlagerung der Ware in Originalkartons sowie die hohe Durchsatzleistung des Systems. Damit bietet OSR Shuttle die nötige Flexibilität, um auf zukünftige Marktveränderungen und Anforderungen verschiedener Absatzkanäle schnell reagieren zu können.

die Verkabelung hergestellt werden. Das ist denkbar einfach: Man muss nur AS-i- sowie AUX-Flachkabel einlegen und die Frontklappe schließen. Die Kontaktierung zum Flachkabel erfolgt werkzeuglos, einfach durch das Schließen der Frontklappe. Weil die Konfigurationen der AS-i-Stränge vorab festgelegt wurden und bereits in den Gateways gespeichert sind, muss bei der Inbetriebnahme nur noch die korrekte Funktion der Fördertechnikelemente im Zusammenspiel geprüft und quergecheckt werden. „Mit diesem Ansatz konnten wir einen erheblichen Anteil der Arbeit ins Haus verlagern und dadurch die Montage vor Ort sehr viel effizienter gestalten“, zieht Claus Blödorn das Fazit „Die Entscheidung für AS-Interface war für uns also goldrichtig.“ ■

Bild: AS-International Association e.V.

Das Motorrollenmodul integriert sich diskret in die Tragschiene.

Firma: AS International Association e.V.
www.as-interface.net

Direkt zur Marktübersicht i-need.de *www.i-need.de/?f8259*

- Anzeige -

Anlagenbau, Industrie und Gebäude
SCHALTSCHRANKBAU
Methoden - Komponenten - Workflow

Jetzt immer aktuell!
Die neuen Normen und Normenentwürfe der DKE VDE DIN

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

ssb-magazin.de

Bild: ©sdecoret-FOTOLIA.com

Bild: Nexans Deutschland GmbH

Die Norm 61850 soll die volle und intelligente Automatisierung des Energienetzes ermöglichen

IEC61850

Eine leise Revolution

Der Ausbau von Energienetzen entwickelt sich sehr dynamisch. Die Einbindung dezentraler Energiequellen (Photovoltaik- und Windkraftanlagen) gewinnt zunehmend an Bedeutung und stellt die Betreiber vor neue Herausforderungen. Die größte davon heißt Smart Grid.

Der Begriff 'Smart Grid' in der Elektrizitätsversorgung beschreibt die kommunikative Vernetzung und Steuerung von Stromerzeugern, Speichern, elektrischen Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzen. Ziel ist die optimierte Energieversorgung auf Basis eines effizienten und zuverlässigen Systembetriebs. Treibende Kräfte sind ein deutlich größeres Informationsvolumen im Netz und die Notwendigkeit eines wesentlich umfangreicheren Datengerüstes in den Leitebenen der Versorger. Langfristig nimmt die Funktionalität der Netzstation zu, was unmittelbar zu einer Vervielfachung des Kommunikationsaufkommens führt. Die bisherigen Standard-Ortnetzstationen, die über keine dedizierte Kommunikationsanbindung verfügen und bestenfalls mittels einer zwei-Draht-Meldung in eine Station mit Fernwirkanbindung übertragen, werden durch intelligente Ortnetzstationen mit einer modernen Kommunikationsanbindung und einer Vielzahl neuer Funktionen abgelöst. Seit einigen Jahren setzt sich ein neuer offener Kommunikationsstandard durch.

Die Norm IEC61850

Die Norm IEC61850 wurde in Zusammenarbeit mit Anwendern und Herstellern definiert und von der IEC verabschiedet. Ziel ist es, Schutztechnik, Steuerung von Schaltanlagen und Kommunikation auf eine einheitliche Basis zu bringen. IEC61850 verwendet TCP/IP als Basisübertragungsprotokoll und hat sich schon weltweit als Kommunikationsstandard in der Automatisierung und Energiewirtschaft etabliert. Um den vollautomatischen oder ferngesteu-

erten Betrieb der Anlagen zu ermöglichen, erfordert die IEC61850 robuste Kommunikationslösungen, insbesondere für betriebskritische Anwendungen. Es geht um Höchstverfügbarkeit in extrem rauen Umgebungen und industriell abgehärtete Netzwerkkomponenten. Für die Übertragung der Daten in den IEC61850 genormten Netzen kommen Ethernet-Switches zum Einsatz und sorgen für den Datenaustausch unter Intelligent Electronic Devices (IED).

Universelles Datenmodell für die Kommunikation im Smart Grid

Für den Netzbetreiber bedeuten die offenen, standardisierten Schnittstellen weniger Aufwand bei der Kopplung von Systemen verschiedener Hersteller und dadurch Investitionssicherung bei Ersatzbeschaffung. Dadurch reduzieren sich auch die Realisierungszeiten von Projekten sowie Investitions- und Betriebskosten. Die Herstellerabhängigkeit entfällt. Es besteht allerdings ein weiterer allgemeiner Handlungs- und Entwicklungsbedarf für die Etablierung von Komponenten mit allgemeingültigen und standardkonformen Datenmodellen. Leider werden die Netzwerkkomponenten heute noch als eigener separater Teil der Anlagen, mit eigenen Servern und eigenem Management betrachtet. Deren Intelligenz und Monitoring-Funktionen werden unzureichend genutzt, z.B. mittels SNMP oder OPC Integration. Die Anbindung erfolgt über eigene, zum Teil proprietäre Systeme. Im Jahre 2012 hat Nexans entschieden, neuartige Systeme auf Basis der SCL-Konfigurationsschnittstelle zu entwickeln. Diese Schnittstelle erlaubt eine nahtlose Modellierung und Betrieb der Stationsleittechnik. Darüber hinaus sollte ein allgemeingültiges und flexibles Kommunikationsdatenmodell mit dezentralisierten Strukturen und Prozessen für die Energieversorgungsinfrastruktur etabliert werden. Das gesamte Kommunikations-Engineering nach IEC61850 ist unabhängig von den unteren Protokollschichten. SCL benutzt für die Systembeschreibung nur das Datenmodell, das in IEC61850-7 definiert ist. Zur Kommunikation zwischen den Geräten werden die abstrakten Datenmodelle und die Kommunikationsdienste von IEC61850-7 mittels konkreter Protokolle so definiert, dass Informationen physikalisch ausgetauscht werden können. Die Datenmodelle werden hierarchisch, baumartig, definiert und aufgebaut. Die Modelle beinhalten 'Logische Knoten', 'Daten Objekte' und 'Kontrollblöcke'. Die Kommunikationsdienste der Teile IEC61850-7-2/3/4 werden entsprechend zum größten Teil auf den Manufacturing Message Specification-Diensten abgebildet. Bei der Übertragung des Modellierungsansatzes wird der Switch als ein physisches Gerät in einem gemeinsamen logischen Knoten mit dazu gehörigen Attributen beschrieben. Dieses Modell ermöglicht die direkte Kommunikation von allen vernetzen Geräten im Stromnetz ohne Datenverluste. Es ergibt sich eine universelle Schnittstelle für die Parametrierung und Auslesen von allen Systemeinstellungen und -funktionen. Es werden auch wertvolle Informationen für das Management des Power Grids geliefert, ggf. über den aktuellen Stand des Netzes, seiner Komponenten, einzelner IEDs sowie Sicherheits- und Alarmmeldungen. Das Kommunikationsmodell wurde im Rahmen des Forschungsprojekts 'Smart Area Aachen' erfolgreich getestet. Die Implementierung von IEC61850 Stack in den Nexans Switches hat alle Kema-Zertifizierungstests bestanden.

Fazit

Im Wandel zu Smart Grid werden die Auslegung und der Betrieb von Kommunikationsinfrastruktur eine zentrale Rolle für die effiziente Netzbetriebsführung spielen. Die nahtlose Integration von unterschiedlichen Systemen unter dem Schirm eines weltweit gültigen Standards wird sich in die Leittechniklandschaft von Versorgungsunternehmen einfügen und eine extrem flexible Nutzung zulassen. Neue Hardware- und Software-Komponenten werden Modellierung, Monitoring und Diagnose schneller und einfacher machen. Die Offenheit und Flexibilität der IEC61850 wird die volle und intelligente Automatisierung des Energienetzes bereits in der nahen Zukunft ermöglichen. ■

Autor: *Fjodor Lamm,*
Head of Marketing (ANS),
Nexans Deutschland GmbH
www.nexans.de

Direkt zur Marktübersicht i-need.de *www.i-need.de/?f15387*

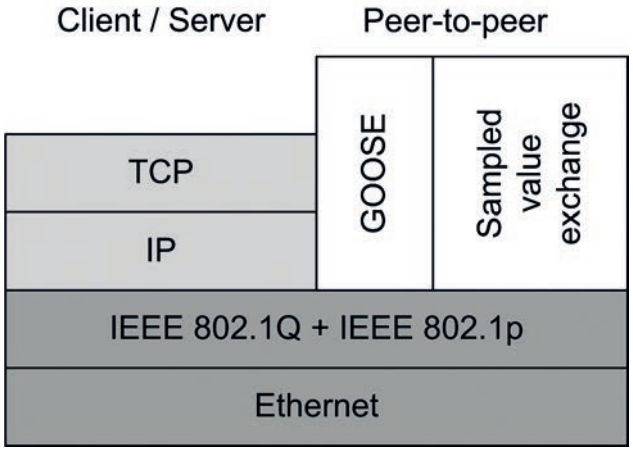


Bild: Nexans Deutschland GmbH

Prinzipielle Abbildung der Kommunikationsmodelle

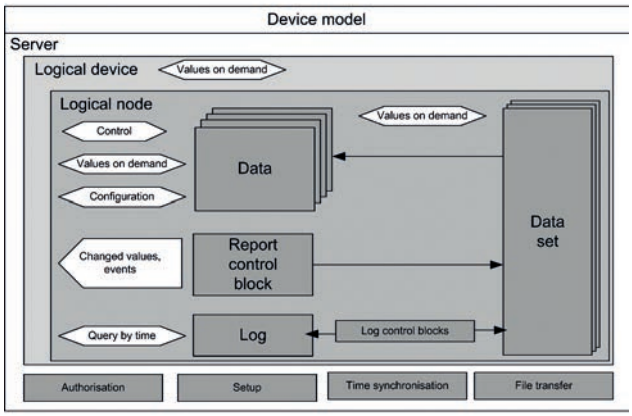


Bild: Nexans Deutschland GmbH

Prinzipielle Darstellung des Gerätemodells gemäß IEC61850

Bild: Phoenix Contact Deutschland GmbH

Intelligente Lösung: Hybridsteckverbinder übertragen Signale, Daten und Leistung gleichzeitig.

Leistung, Daten und Signale auf einer Leitung übertragen

Platzgewinn und schlanke Kabelwege

Maschinen, Anlagen und Automatisierungskomponenten mit jeweils eigenen Leitungen für Signale, Daten und Leistung zu versorgen, ist zeitaufwändig und kostenintensiv. Je komplexer die Regelungs- oder Steuerungsaufgaben, desto größer wird der Verkabelungsaufwand – und damit auch der Einfluss auf die Verfügbarkeit der gesamten Anlage. Einen Ausweg bieten Hybridsteckverbinder zur Übertragung von Signalen, Daten und Leistung über nur eine Leitung.

Bei frequenzgeregelten Antriebslösungen ist heute noch die sternförmige Verteilung vom Schaltschrank zum Motor üblich. Die serielle Verkabelung wurde bisher fast ausschließlich mittels Bussystemen gelöst. Mit dem neuen M40-Hybridsteckverbinder von Phoenix Contact und geeigneten Leitungen ist nun eine serielle Versorgung und Ansteuerung der Verbraucher mit Signalen, Daten und Leistung möglich. Dazu wird jedes Gerät in der Versorgungskette mit zwei Gerätesteckverbindern ausgestattet, von denen je einer mit Stift- und einer mit Buchsenkontakten bestückt wird. Die Steckverbinder basieren auf dem bekannten Servomotor-Steckverbinder und kombinieren entsprechende Kontakte zur Übertragung von Signalen, Daten und Leistung in einem Gehäuse. Damit eignet sich der M40-Hybridsteckverbinder für hohe Spannungen bis 630/850V AC/DC sowie Ströme bis 70A.

Höhere Anlagenverfügbarkeit, geringere Kosten

Die hybride Anschlusstechnik reduziert nicht nur den Platzbedarf am Gerät oder im Schaltschrank. Auch die Maschinen- und Anlagenverkabelung wird übersichtlicher, da nur noch eine einzige Leitung ver-

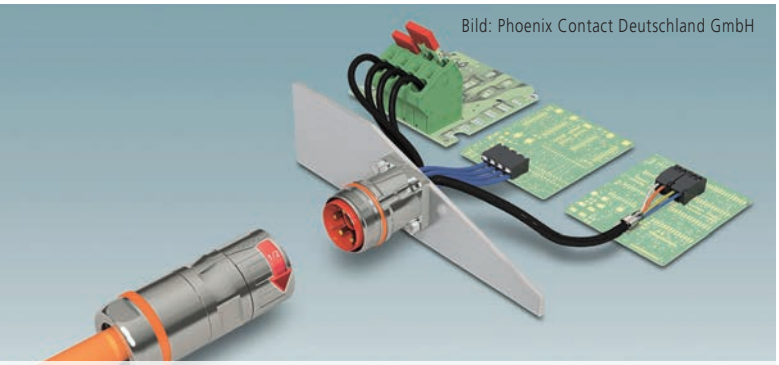


Bild: Phoenix Contact Deutschland GmbH

Schnellverriegelungssystem: Speedcon verriegelt Kabel- und Gerätesteckverbinder mit nur einer halben Drehung.

