SONDERAUSGABE 4/2016
www.sps-magazin.de

INDUSTRIAL COMMUNICATION JOURNAL

ETHERNET WIRELESS SECURITY

Bild: ARBURG GmbH + Co KG

NEUES 3D-DRUCKVERFAHREN SETZT AUF VARAN

Vielseitig, sicher, anpassungsfähig

Seite 6

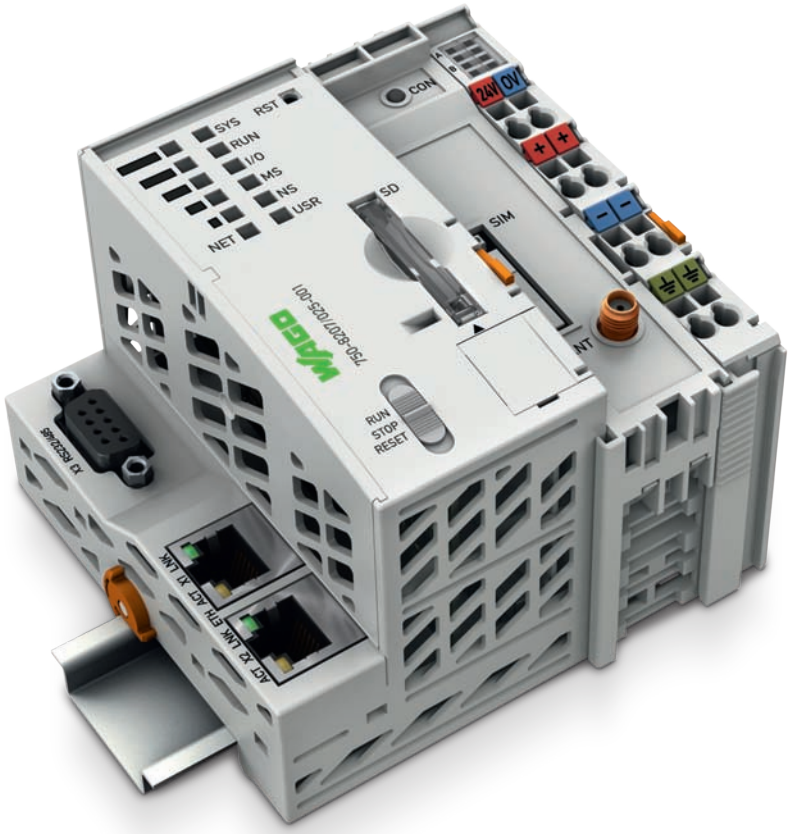
VARAN

INTERVIEW
„Die Marktdurchdringung von IO-Link wird voranschreiten."
Seite 18

SONDERTEIL
CC-Link IE in Action – Lösungen, Konzepte und Produkte
Seite 33

SECURITY
Cybersicherheit mit TSN in modernen Automatisierungsnetzen
Seite 51

VERBINDET DIE WELT DER AUTOMATISIERUNG MIT DEM INTERNET OF THINGS



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

- 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

sps ipc drives

Nürnberg, 22.–24.11.2016

Besuchen Sie uns:
Halle 7, Stand 130

WE INNOVATE!

WAGO

Von Standards und Zahnbürsten

Die meisten Anbieter von Automatisierungstechnik halten es mit Kommunikationsstandards wie mit Zahnbürsten: Jeder hat eine und keiner will die des anderen benutzen. Diese Haltung bringt einige Hürden und Herausforderungen für die Anwender mit sich, die sie ohne proprietäre Protokolle nicht hätten. Mit TSN beginnt nun eine neue Runde im Ringen um weniger Protokollvielfalt, doch der Wunschtraum von nur einem übergreifenden Standard wird sich auch diesmal nicht erfüllen.

Mathis Bayerdörfer, Chefredakteur Industrial Communication Journal

Der Begriff Time-Sensitive Networking, kurz TSN, bezeichnet mehrere Standards, die von den IEEE-Arbeitsgruppen 802.1 und 802.3 spezifiziert werden – teils schon veröffentlicht, teils noch in Vorbereitung –, und als Erweiterung des Standard-Ethernets vor allem auf eine Datenübertragung mit sehr geringer Übertragungslatenz und hoher Verfügbarkeit abzielen. Voraussetzung dafür sind drei Schlüsselkomponenten, die für alle teilnehmenden Geräte gelten: ein gemeinsames Verständnis der Zeit, gleiche Regeln bei der Bearbeitung und Weiterleitung von Datenpaketen sowie gleiche Regeln bei der Reservierung von Bandbreite und Kommunikationspfaden. Mit diesen Eigenschaften und im Zusammenspiel mit OPC UA soll TSN zukünftig Standard-Ethernet auch tauglich für Industrieanwendungen mit hohen Echtzeitansprüchen machen.

Das mag im ersten Moment in vielen Anwenderohren nach der Erfüllung eines Wunschtraums klingen – endlich ein offener Standard, der alles kann –, doch bei der Frage, wann und wie tief TSN Einzug in die Fabriknetze halten wird, gehen die Meinungen heute noch auseinander: Leitebene, Anlagenlevel oder sogar bis in die Maschinen hinein. Zudem tauchen mit TSN auch neue Sicherheitslöcher auf (siehe S. 51). Wiederum keine Frage ist, dass sich die industrielle Kommunikation in den nächsten Jahren verändern wird. Dieser Wandel kommt nicht nur von oben, sondern auch von unten: Denn bei den Anforderungen der smarten Fabrik an die Feldebene reicht der unidirektionale Ansatz der klassischen Analogschnittstelle bei Sensoren und Aktoren nicht mehr aus. Stattdessen kommt hier in absehbarer Zeit z.B. immer öfter IO-Link ins Spiel (siehe S. 18). Die Protokollvielfalt auf der Steuerungsebene wird hingegen erst einmal nicht weniger. Hier muss sich der Anwender nach wie vor entscheiden und prüfen, welches Industrial-Ethernet-Derivat die größten Vorteile für ihn bietet. Wie gewohnt greift die vorliegende Ausgabe des Industrial Communication Journals zahlreiche Aspekte aus diesem Bereich auf. Ich wünsche eine interessante Lektüre.

Mathis Bayerdörfer
mbayerdoerfer@sps-magazin.de

Bild: Varan-Bus-Nutzerorganisation

06

TITELSTORY

Neues 3D-Druckverfahren mit Industrial Ethernet Varan

Beim sogenannten Arburg-Kunststoff-Freiformen lassen sich, basierend auf 3D-CAD-Daten, funktionsfähige Bauteile schnell und ohne Spritzgießwerkzeug aus qualifizierten Standardgranulaten herstellen. Zur sicheren und schnellen Datenübertragung setzt Maschinenbauer Arburg bei diesem neuartigen Verfahren für die industrielle additive Fertigung auf den echtzeitfähigen Ethernetbus Varan. Dessen Vorteile können Messebesucher der kommenden SPS IPC Drives live erleben: Auf dem Stand der Nutzerorganisation VNO ist das additive Fertigungssystem Freeformer ausgestellt.

Interview mit Dr. Robert Bauer, Sick

Bild: Sick AG

„IO-Link erobert sich kontinuierlich ein breites Anwendungsspektrum in der Automatisierung"

Seite 18

Industrial Analytics

Vom Rohstoff zum Wettbewerbsfaktor: Big Data wird in der industriellen Fertigung zunehmend wichtiger

Seite 28

Bild: Bundesministerium für Wirtschaft und Energie

News und Neuheiten

Protokolle und Standards

Schwerpunkt IO-Link

Schwerpunkt Big Data

Sonderteil: CC-Link IE in Action

Wireless und Remote

Sicherheit

Service

Sonderteil CC-Link IE

Bilder: © f9photos / shutterstock.com; CC-Link Partner Association; © eyetronic - Fotolia.com

CC-Link IE findet in Asien große Akzeptanz beim Anwender - ein spannender Aspekt für exportorientierte Maschinenbauer.

ab Seite 33

TSN und Sicherheit

Bild: Belden Electronics GmbH

TSN bietet neue Möglichkeiten, es entstehen aber auch Herausforderungen für die Cybersicherheit.

Seite 51

Bild: Varan-Bus-Nutzerorganisation

Neues 3D-Druckverfahren mit Industrial Ethernet Varan

Vielseitig, sicher, anpassungsfähig

Beim sogenannten Arburg-Kunststoff-Freiformen lassen sich, basierend auf 3D-CAD-Daten, funktionsfähige Bauteile schnell und ohne Spritzgießwerkzeug aus qualifizierten Standardgranulaten herstellen. Zur sicheren und schnellen Datenübertragung setzt Maschinenbauer Arburg bei diesem neuartigen Verfahren für die industrielle additive Fertigung auf den echtzeitfähigen Ethernetbus Varan. Dessen Vorteile können Messebesucher der kommenden SPS IPC Drives live erleben: Auf dem Stand der Nutzerorganisation VNO ist das additive Fertigungssystem Freeformer ausgestellt.

Produktionseffizient, wirtschaftlich und einfach: Der auf die Kunststoffindustrie spezialisierte Maschinenbauer Arburg hat ein völlig neues Verfahren entwickelt: Das sogenannte Arburg-Kunststoff-Freiformen (AKF) macht die Herstellung von Einzelteilen und Kleinserien aus qualifizierten Standardgranulaten möglich – ganz ohne Spritzgießwerkzeuge und mit effizientem Materialeinsatz.

Funktionsfähige Bauteile werden effizient gefertigt

Anders als bei der herkömmlichen additiven Fertigung, dem 3D-Druck, werden beim AKF-Verfahren Standardgranulate wie beim Spritzgießen aufgeschmolzen und Bauteile schichtweise aus kleinsten Tropfen gefertigt. Eine starre Austragseinheit mit spezieller Düse trägt die Kunststofftropfen mittels hochfrequenter Piezo-Technik im vorgegebenen Takt auf einen Bauteilträger auf. Der Durchmesser der unter Druck erzeugten Kunststofftropfen beträgt je nach Düse zwischen 0,18 und 0,3mm. Der bewegliche Bauteilträger wird so positioniert, dass jeder Tropfen exakt auf die vorher berechnete Stelle gesetzt wird. So entsteht Schicht für Schicht das gewünschte dreidimensionale Bauteil. Die CAD-Daten der herzustellenden Bauteile werden an einem herkömmlichen PC offline aufbereitet. Eine spezielle Software erzeugt dabei durch Slicing die erforderlichen Fertigungsdaten. Nachdem die Freeformer-Steuerung diese Daten empfangen hat, welche die Verfahrwege der Achsen festlegen, kann die Produktion starten. Der Datenaustausch zwischen Sensoren, Antrieben, I/O-Baugruppen und der Recheneinheit erfolgt in einem kompakten Netzwerk über den Varan-Bus. Dieses hart echtzeitfähige Bussystem bietet alle Leistungsmerkmale, die bei modernen Industrieanlagen Voraussetzung sind: Schnelle Datenübertragung, hohe Datensicherheit und Verfügbarkeit. Zudem ist die Varan-Technik kostengünstig und als offener Standard konzipiert. „Die Verfahrwege des Bauteilträgers erfordern höchste Präzision von Achsen und Sensoren, die absolut zuverlässig mit

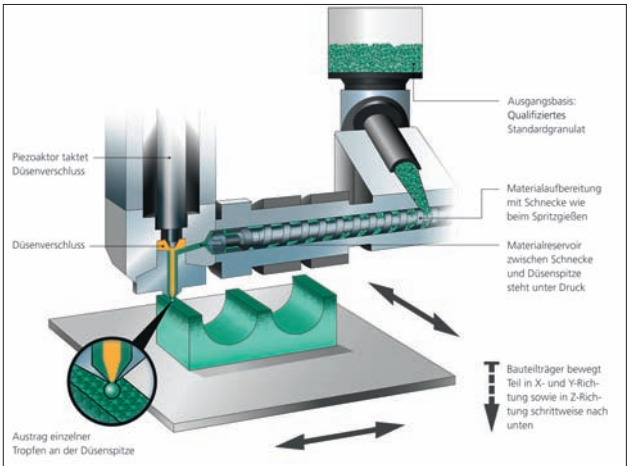
der Recheneinheit kommunizieren“, erklärt der Arburg-Abteilungsleiter der Entwicklung Werner Faulhaber. Mit Varan werde ein schneller und sicherer Prozessablauf garantiert. Auch die Herstellung von Bauteilen aus zwei Komponenten ist mit dem Freeformer möglich. Die zweite Austragseinheit lässt sich für eine zusätzliche Komponente nutzen, um z.B. ein Bauteil in verschiedenen Farben, mit spezieller Haptik oder als Hart-Weich-Verbindung zu erzeugen. Bei Bedarf kann der Freeformer Strukturen aus einem besonderen Stützmaterial aufbauen. Auf diese Weise lassen sich auch ungewöhnliche oder komplexe Bauteilgeometrien realisieren. Die Stützstrukturen lassen sich anschließend in einem Wasserbad entfernen. Optional kann eine Stützstruktur aus dem gleichen Material wie das Bauteil aufgebaut werden. Eine ausgedünnte Zwischenschicht mit gezielt erzeugten Sollbruchstellen sorgt dafür, dass sich die Stützstruktur später einfach mechanisch ausbrechen lässt. Diese Variante wird bevorzugt für Bauteile mit freistehenden Strukturen und klaren Kanten eingesetzt.

Garantierte Datenübertragung

Die hochpräzise Prozesstechnik im AKF verlangt anpassungsfähige Komponenten sowie eine sichere Systemkommunikation in Echtzeit. Der Varan-Bus kann seine Vorteile bei dem neuartigen System von Arburg sehr gut ausspielen: kurze Zykluszeiten, hohe Verfügbarkeit und garantierte Datensicherheit. Basis für das Zusammenspiel der einzelnen Varan-Komponenten ist eine fehlerfreie Datenübertragung, die Varan in der benötigten Prozessgeschwindigkeit realisieren kann. Das Echtzeitsystem nutzt dafür ein außergewöhnliches Daten-Handling. Es stellt sicher, dass nicht übertragene oder fehlerhafte Daten noch im selben Buszyklus wiederholt werden. Der Datenaustausch zwischen Manager und Client erfolgt dabei gemäß des Verfahrens von Request (REQ) and Response (RSP). Jedes vom Varan-Manager gesandte Datenpaket wird unmittelbar vom Varan-Client rückbestätigt. Bleibt die Quittierung innerhalb der definierten Timeout-Zeit aus, wird das Datenpaket noch im selben Buszyklus wiederholt, bis die gültige Antwort vorliegt. Diese Vorgangsweise garantiert, dass am Ende des Buszyklus alle Prozessdaten konsistent sind. Die permanente Überprüfung der Datengültigkeit – auch bei Buszykluszeiten von kleiner als 100µs – wird erst durch die Verwendung der kleinen Varan-Daten-Frames von 0 bis 128 Byte möglich.

Kein Warten auf den nächsten Buszyklus

In hochpräzisen Regelungsprozessen ist das Abholen von Messdaten zu einem genau definierten Zeitpunkt von entscheidender Wichtigkeit. Aber was passiert, wenn dieser Zeitpunkt zwischen zwei Buszyklen liegt? Anders als herkömmliche Bussysteme wartet der Varan-Bus nicht auf den nächst folgenden Zyklus, um die Daten aufzunehmen und an die Recheneinheit weiterzuleiten. Mit dem asynchronen Direktzugriff (DA) kann der Varan-Manager die laufende Kommunikation bis zu 25µs unterbrechen und Prozessdaten zwischen den Zykluszeiten mit den Varan-Clients austauschen. Nach erfolgreicher Datenübertragung wird der laufende Task fortgesetzt. Dadurch lassen sich die hoch priorisierten Daten asynchron zum Buszyklus zu genau vorausberechneten Zeitpunkten senden und empfangen. ■



Das Arburg-Kunststoff-Freiformen (AKF) basiert auf flüssigen Kunststofftropfen – Ausgangsmaterial ist qualifiziertes Standardgranulat, das in einer Plastifziereinheit aufgeschmolzen wird.

Bild: Varan-Bus-Nutzerorganisation

Echtzeitethernet mit Varan

Der Varan-Manager organisiert den Datentransfer im gesamten Varan-Netzwerk völlig selbstständig und entlastet somit die CPU. Anders als bei herkömmlichen Ethernetsystemen ist das Varan-Protokoll zur Gänze in Hardware abgebildet. In Form eines FPGA-Bausteines benötigt der Varan-Bus weder einen eigenen Prozessor noch Rechenleistung vom Steuerungssystem. Die CPU-Einheit im Arburg-Freeformer stellt somit ihre gesamte Rechenleistung der Applikation zur Verfügung, was steigende Performace und gleichzeitige Kostenreduktion mit sich bringt. Überdimensionierte Recheneinheiten fallen weg.

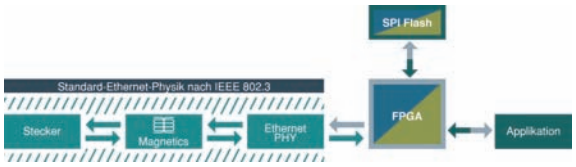


Bild: Varan-Bus-Nutzerorganisation

Beim Freeformer von Arburg kommt für den Datenaustausch zwischen Sensoren, Antrieben, I/O-Baugruppen und der Recheneinheit der Echtzeitethernetstandard Varan zum Einsatz.

Bild: Varan-Bus-Nutzerorganisation

Autor: *David Eisl, Technologieberater , Varan-Bus-Nutzerorganisation www.varan-bus.net*

VDE und internationale Mobilfunkbranche planen Allianz für 5G

Bild: VDE Verband der Elektrotechnik, Elektronik, Informationstechnik e.V.

VDE CEO Ansgar Hinz (links) und NGMN CEO Dr. Peter Meissner (rechts)

Um die Standardisierung und die anschließende Implementierung von 5G voranzutreiben, haben das internationale Mobilfunk-Konsortium NGMN Alliance und der VDE in Frankfurt ein Memorandum of Understanding (MoU) über eine enge Zusammenarbeit zur Förderung von 5G unterschrieben. Mit der Kooperation bündeln NGNM und VDE ihre Synergien für 5G. NGMN vertritt die Global Player der Mobilfunk- und IKT-Branche aus Asien, Europa und Nordamerika bei der Definition von Anforderungen der nächsten Mobilfunkgeneration. Eine erste konkrete Zusammenarbeit mit NGMN ergibt sich über das neu geschaffene Standardization Council Industrie 4.0 (SC I 4.0) der Plattform Industrie 4.0. „Gemeinsam können wir das internationale Zukunftsprojekt 5G und Anwendungen wie Industrie 4.0 schneller zum Erfolg führen, gerade mit Blick auf Themen wie Normung und Standardisierung, Schnittstellen und Interoperabilität", sagte der VDE-Vorstandsvorsitzende Ansgar Hinz bei der Unterzeichnung des Memorandums.

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.
www.vde.com

Plattform Industrie 4.0 und IIC treiben gemeinsam digitale Transformation voran

In der SAP-Zentrale trafen sich im September über 300 Expertinnen und Experten zum zweiten gemeinsamen Arbeitstreffen der Plattform Industrie 4.0 und des Industrial Internet Consortiums (IIC). Die Partner wollen die Kompatibilität ihrer Referenzarchitekturmodelle sicherstellen und gemeinsam Unternehmen den Zugang zu Testumgebungen erleichtern. Die Expertinnen und Experten diskutierten zentrale Herausforderungen der digitalisierten Produktion. Ein Thema war die Erprobung von Industrie 4.0-Anwendungen in Testbeds. Zudem möchten die Experten die praktischen Erfahrungen aus den Tests systematisch zur Weiterentwicklung und Verbindung der bereits etablierten Referenzarchitekturmodelle RAMI 4.0 und IIRA nutzen.