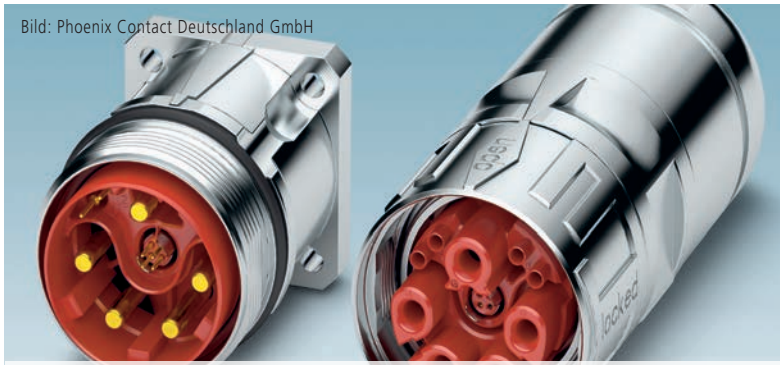


Bild: Phoenix Contact Deutschland GmbH

Platzvorteil: Runde Hybridsteckverbinder bauen kompakt und sparen damit viel Platz.

legt werden muss. Die daraus resultierenden schlankeren Kabelwege reduzieren zudem die Kosten für Trasse und Kabelkanal. Ein weiterer Vorteil der hybriden Anlagenverkabelung: Da bis zu zwei Drittel weniger Anschlüsse erforderlich sind, können Geräte, Maschinen und Anlagenteile einfacher in Betrieb genommen und gewartet werden. Viele Anlagen- und Maschinenbauer führen beispielsweise Vor-Inbetriebnahmen in der eigenen Fertigung durch. Nach erfolgreichem Abschluss dieser Tests müssen die Anlagen schnell und sicher abgebaut, verpackt, versandt und beim Endkunden wieder in Betrieb genommen werden. Hier profitieren Hersteller und Anwender besonders vom Schnellverriegelungssystem Speedcon. Mit einer halben Drehung verriegelt das System den Kabelsteckverbinder zuverlässig mit seinem Gegenstück. So lassen sich Geräte mit nur zwei Handgriffen schnell und sicher anschließen.

Mehr Funktion bei gleicher Baugröße

Der Einsatzbereich des neuen M40-Hybridsteckverbinders ist breit gefächert. Anwender können die einfache Drehstrom-Versorgung mit L1-L3, N, PE, Signalen und Daten bei 630VAC ebenso realisieren wie die Gleichstrom-Versorgungen mit bis zu 850VDC – beispielsweise für dezentrale Servo-Antriebe. Ein Fehlstecken wird verhindert – mechanisch durch vier verschiedene Kodierungen und optisch durch Gehäusemarkierungen mit Farbringen. Die standardisierte Baugröße M40 bietet bei gleicher Leistungsdichte signifikante Platzvorteile gegenüber den am Markt erhältlichen Rechtecksteckverbindern. Ob M23 oder M40 – unabhängig von der Baugröße kommen bei den robusten Hybridsteckverbindern von Phoenix Contact vierpolige Cat5-Elemente zur Datenübertragung zum Einsatz. Hiermit können nahezu alle gängigen Bussysteme sowie kundenspezifische Datenschnittstellen verkabelt werden. Der integrierte Datenstecker ist mit 0,8mm-Kontakten ausgeführt. Diese sind gegenüber den am Markt vorhandenen 0,6mm-Kontakten nicht nur robuster, sie erlauben zudem eine einfache und sichere Konfektionierung.

M40-Hybridsteckverbinder – technische Daten

- Polbilder: 4+4+4+PE sowie 8+4+PE
- Betriebstemperatur: –40 bis +130C°
- Schirmung: 360° Außenschirmung sowie unabhängige Schirmung des Cat5-Daten-Elements
- Verriegelung: Schnellverriegelung mit Speedcon
- Vibrationsfestigkeit: bis 25 g
- Schutzarten: IP66, IP67 und IP68, optional IP69k
- Zubehör: Schutzkappen aus Metall und Kunststoff, Farbringe zur optischen Markierung
- Approbationen: cUL in Vorbereitung
- 2 x 2 Daten: 50VAC/VDC, 3,6A, 0,5mm², optional 4 x Signal: 50VAC/VDC, 8A, 1,0mm²,
- 4 x Signal: 500VAC/VDC, 8A, 1,5mm²
- 4 x Leistung +PE: 630VAC/850VDC, 70A, 16,0mm²
- Berührungsschutz auf der Buchsenseite
- Alle Gehäuse können wahlweise mit Stift- oder Buchseneinsätzen bestückt werden

Ausführungen für zahlreiche Anwendungen

Bei Anwendungen, die keine geschirmte Datenschnittstelle erfordern, kann das Cat5-Daten-Element durch ein vierpoliges ungeschirmtes Signal-Element ersetzt werden. Damit steht – bei ansonsten gleichen Leistungsmerkmalen der Leistungskontakte – ein Steckverbinder mit acht 1mm-Signalkontakten zur Verfügung. Mit Strömen bis 8A pro Kontakt und einem Aderquerschnitt bis 1,5mm² lässt sich beispielsweise eine Steuerelektronik – bis hin zu Hardwareabschaltungen – realisieren. Die Besonderheit der Signalkontakte: Durch geeignete Luft- und Kriechstrecken können selbst Versorgungsspannungen bis 500VAC bereitgestellt werden. Sowohl auf der Kabel- als auch auf der Geräteseite stehen zahlreiche unterschiedliche Gehäusebauformen zur Verfügung. Auch kundenspezifische Konfektionen bis hin zur kompletten Systemverkabelung sind jederzeit möglich. Die Anwender erhalten ab Werk geprüfte Leitungen selbst für hohe Leistungen und Datenraten. ■

Autor: *Dipl.-Ing. Gerhard Liewer,*
Produkt-Marketing, Pluscon circular,
Phoenix Contact Connector Technology GmbH
www.phoenixcontact.com

Direkt zur Marktübersicht i-need.de *www.i-need.de/?f36483*

Einkabellösung für die Antriebstechnik

Leiterplatte und Motor kompakt verbinden

Bild: Weidmüller GmbH & Co. KG

Schaffen eine Verbindung zwischen der IP20- und IP6x-Welt: Leiterplattensteckverbinder Omnimate Power Hybrid und M23-Hybridsteckverbinder.

In der elektrischen Antriebstechnik geht der Trend zur Einkabellösung in Form eines Hybridkabels. Die Verbindung von Motorspannung, internem Temperaturfühler und einer eventuellen mechanischen Bremse sind die klassischen Anforderungen an diese Schnittstelle. Je nach Anwendung wird auch die Verbindung zu einem Encoder oder Resolver benötigt. Dieser Trend hat direkte Auswirkungen auf die Anschlusstechnik.

Als Lösung bietet Weidmüller auf der Leiterplattenseite (IP20) der Frequenzumrichter oder Servoregler sowie auf der Motorenseite (IP6x) entsprechende Steckverbinder an. Die Leiterplattensteckverbinder-Generation Omnimate Power Hybrid verbindet in einem Steckvorgang die Energie- und Signalleitungen sowie den Kabelschirm von Hybridleitungen mit dem Gerät und verriegelt dabei automatisch. Der Hybridsteckverbinder mit Push-In-Anschlusstechnik vereint Sicherheit, Miniaturisierung und den Schirmanschluss in einem Produkt. Der M23-Hybridsteckverbinder stellt die robuste Verbindung am Motor da, er ist speziell auf die rauen Umgebungsbedingungen im Maschinen- und Anlagenbau ausgelegt. Kunden können sich die Verbindung zwischen Leiterplatte und Motor selbst konfektionieren oder anschlussfertig beim Assemblierungsservice von Weidmüller beziehen. Der Vorteil für den Kunden ist: Vereinfachung von Bestellwesen und Lagerhaltung. Er muss nur eine Bestellnummer verwalten, denn die Beschaffung einzelner Komponenten entfällt.

Ein Kabel für Leistung, Signale und Daten

Hybridkabel stellen die Verbindung zwischen Frequenzumrichtern oder Servoreglern und dem Motor her. Zum Anschließen der Leitung benötigte man bisher drei Steckverbinder: Einen Leistungs-

steckverbinder für den Motoranschluss. Einen Signalsteckverbinder zur Erfassung des Motor-Feedbacks und eine Schirmauflage zum Schutz des Datenverkehrs vor elektromagnetischen Störimpulsen. Der Omnimate Hybridsteckverbinder kombiniert alle drei Steckverbinder applikationsgerecht zu einer Gesamtlösung. Dazu gehört beispielsweise die steckbare Schirmauflage oder die automatisch verrastende Einhand-Sicherheitsverriegelung. Die Integration dieser Funktionen sorgt auch bei schwierigen Einbauverhältnissen für eine intuitive, werkzeuglose Handhabung und eine sichere Kontaktierung. Der Hybridsteckverbinder erfüllt den Berührungsschutz gemäß IEC61800-5-1 von 3 oder 5,5mm. Optional ist er auch mit auf- und festellbaren Pushern und geöffneter Kontaktstelle erhältlich. Diese Version vereinfacht die Verdrahtung im Feld.

Referenzen aus der Antriebswelt

Die Firma LTI Motion bietet mit SystemOne CM ein kompakt ausgelegtes Automatisierungssystem an. Das System vereint die Steuerungs- und Sicherheitstechnik, eine zentrale Leistungsversorgung sowie Mehrachsregler. Im Wesentlichen sind es drei Punkte, die das System kompakt machen: die Integration der Safety-Steuerung in die SPS, die Integration eines 500W-Schaltnetzteils in die Versorgungseinheit und schließlich der Einsatz von Doppel- und Dreiachsreglern. Der Servoregler mit einem Nennstrom von 1,5 bis 32A vereint eine hohe Miniaturisierung mit gleichzeitig hoher Leistung. Im Vergleich zu marktüblichen Mehrachssystemen spart SystemOne CM auf diese Weise bis zu 40 Prozent Platz im Schaltschrank. Einen nicht zu vernachlässigen Anteil am hohen Integrationsgrad sowie der Platzersparnis hat der Omnimate-Power-Hybrid-Steckverbinder. Er erfüllt die Forderungen nach hoher Packungsdichte, hoher Stromtragfähigkeit, zuverlässigen Schutz vor elektromagnetischen Störimpulsen (EMV) und komfortabler und sicherer Handhabung. Die Auswahl der richtigen Anschlusstechnik und ihrer Kombination ergibt einen Kostenvorteil der vom Gerätedesign, über die Installation und dem Service der Anlage reicht. Auch Beckhoff verwendet in seinem Multiachs-Servosystem AX8000 eine Hybridlösung für Power und Feedback. Durch den Einsatz des Omnimate-Power-Hybridsteckverbinders reduziert sich die Verkabelung auf die obligatorische Motorleitung, über die auch die Feedback-Signale direkt übertragen werden. Wie bei der sensorlosen Regelung wird dem Anwender der Einsatz einer zusätzlich erforderlichen Feedbackleitung erspart. Alle benötigten Informationen zur Regelung werden, durch die steckbaren Schirmauflage des Hybridsteckverbinders, störsicher und zuverlässig über eine digitale Schnittstelle übertragen.

Herausforderungen im Design gelöst

Der Hybridsteckverbinder ersetzt mit den direkt in den Leistungssteckverbinder integrierten Signalkontakten sowie dem steckbaren Kabelschirm und dem Einhand-Sicherheitsflansch drei Einzelkomponenten und reduziert drei separate Arbeitsgänge zu einem. Er löst verschiedene typische Herausforderungen beim Gerätedesign:

- 1. Rastertreue Integration der Signalkontakte in den Leistungsteil. Dadurch lässt sich eine umfangreiche Miniaturisierung bzw. Packungsdichte auf der Leiterplatte und Gerätefront realisieren. Ein Steckvorgang vereinfacht die Konfektionierung, Inbetriebnahme und Wartung des Gerätes.
- 2. Die steckbare Schirmauflage mit einer Federleiste ersetzt zwei Schraubflansche. Das neuartige Konstruktionsdetail garantiert eine sichere EMV-Abschirmung. Die Kontaktierung des Kabelschirmes erfolgt über die steckbare Federleiste automatisch und bedienerunabhängig. Eine bisher zusätzliche Schraubbefestigung für den Schirmanschluss entfällt. Dadurch werden Platz, Material und Montagezeit gespart.
- 3. Einhand-Sicherheitsverriegelung: Die werkzeuglose Schnellverrastung ist als Mittelflansch ausgeführt und ersetzt zwei Außenflansche. Die sichere Verrastung des Mittelflansches erfolgt