Bild: ©Ingo Cordes/SAP Deutschland SE Co. KG

Industrial Internet Consortium (IIC), Germany, St. Leon-Rot, September 21, 2016

Bundesministerium für Wirtschaft und Energie
www.plattform-i40.de

Echtzeit-Li-Fi für Industrie 4.0

Bild: Fraunhofer-Institut IPMS

Li-Fi-Technologie könnte schon bald störende Kabel- und Steckverbindungen ersetzen.

In intelligenten Fabriken von morgen müssen immer mehr Sensoren, Maschinen, Steuer- und Regeleinheiten miteinander kommunizieren. In vielen Fällen wird eine Taktsynchronität des eingesetzten Kommunikationssystems mit Datenübertragungs-Zykluszeiten von unter einer Millisekunde gefordert. Unternehmen versuchen darum, existierende langsame Kommunikationslinks durch ein Ethernet-basiertes Echtzeit-Feldbussystem ersetzen oder ergänzen. Insbesondere bei beweglichen oder bewegten Anlageteilen wie z.B. Greifarmen oder Hebeeinrichtungen stellt sich das Verlegen einer Signalleitung von der Sensorik oder Aktorik zur Steuereinheit oft als sehr aufwendig oder sogar unmöglich heraus. Genau in diesen Anwendungsfällen soll das LiFi-Kommunikationsmodul des Fraunhofer IPMS mit dem Namen 'GigaDock' seine Vorteile ausspielen. „Unser GigaDock nutzt das weltweit frei von Regulierungen verfügbare Spektrum des Lichts mit Bandbreiten bis 12,5Bit/s. Das ist zehnmal schneller als bei verfügbaren Funklösungen wie WLAN, Bluetooth oder ZigBee", erläutert Projektleiter Dr. Alexander Noack. „Trotzdem konnten wir auf Distanzen bis 50mm sehr gute Echtzeiteigenschaften erreichen und Latenzzeiten von weniger als einer Millisekunde nachweisen."

Fraunhofer IPMS
www.ipms.fraunhofer.de

Task Force: Sichere Identitäten für das Internet der Dinge

Industrie 4.0, Smart Home oder Smart Traffic werden nur funktionieren, wenn jede Maschine, jedes Stück Hardware, jedes Gerät eine eigene, unverwechselbare Identität hat, die gleichzeitig den Anforderungen an den Privatsphärenschutz genügt. Der VDE und das Fraunhofer-Institut für Sichere Informationstechnologie SIT haben deshalb die Task Force 'Trusted Computing zur sicheren Geräte-Identität und –Integrität' gegründet. Ihr Ziel: Anforderungen der Industrie zu sammeln, gemeinsame Lösungen zu identifizieren, sichere Schnittstellen zu entwickeln und Standards zu schaffen. Die Task Force dient dem technologiebezogenen Austausch zwischen den unterschiedlichen Anwendungsdomänen. Deshalb stehen vor allem die Themen Security by Design, Machine-to-Machine Communication, Identität und Integrität von Geräten und Systemen sowie Hardware-Vertrauensanker wie beispielsweise das Trusted Platform Module (TPM) im Fokus. Der VDE und das Fraunhofer SIT laden Experten der Netzbetreiber, Systemtechnikhersteller, Hochschulen bzw. Forschungsinstitutionen dazu ein, in der Task Force mitzuarbeiten.

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.
www.vde.com

Ethernet-Switches für den Netzwerkaufbau

Bild: Vipa GmbH

Die kompakten mit fünf oder acht Ports ausgestatteten Module sind als Unmanaged- oder Managed-Ethernet-Switche lieferbar.

Im Bereich Networking Solutions hat Vipa sein Produktprogramm um intelligente Ethernet-Switche ergänzt. Die kompakten mit fünf oder acht Ports ausgestatteten Module sind als Unmanaged- oder Managed-Ethernet-Switche lieferbar. Beide Versionen unterstützen die Standards IEEE802.3 und IEEE802.3u/x sowie automatische MDI/MDI-X-Erkennung. Sie sind mit ihren speziellen Features für den Einsatz in Profinet-Netzen ausgelegt und ermöglichen die Abfrage von Diagnose- und Statusinformationen. Für Anwender, die das Engineering-Tool Speed7 Studio einsetzen, vereinfacht sich die Verwendung der Managed-Ethernet-Switche dadurch, dass sich die Module per einfaches Drag&Drop in das konfigurierte Profinet-Netzwerk einbinden und zeitsparend konfigurieren lassen. Eine systemoffene Einbindung mittels GSDML-Datei ist ebenfalls möglich. Die kurzen Boot-Zeiten und die Wiederherstellungsfunktionen Turbo Ring und Turbo Chain bewirken zudem eine Leistungsverbesserung bei Profinet-Netzen.

Vipa GmbH
www.vipa.de

Industrial Ethernet Switches für raue Umgebungen

Mit der neuen Produktlinie Scalance XP-200 bietet Siemens kompakte Industrial Ethernet Switches zum Aufbau elektrischer Linien-, Stern- und Ringstrukturen. Die Geräte zeichnen sich durch ihr flaches, robustes Metallgehäuse in hoher Schutzart (IP65/67) und ihren Temperaturbereich von -40°C bis +70°C aus. Dadurch lassen sie sich auch außerhalb von Schaltschränken flexibel im Innen- und Außenbereich einsetzen. Zudem bieten die Layer 2-Switches viele branchenspezifische Zertifikate. So sind sie für explosionsgeschützte Bereiche der Zone 2 (ATEX, IECEx, cULus HazLoc) und damit beispielsweise für die Öl- und Gasindustrie zugelassen. Zudem gibt es für den Einsatz im Schienenverkehr oder in Kraftfahrzeugen widerstandsfähige Varianten. Bei der Anzahl der Ports stehen zwei Varianten zur Verfügung: Der Scalance XP208 verfügt über acht, der Scalance XP216 über 16 Ports. Beide Varianten gibt es als besonders robuste EEC-Version (EEC = Extended Environmental Conditions). Geeignet sind sie für den Einsatz in Bahnen (trainside) und entlang schienengeführter Strecken (trackside). Zudem sind diese Switch-Varianten in Kraftfahrzeugen mit e1/E1-Anforderungen zugelassen.

Siemens AG
www.siemens.de

Switches für den Einsatz auf Schiffen

Bild: Wago Kontakttechnik GmbH & Co. KG

Die Switches sorgen mit ihrer redundanten Spannungsversorgung für eine unterbrechungsfreie Datenkommunikation mit bis zu 1GBit/s.

Auch auf dem Schiff halten immer mehr Ethernet-Anwendungen Einzug. Dafür werden stabile und redundante Netzwerklösungen und Komponenten benötigt, wie die Industrial-Managed-Switches der Serie 852 von Wago. Die individuell konfigurierbaren Industrial-Managed-Switches vernetzen alle Ethernet-Teilnehmer miteinander und sorgen für einen permanenten Zugriff auf Maschinen und Anlagen. Durch die Protokolle Rapid Spanning Tree, Dual Homing, Dual Ring, Jet Ring, ERPS v1/v2 und den schnellen Xpress Ring lassen sich redundante Netzwerkstrukturen mit kurzen Wiederherstellungszeiten von unter 50ms erstellen, um selbst bei gestörten Verbindungen eine sichere Kommunikation zu liefern.

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

Ethernet-Buskoppler

Bild: Beckhoff Automation GmbH & Co. KG

Der Koppler unterstützt das Modbus-TCP-Protokoll und fügt sich damit nahtlos in Ethernet-Netzwerke ein.

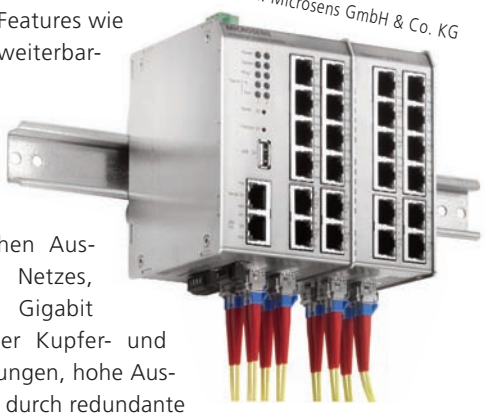
Der Buskoppler EK9000 verbindet Ethernet-Netzwerke mit den EtherCAT-Klemmen (ELxxxx) sowie Ethercat-Box-Modulen (EPxxxx) und setzt die Telegramme von Ethernet auf die E-Bus-Signaldarstellung um. Eine Station besteht aus einem EK9000 und einer beliebigen Anzahl von Ethercat-Klemmen. Der Anschluss an Ethernet erfolgt über RJ45. Mit Ethercat verfügt der Ethernet-Koppler über ein unterlagertes, leistungsfähiges und schnelles I/O-System mit einer großen Klemmenauswahl.

Beckhoff Automation GmbH & Co. KG
www.beckhoff.com

Industrieswitch bietet Power-over-Ethernet mit bis zu 60Watt

Microsens erweitert seine Switch-Reihe Profi Line Modular um High-Power-Ausführungen mit bis zu 60W pro Port. Mit der verdoppelten Leistung für Endgeräte stehen dem Anwender nun neue Einsatzmöglichkeiten zur Verfügung wie die Energieversorgung von LED-/IR-Beleuchtungsanlagen im Security-Umfeld oder die Speisung WLAN- und LoRa-Funksysteme. Die neuen Switches mit erhöhter PoE-Leistung bieten Features wie modulare Erweiterbarkeit bis zu 25 Ports für einen bedarfsabhängigen, wirtschaftlichen Ausbau des Netzes, schnelles Gigabit Ethernet über Kupfer- und Glasfaserleitungen, hohe Ausfallsicherheit durch redundante Stromversorgung und ringförmige Verkabelungsstruktur sowie kurze Wiederherstellungszeiten durch die Speicherung der Firmware und der Konfigurationsdatei auf einer SD-Karte. Durch die Zuverlässigkeit und Sicherheitsmechanismen der robusten Switches mit ihrem strapazierfähigen Edelstahlgehäuse sind sie geeignet für kritische Fertigungsbereiche, in der Energieversorgung, der Gas- und Öl-Gewinnung, zur Überwachung von Pipelines, im Bergbau, im Transportwesen und in der professionellen Sicherheitstechnik

Bild: Microsens GmbH & Co. KG



Die Switches eignen sich für kritische Fertigungsbereiche, zur Überwachung von Pipelines oder der Sicherheitstechnik.

Microsens GmbH & Co. KG
www.microsens.de

TSN Evaluierungs-Kit für Industrie- und Automotive-Anwendungen

Bild: Mocom Software GmbH & Co. KG

Das Kit umfasst alle Tools, die benötigt werden, um die Features der zukünftigen IEEE802.1 Time Sensitive Networking (TSN) Standards zu evaluieren.

Das TSN Evaluierungskit basiert auf der fido5000 REM Switch-Technologie. Vorinstalliert sind auf dem Kit bereits TSN Features wie 802.1AS und 802.1Qbv. Mit der Weiterentwicklung der TSN Standards werden neue Features zur Verfügung gestellt, die kostenfrei vom Innovasic Developer Portal herunter geladen werden können. Die in kommenden Updates unterstützten TSN Standards sind 802.1AS, AS-REV – Time Synchronization, 802.1Qbv – Scheduled Traffic (updates), 802.1Qci – Ingress Policing, 802.1CB – Seamless Redundancy, 802.1Qcc – Centralized Configuration und 802.1bu – Preemption. Bei der Evaluierung von TSN wird das Kit einfach als TSN Gateway eingesetzt. Ethernet fähige Geräte können an den Standard Ethernet Port angeschlossen werden. Die beiden anderen Ports werden mit dem TSN Netzwerk verbunden. Das Ziel ist, dass ein Standard Ethernet Gerät mit jedem anderen TSN fähigen Gerät in einem TSN Netzwerk kommunizieren kann.

Innovasic, Inc.
www.innovasic.de

Mocom Software GmbH & Co.KG
www.mocom-software.de

Neue Funktionen für Infrastruktur-Tool

Der Segment Checker von Pepperl+Fuchs bietet eine intuitive grafische Designoberfläche und erlaubt die Archivierung und den Ausdruck aller vom Anwender erstellten Foundation-Fieldbus-H1- und Profibus-PA-Feldbus-Strukturen. Darüber hinaus besitzt das Tool die Fähigkeit, die Design-Parameter einer Feldbus-Architektur zu überprüfen und die einwandfreie Funktion der Lösung zu bestätigen, noch bevor die Installation beginnt. Eine wichtige Neuerung ist die Aufnahme des Profinet-Gateways in die Liste der unterstützten Infrastrukturkomponenten.

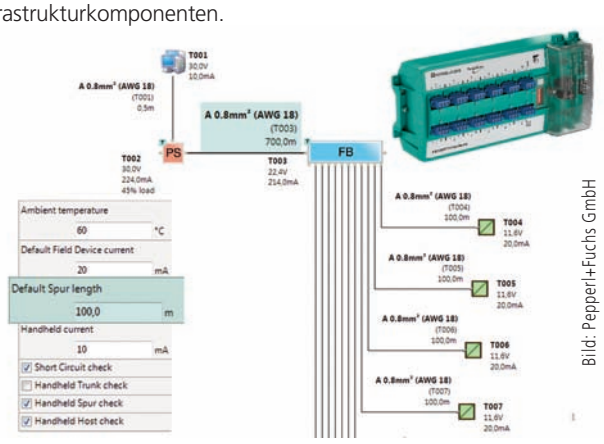


Bild: Pepperl+Fuchs GmbH

Das Tool unterstützt jetzt den Basis-Segmentkoppler KFD2-BR-1.PA.1500 und das Power Hub Gateway HD2-GTR-4PA.PN.

Pepperl+Fuchs GmbH
www.pepperl-fuchs.com

[EC11-156]

Für die einfache Kommunikation mit der Cloud …

… und die Steuerung komplexer Maschinen.

Der Beckhoff IoT-Controller.

Mit den kompakten Embedded-PCs der CX-Serie und dem Softwaremodul TwinCAT IoT ermöglicht Beckhoff die Steuerung komplexer Maschinen mit gleichzeitiger Cloud und Big Data Connectivity. Dabei profitieren Anwender gleich doppelt vom Prinzip der offenen Steuerungstechnik: nach unten ins Feld durch variable Feldbusschnittstellen und Anbindung aller gängigen I/O-Signale; nach oben ins Internet of Things durch freie Wahl einer Private oder Public Cloud über die Standardprotokolle AMQP, MQTT und OPC UA. **www.beckhoff.de/IoT-Controller**

Serie CX8000
CPU: ARM9

Serie CX9020
CPU: ARM Cortex™ A8

Serie CX2000
CPU: bis Intel® Core™ i7, quad-core

sps ipc drives

Halle 7, Stand 406

New Automation Technology **BECKHOFF**

Bilder: ©[vege] / Fotolia.com
©[SG-design] / Fotolia.com

Smart Analytics, Big Data und Cloud

Die Frage nach dem Recht an Daten

Die digitale Transformation ist in vollem Gang. Im Rahmen der Industrie-4.0-Produktion, im Smart Home oder im vernetzten Auto fallen große Datenmengen an. Aber wem gehören diese Daten? Dem Autofahrer? Dem Automobilbauer? Dem Dienstanbieter? Dieser Frage geht Rechtsanwalt Dr. Thomas Thalhofer nach.

Daten werden aufgrund der fortschreitenden Digitalisierung als das neue Öl des Internets und neue Währung der digitalisierten Welt angesehen. Beispielsweise im Rahmen von Smart-Analytics-Verfahren werden Funktions- und Verbrauchsdaten von Produktionsanlagen durch an der Maschine angebrachte Sensoren erfasst oder Nutzungsdaten von internetfähigen TV-Geräten gesammelt. Aber auch im Rahmen der Industrieproduktion und im vernetzten Auto fallen immer größere Datenmengen an. Daten wohnt immer häufiger ein beträchtlicher wirtschaftlicher Wert inne, der einem Unternehmen einen entscheidenden Wettbewerbsvorteil verschaffen kann. Daher stellt sich die Frage, wem die Rechte an diesen Daten zustehen.

Abgrenzung personenbezogener und maschinengenerierter Daten

Personenbezogene Daten sind Einzelangaben und Informationen, die einer bestimmten bzw. identifizierten Person zugeordnet werden können. Bei derartigen Daten stellt sich aufgrund der Möglichkeit, sie einer bestimmten Person zuzuordnen, im Regelfall nicht gleichermaßen die problematische Frage des Rechts an diesen Daten. Denn bei personenbezogenen Daten ist derjenige Rechtsinhaber, der von der Datenerhebung betroffen ist. Eine übertragbare Rechtsposition und damit uneingeschränkte Herrschaft über die Daten wird durch den datenschutzrechtlichen Schutz jedoch nicht erlangt. Maschinengenerierte Daten sind Informationen, die durch Messung, Beobachtung, statistische Erhebung oder sonstige Aktivität durch eine Maschine oder ein Produkt gesammelt oder gespeichert werden. Dies sind beispielsweise Informationen wie Betriebsstunden, Druck, Temperatur, Kraftstoffdurchfluss und Stromverbrauch. Bei diesen Daten besteht bisher keine explizite gesetzliche Regelung, welche die Nutzung oder Erhebung dieser Daten regelt.

Der Begriff von Big Data

Im Zusammenhang mit dem Recht an Daten ist auch der Begriff Big Data näher zu betrachten. Er wird verwendet, um den Einsatz großer schnell wachsender Datenmengen und deren Speicherung in Hochleistungsdatenbanken zu beschreiben. Big Data ermöglicht unter anderem die Erstellung von Nutzerprofilen oder

die Herleitung von wirtschaftlich verwertbaren Korrelationen. Durch eine Big Data Analyse kann ein Unternehmen beispielsweise zielgerichtet Marketing betreiben, aber auch Prozesse oder Produkte verbessern. Im Rahmen von Industrie 4.0 am Beispiel der Smart Factory erfolgt die Optimierung der Produktionsabläufe aufgrund der Vielzahl der Messdaten, die durch Sensoren an den Maschinen erfasst werden. Um auch diese Messdaten in den Analyseprozess aufnehmen zu können und dadurch die Auswertung und Wertschöpfung zu verbessern, ist zu klären, wem diese Daten letztlich zuzuordnen sind. Darf etwa ein Produktionsunternehmen diese Daten überhaupt verwenden, oder gehören diese z.B. dem Hersteller der Maschine, welchen man zuerst um Erlaubnis fragen müsste?

Eigentum an Daten?

Besteht nach der aktuellen Gesetzeslage überhaupt ein Eigentum an Daten? Nach § 903 BGB kann der Eigentümer einer Sache über diese nach Belieben verfahren und andere von jeder Einwirkung ausschließen. Damit verleiht das Eigentum einerseits positiv ein umfassendes Nutzungsrecht und andererseits kann der Eigentümer andere von der Nutzung ausschließen (negatives Abwehrrecht). Voraussetzung ist jedoch, dass Daten eine Sache in Form von körperlichen Gegenständen darstellen. Darunter fällt zwar das physische Medium auf dem Daten gespeichert sind. Daten selbst sind jedoch gerade nicht verkörpert, sodass kein durch das Eigentum begründetes Nutzungsrecht an den Daten besteht. Um dennoch ein eigentumsähnliches Recht an Daten zu begründen, ist zu überlegen, ob das Recht an Daten als sonstiges Recht im Sinne des § 823 Abs. 1 BGB geschützt ist. Dieser Paragraf schützt aber nur die in der Vorschrift aufgezählten absoluten Rechte wie den Körper, das Leben, die Gesundheit und neben dem Eigentum auch sonstige Rechte. Über die Norm kann der Rechtsinhaber Eingriffe in sein Recht abwehren und bei einer Verletzung Schadensersatz verlangen. Voraussetzung für die Einordnung als absolutes Recht ist aber, dass das Recht Wirkung gegenüber jedermann entfaltet. Zwar erkennt die Rechtsprechung an, dass Datenbestände zu den selbstständigen vermögenswerten Gütern gehören. Die Annahme eines absoluten Rechts an Daten konnte sich bisher jedoch nicht durchsetzen. Außerdem ist unter Juristen umstritten, ob die Einordnung als sonstiges Recht neben der Abwehrkomponente auch die positive Nutzungsbefugnis beinhalten soll. Dahin gehen die Überlegungen, wenn man solche Daten als Splitter des allgemeinen Persönlichkeitsrecht ansieht, für welches der BGH eine vermögensrechtliche Stellung der betreffenden Person anerkannt hat.

Recht an Daten durch Schutzgesetz?

Kann man vielleicht ein Recht an Daten aus den strafrechtlichen Normen der §§ 202a-c, 303a StGB herleiten, in dem man diese als Schutzgesetz im Sinne des § 823 Abs. 2 ansieht? Die Normen stellen unter bestimmten Umständen das Ausspähen von geschützten Daten sowie die Beeinträchtigung von deren Integrität von Daten unter Strafe. Zwar ist unter den Juristen anerkannt, dass deren Verletzung auch zivilrechtliche Ansprüche (z.B. Schadensersatz, Unterlassung) auslöst, die der Verletzte durchsetzen kann. Daraus allein folgt jedoch keine ausschließlichkeitsrechtliche Zuweisung von Daten im Sinne eines Eigentums. Im Rahmen der wettbewerbsrechtlichen Zuordnung von Daten wird ein zivilrechtlicher und strafrechtlicher Schutz über das Gesetz gegen Wettbewerbsbeschränkungen (§§ 17, 18 UWG) herbeigeführt. Diese Regelungen führen aber wiederum nicht zu einem eigentumsähnlichen Schutz an Daten, sondern nur zu einem Abwehrrecht hinsichtlich der unbefugten Mitteilung von Betriebs- oder Geschäftsgeheimnissen, die möglicherweise in den Daten enthalten sind.

Urheberrechtlicher Schutz

Ein urheberrechtlicher Schutz von Big Data gemäß § 4 Abs. 2 UrhG als Datenbank setzt voraus, dass ein Sammelwerk, welches eine auf Grund der Auswahl oder Anordnung der Elemente eine persönliche geistige Schöpfung darstellt, vorliegt. Eine erforderliche Schöpfung ist bei einer reinen Datenansammlung in der Regel aber gerade nicht gegeben, sodass ein urheberrechtlicher Schutz hier ausscheidet. In Betracht könnte noch ein Schutz des Datenbankherstellers kommen. Eine Datenbank ist nach § 87 a UrhG eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mithilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Big Data ist oftmals

gerade nicht im herkömmlichen Sinne nach einer bestimmten Weise geordnet. Abzugrenzen ist daher das Vorliegen einer Datenbank vom Vorliegen eines bloßen Datenhaufens, der mangels Vorliegen einer systematischen oder methodischen Ordnung sowie Fehlens eines Zugangs mit elektronischen Mitteln nicht dem Schutz unterfallen kann. Nach Erwägungsgrund 21 der Datenbankrichtlinie (RL 96/9/EG) ist es nicht erforderlich, dass eine physische Speicherung der Daten in geordneter Weise erfolgt. Maßgeblich ist allein, ob auf der Zugriffsebene der Nutzer die einzelnen Elemente systematisch und methodisch recherchieren kann. Das ungeordnete Einspeisen in den physischen Speicher ist insofern für Datenbanken typisch. Ausreichend ist damit, wenn erst das Abfragesystem die schutzbegründende systematische oder methodische Ordnung herbeiführt. Letztlich kann aber auch das Datenbankherstellerrecht nicht zu einem Ausschließlichkeitsrecht am Datum selbst führen, sodass keine eigentumsähnliche Rechtseinräumung folgen kann. Im Ergebnis ist daher festzuhalten, dass nach herrschender Auffassung nach geltendem Recht weder ein Eigentum an Daten besteht noch ein dem Eigentum vergleichbares Recht mit absoluter Wirkung an selbigen. Es werden dem Berechtigten zwar Abwehrrechte gegeben, diese führen jedoch mangels Zuweisung eines umfassenden Nutzungsrechts nicht zu einem dem Eigentum gleichstehenden Schutz.

Zuweisung der Daten

Aufgrund der fehlenden Möglichkeit der eigentumsrechtlichen Zuweisung bleibt die Frage nach der Zuweisung der Daten zu beantworten. Insbesondere Unternehmen haben ein Interesse daran, dass die Zuweisung von Daten zu demjenigen erfolgt, der in deren Herstellung investiert, unabhängig von einem Personenbezug. Die Zuweisungsentscheidung wird letztlich aus wirtschaftlicher Sicht getroffen. Streitig ist dabei aber, auf welche wirtschaftlichen Gesichtspunkte in diesem Zusammenhang abzustellen ist. Nachfolgend wird exemplarisch auf verschiedene Konstellationen einer problematischen Zuordnung eingegangen. Die Frage der Zuweisung der Daten stellt sich z.B., wenn der Hersteller Daten auswerten möchte, die im Rahmen der Nutzung durch den Kunden entstehen. Solche Daten sind beispielsweise bei der Nutzung eines Automobils generierte Messdaten. Teilweise wird vertreten, dass diese Daten dem Betreiber der Maschine, also dem Halter zuzurechnen sind, da der Betrieb der für die Entstehung der Daten maßgebliche Skripturakt ist. Die Sicht der Hersteller geht dahin, dass ihnen die Daten aufgrund ihrer Verantwortlichkeit für die Herstellungs- und Entwicklungskosten, der die Daten erfassenden Technologie, zuzuweisen sind. Dabei wird bei letzterer Auffassung die Zuordnung noch komplizierter, wenn mehrere Unternehmen an der Erstellung der Technologie beteiligt sind. Bei der Analyse von Big Data ist die Zuweisung ebenfalls nicht einfach zu treffen. Problematisch ist diese insbesondere, wenn Daten ausgewertet werden, die vom Dienstleister erhoben worden sind (z.B. bei Smart-Analytics-Verfahren). Nach Ansicht der Dienstleister sind die Daten ihnen zuzuordnen, weil sie Träger der wirtschaftlichen Aufwände sind und sie auch als Datenbankhersteller anzusehen sind. Die Zuweisung bei Speicherung von Daten in der Cloud ist wie oben zu behandeln und in diesem Zusammenhang nach der wirtschaftlichen Zuweisung zu fragen. Allerdings enthalten die Verträge der Cloud-Anbieter in aller Regel Dateneigentumsklauseln, die dem Cloud-Nutzer die Rechte an den Daten zuweisen.

Vertragliche Gestaltung und Fazit

Wie beschrieben, besteht aufgrund der Schwierigkeit, eine eindeutige Zuordnung von Daten nach geltender Rechtslage vorzunehmen, eine große Notwendigkeit für vertragliche Regelungen. Zwar wird durch eine solche schuldrechtliche Vereinbarung keine dingliche und damit eigentumsähnliche Wirkung erzeugt, aber der Nutzungsumfang kann beschränkt werden und durch technische Vorkehrungen, die eine nicht berechtigte Nutzung verhindern, kann eine quasi-dingliche Wirkung erzeugt werden. Nach geltendem Recht besteht kein umfassendes dingliches Recht an Daten, das einem Eigentum an Sachen vergleichbar wäre. Zwar kann man häufig eine Güterzuweisung vornehmen, jedoch muss derjenige, welcher ein Recht an den Daten geltend machen muss, aus einem Flickenteppich von Regelungen sich ein Abwehrrecht heraussuchen, das auf seinen Fall passt, und es ist nicht gesichert, dass der konkrete Fall abgedeckt ist. In Anbetracht der weitreichenden Bedeutung von Daten erscheint eine dingliche Zuweisung überlegenswert. Dafür spricht, dass dadurch das Gesetz die Grundlage für eine geordnete und eine gerechte Verteilung des Nutzens von Big Data Anwendungen bilden würde. Andere Stimmen gehen davon aus, dass die bisher bestehende Gesetzeslage ausreichend ist. Die geltende Rechtslage birgt jedenfalls eine erhöhte Streitgefahr, da beispielsweise im Rahmen von Produktionsabläufen in der Smart Factory gerade verschiedene potenzielle Rechtsinhaber in Frage kommen. Letztlich müsste in einem solchen Gesetz der genaue Umfang der dinglichen Zuweisung geklärt werden, um eine die Arbeit der Praxis tatsächlich erleichternde Regelung zu schaffen. ■

Rechtsanwalt Dr. Thomas Thalhofer ist auf Vertragsgestaltung und rechtliche Projektberatung bei komplexen IT- Projekten sowie auf Unternehmenstransaktionen im Technologiebereich spezialisiert.

Bild: Noerr LLP

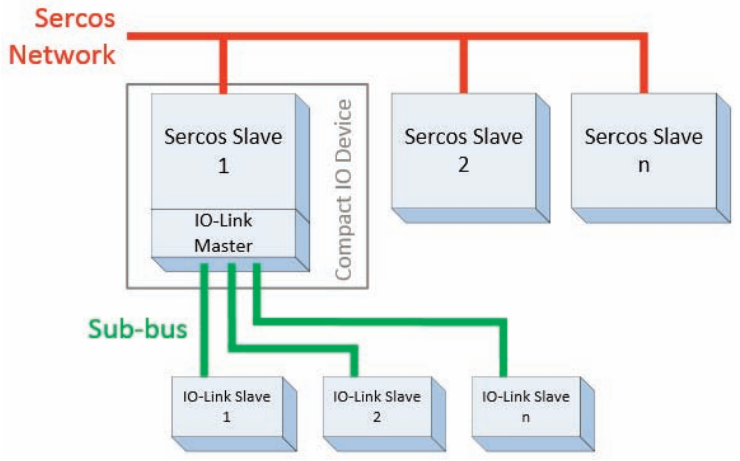
Autor: *Dr. Thomas Thalhofer,*
Partner,
Noerr LLP
www.noerr.com

Durchgängige Vernetzung

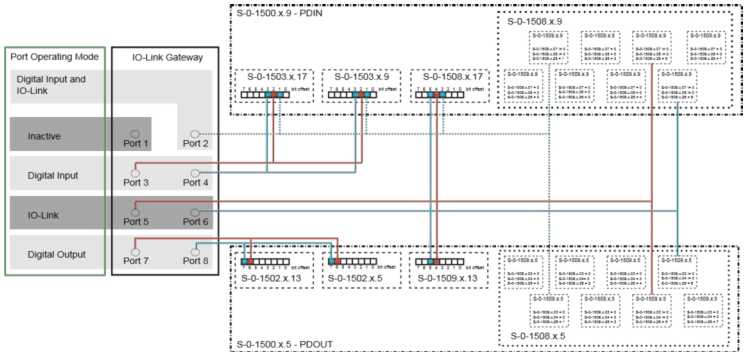
Kombination von IO-Link und Sercos

Bilder: Sercos International e.V.

Der Trend der notwendigen vertikalen Kommunikation erfasst zukünftig mehr und mehr auch die unterste Ebene im Feld. Dort benötigen die intelligent werdenden Sensoren und Aktoren eine Kommunikationsanbindung, die Vorteile der neuen Eigenschaften nach oben weiterreichen kann. Die Punkt-zu-Punkt-Verbindung mit IO-Link bietet sich hierzu an.



Architekturen des Sub-Busses IO-Link: Beispielhafte Topologien mit einer entsprechenden Gateway-Funktion – links ein Standalaone-Gerät, rechts als Teil eines modularen Geräts.



Mapping der zyklischen Datenübertragung

Heutzutage binär oder analog angeschlossene Geräte, wie beispielsweise Temperaturfühler oder Signalleuchten, werden zukünftig mit einer steigenden Intelligenz ausgestattet und erlauben dadurch, Mehrwerte z.B. durch eine umfangreichere Informationsbereitstellung darzustellen. Beispielsweise muss bei intelligenten Näherungsschaltern der Entfernungsbereich parametriert werden. Auch intelligente Temperaturfühler erlauben die Einstellung von Grenzwertüberwachungen und bieten mehrstufige Meldeschwellen bei unterschiedlichen Temperaturen. Um Anwendungen gemäß Industrie 4.0 und dem industriellen IoT zu realisieren, ist eine durchgängige Kommunikation bis zum Sensor und Aktor notwendig. Das kann durch Kombination von IO-Link und Sercos realisiert werden. Die Anforderungen für eine solche Schnittstelle sind u.a.:

- Transport komplexerer Informationen im Gegensatz zu heutigen binären bzw. analogen Geräten
- Integration von Geräten mit dezentraler Intelligenz. Die dezentrale Intelligenz ermöglicht es, eine Vorverarbeitungen nahe am Prozess zu realisieren
- Parametrierungen und Diagnosefunktionen
- Einfach und preiswert: Die Busanschaltung ist einfacher und günstiger zu realisieren als eine Real-Time-Ethernet-Busanschaltung.
- Feldtauglichkeit und Verbindungstechnik für sehr kleine Sensoren
- Störungsfestigkeit und Robustheit im Gegensatz zu analogen Anschaltungen

Aus diesen Forderungen leiten sich typischerweise sogenannte Sub-Busse ab, die topologisch und funktionell unterhalb der heutigen, etablierten Feldbusse anzusehen sind. Hierdurch ergibt sich ein bedeutender Vorteil für die Sensorhersteller, da diese einen Sensor nur mit einer einzigen (digitalen) Schnittstelle anbieten müssen und die Integration in den heterogenen Automationsarchitekturen mittels Gateways erfolgt.

Kernfeatures von IO-Link

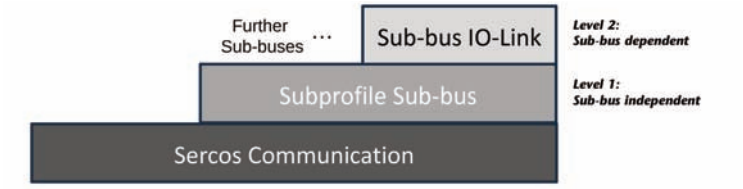
Neben den bekannten Feldbus-Kommunikationssystemen AS-i und CAN ist aktuell IO-Link gemäß IEC61131-9 derjenige Standard, der von vielen Sensorherstellern für Neuentwicklungen verwendet wird. IO-Link ist für die Hersteller von Sensoren und Aktoren deshalb interessant, da es Gateway-Lösungen für nahezu alle aktuellen Real-Time-Ethernet-Protokolle gibt, um IO-Link-Geräte zu integrieren.

Eigenschaften

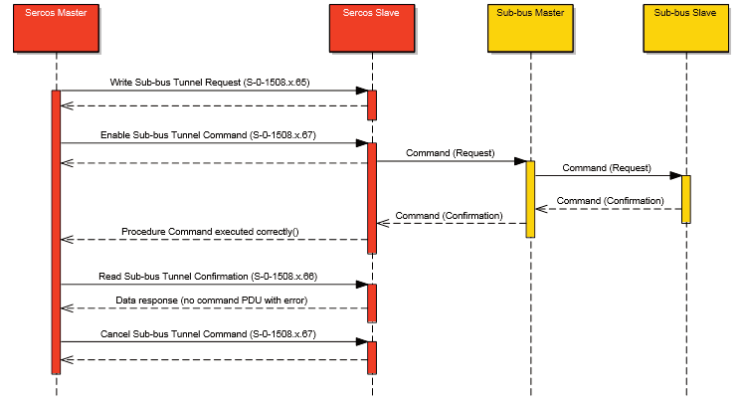
Die besonderen Eigenschaften von IO-Link sind:

- Kompatibilität zu bisherigen Dreidrahtsensoren
- Niedrige Anschalt- bzw. Entwicklungskosten
- Ausrichtung auf IP65/67, das heißt schaltschranklose, dezentrale Verkabelung
- Ausreichende Performance für Sensorik/Aktorik

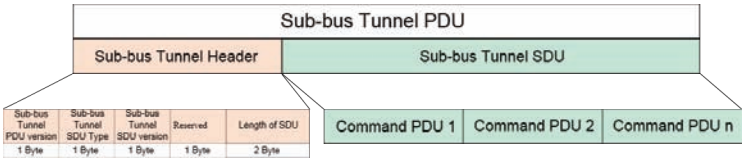
Bilder: Sercos International e.V.



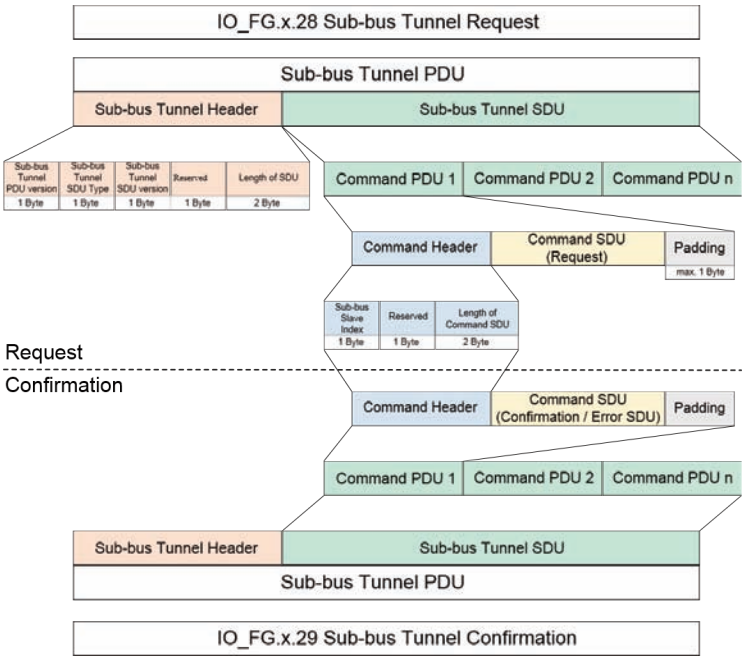
Zwei Schichten der Sub-Bus-Integration



Protokollablauf der azyklischen Übertragung



Protokollablauf der azyklischen Übertragung



Telegrammaufbau von Anforderungs- und Antworttelegrammen (Request/Confirmation)

- Großer Adressraum um die Parameter komplexerer Geräte abzubilden
- Einfacher Gerätetausch (toolfreier Tausch)
- Einfache Konfiguration

Integration von IO-Link in Sercos

Für Sercos wurde eine allgemeingültige Spezifikation zur Integration von IO-Link-Geräten in Sercos spezifiziert. Diese beinhaltet:

- Funktionalität im Betrieb
- Zyklische Datenübertragung
- Azyklische Datenübertragung
- Automatische Neuparametrierung nach einem Gerätetausch des Gateways und einzelner Devices
- Funktionalität während des Anlaufs
- Geräteidentifikation aller IO-Link-Devices
- koordinierter Bushochlauf zum Sercos
- Funktionalität der Konfiguration
- Port-Konfiguration der IO-Link-Masterports
- Konfiguration der IO-Link-Devices
- Funktionalität im Diagnosefall
- Ersatzwertverhalten im Fehlerfall
- Diagnose der IO-Link-Devices und der IO-Link-Masterports

Zyklische Übertragung

Die Spezifikation der zyklischen Übertragung beinhaltet die folgenden Funktionalitäten:

- Das Mapping der zyklischen Daten erfolgt transparent in die zyklischen Daten von Sercos
- Ein Qualifier signalisiert die Gültigkeit der Daten
- Das Ersatzwertverhalten im Fehlerfall spezifiziert, wie bei Kommunikationsfehlern reagiert wird

Azyklische Übertragung

Die Übertragung azyklischer Daten von IO-Link ist mit einem einfachen Sub-Bus-Protokoll im Sercos abgebildet, es kann auf jeden IO-Link-Parameter zugegriffen werden. Es wird auf eine Zweiebenen-Transportschicht aufgebaut:

- Schicht 1 ist ein Sub-Bus-unabhängiger Transport
- Schicht 2 ist der Sub-Bus-abhängige Protokollinhalt

Sub-Bus-unabhängiger Transport

Mithilfe eines Sub-Bus-Tunnelprotokolls werden die Parameteranfragen in Form eines Request/Confirmation-Verfahrens abgewickelt. Daneben sind auch die entsprechenden Fehlerbehandlungen, Anfrageabbrüche und Timeout-Behandlungen im Sub-Bus-Tunnelprotokoll spezifiziert. Durch den Aufbau eines Anfragetelegramms (Sub-Bus-Tunnel PDU) sind Einzel als auch Summenanfragen möglich (mehrere Command PDUs), um die Kommunikation zu optimieren. Der Ablauf einer Parameterübertragung wird durch Telegramme (Command PDUs) abgebildet. Dieser verallgemeinerte Sub-Bus-Tunnel gilt grundsätzlich auch für weitere zu spezifizierende Sub-Bus-Tunnelprotokolle.