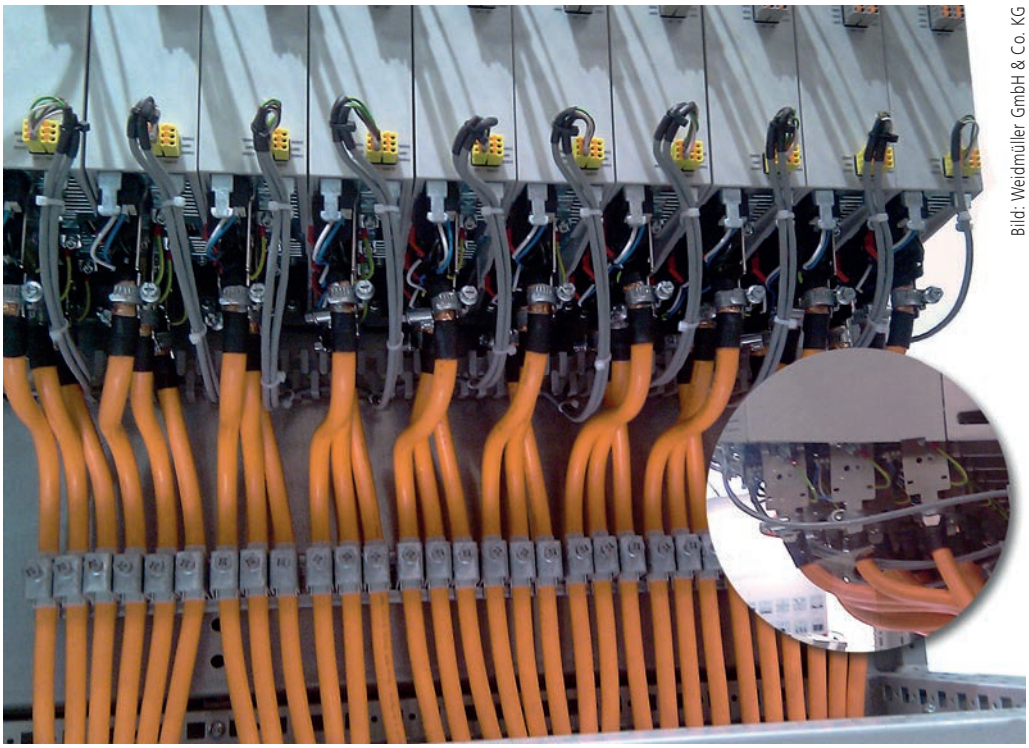


Bild: Weidmüller GmbH & Co. KG

Einsatz am kompakten Dreiachsregler: Die Verbindung zu den drei Servomotoren erfolgt über je einen Hybridstecker.

automatisch und bedienerunabhängig. Durch die baubreitenneutrale Integration der Signalkontakte wird der Platzbedarf am Gerät und auf der Leiterplatte verringert. Ein intuitives Stecken aller vier Funktionen (Energie, Signale, Schirmung und Verriegelung) ist in einem Arbeitsgang möglich – auch ohne Sicht und bei schwierigen Einbauverhältnissen.

Die mehrfache Funktionsintegration von Energie-, Daten- und Signalkontakten sowie der steckbare Kabelschirm und die automatische Verrastung reduzieren die Herstell-, Installations- und Instandhaltungskosten deutlich. Der Abstand zwischen den Gerätereihen kann bis 10cm geringer ausfallen, da die installationsgerechte 30°-Geometrie eine schlanke Leitungsführung ermöglicht und die steckbare Kabelschirmauflage einen geringeren Montageraum benötigt als herkömmliche Schraubflansche. Insgesamt wird die Anlagenverfügbarkeit durch die neuartige Schirmblechkontaktierung, den Einhand-Sicherheitsflansch und die integrierten Signalkontakte erhöht. Die Hybrid-Leiterplattensteckverbinder sind mit Push- In-Anschlusstechnik ausgestattet. Sie ermöglicht eine schnelle Konfektionierung und Installation der Hybrid-Kabel. Der massive oder flexible Leiter mit Aderendhülse versehen, wird einfach in die Klemmstelle gesteckt. Das Anschlusssystem für den Motoranschluss ist mit verrastbaren Push Buttons ausgestattet, um eine geöffnete Klemmstelle zu erhalten. Die geöffnete Klemmstelle ermöglicht einen problemlosen und sicheren Anschluss, der aus ESD-Gründen relativ kurz abgemantelten Motorleitungen. Der Push-In-Kontakt wird nach dem Einstecken des Leiters in die Klemmstelle einfach durch seitliches Drücken auf den Push Button geschlossen. Beim Verwenden von Motoranschlussleitungen ohne Aderendhülsen oder bei Leitungen mit kleinem Querschnitt ist der verrastbare Anschluss ebenfalls von Vorteil. Er hält nach Betätigung die Klemmstelle geöffnet, dass ermöglicht dem Monteur eine leichte und komfortable Handhabung der Leitungen beim Anschließen.

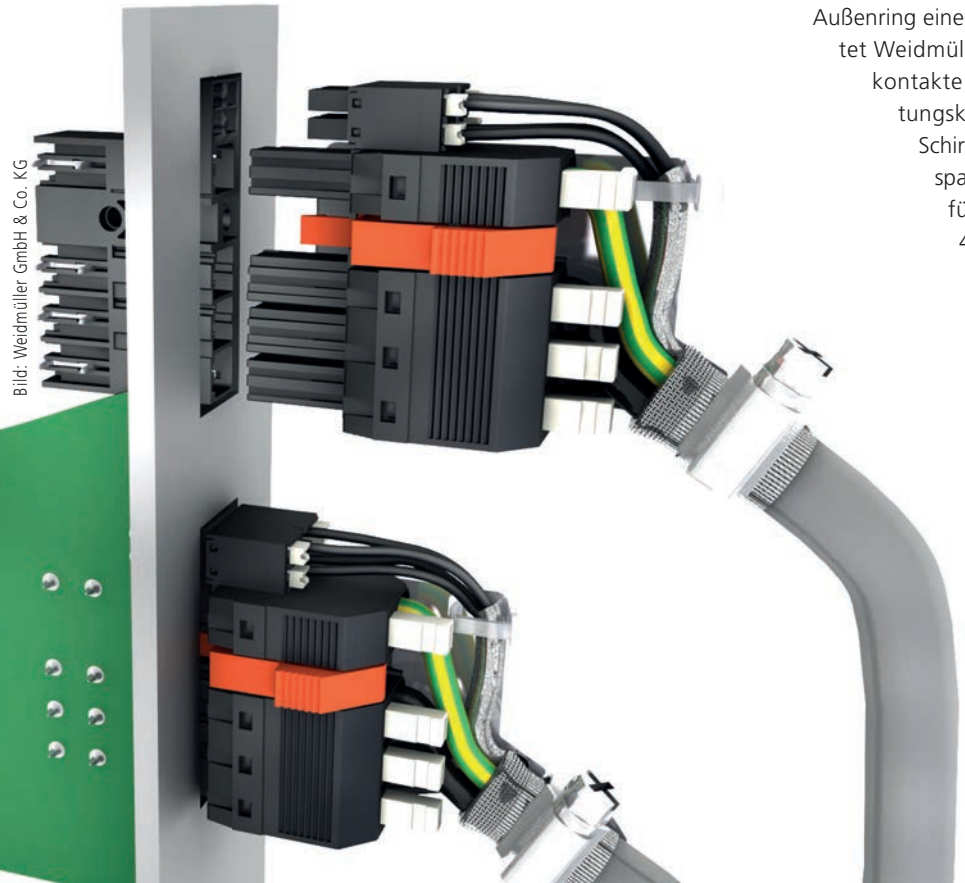


Bild: Weidmüller GmbH & Co. KG

LTI Motion setzt bei SystemOne CM auf Hybridsteckverbinder von Weidmüller.

Bild: LTI Motion/Weidmüller GmbH & Co. KG

M23-Hybridsteckverbinder

Die kompakten und robusten M23-Hybridsteckverbinder sind speziell auf einen industriellen Einsatz sowie den rauen Umgebungsbedingungen im Maschinen- und Anlagenbau abgestimmt, beispielsweise zum Anschließen von elektrischen Antrieben und Servomotoren. Beim Einsatz von Hybridkabeln stellen sie die perfekte Verbindung in die IP6x-Welt da, denn sie gewährleisten die in diesem Bereich geforderte Zuverlässig- und Langlebigkeit. Sie sind resistent gegen das Eindringen von Substanzen, darüber hinaus besitzen die Varianten mit schwarzem Außenring einen Vibrationsschutz. Für Hybridapplikationen bietet Weidmüller die 4+4-Variante an: Sie besitzt vier Signalkontakte mit je einem Nennstrom von 8A und vier Leistungskontakte mit je einem Nennstrom von 28A. Der Schirm wird auf das Metallgehäuse gelegt. Die Nennspannung für die Signalkontakte beträgt 300V und für die Leistungskontakte 800 bzw. 600V. Die 4+4-Variante ist sowohl als Kabel-, Kupplungs- und Winkelsteckverbinder wie auch als Gerätesteckverbinder in folgenden Bauformen lieferbar: Vorderwand, mit Rändelmutter, Hinterwand und abgewinkelt. ■

Der Leiterplattensteckverbinder mit verrastbaren Anschluss verfügt über eine schlanke Leitungsführung mit installationsgerechter 30°-Geometrie.

Autor: **René Arntzen,**
Strategischer Produktmanager
Omnimate – Geräteanschlusstechnik,
Weidmüller GmbH & Co. KG
www.weidmueller.de

i-need.de www.i-need.de/?f13849

- Anzeigen -

Wireless-Produkte

Um die flexiblen Produktionskonzepte von Industrie 4.0 umsetzen zu können, sind Drahtlostechnologien eine Voraussetzung. Aber schon heute wird Wireless in der Fertigung immer mehr eingesetzt.

Wireless-Netze wie Bluetooth und WLAN werden für die Industrie zunehmend interessanter. Zahlen, die diesen Trend belegen, hat HMS kürzlich veröffentlicht. Der Kommunikationsspezialist rechnet damit, dass Wireless-Netze als Basistechnologie für innovative Maschinen- und Bedienkonzepte mit einer Wachstumsrate von 32Prozent sogar das am schnellsten wachsende Segment in der industriellen Kommunikation darstellen. Der Marktanteil von Wireless bei neu installierten Systemen wird 2017 vermutlich bei rund 6Prozent liegen. WLAN und Bluetooth haben sich also von der Sonder- zur Standardlösung im industriellen Umfeld entwickelt. *(mby)* ■

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

HMS Industrial Networks GmbH
76131 Karlsruhe | Tel.: +49 721 989 777-000
info@hms-networks.de
www.hms-networks.de

Industrial Access Point und Bridge

- Mobiler Systemzugriff für Wartung, Überwachung und Konfiguration
- Kostengünstiger Einsatz eigener Anzeigegeräte (Tablet, etc.) – BYOD
- Einfache Montage durch einzigartiges All-in-One-Gehäusekonzept (IP67)
- Anbindung über Ethernet mit Unterstützung für BACnet/IP, PROFINET, EtherNet/IP, Modbus TCP sowie TCP/IP und UDP

LUCOM GmbH
90513 Zirndorf | Tel.: +49 9127 59460-10
info@lucom.de
www.lucom.de

GRENZENLOSE M2M-KOMMUNIKATION

VPN-Industrierouter, Alarmsysteme und VPN-Serviceportal

- Industrielle LAN- und Mobilfunkrouter – von GPRS bis LTE
- Alarm- und Meldesysteme – sofortige Benachrichtigung per SMS, E-Mail, Fax oder Voice, weltweit rund um die Uhr
- Sichere VPN-Verbindungen durch OpenVPN, IPSec, Firewall und Redundanz
- VPN-Serviceportal – Verbindung kompletter Netze ohne zusätzliche Routing-Einstellungen
- Unkomplizierte Beratung und Support inklusive
- Customizing, individualisierte Funktions- und Softwareerweiterungen

MEMBER OF exceet

Siemens AG
Process Industries and Drives
Process Automation
www.siemens.de/iwlan

Making the most of air.

SCALANCE W – Industrial Wireless LAN

Drahtlose Kommunikation mit SCALANCE W bietet unzählige Möglichkeiten für den Einsatz sowohl im Schaltschrank als auch im Innen- und Außenbereich – mit Datenraten bis zu 450 Mbit/s.

siemens.de/iwlan

Bild: Deutsche Telekom AG

Vernetzt Dampfkessel in der Cloud: Thomas Hamacher, Chief Technical Officer bei Certuss

Predictive Maintenance

Dampf in der Cloud

Dampfkessel werden in zahlreichen industriellen Fertigungsanlagen eingesetzt. Ob zum Reinigen von Equipment, Aufheizen von Substanzen, Befeuchten von Kunststoff oder als Belastungsprobe in der Automobilindustrie – als Bestandteil von Produktionsketten müssen sie stets zuverlässig funktionieren. Durch zentrale Vernetzung kann das Unternehmen dies jetzt auch aus der Ferne sicherstellen.

„Unsere Geräte stehen oft im Verborgenen. Fallen sie dann aus, merken wir es häufig zu spät und der gesamte Produktionsprozess ist beeinträchtigt", erklärt Thomas Hamacher, CTO des Dampfkesselherstellers Certuss. Deshalb setzt das Unternehmen auf vernetzte Technik und überwacht seine Geräte mit einer Cloud-Lösung der Deutschen Telekom.

Vernetzung mit der Cloud der Dinge

Das Unternehmen stattet die Maschinen der Produktreihe Universal TC mit einer Reihe von Sensoren, Mobilfunkkarten und passender Hardware aus. Die erhobenen Messwerte können so per Mobilfunk an die Online-Plattform Cloud der Dinge der Telekom übertragen werden. Sie sammelt die gewonnenen Daten aller mit ihr verbundenen Dampfkessel, speichert sie und wertet sie aus. Nutzer können bequem auf übersichtliche Darstellungen der verschiedenen Messwerte zugreifen und die Verbrauchsdaten der einzelnen Geräte analysieren. So werden Muster schnell sichtbar, etwa zu welchen Uhrzeiten besonders viel oder wenig Dampf benötigt wird. Anschließend lassen sich die Einstellungen der Dampfkessel individuell anpassen, wodurch eine höhere Effizienz erreicht wird. „Mit dieser Lösung verbessern wir den Service für unsere Kunden und gehen den Schritt in Richtung Zukunft", so Hamacher.