IO-Link-abhängiger Transport

Die zweite Schicht setzt auf der Ebene Command SDU auf und beinhaltet die weitergehenden, IO-Link-spezifischen Protokollanteile. Innerhalb der jeweiligen IO-Link-Device-Data-Object-Datenfelder werden die IO-Link-Parameterdateninhalte zum/vom IO-Link-Device übertragen, Fehler der Datenübertragung sowohl des IO-Link-Masters als auch der IO-Link-Devices werden über die entsprechenden Error-Code-Datenfelder gemeldet.

Geräteidentifikation und Diagnose

Beim Anlauf werden die Identifikationsdaten aller IO-Link-Devices ausgelesen und in einem eigenen Sercos-Parameter abgelegt. Hierdurch kann eine einfache Überprüfung, z.B. durch ein SPS-Programm erfolgen. Für jeden Port ist eine eigene Portdiagnose auslesbar, wie z.B. die Port-Betriebsart, den Diagnosestatus mit Statuscode, die Geräteidentifikationsdaten (VendorID, DeviceID), Data-Storage-Fehlercodes oder die IO-Link-Revision. Zudem ist eine Gerätediagnose über die bekannten Sercos-Diagnosemechanismen vorhanden. Hierbei werden die bei IO-Link spezifizierten Diagnosecodes und Diagnoseklassen eins zu eins in Sercos abgebildet, dadurch ergibt sich automatisch eine Erweiterung, wenn bei IO-Link neue Diagnosecodes spezifiziert werden.

Gerätetausch

Der Data-Storage-Mechanismus der IO-Link-Devices erlaubt es, alle Parameterdaten eines IO-Link-Devices automatisiert im IO-Link-Gateway zu sichern. Wenn ein IO-Link-Device ausfällt, muss der Anwender das Gerät lediglich durch einen baugleichen Slave ersetzen. Das IO-Link-Gateway erkennt den neuen Teilnehmer automatisch und führt die Parametrierung beim folgenden Hochlauf aus. Es ist keine Parametrierung des IO-Link-Slaves notwendig. Auch bei dem Ausfall des Gateways ist ein Gerätetausch ohne Neukonfiguration möglich: Der Sercos-Master kann die Konfiguration des Gateways sichern, den Gerätetausch automatisiert erkennen und eigenständig die Neuparametrierung durchführen. Eine Neuparametrierung des Gateways bzw. der IO-Link-Devices erfolgt im normalen Sercos-Hochlauf. Es ist kein Eingriff durch den Endanwender erforderlich. Das Deaktivieren dieser Mechanismen ist ebenfalls möglich.

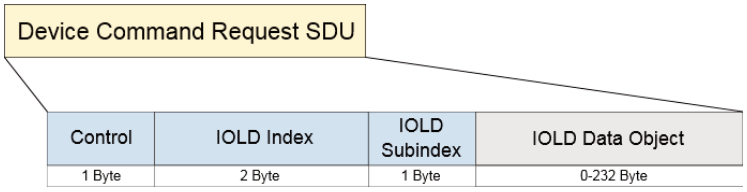
Funktionen aus der SPS heraus

Es sind im Steuerungssystem MLC von Bosch Rexroth mithilfe von Funktionsbausteinen beispielsweise folgende SPS-Funktionen implementiert:

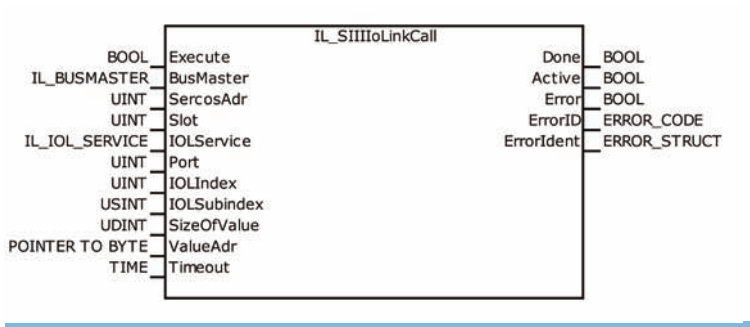
- IOL_CALL quasi als Mutter aller IO-Link-Bausteine
- Geräteidentifikation
- Device-Diagnose, Port-Diagnose
- Kommandoabarbeitung
- Port-Konfiguration
- Backup/Restore eines IO-Link-Devices

Der Nutzen für den Anwender ist, dass er sich nicht mit dem Tunnelprotokoll, sondern nur mit den IO-Link-Parametern (Index, Subindex) auskennen muss. Mit den Funktionsbausteinen können aus dem SPS-Programm z.B. Parameteränderungen, Device-Diagnosen, Kommandoabarbeitungen oder Port-Diagnosen durchgeführt werden. In Summe sind 15 Funktionsbausteine rund um die Integration von IO-Link in Sercos implementiert, sodass ein großer Umfang an Funktionalität zur Verfügung steht.

Bild: Sercos International e.V.



Device Command Request SDU



FB IO-Link Call

Zusammenfassung

Die Spezifikation der Integration von Sub-Bussen in Sercos bietet sehr viele komfortable Möglichkeiten. Die Zweistufigkeit der Spezifikation erlaubt es auf einfache Weise, neben IO-Link noch weitere Sub-Busse zu integrieren. Bei einem Wechsel des Sub-Busses bleiben die Sercos-Mechanismen für den Anwender identisch. Auch in der Applikation auf der Steuerung ändert sich für den Anwender wenig, da die Funktionsbausteine für unterschiedliche Sub-Busse eine identische Schnittstelle haben. Die Basis hierfür sind Standard-Sercos-Mechanismen, die jede Sercos-Steuerung heute beherrscht. Die Spezifikation der Integration von IO-Link beinhaltet umfangreiche Funktionen, die alle notwendigen Anwendungsfälle komfortabel und anwendergerecht abdecken. Hierbei wurde insbesondere sowohl großer Wert auf die Diagnose, Parametrierung der IO-Link-Masterports im Gateway gelegt als auf das Handling bei einem Tausch des Gateways. Diese Eigenschaften zeichnen die Integration in Sercos gegenüber anderen Feldbussen aus. Erste Implementierungen sind vorhanden und werden in Prototypanwendungen bereits angewandt. ■

Interview mit dem Sick-Vorstandsvorsitzenden Dr. Robert Bauer

„Die Marktdurchdringung von IO-Link wird voranschreiten“

Bild: Sick AG

Wie weit hat IO-Link schon Einzug in die Kommunikation auf der Feldebene gehalten? Und welche Rolle kann der Sensor/Aktor-Standard in den Szenarien von Industrie 4.0 übernehmen? Über diese Fragen hat sich Dr. Robert Bauer mit dem INDUSTRIAL COMMUNICATION JOURNAL unterhalten. Der Vorstandsvorsitzende des Sensorherstellers Sick ist überzeugt, dass IO-Link kontinuierlich ein breites Anwendungsspektrum in der Automatisierung erobert.

Die IO-Link-Gemeinschaft ist vom großen Potenzial des Sensor/Aktor-Kommunikationsstandards für moderne Automatisierungskonzepte überzeugt. Spiegelt sich dieser Anspruch heute bereits in der Praxis wider, Herr Dr. Bauer?
Dr. Robert Bauer: *Der Bekanntheitsgrad von IO-Link im Markt ist schon sehr zufriedenstellend, schließlich sind von Seite der Sensoranbieter und Komponentenhersteller auch bereits eine Vielzahl an Produkten verfügbar. In der Folge gibt es mittlerweile verschiedene Anwendungen, in denen sich IO-Link durchgesetzt hat. Nämlich dort, wo sich die Möglichkeiten der bidirektionalen Kommunikation besonders gut nutzen lassen und wo Parameter auf die Sensoren oder Feldgeräte zu laden sind.*

> *„IO-Link bietet viele Möglichkeiten und der daraus resultierende Effizienzgewinn lässt sich relativ schnell realisieren.“*
> *Dr. Robert Bauer, Sick*

Es lässt sich feststellen, dass IO-Link an Fahrt aufnimmt?
Dr. Bauer: *Ja, die Anwendung des Standards nimmt zu, was man gut an den Zahlen der verbauten Kommunikationsknoten ablesen kann, die regelmäßig veröffentlicht werden. Aber leider gibt es noch ein paar SPS-Hersteller, die keine standardmäßig integrierte Schnittstelle anbieten.*

Bedeutet das, der große Erfolg von IO-Link steht noch bevor?
Dr. Bauer: *Nun ja, es ist sicherlich ein kontinuierlicher Einführungsprozess. Zudem sind die Lebenszyklen im Maschinen- und Anlagenbau recht lang. Doch wenn unsere Kunden eine neue Maschinengeneration einführen, dann wird die Grundstruktur heute schon oft auf den Einsatz von IO-Link ausgerichtet. Der weitere Erfolg hängt aus meiner Sicht aber von entsprechenden Tools auf SPS-Ebene ab. Dort wird eine zusätzliche Softwareumgebung nur für IO-Link vom Anwender nicht akzeptiert. Nach und nach, davon gehe ich stark aus, werden diese Hindernisse in der Softwarewelt aber abgebaut werden und die Durchdringung von IO-Link voranschreiten.*

Sehen Sie in dem Standard denn eine reine Ergänzung im Spektrum der industriellen Kommunikation für die Sensor/Aktor-Ebene oder kann IO-Link zukünftig auch einen Teil der klassischen Feldbusaufgaben übernehmen?
Dr. Bauer: *Meiner Ansicht nach ist die Arbeitsteilung ziemlich klar verteilt: IO-Link deckt als Punkt-zu-Punkt-Verbindung die unterste Ebene ab, während Feldbusse und Industrial-Ethernetprotokolle entsprechende Bandbreiten und Zykluszeiten in der Kommunikation oberhalb davon sicherstellen. Dieses Zusammenspiel funktioniert ausgezeichnet und wird sich technisch nicht mehr viel verändern. Aber natürlich bleiben die Kosten pro Knoten ein wichtiger Aspekt. Sie sind bei IO-Link sehr günstig. Bei Ethernetstandards muss der Kunde hingegen eher prüfen, ob sich dieser Mehraufwand für die zusätzliche Funktionalität auch wirklich lohnt.*

Welches Potenzial schreiben Sie IO-Link als Enabler von Industrie 4.0 und der durchgängig vernetzten Fabrik zu?
Dr. Bauer: *IO-Link lässt sich in Bezug auf Industrie 4.0 ganz klar dem Effizienzgewinn zuordnen. Die einzige Schnittstelle zum Sensor war bisher der Schaltausgang und damit unidirektional. Die über IO-Link mögliche bidirektionale Kommunikation bringt*

viele Vorteile. Einfach gesagt: Der Teil von Industrie 4.0, der in Richtung vorausschauender Wartungslösungen geht, ist eins zu eins mit IO-Link umsetzbar. Auch ein schneller Austausch von Geräten im Servicefall ist kein Problem mehr – es muss per Software nur der jeweilige Parametersatz geladen werden. Dazu kommen zusätzliche smarte Funktionen, indem man Metadaten wie z.B. Zeitverhältnisse aus dem Sensor erfasst, die dem Anwender Auskunft über die Qualität seines Produktionsflusses geben.

IO-Link bietet also eine Basis für moderne wie zukünftige Datenerfassungs- und Analysekonzepte?

Dr. Bauer: *Hier bietet IO-Link in der Tat viele Möglichkeiten und der daraus resultierende Effizienzgewinn – das ist das Schöne daran – lässt sich relativ schnell realisieren. Man muss hier nicht weit in die Zukunft planen.*

> *„Der weitere Erfolg von IO-Link hängt aus meiner Sicht von entsprechenden Tools auf SPS-Ebene ab.“*
> *Dr. Robert Bauer, Sick*

Lässt sich denn IO-Link in Hinsicht auf das Zukunftspotenzial noch verbessern?

Dr. Bauer: *Die Grundausrichtung ist in Bezug auf die standardisierte Hardware heute schon gegeben. Der nächste große Schritt in einer einfachen Softwarehandhabung auf SPS-Ebene. Dafür werden – und das ist aktuell auch in der IO-Link-Community in Arbeit – einheitliche Masterprofile benötigt, um durch einfache und standardisierte Arbeitsweisen die Profitabilitätsschwelle weiter zu senken.*

Wie kriegt man die SPS-Hersteller, die sich bislang noch weigern, dazu, IO-Link standardmäßig zu integrieren und sich zu öffnen?

Dr. Bauer: *Ursprünglich ist IO-Link ja eine deutsche Erfindung und so zeichnet sich auch regional ab, welche Steuerungsanbieter für IO-Link noch nicht empfänglich sind. Im Prinzip kann nur die Marktmacht der Endanwender etwas bewirken. Hierzulande ist IO-Link durch den hohen Durchdringungsgrad der deutschen Automatisierungstechnik bereits gut positioniert. Das ist aber offensichtlich in einigen anderen Regionen noch nicht gegeben.*

> *„IO-Link ist im Hause Sick längst Standard – selbst bei relativ einfachen Geräten wie induktiven Sensoren.“*
> *Dr. Robert Bauer, Sick*

Es hilft ja immer, wenn man große Anwender auf seiner Seite hat. Wie steht es diesbezüglich um die Automobilindustrie? Kann sie nicht entsprechenden Druck ausüben?

Dr. Bauer: *Möglicherweise könnte sie das außerhalb von Deutschland. Aber die Automobilisten legen ihren Hauptfokus hinsichtlich der Kommunikation eher auf die Industrial-Ethernet-ebene. Die deutsche Automobilindustrie hat jedenfalls keinen Grund, um Druck auszuüben. Wenn sie den Sensor/Aktor-Standard einsetzen will, dann kann sie das ja heute schon. Insgesamt sind in Deutschland Aufmerksamkeit und Marktbedürfnis für IO-Link sehr wohl schon vorhanden. Das merkt man schnell, wenn man ein neues Produkt ohne IO-Link herausbringt. Denn dann fragt der Markt sofort einen IO-Link-Knoten nach. Entsprechend haben wir auch inzwischen alle betreffenden Produkte mit einer entsprechenden Schnittstelle ausgerüstet.*

Sick hat IO-Link als Gründungsmitglied maßgeblich mit getrieben. Welchen Stellenwert hat der Standard heute in Ihrem Portfolio?

Dr. Bauer: *Wir haben die IO-Link-Funktionalität in jede neu entwickelte Sensorgeneration aufgenommen und ganz konkret auch in den ASICs integriert, um zusätzliche Kosten auf ein Minimum zu reduzieren. Damit ist IO-Link im Hause Sick und der daraus entstehende Mehrwert für unsere Kunden längst Standard – selbst bei relativ einfachen Geräten wie induktiven Sensoren.*

Gibt es denn überhaupt Bereiche in Ihrem Programm, in denen IO-Link keinen Mehrwert bietet?

Dr. Bauer: *Der Mehrwert von IO-Link endet dort, wo die Datenrate sehr hoch ist. Das ist z.B. in einigen Anwendungen der industriellen Bildverarbeitung der Fall. Dort übernehmen dann oft Ethernetschnittstellen die Kommunikation nach oben. Bei vielen der smarten Vision-Sensoren, die quasi nur noch ein Ergebnis übertragen, lässt sich IO-Link hingegen gut einsetzen.*

Welche Erwartungen haben Sie in den IO-Link-Markt? Können Sie einen Ausblick geben?

Dr. Bauer: *Wir glauben, dass IO-Link ein wichtiger Standard für die Zukunft ist und gehen von einer kontinuierlichen Weiterentwicklung des Marktes und einem kontinuierlichen Kompetenzaufbau auf Anwenderseite aus. Große disruptive Effekte erwarten wir hingegen nicht.*

Herr Dr. Bauer, vielen Dank für das Gespräch. ■

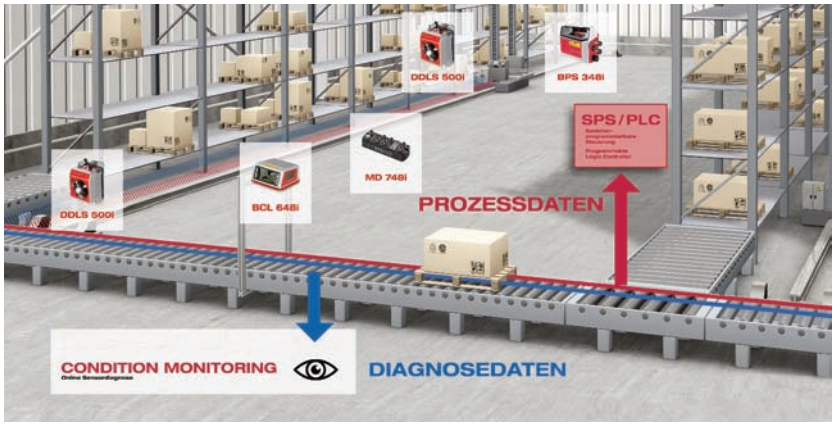


Bild: Leuze Electronic GmbH+Co.KG

Zukunftsfähige Anbindung von Sensoren

Parallele Datenkanäle

Damit ihre Produkte als zukunftsfähig gelten, müssen sich Automatisierer den Anforderungen nach paralleler Verarbeitung von Prozess- und Diagnosedaten stellen. IO-Link als standardisierte Schnittstelle für den letzten Meter im Feld spielt hierbei eine wichtige Rolle.

Hersteller von Sensoren erhalten verstärkt Anfragen aus der Industrie nach zusätzlichen, über die bisherigen Standardsensormeldungen hinausgehende Daten, die im Sinne von Predictive Maintainance, Anlagenverfügbarkeit und Funktionssicherheit auch von außen abrufbar sind.