Mehr Zuverlässigkeit durch Fernwartung

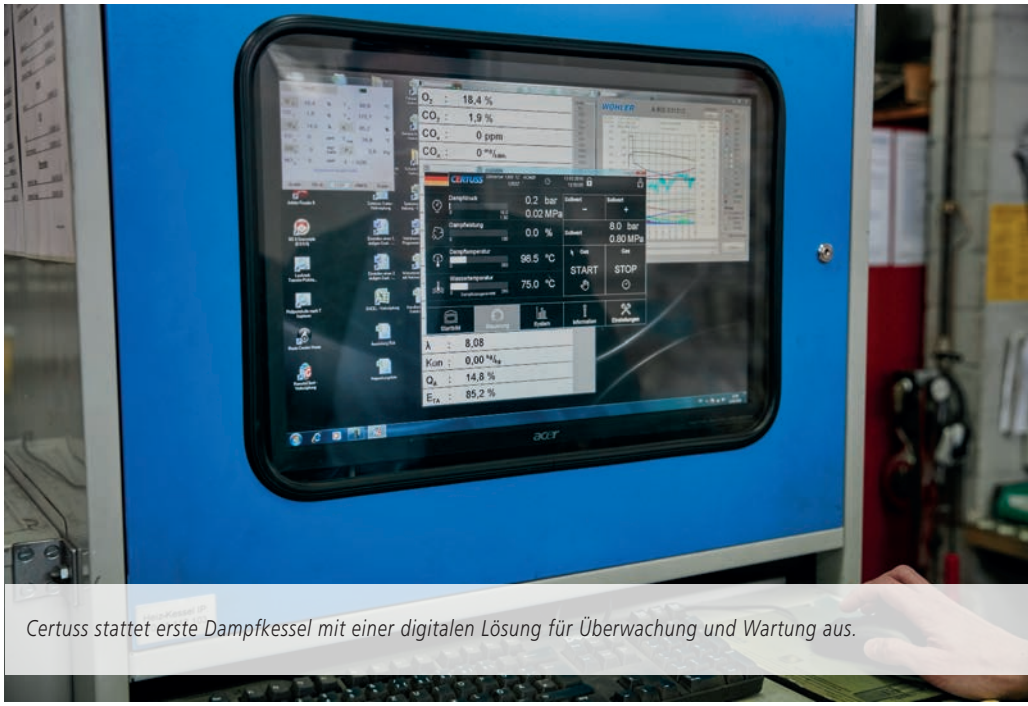
An den Dampfkesseln angebrachte Sensoren messen insgesamt 60 verschiedene Parameter, etwa Druck, Temperatur, Verbrennungszustände oder Wasserstand. Durch die Übertragung in die Cloud können diese Werte aus der Ferne einfach überwacht werden. Anwender können für jede einzelne Kategorie Schwellenwerte definieren. Werden diese überschritten, löst die Platt-

form selbstständig Alarm aus. So werden Probleme schnell bemerkt und behoben. „Wir erhöhen damit die Zufriedenheit unserer Kunden in zwei Bereichen: Im Falle eines Ausfalls benachrichtigen wir automatisch unsere Kunden und einer unserer Techniker kann schnell reagieren und den Schaden so gering wie möglich halten. Viele Störungen lassen sich aus der Ferne beseitigen, ohne dass ein Servicetechniker vor Ort sein muss“, erklärt Hamacher.

Potenzial für Predictive Maintenance

Die detaillierte Datenerhebung Cloud der Telekom bietet noch weitere Möglichkeiten: Mit ergänzender Software zur Datenanalyse können Certuss-Techniker die Betriebsdaten der Dampfkessel genau unter die Lupe nehmen und so feststellen, wie und wann Störungen überhaupt entstehen. So können sie sich mögliche Schäden schon frühzeitig anzeigen lassen, Fehler werden erkannt und behoben, bevor sie einen Ausfall überhaupt verursachen. Diese Predictive Maintenance erinnert außerdem rechtzeitig daran, wann regelmäßige Kontrollen anstehen. Ein enormer Wettbewerbsvorteil, zeigt eine aktuelle Studie des Weltwirtschaftsforums und des Beratungsunternehmens Accenture. Sie fand heraus, dass Predictive Maintenance Einsparungen bei geplanten Reparaturen von zwölf Prozent ermöglicht. Wartungskosten sinken damit um fast 30 Prozent. Ungeplante Stillstände gehen der Studie zufolge um 70 Prozent zurück. „Mit der Datenanalyse durch die Cloud der Dinge und weiteren Systemen gehen wir auf Spurensuche, um anhand der interpretierten Daten die Geräte vorausschauend zu warten“, sagt Hamacher. Beide Funktionen – die schnelle Störungsbeseitigung und die vorausschauende Wartung – bringen Certuss-Kunden Zeitersparnis durch Fernüberwachung, mehr Produktivität durch geringere Ausfallzeiten sowie Kostenersparnisse durch präventive Wartung.

Bild: Deutsche Telekom AG



Certuss stattet erste Dampfkessel mit einer digitalen Lösung für Überwachung und Wartung aus.

Bild: Deutsche Telekom AG

Durch Langzeitanalysen der Daten können Störungen proaktiv vermieden werden.

Sicherheit im Fokus

Sicherheitsbedenken bezüglich des Datenschutzes sind jedoch immer noch eine große Hürde auf dem Weg von Unternehmen hin zur vernetzten Produktion, werden doch sowohl sensible Unternehmen- als auch Kundendaten auf einer Online-Plattform gespeichert und verarbeitet. Die Deutsche Telekom verschlüsselt die Übertragung, schafft zuverlässige Netzwerke und sichere, ISO-zertifizierte deutsche Rechenzentren, die eine Verfügbarkeit von mehr als 99 Prozent garantieren. Zusätzlich erfolgt die Übertragung der Maschinendaten über das Mobilfunknetz der Telekom. So muss nicht in die IT des Nutzers vor Ort eingegriffen werden. „Ein wichtiges Argument für unsere Kunden“, betont der Chefingenieur. ■

Autorin: ***Lena Tausend,***
IT-Redakteurin,
Palmer Hargreaves GmbH
www.palmerhargreaves.de

Bild: Glaston Finland Oy

Die Wireless-Verbindung ist sofort einsatzbereit und es müssen keine Kabel mehr angeschlossen werden.

Remote-Lösung für die Glasveredelung

Sichere Verbindung ohne IT-Kenntnisse

Ein Anbieter von Glasveredelungstechnik benötigt für die Komissionierung und Kundenbetreuung eine zuverlässige Fernzugriffslösung. Die Inbetriebnahme der Anlagen muss unabhängig von der Art, der Umbegung und den Verbindungen des Netzwerks am jeweiligen Standort möglich sein. Mit einem neuen Konzept kann das Unternehmen flexibel über gesicherte Fernzugriffsverbindungen auf ausgelieferte Anlagen einwirken.

Wenn eine neue Anlage in Betrieb genommen wird, ist für die Unterstützung der eigenen Installationstechniker des Unternehmens Glaston eine Remote-Verbindung erforderlich. Nach der Inbetriebnahme sorgt ein Remote-Desktop dafür, dass dem Kunden Support bereitgestellt werden kann und verschiedene Aufgaben, wie beispielsweise Beschwerden, geregelt werden können. Außerdem lassen sich über diese Verbindung die Ursachen von Problemen identifizieren, die im Rahmen von Prozessen auftreten. Die vorherige Verbindungslösung hatte sich aufgrund ihrer komplexen und zeitaufwendigen Bereitstellung als problematisch erwiesen. Netzwerkgeräte mussten stets so konfiguriert werden, dass sie mit dem Netzwerk des Kunden kompatibel waren. Daher war auch immer die Hilfe der IT-Abteilung erforderlich. Es traten fortlaufend Probleme mit der Herstellung von Remote-Verbindungen, der Änderung von Einstellungen und der Bereitstellung von Geräten auf. In der Folge musste die IT oft einspringen, um diese Herausforderungen zu bewältigen. Die Installationstechniker von Glaston sind keine IT-Experten und bei der Lösung von Problemen war aufgrund der Beteiligung verschiedener Parteien unklar, wer genau verantwortlich war. Das führte wiederum zu Verzögerungen im Zeitplan.

Einfache Installation

Mit der heute verwendeten Lösung kann die Verbindung ohne besondere IT -Kenntnisse eingerichtet werden, was die Kommissionierung erleichtert und über die gesamte Nutzlebensdauer der Anlage eine einfachere und effektivere Betreuung durch den Kundendienst ermöglicht. Die von dem Tosibox-System eingesetzten starken Datensicherheitsstandards lassen auch die Nutzung unternehmenskritischer Daten zu. "Wir setzen die Fernzugriffstechnik von Tosibox jetzt schon einige Zeit ein und wollen auch all unsere neuen Anlagen werden ab sofort damit ausstatten", so Kimmo Kuusela, Senior Product Development Manager bei Glaston. „Der größte Vorteil ist die Leichtigkeit, mit der eine drahtlose Fernzugriffsverbindung einrichten und in Betrieb nehmen können. Zudem bietet uns Tosibox verschiedene weitere Vorzüge. Starke Datensicherheitsstandards ermöglichen beispielsweise die Nutzung unternehmenskritischer Daten durch unseren neuen Cloud-Service."

Flexibler, zuverlässiger Fernzugriff

Glaston ist für die Kommissionierung seiner Anlagen und die Betreuung seiner Kunden auf leistungsfähige und zuverlässige Fernzugriffs-

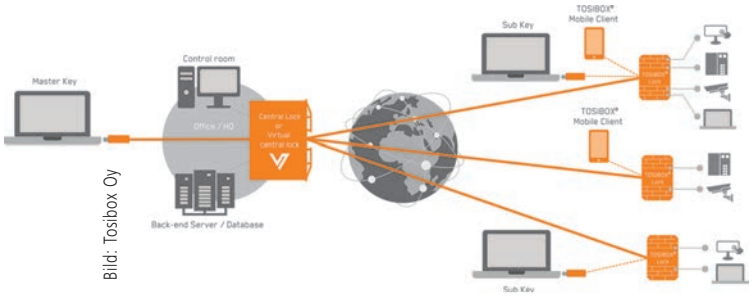


Bild: Tosibox Oy

Mit Tosibox-Technologie können komplette Netzwerkstrukturen einfach aufgebaut und verwaltet werden.

Bild: Tosibox Oy

Die Tosibox Plug&Go-Verbindungsmethode ist weltweit patentiert.

verbindungen angewiesen. Die Inbetriebnahme der Anlagen muss unabhängig von der Art, der Umgebung und den Verbindungen des Netzwerksam jeweiligen Standort möglich sind. Durch die Produkte von Tosibox kann Glaston seine Anlagen mühelos und ohne spezielle IT-Kenntnisse seitens Glaston oder des Kunden über eine drahtlose Fernzugriffsverbindung mit seinem Überwachungszentrum verbinden. Das beschleunigt sowohl die Installation der Anlage vor Ort als auch Kundendiensteingriffe über die Fernzugriffsverbindung. Glaston kann sein Anlagennetz von einer einzigen Stelle aus fernüberwachen. Zudem bieten die Informationssicherheitsfunktionen von Tosibox das erforderliche Maß an Sicherheit, um Daten zwischen Anlagen und dem neuen Cloud-Service von Glaston übertragen zu können.

Benutzerfreundlichkeit im Fokus

Die Lösung arbeitet unabhängig von der Endkundenumgebung und die Konfiguration erfolgt mit wenigen Klicks über den Tosibox Key, der die relevanten Einstellungen enthält. Außerdem verfügt das Tosibox Lock über eine eigene WiFi-Verbindung. Zuvor mussten bei Glaston Installationstechniker temporäre Kabel verlegen, um Anlagen während der Inbetriebnahme miteinander zu verbinden. Jetzt ist die Wireless-Verbindung sofort einsatzbereit und es müssen keine umständlichen Kabel mehr angeschlossen werden. Das spart vor allem Zeit.

Sicherheitsbedenken ausgeschlossen

Damit Daten zwischen Anlagen und dem neuen Cloud-Service von Glaston übertragen werden können, bietet die neue Lösung ein erforderliches Maß an Sicherheit. Geschäftskritische Informationen, wie Anlagenstatusdaten, Betriebsdaten und -statistiken, wurden zuvor rein auf lokaler Ebene verarbeitet. Durch die neue Verbindung können die Daten nun auf sicherem Weg und ohne Risiko, in die private Cloud von Glaston übertragen werden. ■

Autorin: Anu Rosberg,
Chief Marketing Officer,
Tosibox GmbH
www.tosibox.com

Direkt zur Marktübersicht i-need.de *www.i-need.de/?f44399*

- Anzeige -

HANNOVER MESSE
Besuchen Sie uns!
24.-28.04.2017
Halle 9 / Stand D80

15 JAHRE 2002 - 2017 Indu Sol Industrial Solutions

Indu-Sol GmbH – Spezialist für industrielle Netzwerke

PROFINET

Schmerzhafte Erfahrungen vermeiden.

Monitoring für Ihr PROFINET-Netzwerk.

NEU PROFINET-INspektor® NT mit SECURITY Funktion

Indu-Sol GmbH · Blumenstraße 3 · 04626 Schmölln · www.indu-sol.com · info@indu-sol.com · Tel.: +49 34491 58 18-0 · **Service-Hotline: +49 172 7438044**

Wartung mit dem kognitiven System Watson

Im Dialog mit der App

Auch in einer modernen Fabrik gibt es Maschinenfehler und -störungen. Eine mit künstlicher Intelligenz ausgestattete App lässt sich in der Fertigung einsetzen, um das Beheben von Fehlern an der Produktionslinie zu unterstützen. Mithilfe eines Fotos erkennt die App eine Maschine nicht nur, sondern diskutiert mit dem Wartungsmitarbeiter mögliche Maßnahmen. Eine echte sprachliche Konversation ist ein wesentlicher Schritt hin zur Cognitive Factory.

Bild: IBM Deutschland GmbH

Watson gibt Werkern Hilfestellung bei Wartungsarbeiten und diskutiert Lösungsvorschläge.

Auf der Hannover Messe 2016 zeigte IBM im Rahmen eines Pilotprojekts gemeinsam mit John Deere, wie das kognitive System Watson Werkern in der Fabrik Hilfestellungen bei Wartungsarbeiten und Lösungsvorschläge bei Störungen bieten kann. Jetzt steht die App jedem Kunden und Partnern zur Verfügung und lässt sich auf die eigene Anwendung trainieren.

Repair Experience with Watson

Ein Werker in der Produktion kann per Knopfdruck einen Fehler melden. Dieser Fehler wird einem Wartungsmitarbeiter in einer Smartphone-Anwendung zugeordnet. Indem der Mitarbeiter ein Foto von der fehlerhaften Maschine aufnimmt, erkennt Watson, um welche Maschine es sich handelt. Anschließend wird der Fehler im Dialog mit Watson diskutiert und dieser benennt Maßnahmen zur Behebung. Auf diese Weise wird das klassische Human Machine Interface abgelöst. Auf der Cloud-Plattform Bluemix wurde die Anwendung aus verschiedenen Watson-Funktionen zusammengestellt, konfiguriert und verwaltet. Für die Anwendung wurden folgende Watson-Funktionen verwendet: Document Conversion, Retrieve and Rank, Dialog, Text to Speech, Speech to Text, Push Notification und Visual Recognition. Das anschließende manuelle Training für den Prototyp war auf die Wartung von zwei verschiedenen Maschinen mit jeweils fünf verschiedenen Fehlern ausgerichtet. Nach dieser ersten Version war der nächste Meilenstein, aus dem Prototypen eine wiederverwendbare Lösung zu bauen, ohne dass für Nutzer manueller Entwicklungsaufwand für Installation und Konfiguration der Anwendung und insbesondere für das Trainieren auf neue Maschinen anfällt.

Funktionen der App ‘Repair Experience with Watson’

- Meldung eines Fehlers vom Arbeitsplatz an die Mobile Maintenance App des Servicetechnikers
- Erkennung der fehlerhaften Maschine auf Basis Watson Visual Recognition
- Vorsprechen der Fehlerbeschreibung aus dem Fehlerspeicher der Maschine auf Basis Watson Text2Speach
- geführte Unterhaltung zwischen Servicetechniker und Watson auf Basis Watson Dialog
- freie Unterhaltung zwischen Servicetechniker mit Watson auf Basis Watson Retrieve & Rank
- automatische Trainings-Pipeline für die o.g. Services per Deploy to Bluemix
- Anpassung der Training-Pipeline auf die eigene Maschine durch Hochladen eigener Fotos, Service Manuals und Trainingsfragen-Anpassung
- weitere Ausbaumöglichkeit, um die Anwendung zu erweitern sind frei in Bluemix verfügbar.

Installation auf Knopfdruck

Nun ist es möglich die Anwendung auf IBM Bluemix automatisch per Knopfdruck zu installieren. Dabei wird die App-Logik übernommen und alle benötigen Watson-Funktionen werden an die Anwendung angebunden. Anschließend kann über eine grafische Benutzeroberfläche das Training für den individuellen Einsatz an den Maschinen der Kunden erfolgen. Es sind keine Programmier-Kenntnisse oder Kenntnisse der einzelnen Watson-Funktionen notwendig, da diese automatisch eingespielt werden. Die für den individuellen Einsatz benötigten Dateien, wie beispielsweise Benutzerhandbücher der Maschinen und Fotos oder Grafiken für die Bilderkennung, können einfach hochgeladen werden. Es ist auch möglich, die Funktionalität der Anwendung für die eigenen Zwecke auf Basis des zur Verfügung gestellten Beispiels weiterauszubauen. Der Quellcode ist auch mitgeliefert. ■

Autor: ***Plamen Kiradjiev,***
Chief Architect Industrie 4.0,
IBM
www.ibm.com/de

Autor: ***Benedikt Krüger,***
Master@IBM, IBM Cloud
IBM
www.ibm.com/de

Infrastruktur für smarte Kommunikation

Bereit fürs IIoT?

Das industrielle IoT entwickelt sich stetig: Immer mehr Komponenten und Lösungen in der Fertigung sind online angebunden, um die Überwachung, Steuerung und Sicherheit in der Fabrik zu verbessern. Die ersten beiden Teile dieser Artikelserie sind auf die Herausforderungen eingegangen, denen sich der Anwender beim Thema Internet der Dinge stellen muss. Der nun folgende Teil 3 beantwortet die fünf meist gestellten Fragen zum Industrial Internet of Things.

Das Industrial Internet of Things zielt darauf ab, die Effizienz und Produktivität in der Industrieautomation durch die Vernetzung verschiedener Geräte sowie die Erfassung und Analyse großer Datenmengen zu steigern. Bevor die Implementierung des IIoT beginnen kann, muss allerdings erst einmal die korrekte Infrastruktur geschaffen werden. Das IoT soll es den Anwendern letztlich ermöglichen, mithilfe umfassender Datenanalysen bessere Entscheidungen zu treffen. Um den Mehrwert auszuschöpfen, muss eine durchdachte Netzinfrastruktur vorhanden sein, die wichtige Voraussetzungen bezüglich Bandbreite, Sicherheit, Effizienz, Flexibilität und Verfügbarkeit erfüllt.

Ununterbrochene Datenübertragung sicherstellen

Quad-Play-Dienste, das heißt zusammengefasste Daten-, Voice-, Video- und Steuerungsdienste, sind immer häufiger Bestandteil moderner Industrienetzwerke. Als Ergebnis dessen ist die Netzwerkübertragung komplexer geworden und erfordert mehr Bandbreite, verschiedenen Arten von Daten zu übertragen – insbesondere Videodaten. Bei der Einrichtung eines Netzwerkes sollte man für langfristig ausreichend Bandbreite (z.B. mit GBit-Ethernet oder Wireless gemäß 802.11n) sorgen, da die Menge der eingesetzten Geräte über die Zeit eher zu- als abnimmt. Entsprechend ist durch den Einsatz moderner Technik dafür zu sorgen, dass ein ununterbrochener Betrieb sichergestellt werden kann.

Video-Streams übertragen

Neben der Bandbreite stellt die Übertragung von Video-Streams verglichen mit der Datenübertragung weitere Herausforderungen. Automatisierungsingenieure setzen üblicherweise Multicast-Übertragung über eine schnelle, redundante Ringstruktur ein, um die Bandbreitennutzung zu verringern. Um Video-Datenpakte zu übertragen, werden jedoch verschiedene Protokolle eingesetzt. Beispielsweise erneuert das IGMP-Protokoll Multicast-Group-Tables alle 125s. Falls sich also ein Netzwerkkabel löst oder ein Ethernet Switch Strom verliert, werden die Multicast-Streams nicht automatisch an einen Back-up-Pfad weiter geleitet – man verliert die Video-Frames. Fortschrittliche Ansätze mit Wiederherstellungsfunktion im ms-Bereich schaffen hier Abhilfe.

Wie lässt sich ein Industrienetzwerk sicherer machen?

Industrielle Steuerungsnetzwerke erleichtern den effizienten und sicheren Betrieb in kritischen Branchen wie Öl und Gas, Transportwesen und Produktion. Ein widerstandsfähiges Steuerungsnetzwerk muss in der Lage sein, ungewollten Traffic zu erkennen und zu filtern. Wenn ein Industrienetzwerk beeinträchtigt wird, öffnen sich unter Umständen Hintertüren für Hacker und nicht autorisiertes Personal. Kurz gesagt – ein klares Verständnis von Sicherheit für industrielle Steuerungsnetze ist essenziell. Es gibt

Moderne Industrienetzwerke sind zahlreichen Gefahren ausgesetzt. Effiziente Systemlösungen und durchdachtes Management helfen dabei, diese zu verhindern.

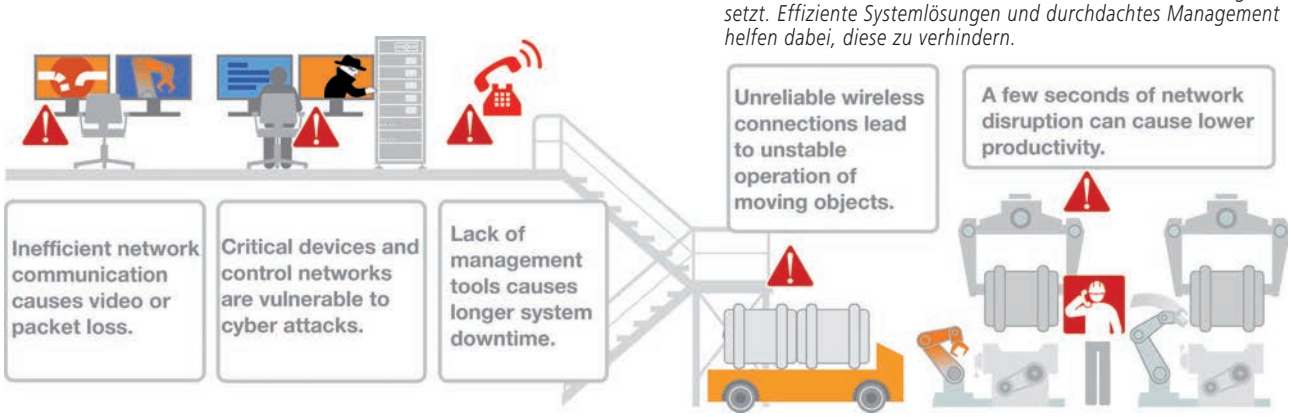
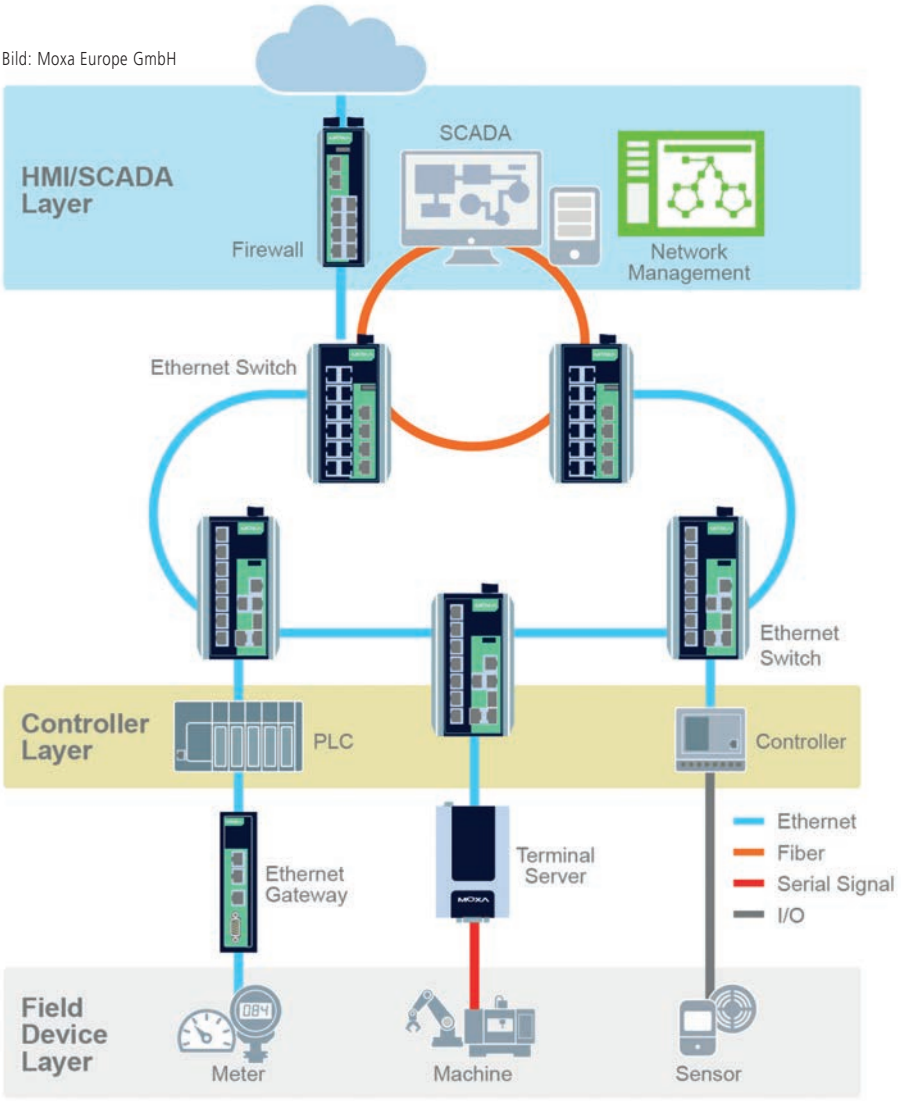


Bild: Moxa Europe GmbH

Bild: Moxa Europe GmbH



Vom Feldgerät bis in die Cloud – die Ebenen des IIoT.

mehrere Optionen, um das Netzwerk in einem Defense-in-Depth-Ansatz sicherer zu machen. Mit einem solchen Zonen- und Kanal-Modell kann die Kommunikation innerhalb jeder spezifischen Zone frei stattfinden. Sofern jedoch verschiedene Zonen miteinander kommunizieren müssen, können sie dies nur über einen speziellen Kanal tun. Er wird von einer Firewall geschützt und erlaubt ausschließlich die Kommunikation jener Informationen, die für die Zone spezifisch sind – alle anderen Informationen werden blockiert. Der Defense-in-Depth-Ansatz kann auf industrielle Steuerungssysteme angewendet werden, um betriebskritische Ausstattung zu schützen und die Sicherheit auf Automatisierungsnetze an verschiedenen Standorten, in Gerätezellen, Funktionszonen und Fabrikanlagen auszuweiten.