Erster Anfang ist gemacht

Mit zusätzlichen Warnmeldungen, z.B. bei der Verschmutzung eines Sensors, wurde ein erster Anfang gemacht. Diese entwickelten sich schnell in Richtung eines Mehr an Parametriermöglichkeiten der Sensoren über eine einfache Schnittstelle weiter. Gespräche und Diskussionen in Gremien von Sensorexperten und Anwendern führten schon bald zur Spezifikation der einheitlichen IO-Link-Schnittstelle, die selbst bei einfachen, binär schaltenden Sensoren wirtschaftlich ist. Auch die Vision und Diskussion über Industrie 4.0 verstärkte das Interesse für IO-Link als standardisierte Schnittstelle für Sensoren, um die von ihnen ausgegebenen Daten in die Vernetzung verschiedener Ebenen einbinden zu können. Zu erwähnen ist hier besonders die Variante als Dual-Channel mit einem Kanal für die digitalisierten Schaltsignale für den Prozessbetrieb und parallel einen zweiten Kanal für den Zugriff auf Parameterdaten und Meldungen der Sensoren. Bei komplexeren Geräten und Sensoren hat sich bereits der Feldbuszugang durchgesetzt, der auf diesem Weg den Datenzugriff möglich macht. In der Vergangenheit galt das Hauptinteresse überwiegend prozessrelevanten Daten, um die Anlage oder den Prozessschritt bestmöglich steuern zu können. Elementare Daten wie beispielsweise Warn- oder Alarmmeldungen wurden über denselben Datenkanal an die Steuerungsebene weitergegeben. Seit die Schnittstellen zu den Steuerungen vermehrt Ethernet-basierend und damit leistungsfähig genug sind, zwei Datenkanäle gleichzeitig zu bedienen, eröffnen sich völlig neue Möglichkeiten – und genau diese sind es, die für die vernetzte Welt der Industrie 4.0 erforderlich sind, um die Daten an unterschiedliche Ziele und Ebenen zu bringen.

Zweiter Datenkanal ist verfügbar

Die dargestellten Entwicklungen ermöglichen es nun, zum klassischen Prozess-Datenkanal einen weiteren naheliegenden Datenkanal, ausschließlich für Zustandsinformation, Umgebungswarnungen und weitere Daten aus den Sensoren, die zum stillstandfreien Betrieb hilfreich sind, zur Verfügung zu stellen. Leuze Electronic verfolgt diese Entwicklung und hat schon früh auf den direkten Feldbuszugang zu komplexen Identgeräten und messenden Sensoren gesetzt. „Deshalb kommt auch die Einbeziehung der schaltenden Sensoren in diese Entwicklung für uns nicht überraschend“, so Dieter Eßlinger, Produkt Marketing Manager bei Leuze Electronic. „Wir bieten dem Anwender entweder über IO-Link im COM-2-Mode und schnellem Schaltausgang sowie über unsere Sensorstudio-Software oder andere IO-Link-Master-Tools mit den geeigneten IODDs oder per integriertem Webserver die erforderlichen beiden Kanäle, um Prozess- und Zustandsdaten parallel zu verarbeiten.“ Viele Leuze-Sensoren bieten bereits heute vom Kunden benötigte Daten an. „Wir gehen aber davon aus, dass durch die vermehrte Vernetzung weitere Anforderungen auf uns zukommen, die gleichzeitig die Chance für völlig neue Geschäftsmodelle bieten“, so CEO Ulrich Balbach. Die Basis hierfür, in Form von zwei Datenkanälen sei vorhanden – durch Dual-Channel IO-Link bei einfachen Sensoren oder durch eine integrierte Feldbus-Schnittstelle mit zusätzlichem TCP/IP-Kanal. ■

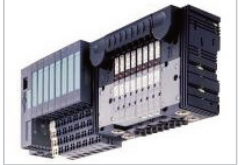
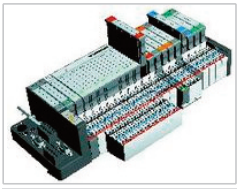
E/A-Systeme für den Ex-Bereich

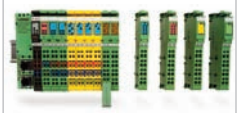
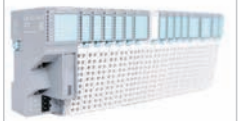
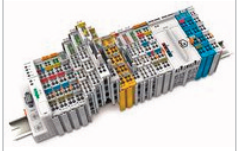
Während der Schutzgrad eines Gehäuses den Fremdkörper- und Berührungsschutz sowie den Schutz gegen das Eindringen von Wasser festlegt, dient die ATEX-Richtlinie zur Kennzeichnung explosionsgeschützter Betriebsmittel wie auch den E/A-Systemen.

Im Vergleich zum IP-Code, der mit zwei Kennziffern auskommt, ist die ATEX-Kennzeichnung wesentlich komplexer. Dadurch, dass die E/A-Einheiten vermehrt dezentral installiert werden, sind sie auch den unterschiedlichen Gefahren von explosionsfähigen Atmosphären ausgesetzt. Die ATEX-Kennzeichnung teilt brennbare Stoffe wie Gase, Nebel, Dämpfe sowie Stäube in Zonen ihres Auftretens ein. Dadurch wird auch festgelegt, ob ein Betriebsmittel in der betreffenden Zone eingesetzt werden kann oder nicht. Eine weitere Einsatzfähigkeit wird über Explosionsgruppen und Temperaturklassen beschrieben. Schließlich geben Zündschutzarten Auskunft darüber, welche konstruktiven Maßnahmen den Einsatz in bestimmten explosionsgefährdeten Bereichen erlauben. Alle diese Eigenschaften münden in einer Kennzeichnung, die durch Richtlinien beschrieben wird. Aktuell wurde die Richtlinie 94/9/EG durch die Richtlinie 2014/34/EU ersetzt, die seit dem 20. April 2016 gilt. Es fanden jedoch keine grundlegenden Veränderungen statt und die unter ATEX 94/9/EU ausgestellten Bescheinigungen behalten ihre Gültigkeit. *(ghl)* ■

Anbieter	
Ort	
Telefon	
Internet-Adresse	
Produktname	
Max. Anzahl E/A-Stationen im Gesamtsystem	
Ex-Schutz (Buskoppler bzw. E/A-Einheiten)	
Max. dig. E/A pro Buskoppler bzw. Remote E/A	
Max. an. E/A pro Buskoppler bzw. Remote E/A	
Statusanzeige Diagnoseinformationen	
Program. Ethernet-Buskopplers/Feldbus-Contr.	
Besonderheiten des Buskopplers	
Industrial Ethernet-Kommunikationsprotokolle	
Weitere Industrial Ethernet Protokolle	
Feldbus-Kommunikationsprotokolle	
Besonderheiten/Optionen bei den Eingängen	
RS232 , TTY 20-mA-Current-Loop , S422/RS485	
Safety-Bussystem	

					
Anbieter	HIMA Paul Hildebrandt GmbH	ifm electronic gmbh	ifm electronic gmbh	Pepperl+Fuchs GmbH	Phoenix Contact Deutschland GmbH
Ort	Brühl	Essen	Essen	Mannheim	Blomberg
Telefon	06202/ 709-405	0800-1616164	0800-1616164	0621/ 776-1215	05235/ 3-41713
Internet-Adresse	www.hima.de	www.ifm.com	www.ifm.com	www.pepperl-fuchs.com	www.phoenixcontact.com
Produktname	HIMatrix RIO	AC1402 Profinet AS-i Gateway	AC1422 EtherNet/IP AS-i Gateway	LB / FB Remote I/O	Fieldline
Max. Anzahl E/A-Stationen im Gesamtsystem	128			10-15 abhängig von gewünschter Reakt.	netzwerkspezifisch
Ex-Schutz (Buskoppler bzw. E/A-Einheiten)	ATEX Zone 2	—, ATEX 3D	—, ATEX 3D	Ex ia, Ex ib, Ex ic	Ex Zone 2
Max. dig. E/A pro Buskoppler bzw. Rem. E/A	20 / 16	496 / 496	496 / 496	184 / 184	256 / 256
Max. an. E/A pro Buskoppler bzw. Rem. E/A	8 / 4	248 / 248	248 / 248	80 / 80	64 / 64
Statusanzeige Diagnoseinformationen	Status, Kurzschluss, Überlast, Drahtbruch	Farbdisplay für Konfiguration, Status und Diagnose	Farbdisplay für Konfiguration, Status und Diagnose	LED, Status	Netzwerkstatus, Busstatus, Status, Kurzschluss, Überlast
Program. Ethernet-Buskoppler/Feldbus-Con.	IEC 61131-3 FUP, AS, ST, C-Code				
Besonderheiten des Buskopplers	integrierter Fast Ethernet Switch	Konfigurationsspeicher, Farbdisplay, WEB-Interface, flexibles Versorgungskonzept	Konfigurationsspeicher, Farbdisplay, WEB-Interface, flexibles Versorgungskonzept		integrierter 3 Port-Switch auf dem Buskoppler, digitale E/As onBoard
Industrial Ethernet-Kommunikationsprotok.	safeethernet	Profinet	EtherNet/IP	Modbus-TCP	EtherNet/IP, Modbus-TCP, Profinet
Weitere Industrial Ethernet Protokolle					
Feldbus-Kommunikationsprotokolle		AS-Interface	AS-Interface		Interb., Profibus-DP, DeviceNet, CANopen
Besonderheiten/Optionen bei Eingängen	Leitungsdiagnose, IEC 61508 SIL3, IEC 62061 SIL3, ISO 13849 PLe	LED Statusanzeige, Diagnoseinformationen, kurzschlussfeste Sensorversorgung	LED Statusanzeige, Diagnoseinformationen, kurzschlussfeste Sensorversorgung	Leitungsbruch, Leitungskurzschluss, NAMUR, Ex, Eingangsfilter	Signalzustand durch Leuchtdioden angezeigt, elektronischer Kurzschluss, und Überlastschutz
RS232, TTY 20-mA-Current-Loop, S422/RS485	-, -, -	-, -, -	-, -, -	-, -, ✓	-, -, -
Safety-Bussystem	safeethernet	AS-i Safety at Work	AS-i Safety at Work		

					
ABB Automation GmbH Mannheim 0621/ 381-4480 www.abb.de/controlsystems	Bartec GmbH Bad Mergentheim 07931/ 597-0 www.bartec.de	Beckhoff Automation GmbH & Co. KG Verl 05246/ 963-0 www.beckhoff.de	Bürkert GmbH & Co. KG Ingelfingen 07940/ 10-91111 www.buerkert.com	Haehne Elektronische Messgeräte GmbH Erkrath 0211/ 92591-0 www.haehne.de	Hans Turck GmbH & Co. KG Mülheim 0208/ 4952-0 www.turck.com
S900	Antares	Ethercat Box	AirLINE	Profibus-Messverstärker	BL20
keine Obergrenze		65.535	n.n	2	unbegrenzt
Zone 1 u. 2	ATEX Zone 1/21, IECEx, TC RU, DNV, etc.	✓	ATEX Kat. 3 G	✓	Zone 2, Class1 DIV2, IECEx Zone2
128 / 128	512 / 104	16 / 24	/	/	288 / 288
64 / 64	104 / 84	4 /	/	1 /	126 / 126
Status, Kurzschluss, Überlast, Drahtbruch	Status, Kurzschluss, Überlast, Drahtbruch	Status, Kurzschluss, Drahtbruch, Kommunikationsfehler etc.	Status, Kurzschluss, Drahtbruch	Status	Status, Kurzschluss, Überlast, Drahtbruch
		unzutreffend			IEC 61131-3 Programmiersprachen KOP, FUP, AWL, ST und AS (Ablaufsprache)
Hot configuration on run, eigensicher, redundant, HART-durchgängig	integrierter Switch, HOT-Swap	E/A-Konfigurationseinstellung, Debug-Funktionalität, Zykluszeit-einstellung und -messung			Integrierter Switch auf dem Buskoppler, Busklemme speichert E/A-Konfigurationseinstellung
Profibus-DP	EtherNet/IP, Modbus-TCP, Profinet Profibus-DP	Ethercat Gateway zu Profinet -	Profinet AS-Interface	Profibus-DP	EtherNet/IP, Modbus-TCP, Profinet, Ethercat CANopen, DeviceNet, Profibus-DP,
Kurzschluss, Leitungsbruch, Versorgung, Ex-Einsatz, Namur-Näherungsschalter	Kanäle optional, 2x Zähler	Signalzustand durch Leuchtdioden angezeigt, Diagnoseinformationen wie Kurzschluss oder Leitungsbruch, Eingangsfilter, kurzschlussfeste Sensorversorgung etc.			Signalzustand durch LED angezeigt, Diagnoseinformationen wie Kurzschluss oder Leitungsbruch (Namur), Eingangsfilter, positiv und negativ schaltend, kurzschlussfeste Sensorversorgung, Ex-Einsa.
-, -, -	-, -, -	✓, -, ✓	-, -, -	-, -, ✓	✓, -, ✓
		TwinsafeE			

					
Phoenix Contact Deutschland GmbH Blomberg 05235/ 3-00 www.phoenixcontact.com	Rockwell Automation GmbH Düsseldorf 0211/ 41553-0 www.rockwellautomation.de	Schneider Electric GmbH Ratingen 01805/ 753575 www.schneider-electric.de	Helmholz GmbH & Co. KG Großenseebach 09135/ 7380-0 www.helmholz.de	Wago Kontakttechnik GmbH & Co. KG Minden 0571/ 887-0 www.wago.com	Wago Kontakttechnik GmbH & Co. KG Minden 0571/ 887-0 www.wago.com
Inline	FlexI/O	Advantys STB	TB20	Wago-I/O-System 750/753	Wago-I/O-SYSTEM 750 XTR
	abhängig vom Schnittstellenmodul		je n. Bussystem, bei Ethernet IP gebunden	IP gebunden	IP gebunden
Ex Zone 2, Ex-i (bis Ex Zone 0)	verfügbar für E/A- Einheiten	ATEX II 3 G Ex nA IIC T4 Ta=0°- 60°C	in Vorbereitung	ATEX, ANSI/ISA (UL1604) = Zone 2 usw.	ANSI/ISA 12.12.01
2016 / 2016	256 / 256	512 / 512	1024 / 1024	max. 4000 / max. 4000	max. 1024 / max. 512
1024 / 1024	96 auf 8 Modulen / 96 auf 8 Modulen	256 / 64	256 / 256	max. 1000 / max. 1000	max. 256 / max. 256
Netzwerkstatus, Busstatus, Status, Kurzschluss, Überlast	Status	Status, Kurzschluss	Status LEDs, kostenlose Toolbox zur Diagnose	Status, Kurzschluss, Überlast, Drahtbruch	Status, Kurzschluss, Überlast, Drahtbruch
IEC 61131-3 Programmiersprachen KOP, FUP, AWL, ST und AS (Ablaufsprache)	Über SPS: IEC 61131-3 Program. KOP, FUP, AWL, ST und AS (Ablaufsprache)			IEC 61131-3 Programmiersprachen KOP, FUP, AWL, ST und AS; CoDeSys 2/3	IEC 61131-3 Programmiersprachen KOP, FUP, AWL, ST und AS; CoDeSys 2 + 3
integrierter 3 Port-Switch auf dem Buskoppler, digitale E/As onBoard	integrierter Switch auf dem Buskoppler mit Device-Level-Ring DLR Protokoll	integrierter 2port-Switch, Konfigurations-speicherung auf SIM-Karte, Debug-Funktinalität	Powermodul int., 2 Port Switch, Hot-Plug der Module, USB f. Online-Diag. mit TB20 Toolbox, kein Abschlussmodul benötigt	integ. Switch auf dem Buskoppler, Busklemme speichert E/A-Konfigurationsein-stellung, Debug-Funkt., Ethernet-Switch	integ. Switch auf dem Buskoppler, Busklemme speichert E/A-Konfigurationsein-stellung, Debug-Funkt., Ethernet-Switch
EtherNet/IP, Modb.-TCP,Profinet,Sercos-III TCP/IP CANo., Dev.Net,Interb.,Modb.,Profib.-DP	EtherNet/IP u. EtherNet/IP mit DLR Protok. ControlNet, DeviceNet, Profibus-DP,	EtherNet/IP, Modbus-TCP CANo., Dev.Net, Interb., Mod., Profib.-DP	Ethercat,EtherNet/IP,Modb.-TCP,Profinet CANo.,DeviceNet,Ethernet, Profibus-DP	Ethernet/IP, Ethercat, Mod. TCP, Profinet, Fernwirkpr. IEC 60870, IEC 61850, DNP3 Dev.Net, Profib.-DP, Mod., Interb., CANo.	Fernwir. IEC 60870, 61850, 61400, DNP3
Signalzustand durch Leuchtdioden angezeigt, positiv und negativ schaltend, Ex Zone 2	Signalzustand durch Leuchtdioden angezeigt, Diagnoseinformation zu Kurz-schluss- o. Leitungsbruch, Eingangsfilter, Version XT für agressive Umgebungen u. extr. Temperatur, Ex-Einsatz bei Flex Ex	LED Zustandsanzeige	Eingänge potentialgetrennt zum Rück-wandbus, 2-Draht-Näherungsschalter möglich, Betriebszustands des Moduls durch blaue LED, Zustandsanzeige durch grüne LED, Verpolungsschutz d. Eingänge	Signalzustand durch LED, Diagnoseinfor-mationen (Kurzschluss, Leitungsbruch) (Namur), Eingangsfilter, positiv und negativ schaltend, kurzschlussfeste Sen-sorversorgung, Ex-Einsatz, Profisafe	Signalzustand durch Leuchtdioden, Diagnoseinformationen (Kurzschluss, Leitungsbruch), Eingangsfilter, kurzschlussfeste Sensorversorgung, Ex-Einsatz
✓, -, ✓	-, -, -	✓, -, -	✓, , ✓	✓, ✓, ✓	✓, -, ✓
SafetyBridge, InterbusSafety, Profisafe für Profibus, Profisafe für Profinet				Profisafe V2.0: 4FDI, 8FDI, 4FDI/4FDO 2A, 4FDI/1FDO 10A	

Alle Einträge basieren auf Angaben der jeweiligen Firmen.

Ethercat P

Power und Daten auf einer Leitung

Vor kurzem wurde die klassische Ethercat-Kommunikation um eine Stromversorgungskomponente erweitert und diese Erweiterung von der Nutzerorganisation ETG akzeptiert. Doch was hat es mit dem sogenannten Ethercat P konkret auf sich? Wer profitiert von der Erweiterung? Und wird der bisherige Ethercat-Standard abgelöst? Diese Fragen beantwortet der folgende Beitrag.

Bilder: Beckhoff Automation GmbH & Co. KG

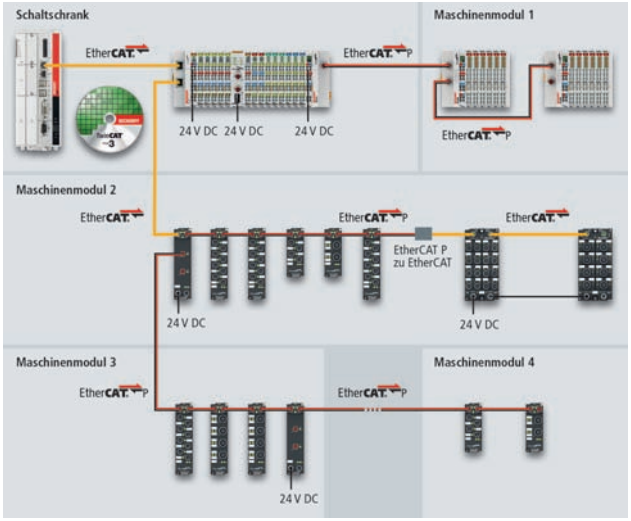
Mit Ethercat P hat die Firma Beckhoff Automation eine Erweiterung zu Ethercat entwickelt, die den Kommunikationsstandard um die Komponente der Stromversorgung auf demselben Kabel erweitert. Wer Ethercat P verwendet, profitiert demnach nicht nur von der gewohnten Performance und Flexibilität von Ethercat, sondern hat nun zudem die Möglichkeit, über zwei galvanisch getrennte, auch einzeln schaltbare 24V-Versorgungen die Energie direkt mit zu übertragen. Aufgrund der Stromweiterleitung kann der Nutzer mehrere Ethercat-Geräte kaskadieren und benötigt hierzu nur ein Kabel.