Industrielle Netzwerksicherheit

Eine konventionelle Firewall ist für die Paketinhalte industrieller Kommunikationsprotokolle (z.B. Modbus TCP) blind. Das ist ein besonders kritisches Problem, denn industrielle Kommunikationsprotokolle verfügen grundsätzlich über begrenzte Sicherheit und antworten einfach auf alle Pakete, die sie empfangen – ohne vorher zu prüfen, woher die Pakete kommen oder welche Informationen sie enthalten. Dazu gehören Leseanfragen, Abschaltbefehle, Firmware-Updates und Steuerungsbefehle. Welches Potenzial für verheerende Schäden das bietet, ist klar. Starke Firewalls mit zusätzlichen Sicherheitsfunktionen wie Deep Packet Inspection sind also erforderlich, damit das Netzwerk nicht beeinträchtigt wird. Des Weiteren ist das Netzwerk in IIoT-Anwendungen, insbesondere im Bereich Abwasser, Öl und Gas sowie Transportwesen, oftmals mit dezentralen Anwendungen verbunden. Für solche Anforderungen können Unternehmen IPsec oder Open VPNs einsetzen, die als verschlüsselte Datentunnel für sichere Übertragung und Fernzugriff fungieren.

Effizienz und Verfügbarkeit verbessern

Wie lässt sich die Effizienz der Netzwerkverwaltung erhöhen, um die Verfügbarkeit zu verbessern? Bei immer komplexeren Strukturen ist eine einfache Form der Überwachung und Verwaltung notwendig, damit das Netz nicht durch Ausfallzeiten beeinträchtigt wird. Im allgemeinen umfasst der Lebenszyklus des Netzwerkmanagements die Installation, den Betrieb, die Wartung und die Diagnose. Auf jeder Stufe stehen Administratoren vor verschiedenen komplexen und zeitaufwändigen Aufgaben. In der Installationsphase erfordern die manuelle Konfiguration und das Testen der Netzgeräte mehrere Arbeitstage. Ein weiterer Punkt ist, dass die manuelle Konfiguration einer Vielzahl von Geräten zu Eingabefehlern und folglich Verzögerungen aufgrund der nötigen Fehlerbehebung führen kann. Die übliche Unternehmens- und Managementsoftware, die komplexe Funktionen und fortschrittliche Benutzerschnittstellen unterstützt, ist in der Industrieautomation nicht hilfreich. Um automationsspezifische Zwecke zu erfüllen, sollte die Managementsoftware den Administratoren ermöglichen, mittels einer benutzerfreundlichen Schnittstelle Echtzeitüberwachung durchzuführen sowie eine historische Ereignisanalyse unterstützen. Zusätzlich dazu sollte eine industrielle Software in der Lage sein, mit bestehenden Scada-Netzen zusammen zu arbeiten, sodass es für Ingenieure einfacher ist, den Gesamtbetrieb auf einer einzigen Plattform auszuführen und zu verwalten. Der Einsatz von mobilen Geräten ist hierbei hilfreich. Die Prüfung des Netzwerkstatus über das Smartphone ermöglicht es, sofort auf Ereignisse zu reagieren. Einige der aktuellen Netzüberwachungs-Apps un-

terstützen sogar eine Schnellsuche für Feldgeräte, mit der die langwierige Suche nach Geräten auf Fabrikebene entfällt.

Drahtlose Verbindungen halten

Wie lässt sich sicherstellen, dass mobile Ausstattung ihre Wireless-Verbindung aufrecht erhalten kann? Wi-Fi-Netzwerke haben eine begrenzte Signalabdeckung, deshalb ist eine Vielzahl von Access Points erforderlich, um zum Beispiel über ein ganzes Warenlager hinweg volle Abdeckung zu erzielen. Es ist betriebskritisch, dass Clients zwischen den Access Points ununterbrochen mit sehr kurzer Handover-Zeit roamen können. Bei älteren Wi-Fi-Geräten tritt üblicherweise eine Unterbrechung von 3 bis 5Sek. auf, wenn sie sich zwischen den Abdeckungszonen von zwei Access Points bewegen. Folglich entstehen Unterbrechungen im Betrieb. Passiert dies z.B. bei einem autonomen Transportsystem, stoppt es so lange, bis die Verbindung wieder steht. Das kann zu Produktionsverzögerungen und damit zu erhöhten Betriebskosten führen.

Verschiedene Kanalfrequenzen

Darüber hinaus erfolgt oftmals eine Beschränkung der Bandbreite über die verschiedenen Kanalfrequenzen. Um das zu vermeiden, müssen Systemintegratoren mehrere verschiedene Kanalfrequenzen einsetzen, um die Überlastung der Kanäle zu verhindern. Systemintegratoren können die Roaming-Parameter so konfigurieren, dass eine ortsabhängige Lastverteilung erfolgt, sodass sich die Clients immer mit dem nächstgelegenen Access Point verbinden und eine Überlastung des Netzwerkes vermieden wird. Um Sicherheitsrisiken zu begrenzen, müssen Verschlüsselungsprotokolle eingesetzt werden. Werden allerdings Sicherheitsfunktionen wie WPA/WPA2 eingestellt, kann dies Auswirkungen auf die Roaming-Leistung haben.

Schutz vor Störungen

In der Fabrikumgebung sind automatische Regalbediengeräte und unbemannte Fahrzeuge ständig in Bewegung, um Materialien für den Produktionsprozess zur Verfügung zu stellen und fertige Waren zu lagern. Geräte, die guten Gewissens in Industrieumgebungen eingesetzt werden können, sollten dem Standard IEC60068-2-6 entsprechen, der auch die Richtlinien zum Schutz von Wireless-Geräten vor Schock und Vibration umfasst. Auch elektromagnetische Störungen können Wireless-Geräte und ihre sensiblen Strom- und Antennenschnittstellen beeinflussen, daher nutzen die meisten Systemintegratoren Zubehör zur Isolierung. Dieses Zubehör erhöht allerdings die Installationskosten und erfordert zusätzlichen Raum.

Ausfallzeiten verhindern

In IIoT-Anwendungen haben Systemausfälle Produktionsverluste und somit erhebliche finanzielle Ausfälle zur Folge. Dem entsprechend erwarten Anwender eine Systemverfügbarkeit von 100 Prozent. Industrieanwendungen befinden sich jedoch oft an dezentralen Standorten und sind an weit entfernte Leitstellen angebunden. Wartung, Fehlersuche- und -behebung werden dadurch erschwert und teurer. Zwei kritische Faktoren, die sich auf die Netzwerkleistung im Feld auswirken, sind die Wiederherstellungszeit und die Qualität bzw. das Design der Netzwerkgeräte. Industrienetzwerke werden oft in rauen Umgebungen installiert, in denen elektromagnetische Interferenzen von Feldgeräten hervorgerufen werden oder die Umgebungsbedingungen, wie Schock und Vibration, Feuchtigkeit und Erosion oder extrem heiße und kalte Temperaturen negative Auswirkungen auf Geräte haben können. Daher sollten die Qualität und die Art der Konstruktion beim Kauf beachtet werden. In manchen Branchen sind zusätzlich bestimmte Zertifizierungen erforderlich.

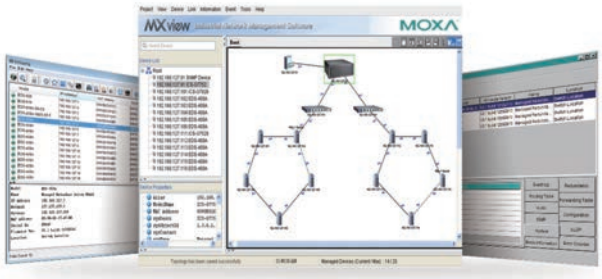


Bild: Moxa Europe GmbH

Moderne Management-Software gibt in Echtzeit einen Überblick über das gesamte IIoT-Netzwerk.

Schnelle Wiederherstellungszeiten

Die Industrieautomation erfordert sehr schnelle Wiederherstellungszeiten, um ununterbrochenen Betrieb sicher zu stellen. Mit industriellen Redundanzprotokollen, die Wiederherstellung auf ms-Ebene erzielen, sind Anwender auf der sicheren Seite. Gleiches gilt für die Drahtloskommunikation: Auch hier sind Anwender mit Geräten, die eine Ausfallsicherung im ms-Bereich anbieten, gut beraten. Neben der Wiederherstellungszeit sollten die Skalierbarkeit der Installation, die maximale Geräteanzahl, die unterstützt wird sowie zu guter Letzt die Kosten in Betracht gezogen werden. ■

Artikelserie: Herausforderung im Internet der Dinge

Teil 1 - Industrial Communication Journal 1/2016
Teil 2 - Industrial Communication Journal 2/2016

Autor: *Matthias Laubner,*
Field Application Engineer,
Moxa Europe
www.moxa.com

Direkt zur Marktübersicht i-need.de www.i-need.de/f36980

Sicherer Remote Service

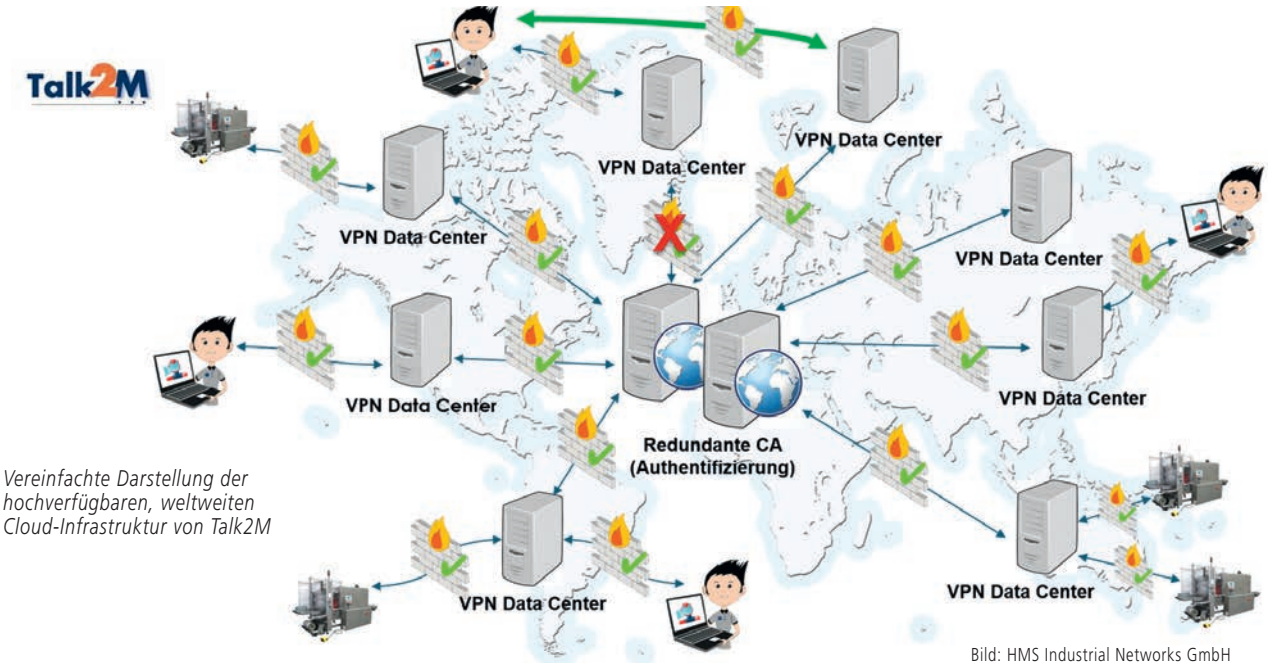
Basis für neue Geschäftsmodelle

Der Fernzugriff auf Maschinen ist aus der Automatisierungswelt nicht mehr wegzudenken. Zeiten, in denen er nur bei Störfällen genutzt wurde, sind längst vorbei. Denn schließlich bietet der Zugriff aus der Ferne – sofern sicher und zuverlässig eingerichtet – vielfältige Möglichkeiten für neue datenbasierte Dienstleistungen. Der durch vorausschauende Wartung, Prozessoptimierung oder standortübergreifender Zusammenarbeit generierte Mehrwert ist erheblich und eröffnet komplett neue Geschäftsfelder.

Bei Industrie 4.0 geht es weniger um die Entwicklung neuer Geräte und Maschinen. Es geht vielmehr darum, relevante Informationen zum richtigen Zeitpunkt zur Verfügung zu stellen, auf deren Basis sich fundierte Entscheidungen schneller treffen lassen. In diesem Szenario kommen Lösungen und Dienstleistungen rund um Fernzugriff, Fernwartung und Datenmanagement eine zentrale Rolle zu. Solche Remote Solutions gehen über den reinen Fernzugriff weit hinaus. Sie stellen einen sicheren Kommunikationskanal bereit, um Daten zu sammeln, zu visualisieren oder vorzuverarbeiten und sie für übergeordnete Systeme (z.B. MES oder ERP) bereitzustellen. Auch der automatische Versand von Alarmen ist über diesen Kommunikationskanal möglich. Mit Ewon bietet HMS eine skalierbare Komplettlösung für sicheren Fernzugriff und industrielle Datendienste. Plattformunabhängig und weltweit verfügbar lassen sich so Steuerungen aller bekannten Anbieter in ein herstellerneutrales und globales Gesamtkonzept integrieren. Der Maschinenbauer erhält über ein einheitliches System Zugriff auf all seine Maschinen und Anlagen. Ewon besteht aus drei Komponenten:

Komponente 1: die Hardware

Die Hardwarebasis bilden vielseitige industrielle VPN-Router, die an der Maschine vor Ort montiert und mit der jeweiligen Steuerung seriell, über Ethernet, per WLAN oder USB verbunden werden. Sie sprechen die Sprache der jeweiligen SPS. Je nach Anforderung kommen verschiedene VPN-Router zum Einsatz: Das Modell Ewon Cosy für einfache Applikationen und Ewon Flexy mit individueller Anpassungen für die Datenvorverarbeitung für anspruchsvolle Anwendungen und umfassende Datendienste.



Vereinfachte Darstellung der hochverfügbaren, weltweiten Cloud-Infrastruktur von Talk2M

Bild: HMS Industrial Networks GmbH

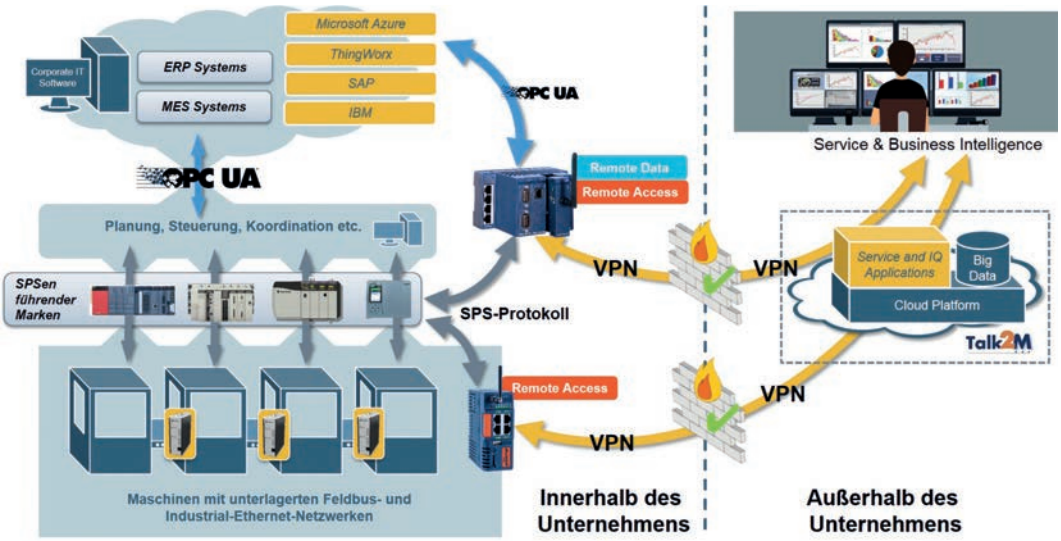


Bild: HMS Industrial Networks GmbH

Fernzugriff und IT/OT-Integration mit Ewon im Kontext von Industrie 4.0

Komponente 2: der Server

Der cloudbasierte Rendezvous-Server Talk2M, Dreh- und Angelpunkt der Ewon-Lösung, ermöglicht den einfachen Verbindungsaufbau und garantiert eine Verfügbarkeit von 99,6 Prozent. Der Dienst ist weltweit verfügbar und besteht aus derzeit 26 hochverfügbaren Servern, die die VPN-Verbindungen verwalten und gegen unberechtigte Zugriffe schützen. Durch den vernetzten Serververbund unterstützt Talk2M Redundanz und Lastmanagement sowie weltweite, garantierte Verfügbarkeit. Jeder Ewon-VPN-Router verbindet sich ausschließlich über den Talk2M-Server mit einer Maschine. Ein Authentifizierungsmechanismus stellt sicher, dass jeder Ewon-Router mit dem Talk2M-Server spricht, der denselben Schlüssel hat. Ein ähnlicher Mechanismus garantiert, dass Anwender nur mit den Routern kommunizieren können, für die Zugriffsrechte eingeräumt sind. Der Rendezvous-Server unterstützt alle etablierten Kommunikationsstandards. Talk2M basiert auf den offenen Standards openVPN und HTTPs. Kunden können über APIs auf dem Router oder in Talk2M eigene Anwendungen entwickeln.

Komponente 3: die Software

Die Ewon-Software eCatcher ist Client für Fernzugriff und für Anlagen- bzw. Nutzerverwaltung. Die Software wird auf dem Windows-PC installiert. In Vorbereitung sind auch Versionen für mobile Geräte wie Tablets und Smartphones. Mithilfe des Tools verbinden sich Anwender von ihrem PC aus mit der entfernten Anlage. Bei Talk2M wurde besonders hoher Wert auf die Security gelegt. Ewon wendet die Guidelines für Cyber Security in industriellen Anwendungen gemäß ISA62443 und NIST SP800 nach dem Defence-in-Depth-Prinzip für die gestaffelte Verteidigung konsequent an. Die Security-Merkmale beinhalten:

- Der gesamte Datenverkehr wird zertifikatsbasiert und verschlüsselt über VPN-Verbindungen nach dem openVPN-Standard übertragen.
- Es sind nur ausgehende Verbindungen erlaubt. Daher müssen keine Firewall-Ports für eingehende Daten im Internet zugänglich gemacht werden.
- Es werden keine statischen IP-Adressen verwendet.
- Der Zugriff kann über eine zweistufige Authentifizierung und eine abgestufte Benutzerverwaltung erfolgen.

Basis für neue Geschäftsmodelle

Remote Services sind Basis für intelligentere und flexiblere Fabriken und ermöglichen neue digitale Geschäftsmodelle mit Fokus auf einer Lebenszyklus- und Serviceoptimierung. Unternehmen können unter den Rahmenbedingungen von Industrie 4.0 ihre Produkte auf ganz neue Weise anbieten oder zusätzlichen Kundennutzen durch Mehrwertservices über den Produktlebenszyklus hinweg erzeugen. Die Wertschöpfungspotenziale lassen sich in folgenden Stufen anschaulich darstellen:

- Verbinden und Zugreifen: Über die physikalische Verbindung erfolgt über das Internet der Fernzugriff auf Maschinen, Steuerungen und Feldequipment. Per Fernzugriff können Außendiensttechniker bei der Inbetriebnahme unterstützt werden. Auch Fehlersuche, Fehlerbehebung oder SPS-Programmierung lassen sich per Fernzugriff lösen. Vorausschauende Wartung beginnt hier und geht fließend in die nächste Stufe über.
- Überwachen: Durch Monitoring und Alarmierung lassen sich Maschinendaten online visualisieren und Fehlermeldungen automatisch absetzen. Das hilft bei der Fehlerbehebung, zudem erhält der Anwender Informationen über den Maschinenstatus und die wichtigsten Kennzahlen.
- Sammeln: Bei der vierten Stufe geht es um das Sammeln von Maschinen- oder Anlagendaten. Hier ist das Stichwort Big Data einzuordnen. Hier kann der Ewon-Router Flexy Daten vorverarbeiten und das Auswerten aufbereiteter Daten erleichtern.
- Integrieren: Für eine vollständige Industrie-4.0-Anwendung gehört die Integration der Fernwartungslösung in ERP-Systeme und Unternehmenssoftware unbedingt dazu. ■

Autor: *Dipl.-Ing. Michael Volz,*
Geschäftsführer,
HMS Industrial Networks GmbH
www.hms-networks.de
Vertriebspartner:
www.wachendorff-prozesstechnik.de

Direkt zur Marktübersicht i-need.de *www.i-need.de/?Produkt=16795*

Unternehmenskritische Sicherheitsvorfälle schneller erkennen und neutralisieren

Wenn der Feind bereits im Haus ist

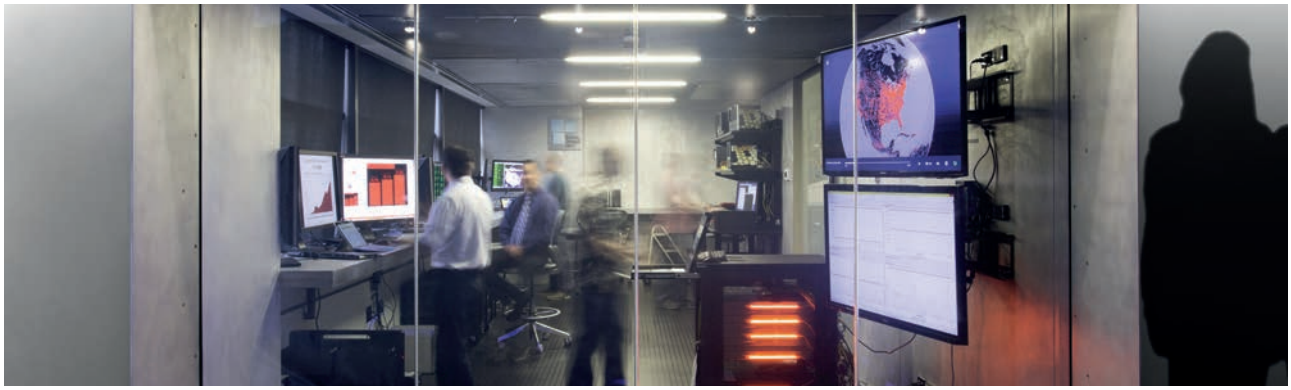


Bild: Microsoft Deutschland GmbH

Cyber-Attacken 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. Der folgende erste Teil des Artikels beleuchtet den Stand heute sowie die Ausgangsbasis und die speziellen Anforderungen der Industrie.

Es war nur ein Experiment, aber das Ergebnis war eindrucksvoll: Der TÜV Süd ging 2015 mit einem virtuellen kleinen Wasserwerk ans Netz. Acht Monate war es aktiv. In diesem Zeitraum gab es mehr als 60.000 feindliche Zugriffe auf das Werk und seine Infrastruktur. Die meisten Zugriffe nach IP-Adresse kamen dabei aus China, den USA sowie Südkorea – aber auch 147 weitere Länder interessierten sich für das kleine deutsche Wasserwerk und seine Daten.

Minuten gegen Monate

Gegen derartige Angriffe nicht vorbereitet zu sein, ist heute eine der größten Gefahren, denen sich ein Unternehmen aussetzen kann. Für eine Cyberattacke benötigt ein Angreifer je nach Unternehmensgröße nur wenige Minuten. Das firmeninterne Sicherheitsteam hingegen braucht durchschnittlich 200 Tage, um einen solchen Einbruch zu erkennen sowie weitere 80 Tage, um das Problem zu lösen. Aktuelle Studien belegen, dass nahezu jedes Unternehmen quer über alle Branchen schon einmal angegriffen wurde. Die weltweite IT-Sicherheit Studie 'Cyber Security Intelligence Index 2016' von IBM X-Force zeigt, dass die Zahl der schweren Sicherheitsvorfälle steigt. Im Jahr 2015 wurden rund 64 Prozent mehr Vorfälle registriert als 2014. Zu den Branchen, die 2015 beliebte Angriffsziele von Cyberkriminellen waren, gehören aber nicht nur das Gesundheitswesen, Behörden, das Transportwesen und die Finanzwirtschaft, sondern auch die Fertigungsindustrie.

Eiserne Regel: Produktion muss laufen

Laut BSI sind die zentralen Bedrohungen, denen Steuerungssysteme in Deutschland ausgesetzt sind: Infektion von Steuerungskomponenten mit Schadsoftware über Büronetze, Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware, Social Engineering, menschliches Fehlverhalten und Sabotage sowie Einbruch über Fernwartungszugänge. Das BSI demonstriert das Ausmaß des Risikos mit dem Beispiel eines erfolgreichen Cyberangriffs auf ein Stahlwerk in Deutschland, der im Lagebericht zur IT-Sicherheit 2015 publik gemacht wurde. Hackern war es über Social-Engineering gelungen, zunächst in das Büronetzwerk des Unternehmens einzudringen und dann auf das Produktionsnetzwerk zuzugreifen. Das zwang die Betreiber dazu, die Produktion einzustellen und die Anlage herunterzufahren. Der wirtschaftliche Schaden war enorm. Marktforscher Gartner sieht vor dem Hintergrund dieser Entwicklung die IT-Leaders in der Pflicht, frühzeitig auf Attacken zu reagieren. Das Thema sei ganz besonders für die Industrie hoch relevant, da hier schon der kurzzeitige Ausfall einzelner Systeme zu enormen Schäden führen kann. Schnell steht in Produktionshallen unter Umständen eine ganze Schicht am Band und kann nicht arbeiten. Aber gerade beim Schutz von Produktionsanlagen gibt es großen Nachholbedarf, denn diese sind durch die digitale Integration sehr angreifbar geworden. Mit neuen Analyseverfahren, die Unregelmäßigkeiten schon früh erkennen, kann am Ende ein Sicherheitssystem stehen, das individuell auf Bedrohungen reagiert. Bei der Sicherung vor Angriffen müssen allerdings die spezifischen Anforderungen der fertigenden Industrie beachtet werden.