Ein Kabel für die ganze Maschine

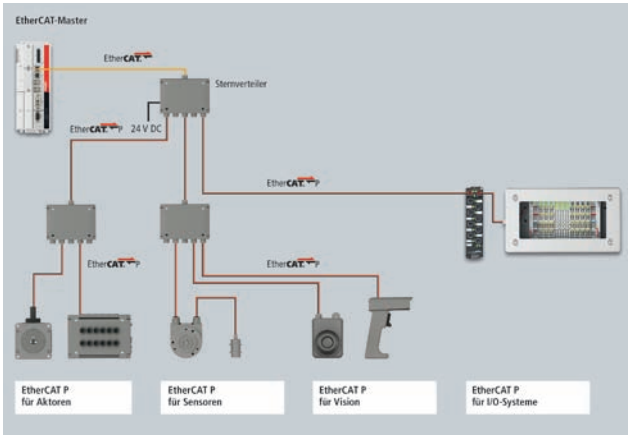
Eine der zentralen Ideen hinter der Entwicklung von Ethercat P war es, ein praxistaugliches System zur Stromversorgung von Ethercat-Geräten über dasselbe Kabel zur Verfügung zu stellen, das auch für die Kommunikation genutzt wird. Zwar war dies bereits vorher mit Power over Ethernet (PoE) möglich, jedoch für den industriellen Gebrauch nur bedingt geeignet. Mit Ethercat P ist das jetzt anders: Profitierend von der Erfahrung mit dem Einkabelkonzept seiner Antriebstechnik hat Beckhoff dieses Prinzip nun auf die ganze Maschine übertragen und auch auf die Sensor- und I/O-Ebene umgesetzt. Durch die reduzierte Verdrahtung werden die Systemkosten und auch potentielle Fehlerquellen beim Anschluss der Geräte reduziert: Aufgrund eines eigens für Ethercat P kodierten M8-Steckers, wird ein Fehlstecken ausgeschlossen. Zudem kann der Maschinenbauer kompaktere Schleppketten einsetzen und mit integrierter Energieverteilung auf bestimmte Schaltschrankteile verzichten.

Leitungswiderstand berücksichtigen

Je nach Anforderung des Endgeräts an die Stromaufnahme und je nach Distanz, die es zu überbrücken gilt, muss im konkreten Einzelfall abgewogen werden, ob der Einsatz von Ethercat P möglich und sinnvoll ist. Hintergrund ist, dass hier, genau wie bei separat geführten Versorgungsleitungen, der Spannungsabfall aufgrund des Leitungswiderstands berücksichtigt werden muss, weshalb ggf. nur kürzere Strecken überbrückt werden können. Besonders interessant ist die Erweiterung daher für Maschinenteile, welche in sich abgeschlossen ein wenig abgesetzt



Besonders interessant ist Ethercat P für Maschinenteile, welche in sich abgeschlossen ein wenig abgesetzt sind.



Ethercat P ist als Erweiterung des bisherigen Standards auf physikalischer Ebene zu sehen, welche nun auch die Spannungsversorgung enthält.

sind und mit Ethercat P durch eine einzige Stichleitung mit Daten und Leistung versorgt werden. Auch für Sensoren aller Art ist Ethercat P gut geeignet: über einen kompakten M8-Stecker werden sie ins Highspeed-Netzwerk integriert und an die Versorgungsspannung angeschlossen.

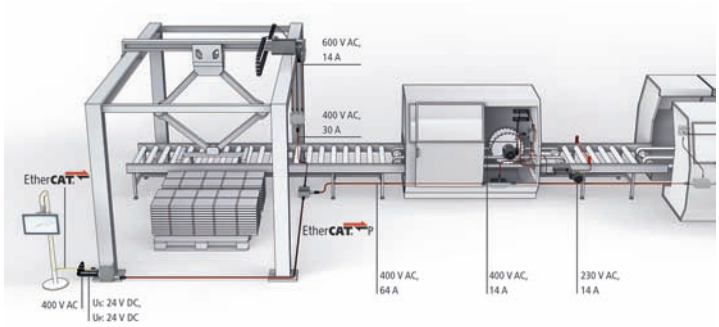


Bild: Beckhoff Automation GmbH & Co. KG

Ethercat P kombiniert auf einem vieradrigen Standard-Ethernet-Kabel die leistungsfähige Ethercat-Kommunikation mit der bislang getrennten Leistungsversorgung für die angeschlossenen Verbraucher.

Erweiterung des Standards

Löst Ethercat P als neue Version von Ethercat das klassische Ethercat-Protokoll ab? Nein. Vielmehr muss Ethercat P als Erweiterung des bisherigen Standards auf physikalischer Ebene gesehen werden, welche nun auch die Spannungsversorgung enthält. Abgesehen davon sind Ethercat und Ethercat P protokolltechnisch identisch, weshalb auch keine neuen Ethercat Slave Controller beim Einsatz von Ethercat P erforderlich sind. Zusammengefasst bedeutet dies, dass die neue Lösung dieselben kommunikationstechnischen Vorteile wie Ethercat bietet – bei Schnelligkeit, Flexibilität oder Leistung – zusätzlich jedoch die Stromversorgung über das Kommunikationskabel enthält und damit für bestimmte Applikationen attraktive Vorteile und Verbesserungen bietet. Ethercat P kommt also da zum Einsatz, wo es sinnvoll ist, und gerne auch im gleichen Netzwerk und im Verbund mit Standard-Ethercat. Entsprechende Einspeisegeräte setzen von der herkömmlichen Ethercat-Physik auf Ethercat P um, wobei die Ethernet-Datenkodierung voll erhalten bleibt. Genauso kann ein Gerät auch für sich mit Ethercat P versorgt werden, selbst aber herkömmliches Ethercat weiterleiten.

Nahtlose Einbindung

Um die Implementierung und Verbreitung von Ethercat P voranzutreiben und potentielle Nutzer zu unterstützen, hat sich die Ethercat Technology Group entschieden, die Erweiterung in ihr Technologie-Portfolio aufzunehmen. Seit der einstimmigen Akzeptanz von Ethercat P als Ergänzung der Technologie durch das Technical Committee der Organisation ist man damit beschäftigt, Ethercat P in die Abläufe der ETG zu integrieren. Ziel ist es, die Einkabelerweiterung in die bisherigen Inhalte, den Support sowie die Schulungen der ETG einzubinden. So soll es künftig beispielsweise bei den Entwicklungsschulungen einen Teil geben, der sich gezielt mit Ethercat P befasst, und auch auf der Master-Konfigurationsseite bietet die ETG ihren Mitgliedern den entsprechenden Support zur Einbindung. Darüber hinaus arbeitet die ETG derzeit an der offiziellen Spezifikation von Ethercat P, welche die Integration für alle Hersteller möglichst einfach gestalten soll, und deren erster Entwurf seit kurzem verfügbar ist. Und auch das Testwesen wird um Ethercat P entsprechend erweitert: Sowohl das Conformance Test Tool als auch die Test Cases werden entsprechend ergänzt. So soll es schon bald einen automatisierten Hardware-Test geben, der die vom Gerätehersteller spezifizierten Randparameter zu Ethercat P mit abtestet. Schon jetzt haben große Anwender den Einsatz von Ethercat P angekündigt, was wiederum die Gerätehersteller ermutigt, in die neue Lösung zu investieren. Mit der Öffnung von Ethercat P durch die ETG soll die Erweiterung genauso wie Ethercat selbst keine proprietäre Beckhoff-Technik bleiben, sondern ein von vielen Herstellern getragener Industriestandard. ■

Autor: *Thomas Rettig,*
Technology Expert,
Ethercat Technology Group
www.ehtercat.org

Halle 2
Stand 338
sps ipc drives

- Anzeigen -

Industrial-Ethernet-Komponenten

Industrial Ethernet ist heute State of the Art in der industriellen Kommunikation. Auch in den zukünftigen Szenarien von Industrie 4.0 und Co. bleibt Ethernet als Basis für die Fertigung gesetzt. Inklusive der durchgängigen Anbindung in die Datenwolke.

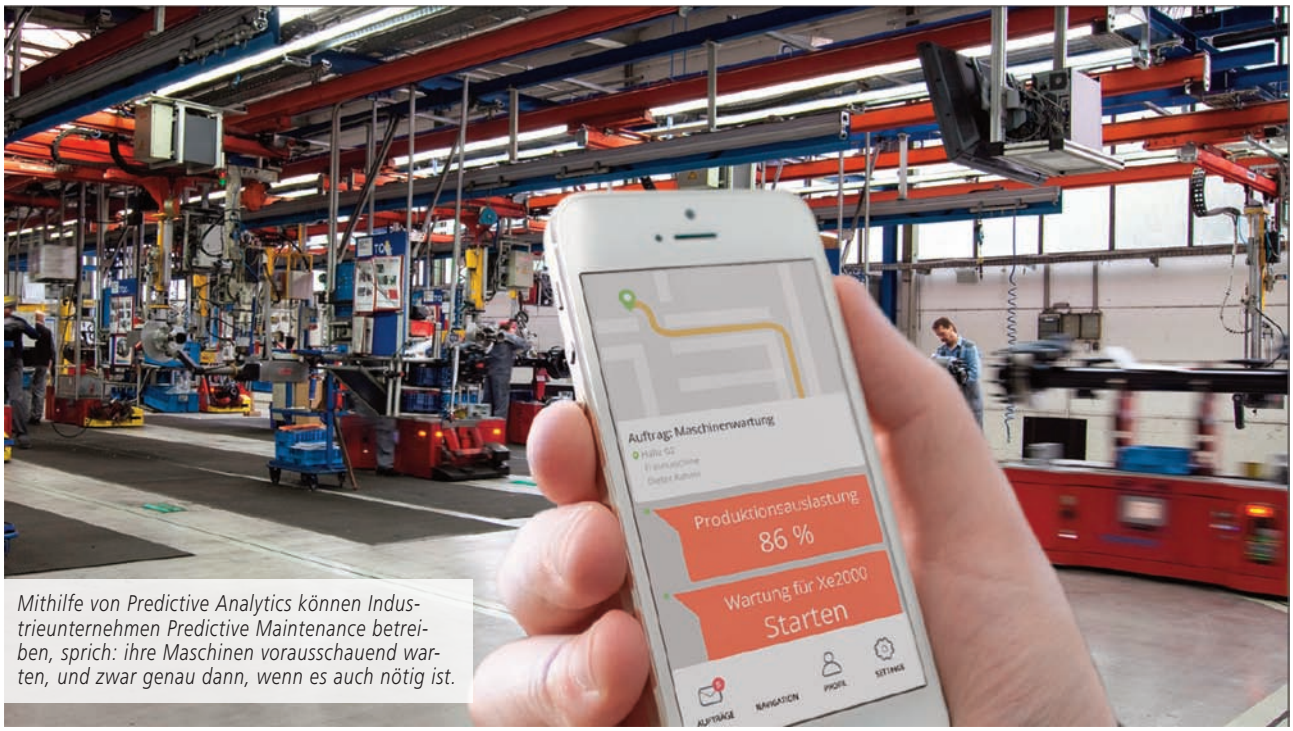
Die Bedeutung von Ethernet in der Automatisierungstechnik nimmt zu und damit auch das Spektrum der auf dem Markt verfügbaren Produkte, angefangen von Infrastrukturkomponenten und Steuerungen über die Antriebs- und Messtechnik bis hin zu Safety, Sensorik und natürlich die Verbindungstechnik. Unsere Übersicht bietet auf den folgenden Seiten einen spannenden Auszug aus dem Spektrum der verfügbaren und neu vorgestellten Produkte und Lösungen. *(mby)* ■

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

Big Data: Vom Rohstoff zum Wettbewerbsfaktor

In der industriellen Fertigung zunehmend wichtiger

Bild: Cancom GmbH



Mithilfe von Predictive Analytics können Industrieunternehmen Predictive Maintenance betreiben, sprich: ihre Maschinen vorausschauend warten, und zwar genau dann, wenn es auch nötig ist.

Durch die intelligente Vernetzung von Maschinen entlang der gesamten Produktionskette entstehen in der Fertigungsindustrie immer größere Datenmengen. Für Unternehmen bergen diese Daten ein immenses Potenzial zur Verbesserung der eigenen Produktionsprozesse – man muss sie allerdings zu händeln wissen. Um aus Big Data Smart Data zu machen und das Beste aus den Daten herauszuholen, sind Dienstleister gefragt.

Daten sind die Rohstoffe des 21. Jahrhunderts. Aber wie jeder Rohstoff entfalten sie ihren vollen Wert erst, wenn sie fachmännisch verarbeitet werden. Das gilt auch für die Produktionsindustrie: Längst sind nahezu alle Maschinen mit intelligenten Sensoren und IT-Komponenten ausgestattet und liefern kontinuierlich präziseste telemetrische Daten – aber nur die wenigsten Unternehmen wissen bislang mit diesem Rohstoff etwas anzufangen. Denn die Datenmengen sind inzwischen nicht nur unüberschaubar groß, sondern auch heterogen: So werden in der industriellen Fertigung z.B. Temperatur, Stromverbrauch und Druck gemessen, Leistungsdaten von Motoren und Dicken von Lackschichten erfasst. Hinzu kommen die Log-Dateien der jeweiligen Fertigungskomponenten zu anderen Maschinen in der Prozesskette und Umgebungsdaten wie Luftfeuchtigkeit und Raumtemperatur.

Big Data entscheidend bei der Prozessoptimierung

Unternehmen, die diese Daten systematisch auszulesen wissen, verschaffen sich damit Marktvorteile: Sie erhalten valide Entscheidungsgrundlagen zur Verbesserung ihrer Fertigungsprozesse und können die Produktivität in ihren Werken immens steigern – z.B. indem sie ihre Arbeitsprozesse an die Umgebungstemperatur anpassen, da durch eine Analyse der Daten ein Effekt auf das Produkt festgestellt wurde. Mitunter entstehen für Unternehmen aus dem systematischen Auslesen von Daten sogar neue Geschäftsmodelle. So könnte ein Automobilhersteller die in seinen Fahrzeugen verbauten Wettersensoren beispielsweise nutzen, um einen eigenen Wetterdienst ins Leben zu rufen. Allerdings liegt das große Potenzial der fast beiläufig erhobenen Messwerte in vielen Industrieunternehmen bislang

brach: Sie sammeln alle anfallenden Daten gleich welchen Typs in einem zentralen Data Lake, ohne sie sinnvoll aufzubereiten. Erst mithilfe entsprechender Data-Analytics-Methoden entsteht aus Big Data ein wirklicher Mehrwert. Noch vor wenigen Jahren konnte man Messdaten in der Fertigung allenfalls im Nachhinein betrachten und rückblickend beschreiben, dass ein Fehler passiert war – Descriptive Analytics nennt sich dieses Verfahren. Durch die Kombination verschiedener Messwerte ließ sich auch eruieren, warum eine Maschine ausgefallen ist, z.B. weil der Schwellenwert für die Temperatur einer bestimmten Maschine überschritten wurde. Man spricht hier von Diagnostic Analytics. Inzwischen sind allerdings selbst sogenannte Predictive Analytics möglich: vorhersagende Analysen, die die anfallenden Daten nicht mehr rückblickend betrachten, sondern bereits zum Zeitpunkt ihrer Erhebung Vorhersagen für die Zukunft treffen: Wann wird diese Maschine ausfallen? Wann muss ich sie warten, damit eben das nicht passiert? Die Königsklasse der Data Analytics sind schließlich Prescriptive Analytics: Dabei wird nicht nur analysiert, was in Zukunft passieren wird, sondern der Maschine auch direkt konkrete Lösungsvorschläge gegeben, sodass sie autonom entscheidet, was als nächstes passieren soll.

Kosten sparen durch Predictive Maintenance

Solche präskriptiven Verfahren sind zum jetzigen Zeitpunkt in der Fertigung freilich noch weitestgehend Zukunftsmusik. An der Vorstufe, den Predictive Analytics, führt inzwischen aber kein Weg mehr vorbei. Mit ihrer Hilfe können Industrieunternehmen Predictive Maintenance betreiben, sprich: ihre Maschinen vorausschauend warten, und zwar genau dann, wenn es auch nötig ist. Durch speziell programmierte Logarithmen, die über die entstehenden Daten gelegt werden, lässt sich exakt berechnen, wann der Verschleiß einer Maschine so hoch ist, dass bestimmte Komponenten ausgetauscht werden müssen. Durch dieses Verfahren müssen Maschinen nicht mehr auf Verdacht gewartet werden, sondern haben mitunter sogar längere Laufzeiten als vermutet. Und statt während bestimmter Wartungsfenster ein ganzes Werk stilllegen zu müssen, kann jede einzelne Maschine bedarfsgenau gewartet werden. Die Kosteneinsparungen durch Predictive Maintenance sind enorm: Wenn durch das neue Verfahren allein ein Prozent Verbesserung erreicht wird, liegen die Einsparungen bei einem Automobilhersteller mit mehreren Fertigungswerken beispielsweise bereits bei einem mittleren einstelligen Millionenbetrag. Allerdings birgt das Thema durchaus einige Herausforderungen. Es gilt genau hinzuschauen, welche Daten überhaupt benötigt werden, um eine solide Entscheidungsgrundlage zu schaffen.

Wahl des passenden Analytics-Tools erfordert hohe Fachkenntnis

Eine weitere Herausforderung ist die Wahl des richtigen Analytics-Tools, mit dem die erhobenen Daten ausgewertet werden sollen. Denn die Tool-Landschaft wird von Tag zu Tag größer und die verschiedensten Anbieter stellen inzwischen Lösungen bereit, die sich in Reifegrad und Usability allerdings noch sehr stark unterscheiden. Einsteiger in das Big-Data-Thema brauchen eine anwenderfreundliche Out-of-the-box-Lösung, Unternehmen, die schon tiefer im Thema stecken, suchen vielleicht eher nach einem Toolset, das sie präzise an ihre Use-Cases anpassen können. In beiden Fällen darf auch die Infrastruktur im Unternehmen nicht vergessen werden: Viele Analytics Tools sind nämlich Cloudlösungen – und gerade in der Automobilindustrie, aber auch in anderen Branchen sind nicht in allen Werken die entsprechenden Voraussetzungen für einen reibungslosen Cloudbetrieb gegeben, sondern die Daten müssen vor Ort ausgelesen werden. Hier kann ein entsprechender Dienstleister beratend zur Seite stehen. Die Zusammenarbeit sollte mit einem Anforderungsworkshop starten, um zunächst die genaue Fragestellung herauszuarbeiten, die mithilfe von systematischen Datenanalysen beantwortet werden soll. Durch die Evaluierung können sinnvolle Lösungsansätze identifiziert werden. Statt etwa für teures Geld eine umfassende Predictive-Maintenance-Lösung für eine Maschine zu entwickeln, gilt es sogenannte Quick-Wins zu finden: schnell umsetzbare Lösungen mit möglichst hohem Optimierungspotenzial für den laufenden Betrieb.

Strukturierter Projektansatz inklusive Lifecycle-Management ist gefragt

Ist die Aufgabenstellung bzw. der jeweilige Use Case präzise umrissen, geht es in die Explorationsphase: Hier analysiert der Dienstleister, welche Daten überhaupt vorliegen und welche benötigt werden. In einer anschließenden Evaluationsphase muss dann noch einmal kritisch überprüft werden, ob die ausgewählten Daten tatsächlich valide sind und die gewünschten Ergebnisse bringen. Erst wenn das sichergestellt ist, geht es in die Deployphase, bei der die passenden Tools aufgesetzt und angepasst werden. Wichtig ist in diesem Zusammenhang, dass der Dienstleister einen lösungs- und herstellerunabhängigen Ansatz verfolgt, um eine unabhängige Beratung sicherzustellen. Ein Dienstleister auf diesem Gebiet ist Cancom. Cancom begleitet Unternehmen aus dem produzierenden Gewerbe von der Analyse ihrer Anforderungen bis zum Betrieb der implementierten Data-Analytics-Lösung. Dabei setzt der IT-Dienstleister auf ein iteratives Vorgehen: Statt die gesamten Produktionsabläufe auf einmal zu verbessern, wird mit den Quick-Wins begonnen und die gefundene Lösung bei Bedarf Schritt für Schritt auf andere Bereiche ausgeweitet. Der Anbieter wartet mit einem umfassenden Partner-Ecosystem auf und kann damit die Auswahl der passenden Umsetzungspartner steuern. Und er bleibt auch dann im Boot, wenn die gewünschte Industrial-Analytics-Lösung einmal implementiert wurde. Denn das Big-Data-Zeitalter ist schnelllebig und schon das Aufrüsten einer einzelnen Maschine auf ein neueres Modell kann wieder neue Daten in unbekannten Formaten hervorrufen, sodass der Logarithmus zur Auswertung gegebenenfalls nicht mehr korrekt funktioniert. Ein Lifecycle-Management ist also sinnvoll, damit Produktionsunternehmen auch in Zukunft den größten Mehrwert aus ihren Daten schöpfen. Und das ist unverzichtbar, wird doch die intelligente Nutzung des Rohstoffs Big Data in der Industrie immer mehr zum entscheidenden Wettbewerbsfaktor. ■

Autor: ***Oliver Bischoff,***
Competence Team Industrial Solutions,
Cancom GmbH,
www.cancom.de

Web 3.0

Ein smartes Wissensnetz für deutsche Unternehmen

Bild: Smart Data/BMWi

Smart Data-Web auf der CeBIT 2016: Echtzeitanalyse und Visualisierung großer und heterogener Datenbestände für firmen- und mobilitätsrelevante Ereignisse und ihre geographische Lokalisierung.

Für die produzierende Industrie ist es wichtig, so früh wie möglich über Ereignisse informiert zu werden, die zu einer Störung oder Unterbrechung der Wertschöpfungs- und Lieferketten führen können. Informationen darüber liefern verschiedene Quellen: Nachrichtenseiten, Social Networks oder Websites konkurrierender Unternehmen. Ein Smart Data-basiertes Wissensnetz will verfügbare Informationen aus unterschiedlichen Quellen nun bündeln und den deutschen Unternehmen zur Verfügung stellen.

Für Unternehmen ist es wichtig, rechtzeitig auf produktionsgefährdende Vorkommnisse reagieren zu können. Dabei können sowohl Naturkatastrophen und Streiks als auch politische Unruhen zu Störfaktoren werden, die sich negativ auf die Lieferketten auswirken. Besonders die Schlüsselindustrien Deutschlands – wie der Maschinenbau, die Automobil-, Chemie-, oder Elektroindustrie – arbeiten in Netzwerken mit hochspezialisierten mittelständischen Unternehmen. Diese Vernetzung führt zu komplexen Wertschöpfungs- und Lieferketten. Störungen dieser Ketten führen zu enormen Kosten und haben im Extremfall gerade für den KMU existenzbedrohende Auswirkungen. Gleichzeitig wollen Unternehmen vor dem Hintergrund der Digitalisierung frühzeitig auf neue Technologien, Verordnungen und Gesetze sowie auf neue Produkte von Konkurrenten aufmerksam gemacht werden, um die eigene Produktion anpassen zu können. Obwohl die meisten Informationen oft schon relativ lange verfügbar sind, erreichen sie die Unternehmen häufig erst spät. Nötig wäre hier ein ständiger Kontakt mit Zulieferern, Dienstleistern und den Regulatoren, die den Wettbewerb kontrollieren. Zudem bräuchte es eine aufwendige und kontinuierliche Recherche in verschiedenen Quellen, um alle produktions- und unternehmensrelevanten Informationen rechtzeitig sammeln zu können – eine Aufgabe, die insbesondere KMU häufig nicht leisten können.

Intelligente Daten für bessere Produktionsplanung

Durch eine automatische und systematische Verknüpfung öffentlicher Informationsquellen mit unternehmensinternen Netzwerken wären Produktionsbetriebe in der Lage, schneller und sicherer auf produktionsrelevante Veränderungen reagieren zu können. Genau an diesem Punkt setzt das Projekt ‘Smart Data-Web – Datenwertschöpfungsketten für industrielle Anwendungen’ an, das im Rahmen des Technologieprogramms ‘Smart Data – Innovationen aus Daten’ vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird. Innerhalb des Projektes soll eine Brücke zwischen zwei bisher voneinander getrennten Datenwelten gebaut werden: dem öffentlich zugänglichen Internet und den firmeninternen Netzwerken. Dafür entwickelt das Smart Data-Webteam derzeit ein neuartiges Wissensnetz, das unternehmensrelevante öffentliche Daten sammelt, analysiert, individuell aufbereitet und zur Verfügung stellt. Die Informationen aus den unterschiedlichen Quellen werden so zu nützlichen und hilfreichen Daten – Smart Data – umgewandelt. Um diese intelligenten Daten aus einer riesigen Datenmenge zu gewinnen, kombiniert Smart Data-Web bewährte Analysemethoden mit neuen Verfahren für die tiefere semantische Aufbereitung von Massendaten. Auf diese Art wird die

deutsche Industrie direkt an das sogenannte Web 3.0 angeschlossen. Das Web 3.0 bezeichnet eine Erweiterung des herkömmlichen Internets, in dem Informationen mit exakten Bedeutungen versehen werden, um die Zusammenarbeit zwischen Mensch und Maschine zu erleichtern. Mithilfe dieses neuen Informationsnetzes sollen Unternehmen zukünftig bei Planungsprozessen und der Entscheidungsfindung besser eingebunden und unterstützt werden. Ein weiteres Einsatzszenario von Smart Data-Web sind die Marktbeobachtung und die Marktforschung. Durch unternehmens- oder marktspezifische Analysen können sich Unternehmen künftig schneller einen Überblick über die Wettbewerbssituation verschaffen, mögliche neue Kunden identifizieren oder günstigere und innovativere Lieferanten für eigene Produkte finden. Dazu hat die Smart Data-Webtechnologie noch einen weiteren Vorteil, der besonders für KMU interessant werden kann. Das Wissensnetz unterstützt nicht nur Unternehmen der produzierenden Industrie, die veredelte Daten nutzen wollen, sondern hilft auch KMU der Datenwirtschaft, die Datenveredelungsdienste anbieten: Für Datenanalytikdienstleister senken sich die Einstiegsbarrieren durch den zentralen Einsatz offener Quellen, Standards und Werkzeuge. Dennoch können kleine und mittlere Unternehmen Daten auch unabhängig von diesen Dienstleistern organisieren und nutzen, da Smart Data-Web die Kosten für Datenanalytikprodukte reduziert und sie damit auch für KMU erschwinglich macht. So können Unternehmen der deutschen Industrie zukünftig an das hochvernetzte Web 3.0 angeschlossen werden und von diesem Anschluss profitieren. ■

Autor: *Prof. Dr. Stefan Jähnichen,*
Direktor der Außenstelle Berlin des FZI – Forschungszentrums Inormatik und Leiter der Begleitforschung des Technologieprogramms 'Smart Data – Innovationen aus Daten' des Bundesministeriums für Wirtschaft und Energie (BMWi)
www.smart-data-programm.de

Vor- und Nachteile eines Database-as-a-Service

Data Warehouse aus der Cloud

Die Themen Big Data und Cloud beschäftigen die Unternehmen in allen Branchen. Digitalisierung, Internet of Things, Social Media und cloudbasierte Geschäftsmodelle produzieren massenhaft Daten, die verwertbar und überall zugänglich sein sollen. Doch wohin damit? Am besten wäre es doch, alle Daten je nach Bedarf in ein über die Cloud flexibel erweiterbares Data Warehouse abzulegen, also Database-as-a-Service zu nutzen. Experten mahnen hier aber zur Vorsicht.

Schnell anpassungsfähige Cloudangebote wie Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) oder Database-as-a-Service (DBaaS), sozusagen ein cloudbasiertes Data Warehouse (DWH), gewinnen in sämtlichen Branchen immer mehr an Bedeutung. In einer Studie von IBM zum Thema Hybridcloud, einem Mix aus On-Premise- und Cloudlösungen, wurden weltweit IT-Verantwortliche befragt. 85 Prozent der Unternehmen, die bereits eine sehr gut integrierte hybride IT-Infrastruktur aufweisen, gaben an, dass sie ihre Kosten durch den Cloudeinsatz signifikant reduzieren konnten. Bei den Firmen mit weniger gut integrierter Hybridcloud gelang dies gerade einmal der Hälfte.

Flexibler: Data Warehouse als Cloudservice

Dabei arbeitet ein DWH eher im Hintergrund. Es sammelt strukturierte und unstrukturierte Daten, die gesäubert, analysiert und für die Weiterverarbeitung in anderen Systemen aufbereitet werden. Ein Schattendasein hat es jedoch nicht verdient: Denn um unternehmensrelevante Informationen gewinnen und auswerten zu können, müssen stets historische Daten sowie Muster für einen Vergleich herangezogen werden – und diese liefert das Data Warehouse. „Deshalb arbeiten wir gerade mit unseren Kunden daran, Data Warehouse-, Echtzeit- und Big Data-Technologien stärker zu integrieren“, meint Ursula Flade-Ruf, Gründerin und Geschäftsführerin von MIP. „Die Kunden müssen schneller sowie flexibler auf neue Technologien und Entwicklungen in den Märkten reagieren können. Darum greifen sie vermehrt auf Cloudprodukte zurück, die sich rasch und ohne große Anfangsinvestition einbinden lassen.“ Laut Flade-Ruf eignet sich die Cloud vor allem für Testzwecke oder zeitlich begrenzte Services: „Über die Cloudplattform Bluemix können etwa Watson-Services bezogen werden – mithilfe des kognitiven Supercomputers lassen sich Datenpakete schnell analysieren.“ Dieses bedarfsorientierte Vorgehen ist viel kosteneffizienter als die Installation von Watson im Unternehmen.

Alles immer noch eine Frage der Cloudsicherheit

Mit dem Cloudeinsatz geben Unternehmen aber auch den Betrieb ihrer Software, teils ihre komplette IT-Infrastruktur in die Hände der Cloudanbieter – und damit auch Performance und Datensicherheit. Eine andere Studie zeigt in diesem Zusammenhang, dass besonders die Sicherheitsbedenken sowohl bei Cloudverweigerern (83,6 Prozent) als auch bei Cloudbefürwortern (68 Prozent) noch hoch sind. „Cloudprovider können allerdings einen viel höheren und professionelleren Sicherheitsstandard anbieten, als etwa ein kleines mittelständisches Unternehmen“, so Flade-Ruf. Die großen Provider suggerieren dabei oft ein Gefühl von Sicherheit. Cyberattacken und Datendiebstähle, wie etwa der jüngst bekannt gewordene Hacker-Angriff auf Microsoft-, Google- und Yahoo-Konten belegen aber immer wieder das Gegenteil. Zudem haben die Rechtsstreitigkeiten von Apple mit der US-Regierung gezeigt, dass Staaten wie die USA weiterhin unter bestimmten sicherheitsrelevanten Bedingungen auf Daten von US-Firmen zugreifen können. „Wir beobachten, dass die deutschen Unternehmen immer noch zögerlich sind, ihre sensiblen, für Auswertungen relevanten Daten in die Cloud zu legen“ konstatiert Flade-Ruf.

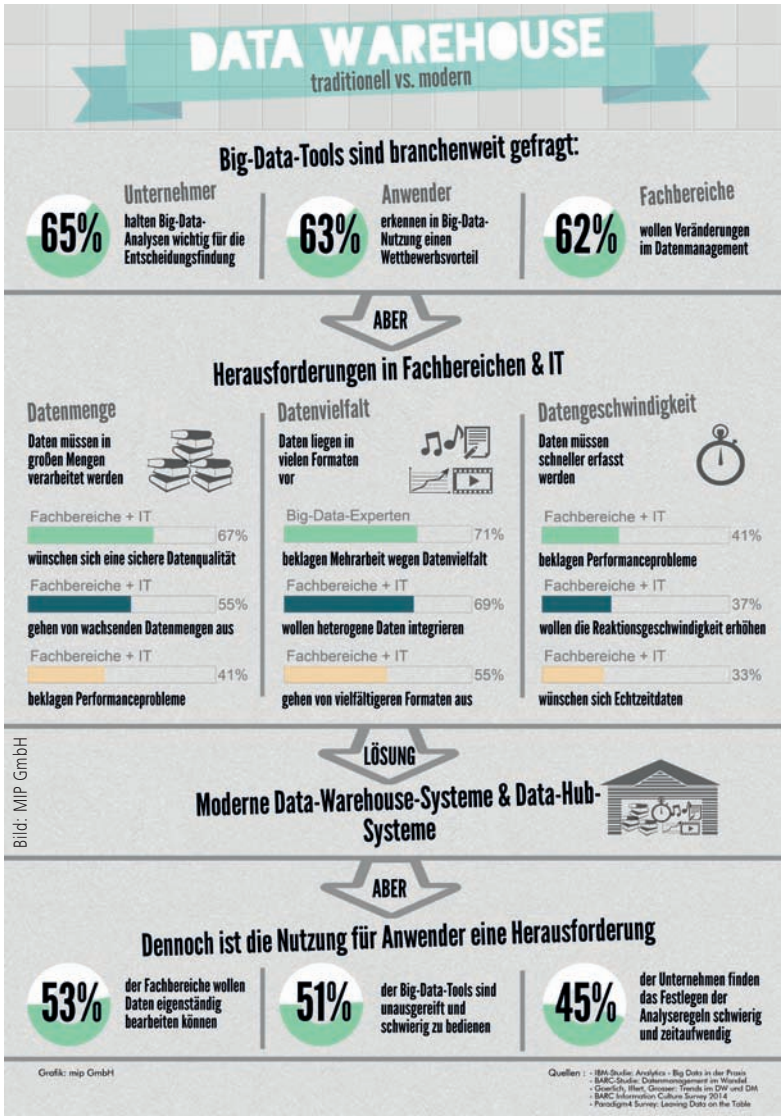


Bild: MIP GmbH

Keine Performancegarantie über die Cloud

Ein anderer Nachteil der Cloud sind Performanceprobleme, die etwa beim Verschieben von großen Datenmengen auftreten. „Im Gegensatz zu einem operationalen System, das nur nacheinander Transaktionen abwickelt, sind Data Warehouse- und auch künftige Big Data-Anwendungen nach wie vor stark Input/Output-lastig“, erklärt Flade-Ruf. „Beim Thema Cloud und Übertragungsgeschwindigkeit sind wir in Deutschland selbst in Großstädten einfach noch nicht schnell genug.“ Ruf ergänzt: „Cloud-Provider werden niemals eine bestimmte Leistung oder I/O-Werte garantieren. Derartige Service Level Agreements auf Performance oder auf eine bestimmte Anzahl an CPU-Kernen, RAM- und Festplattenspeicher gibt es nicht.“ Dieses Thema wird in der medialen Diskussion umgangen, da bisher niemand genau messen kann, wo der Geschwindigkeitsverlust entsteht: Verliert der Rechner selbst die Zeit oder wird die Zeit auf dem Weg dorthin eingebüßt? „Der Cloudkunde erhält daher nur eine virtuelle Maschine“, erläutert Ruf. „Diese bekommt bestimmte Prozessoren zugewiesen, die aber over provisioned sind, sprich: die Prozessoren sind mehreren Rechnern zugewiesen. Nur wenn eine Bare-Metal-Maschine angemietet wird, lassen sich vorgegebene Leistungsparameter in etwa einhalten. Diese werden aber seltener angeboten und sind natürlich dementsprechend teurer.“ Für flexible und schnelle Hilfe bei Analysen oder für Testzwecke sind Cloud- und DBaaS-Angebote schon heute sehr gut geeignet, weil keine eigene kostenintensive Infrastruktur aufgebaut werden muss. „Zudem werden die Menschen in Zukunft sicher auch etwas lockerer mit ihren Daten umgehen, wie Facebook, Twitter und Co es bereits andeuten – ganz nach dem Motto: Information for everybody“, so Flade-Ruf. „Aber hier benötigt es noch ein wenig Zeit. Zu klären ist unter anderem auch die Frage, wie belastbar die Rechtslage rund um die Cloud einzuschätzen ist.“ Ansonsten werden deutsche Unternehmen zumindest in Bezug auf ihre sensiblen, erfolgsrelevanten Daten weiterhin einen Bogen um das Data Warehouse in der Cloud machen. ■

Autor: *Marian Spohn, Redakteur, MIP GmbH www.mip.de*

SONDERAUSGABE 2/2016
www.sps-magazin.de

CC-Link Partner Association
www.clpa-europe.com

INDUSTRIAL COMMUNICATION JOURNAL

ICJ

ETHERNET WIRELESS SECURITY

CC-Link IE IN ACTION

CC-Link IE in der Praxis

Die CC-Link Partner Association (CLPA) präsentiert gemeinsam mit dem Industrial Communication Journal (ICJ) eine weitere Sonderpublikation, die sich mit der offenen Automationsnetzwerktechnologie CC-Link IE beschäftigt. Sie zeigt eines deutlich: Die Frage lautet heute nicht mehr, ob wir Gigabit brauchen, sondern wie schnell wir es implementieren können.

CC-Link hebt sich durch seine momentane Einzelstellung als einziges offenes industrielles Ethernet mit Gigabit-Leistung ab. Diese unübertroffene hohe Bandbreite machte CC-Link IE zur ersten Wahl von führenden globalen Herstellern, die einen Vorteil gegenüber ihren Wettbewerbern suchen. Diese Bandbreite bildet im Hinblick auf die Ausrichtung auf Industrie 4.0 in der Produktion die Basis, die sicherstellt, dass alle Prozesse und Komponenten notwendige Informationen in Echtzeit austauschen können. So können Produktionsentwicklungen erfolgreich weiter in Richtung Zukunft getrieben werden. Von seinen Ursprüngen auf dem japanischen Markt vor über fünf Jahren wird CC-Link IE heute weltweit eingesetzt und von einer Vielzahl führender Automatisierungsanbieter unterstützt.

Bild: CC-Link Partner Association-Europe

CLPA: global Organisation – starker Support

Die CLPA vereint derzeit über 300 Partnerunternehmen, die eine Vielzahl an Komponenten entweder für CC-Link IE oder sein Feldbusgegenstück CC-Link anbieten. Die CLPA ist mit einer Mitgliederzahl von ca. 2600 Unternehmen eine der größten Organisationen für offene Netzwerktechnologie und somit in der Lage, einen weltweiten Support zu leisten. Ungefähr 17 Millionen installierte Geräte beweisen die führende globale Bedeutung der CC-Link-Technologie. In den letzten beiden Sonderteilen beschäftigten wir uns mit dem Thema, wie Unternehmen die Vorteile und Stärken der CLPA für sich nutzen können, um ihre Geschäfte mithilfe unseres 'Gateway to Asia' (G2A)-Programms ausbauen zu können. Es gab einen umfassenden Überblick über die CC-Link IE-Technologie mit seinen offenen Netzwerk-Protokollen, die ebenfalls von vielen Drittanbietern genutzt werden. In dieser Ausgabe zeigen wir Ihnen anhand von Anwendungsbeispielen, wie sich CC-Link gezielt und erfolgreich in der Praxis umsetzen lässt.