Das Produktionsumfeld hat eigene Regeln

Dabei gelten im Zeitalter der Digitalisierung eigene Regeln für die IT-Sicherheit im Produktionsumfeld. Die Steuerungssysteme in der Produktion werden der Büro-IT immer ähnlicher. Die Steuerung und

Überwachung wird zunehmend digitalisiert; Computer und mobile Geräte kommen als Steuerungskonsolen zum Einsatz und vermitteln dem Anwender das Gefühl, sich eher in einer Office-Umgebung, als in einem produzierenden Gewerbe zu bewegen. Doch ein elementarer Unterschied wird immer bestehen bleiben: Die Betriebssysteme und Anwendungen in der Industrie erlauben in der Regel keine aktiven Maßnahmen, und die Sicherung der Netzwerke muss auf passivem Wege geschehen. Sicherheits-Tools dürfen nicht in den Produktionsprozess eingreifen, trotzdem müssen Fernwartungstunnel geschützt werden. Fehlerhafte Wartung kann Systeme stören und zum Stillstand führen. Außerdem sind vielfach proprietäre Systeme im Einsatz, die spezielle Anforderungen stellen. Die eiserne Regel der Fertigungsindustrie besagt, dass die laufende Produktion unter allen Umständen gewährleistet bleiben muss.

Insellösungen abseits des Internets

Im Allgemeinen finden Produktionsprozesse in einer Umgebung statt, die schwer zu überwachen ist. In der Produktion werden häufig Insellösungen genutzt, die nicht für den Onlinebetrieb konzipiert wurden. Sie sind in der Regel auch heutzutage nicht direkt mit dem Internet verbunden, werden aber an das Unternehmensnetzwerk angeschlossen. Schadsoftware kann über andere Geräte in das Netzwerk gelangen und dann die Anlagen befallen. Im Vergleich zu einem klassischen Büro ist die Gruppe der zugreifenden Personen dabei größer und heterogener. Mitarbeiter, Dienstleister, Freiberufler und andere Beteiligte melden sich mit eigenen Geräten in einer unübersichtlichen Umgebung im Netzwerk an. Die Herausforderung besteht darin, ein Konzept zu finden, das eine nahtlose Integration in eine zeit- und geschäftskritische Umgebung mit einer Vielzahl verschiedener Nutzer und Geräte ermöglicht, ohne dass aktive Eingriffe vorgenommen werden müssen. Insbesondere die Fernwartung erweist sich dabei als kritisch: Hierbei wird von außerhalb der Netzwerkperimeter auf die Anlage zugegriffen. Wartungstunnel brauchen besonderen Schutz, denn ohne entsprechende Vorkehrung kann Malware durch diese Tunnel ansonsten direkt die Anlage befallen.

Erste Schritte nach dem Angriff

Post Breach Security oder Advanced Threat Detection werden derzeit immer wichtiger und sind neben etablierten präventiven Schutzmaßnahmen wie Firewalls, Verschlüsselung und Antiviren-Software zentraler Bestandteil jeder wirkungsvollen Sicherheitslösung. Post Breach steht für ‘nach dem Einbruch / Cyberangriff’ und meint konzernweite Sicherheitsmaßnahmen, die greifen, wenn der Einbruch ins Firmennetzwerk bereits passiert und der Feind schon im Netz war oder ist. Einer aktuellen Umfrage der Unternehmensberatung KPMG zufolge sind 40 Prozent der deutschen Unternehmen in den vergangenen zwei Jahren Cyberattacken zum Opfer gefallen. Solche Angriffe auf geistiges Eigentum und kritische geschäftliche Informationen nehmen stetig zu. Dabei erweisen sich die Hacker als überaus geschickt und erfolgreich, auch gegenüber gut geschützten Umgebungen. Ferner nutzen Eindringlinge das primär angegriffene Netzwerk als Sprungbrett, um an wichtige Informationen von Geschäftspartnern oder Kunden zu gelangen. Netzwerke, die mit veralteter Technik arbeiten oder nur rudimentäre Schutzmechanismen einsetzen, sind dabei besonders anfällig.

Sicherheitsvorfälle schneller erkennen

Was aber, wenn der Feind trotz aller Vorsichtsmaßnahmen bereits im Haus ist? Mit dem Post-Breach-Ansatz können unternehmenskritische Sicherheitsvorfälle schneller erkannt und neutralisiert werden. Eine professionelle Softwareumgebung, die nicht nur vor Angriffen schützt, sondern auch schnell agiert, wenn bereits ein Einbruch vorliegt, ist daher besonders wichtig. Windows 10 von Microsoft ist das erste Betriebssystem, das über umfangreiche, integrierte Post-Breach-Funktionen verfügt. Sie erkennen den Eindringling nicht nur zeitkritisch, sondern liefern IT-Verantwortlichen zusätzlich zur Krisenanalyse auch Handlungsempfehlungen zur Behebung des Angriffs. Der zweite Teil dieses Artikels erscheint im INDUSTRIAL COMMUNICATION JOURNAL 2/2017 und geht konkret auf Post-Breach-Funktionalität und entsprechende Sichrheitsstrategien ein. ■

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

Impressum

VERLAG/POSTANSCHRIFT:
TeDo Verlag GmbH®
Postfach 2140, 35009 Marburg
Tel.: 06421/3086-0, Fax: -38
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, Sina Müller,
Melanie Novak, Kristina Sirjanow,
Marco Steber, Florian Streitenberger,
Natalie Weigel

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

ANZEIGENDISPOSITION:
Michaela Preiß
Tel. 06421/3086-0

Es gilt die Preisliste der Mediadaten 2017.

GRAFIK & SATZ:
Jana Berger, Anja Beyer, Tobias Götze,
Moritz Klös, Timo Lange, Ann-Christin Löllkes, Verena Vornam, Laura Jasmin Weber,
Nadin Rühl

DRUCK:
Offset vierfarbig
Grafische Werkstatt von 1980 GmbH
Yorkstraße 48, 34123 Kassel

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

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

ISSN 0935-0187
Vertriebskennzeichen G30449

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

© Copyright by
TeDo Verlag GmbH, Marburg.

Key-Management und Datenverschlüsselung

Schlüssel zur Sicherheit

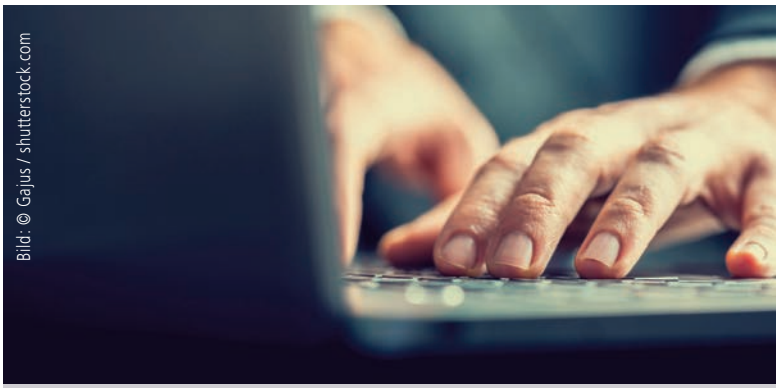


Bild: © Gajus / shutterstock.com

Entscheidend für ein wirksames Key-Management ist, dass der digitale Schlüssel im Unternehmen bleibt.

Mit der Vernetzung von Maschinen werden auch Industrieanlagen anfällig für Angriffe durch Hacker. Dass solche Attacken zuweilen drastische Folgen haben können, zeigen Szenarien aus der jüngeren Vergangenheit. Zu den wichtigsten Sicherheitsvorkehrungen gehören ein professionelles Key-Management und Verschlüsselungstechnologien.

Das Risiko, Opfer eines Anschlags aus dem Internet zu werden, wächst für Industrieunternehmen. Der Grund: Mit Entwicklungen wie Industrie 4.0 und dem Internet of Things sind Produktionssysteme, aber auch Kraftwerke oder Pipelines immer häufiger teils ungeschützt über das Internet erreichbar. Doch auch das Profil der Angreifer selbst hat sich verändert. Sie verfügen nicht mehr nur über Kenntnisse aus dem Bereich IT-Sicherheit, sondern auch über Fachwissen zu industriespezifischen Steuerungskomponenten und Produktionsprozessen. Selbst die Motive haben sich verändert: War in der Vergangenheit größtenteils Neugierde auf die Kompromittierbarkeit von Systemen der Auslöser, mischen sich zunehmend auch Kriminelle mit handfesten wirtschaftlichen Interessen sowie Konkurrenten unter die Angreifer. Damit stellt sich die Frage nach einem wirksamen Schutz vor solchen Attacken. Hier gilt zunächst die Faustregel: Maschinen, die nicht zwingend kommunizieren müssen, sollten vom Internet getrennt sein und sich idealerweise in einem abgeschotteten Netz befinden. Bei allen anderen Anlagen muss ein umfassendes Sicherheitskonzept greifen, das die Themen Datenverschlüsselung und Key-Management in den Mittelpunkt stellt. Erfahrungsgemäß fehlen dafür allerdings oft die nötigen Werkzeuge und ein zentrales Management für die Schlüssel, weshalb Unternehmen ihre Keys in der Regel einfach in der Software speichern, in der die verschlüsselten Informationen genutzt werden, oder das Management einem Provider überlassen.

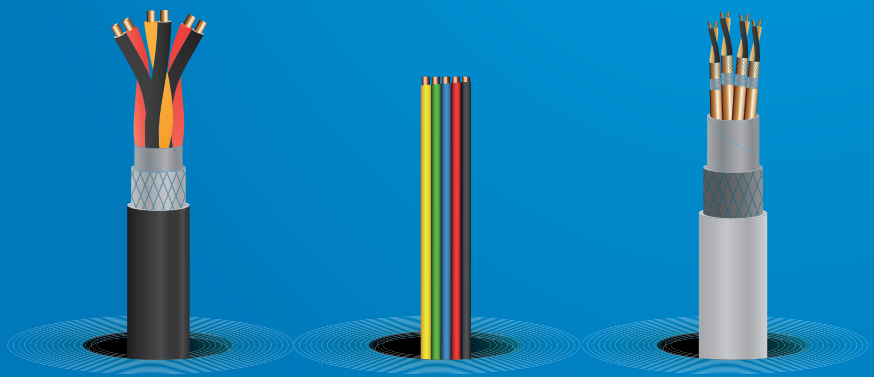
Hardware-Security-Module in Kombination mit einem Key-Management-System

Eine wirksame Verwaltung der Keys beginnt mit der Planung: Wer soll für die Schlüssel verantwortlich zeichnen, wie und wo werden Schlüssel abgelegt und wer darf sie wann benutzen? Diese Fragen müssen geklärt werden. Hinzu kommt die Anforderung, jederzeit nachvollziehen zu können, wer Zugriff auf individuelle Informationen erhalten darf (Authentifizierung) und wer welchen Schlüssel wozu verwendet hat (Auditing). Mithilfe einer zentralen Lösung lässt sich nebenbei auch das typische Problem mit so genannten Islands of Encryption vermeiden, in denen unterschiedliche Schlüssel für einzelne Anwendungsfälle existieren, die eine zentrale Administration erschweren. Entscheidend für ein wirksames Key-Management ist also zunächst, dass der digitale Schlüssel – und damit die Möglichkeit der Entschlüsselung von sensiblen Informationen – in den Händen des Unternehmens verbleibt. Schlüssel müssen getrennt von den eigentlichen Daten gespeichert und verwaltet werden können. Hierfür bieten sich etwa Hardware-Security-Module (HSM) an, die das Schlüsselmaterial in einer sicheren Hardwareumgebung aufbewahren und auch nur dort verwenden. Im Idealfall verlassen die Schlüssel während ihres gesamten Lebenszyklus nie die Hardware: Generierung, Nutzung, Löschung des Schlüsselmaterials – alles findet geschützt in einer sicheren Umgebung statt, so dass der Schlüssel niemals im Klartext vorlag. HSMs gewährleisten außerdem, dass das Unternehmen die Kontrolle über die Zugriffe behält, indem es die Verwaltung und Verteilung für jeden einzelnen Schlüssel ermöglicht. Neben der sicheren Aufbewahrung unterstützt ein professionelles Key-Management auch die Vergabe neuer Schlüssel sowie die Authentifizierung legitimer Nutzer und Administratoren. So lassen sich beispielsweise klare Richtlinien dafür definieren, wer welchen Schlüssel wann und wie oft verwenden darf. Gleichzeitig ist es möglich, beispielsweise einem bestimmten Maschinenpark den Zugriff auf eine Partition im HSM zu erlauben, die zuvor von bestimmten Personen freigegeben wurde und auch nur für authorisierte Nutzer und Systeme zugänglich ist. Hinzu kommen klare Richtlinien für den Entzug von Zugriffsberechtigungen: Sicherheitsoptionen innerhalb des HSM erlauben es beispielsweise, Schlüssel remote zu löschen, zu erneuern, sowie temporär oder dauerhaft deren Nutzung zu beschränken. Eine integrierte Schlüsselrevisionsverwaltung hilft hierbei den Überblick zu behalten. ■

Autor: ***Christopher Meyer, Pre-Sales Manager, Gemalto www.gemalto.com***

DIE DNA VON METROFUNK.

Metrofunk liefert über 2000 isolierte Leitungen - ab Lager!
Schnell. Zuverlässig. Metrofunk.



Datenleitungen, Steuerleitungen, geschirmt

Flachbandleitungen

Datenübertragungsleitungen, flexibel

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

metrofunk KABEL-UNION

Zukunftsichere Plattform für Industrial Automation und Industrial Internet of Things

www.odva.org

ODVA®