Industrial Ethernet ist richtungsweisend

Das offene Giga Ethernet bringt häuftig den entscheidenen Unterschied. Zwar wird in vielen Applikationen heute immer noch Feldbus-Technologie eingesetzt, aber man ist sich einig, dass das Industrial Ethernet richtungsweisend für die zukünftige Industrie ist. Während noch die Frage diskutiert wird, ob Gigabit-Ethernet auch zuverlässig funktioniert, zeigt eine Blitzbefragung von Unternehmen mit Industrial-Ethernet-Infrastruktur, dass Gigabit bereits heute erfolgreich eingesetzt wird. Darüber hinaus werden Industrie 4.0 sowie seine globalen Äquivalente heute als Konzepte akzeptiert, die es so schnell wie möglich in der Produktion umzusetzen und nicht länger als eine Art Modeerscheinung zu betrachten gilt. Zusammen mit den Praxisbeispielen, die wir Ihnen in diesem Sonderteil präsentieren, lautet die Frage nicht mehr, ob wir Gigabit brauchen, sondern wie schnell wir es implementieren können. Mit der steigenden Akzeptanz von Industrie 4.0 wird deutlich, dass die ersten Anwender von Gigabit, so wie die hier vorgestellten Firmen, Wegbereiter der nächsten industriellen Revolution sein werden. Wir hoffen, Ihnen mit dieser Sonderausgabe Anregungen geben zu können, wie Sie Ihr Unternehmen fit für die zukünftigen Anforderungen des Marktes machen können. Sprechen Sie uns an, wir helfen Ihnen gerne bei der Umsetzung Ihrer Vorstellungen! ■

John Browett
General Manager, CLPA Europe
www.clpa-europe.com

Die Weiterentwicklung von CC-Link IE:

Integriertes Industrie-Netzwerk für das Internet of Things (IoT)

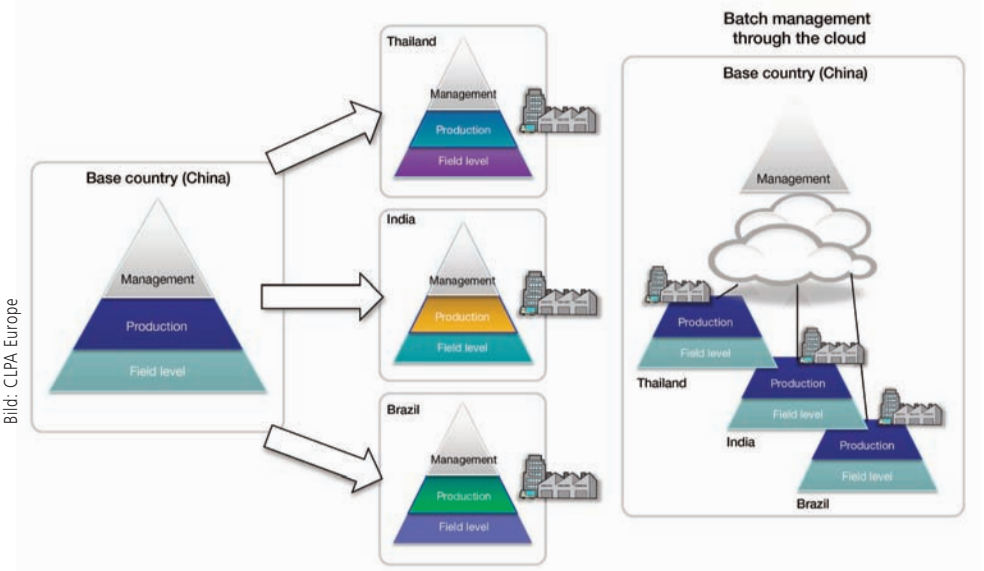


Bild: CLPA Europe

Bild1: Globales Fertigungs-IT-System und Batch Management über die Cloud

Die Anwendung moderner Konzepte wie e-F@ctory und Industrie 4.0 in der IT-gesteuerten Produktion erfährt derzeit große Aufmerksamkeit. Gemeinsamer Grundgedanke dieser Technologien ist die Integration und Optimierung der IT auf Management-, Produktions- und Maschinenebene. Zu den Herausforderungen bei der Einbindung von Produktionsnetzwerken in übergeordnete IT-Systeme zählen nicht nur die notwendigen hohen Geschwindigkeiten und großen Datenkapazitäten des Netzwerks, sondern auch z.B. die nahtlose Konnektivität. Die CC-Link-Familie ist ein integriertes Industrie-Netzwerk, das alle diese Anforderungen erfüllt.

Die CC-Link-Familie bestehend aus der RS485-basierten-CC-Link-Serie und der Gigabit-Ethernet-basierten CC-Link IE-Serie beinhaltet CC-Link, CC-Link Safety und CC-Link/LT. Es ist ein Netzwerk, das sich auf Leistung und Zuverlässigkeit bei möglichst geringen Kosten konzentriert. Die CC-Link IE-Serie umfasst CC-Link IE Control, CC-Link IE Field, CC-Link IE Field/Motion und CC-Link IE Safety. Die wichtigsten Merkmale von CC-Link IE sind u.a. die hohe Geschwindigkeit und die enorme Datenkapazität. Damit hält es auch für zukünftig neue Anwendungen genügend Leistungsreserven bereit.

CC-Link IE Control: Echtzeit-Performance und Integrationskomfort

Aufgrund der Geschwindigkeitsleistung und der erweiterbaren Echtzeit-Performance findet CC-Link IE Control verstärkt in der Flachbildschirm-Produktion und im Automobilbau Anwendung. CC-Link IE drückt Echtzeit-Performance mithilfe des 'Link-Scan-Time'-Index aus. Abb. 3 zeigt die Link Scan Time für eine Anordnung von 32 Stationen mit gleicher Speicherzuweisung über CC-Link IE Control. Im Vergleich zu anderen Controller-Netzwerken werden beeindruckende Geschwindigkeiten erreicht, und man kann sehen, dass die Leistung selbst bei einem größeren Datenaustausch im Netzwerk (Gesamtanzahl an Link Points) nicht an Geschwindigkeit verliert. Rezept- und Qualitätskontrolle sind weitere wichtige Managementaspekte auf der Produktionsebene. CC-Link IE Control ist ein Netzwerk, dass die Koordination und Integration mit der Produktionsebene, z.B. Rezeptweitergabe, Qualitätsdatenerfassung usw., berücksichtigt. Neben der zyklischen Kommunikation in Echtzeit bietet CC-Link IE transiente Kommunikation für Rezeptweitergabe, Qualitätsdatenerfassung usw. Außerdem kann die hohe Bandbreite von 1Gbps zwischen zyklischer und transienter Kommunikation aufgeteilt werden. Auf diese Weise werden Störungen der zyklischen Kommunikationsperiode durch transiente Kommunikation vermieden. Steckkartenprodukte für PCs existieren ebenfalls. Damit lassen sich Lösungen zur Qualitätsanalyse erstellen, um die PC-Analysewerkzeuge für die über die Steckkarte erfassten Daten anzuwenden.

Gewährleistung von kontinuierlicher Produktion und Sicherheit mit CC-Link IE

Die CC-Link-Familie bietet gegenwärtig keine Spezifikationen für Datensicherheit im Sinne von Security. Was die drei Ebenen Management, Produktion und Maschinen angeht, so liegt das daran,

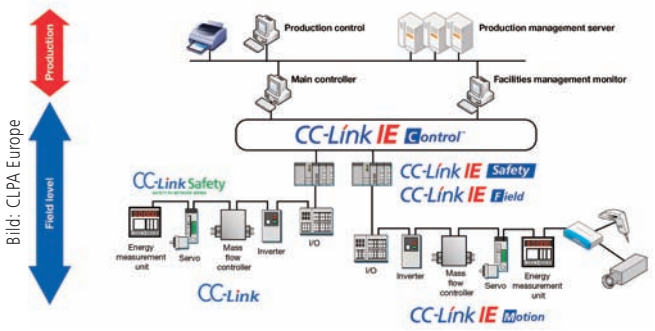


Bild: CLPA Europe

Bild 2: Die CC-Link-Protokollfamilie

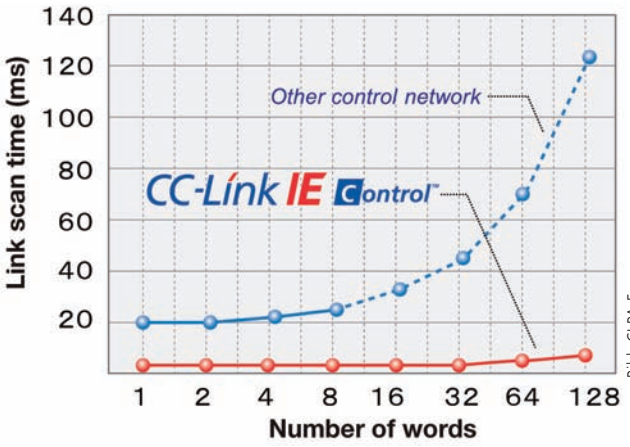


Bild: CLPA Europe

Bild 3: Link Scan Time

dass die Datensicherheit durch OPC UA usw. auf der Produktionsebene realisiert ist und Maschinennetzwerke unter Produktivitätsaspekten wie Verarbeitungszeit kostenoptimiert gestaltet sind. Im Hinblick auf die Zukunft und unter der Berücksichtigung von Markttrends muss die Koordination für ISASecure®, EDSA-Zertifizierung usw. noch diskutiert werden. Für das Thema Sicherheit im Sinne von Safety wurde CC-Link IE Safety definiert. Sicherheitskommunikation kann die Kommunikation zwischen Sicherheitsfeldgeräten und einem Sicherheitscontroller sowie das Senden und Empfangen von Sicherheitsdaten zwischen Sicherheitscontrollern umfassen. Das heißt, beim Stoppen eines Prozesses durch eine Sicherheitsfunktion werden abhängige Prozesse synchron gestoppt, sodass der Neustart nach der Fehlerbehebung beschleunigt wird.

Nahtlose Anbindung verschiedener Netzwerke

Für die CC-Link-Familie wurde das Seamless Message Protocol (SLMP) als Mechanismus für die Integration und nahtlose Anbindung verschiedener Maschinennetzwerke definiert. Dieses Protokoll ermöglicht die Verbindung zwischen einem System auf höherer Ebene und den Feldgeräten ohne Rücksicht auf die Unterschiede zwischen CC-Link IE, CC-Link und TCP/IP. Seit einigen Jahren werden in Maschinen-Netzwerken verstärkt Open-Sensor-Netzwerke eingesetzt, wie z.B. I/O Link. Die CC-Link Partner Association prüft darüber hinaus die Entwicklung von Spezifikationen für die nahtlose Konnektivität mit anderen offenen Netzwerken.

Einfache Netzwerkkonfiguration mit CC-Link IE

CC-Link IE verwendet Ethernet als unterste Kommunikationsebene und Token Passing Methode für die Kommunikationssteuerung auf höherer Ebene. Hierbei werden die Datenübertragungsrechte ('Tokens') im Netzwerk auf einer festgelegten Route von Station zu Station weitergegeben. Nur diejenigen Stationen mit Datenübertragungsrechten können Daten übertragen. Derzeit werden Tokens auf einer statisch festgelegten Route weitergegeben, aber es ist auch technisch möglich, diese Route dynamisch in beliebigen Intervallen zu ändern. In der Zukunft wird dies Routen-Switching in Abhängigkeit von dem zu fertigenden Produkt ermöglichen. Simultane Fehlersuche ist bei der Netzwerkkonfiguration ebenfalls wichtig. Bei Störungen im Netzwerk muss die betreffende Stelle schnell zu finden sein. CC-Link IE bietet verschiedene Werkzeuge zur schnellen Diagnose im Fehlerfall, beispielsweise ein Management-Werkzeug für Netzwerkereignisse, Historie, ein Netzwerkdiagnosewerkzeug usw.

Zusammenfassung

- CC-Link IE bietet viele Vorteile für Anwender. Es ermöglicht die einfache Integration umfangreicher Datenübertragungsanforderungen in die Produktionsebene durch transiente Kommunikation ohne Beeinträchtigung der Echtzeitkommunikation.
- CC-Link IE sorgt für kürzere Ausfallzeit bis zum Neustart nach Sicherheitsabschaltung, da die Sicherheitskommunikation die Prozesse beim Wiederanlauf koordiniert. Unterstützung für Datensicherheit (Security) ist ein Thema, mit dem sich CC-Link IE derzeit beschäftigt.
- Neben CC-Link können auch andere offene Netzwerke nahtlos in CC-Link IE-Architekturen eingebunden werden.
- CC-Link IE ist zukunftssicher: Das Kommunikationssystem bietet eine hohe Geschwindigkeit und Kapazität, das genügend Reserven auch für die Anforderungen der Zukunft bereithält.
- CC-Link ermöglicht eine logische Topologie ohne Abhängigkeit von der physikalischen Topologie unter Verwendung der Token Passing Methode. Darüber hinaus bietet das System außerdem eine vereinfachte Fehlersuche.

Literaturhinweise:

[1] Yoshimoto, Yasuhiro: Increased productivity and energy-saving using 'e&eco-F@ctory', OHM, Vol.100, No.4, S.34-36 (Apr. 2013)
[2] Industrie 4.0 Working Group: 'Recommendations for implementing the strategic initiative INDUSTRIE 4.0' (Apr. 2013)
[3] Koren, Y.: 'The Global Manufacturing Revolution: Product-Process-Business Integration and Reconfigurable Systems,' Wiley Series in Systems Engineering and Management (2011)

Autor: ***Haruyuki Otani,***
Vorsitzender der technischen Arbeitsgruppe
der CC-Link Partner Association
www.clpa-europe.com/de_EU/

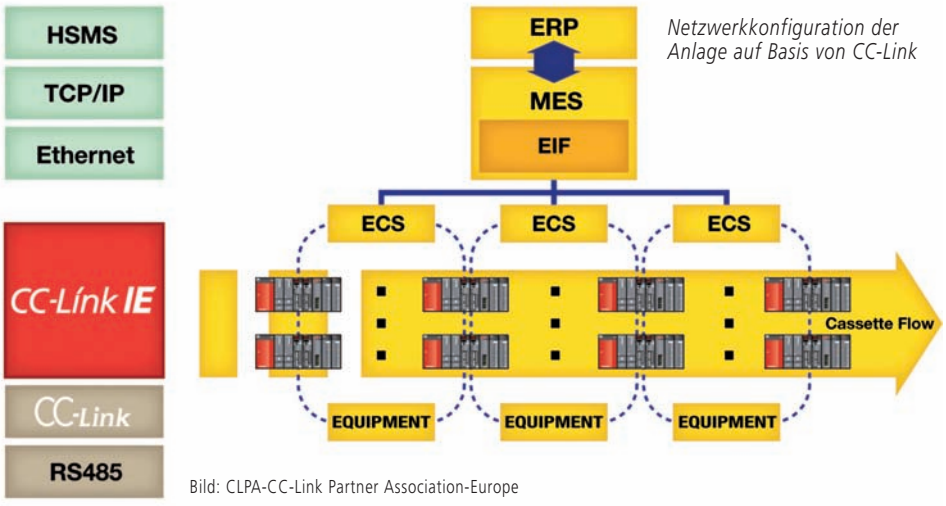
CC-Link ermöglicht höhere Produktivität für Hersteller von Flachbildschirmen

Die Produktion von Flachbildschirm-Displays hat sich in einer der größten Fertigungsanlagen in Asien ständig beschleunigt, um die immer steigenden Ansprüche zu bedienen. Der Prozess ist nun hoch automatisiert, weshalb die Datenkommunikation besonders entscheidend geworden ist. Die Wahl eines High-Speed-Ethernet-basierten offenen Automatisierungs-Netzwerkes, CC-Link IE, könnte zukunftsweisend für viele weitere Automatisierungsinstallationen in Asien und Europa sein.

Bild: CLPA-CC-Link Partner Association-Europe

Flachbild-Fernseher und -Monitore sind eines der am stärksten wachsenden Konsumgüter der letzten Jahre. Die Produktionskapazitäten sind hierfür genauso gewachsen wie die Anzahl der Produktvarianten. Logischerweise fordert der Preisdruck eine ständige Verbesserung in der Leistungsfähigkeit. All dies kann nur durch effektivere Kommunikation und Datenaustausch zwi-

schen den Fertigungsinseln, die eine Fertigungsanlage ausmachen, erreicht werden. Automatisierungsingenieure wissen aus Erfahrung, dass sich Verbrauchsgüteranlagen üblicherweise schrittweise weiterentwickeln, wenn sich der Kapazitäts-Bedarf erhöht. Deshalb muss sich die Steuerungsarchitektur oftmals mit diversen Subsystemen verbinden, was eine suboptimale Gesamtperformanz zur Folge hat. In der hier beschriebenen Fertigungsanlage kommt für die überlagerte Ebene (High-Level-Manufacturing Execution System sowie Enterprise Resource Planning-System) Standard Ethernet TCP/IP Ethernet zum Einsatz, während das Shopfloor-System Melsecnet/H von Mitsubishi Electric auf der Steuerungsebene einsetzt und für die Kommunikation den offenen Standard CC-Link verwendet. Während diese Architektur in der Vergangenheit der Anlage gut funktioniert hat, wurde deutlich, dass die Kapazität der Datenkommunikation und die Geschwindigkeit von Melsecnet/H hinter den heutigen Anforderungen zurück lag. Mehr noch war man der Meinung, dass Standard-Glasfaserkabel die Instandhaltung und Rekonfiguration erleichtern würden und zudem eine bessere Anschlussfähigkeit zu den verwendeten PC-Systemen bieten könnte. CC-Link IE basiert auf Gigabit-Ethernet. Es wurde aufgrund einer verbesserten Datenkapazität und -geschwindigkeit, der Verwendung von gewöhnlichen Glasfaserkabeln und besserer PC-Konnektivität als Verbesserung für das Kommunikationssystem ausgewählt. Von großer Bedeutung war außerdem, dass sich durch die Diagnosefähigkeit ebenfalls die Instandhaltung erleichtert. CC-Link ist ein offenes Industrienetz, das Baugruppen unterschiedlicher Hersteller ermöglicht, über ein einziges Netzwerk miteinander zu kommunizieren.



Netzwerkkonfiguration der Anlage auf Basis von CC-Link

Bild: CLPA-CC-Link Partner Association-Europe

Vorteile von CC-Link IE in der Anwendung

CC-Link ist in etlichen verschiedenen Formaten erhältlich, darunter CC-Link IE. Mit einer Übertragungsrate von 1Gbps ist CC-Link IE das schnellste momentan verfügbare Ethernet für die Vernetzung von multiplen Feldgeräten und Reglern. Als entscheidendes Element in industriellen Applikationen ist es vollkommen deterministisch und sichert volle Systemstabilität für kritische Fertigungsaufgaben. Seine fehlertoleranten Funktionen verbessern die Leistungsfähigkeit und Produktivität und verwenden weit verbreitete Standard-Glasfaserkabel und Verbindungsteile. Um die Einschränkungen durch das bestehende Steuerungssystem zu beseitigen, entschied man sich bei der Erweiterung und Modernisierung der hier beschriebenen Anlage dazu, die gesamte LCD-Fertigung auf ein CC-Link IE-Netzwerk aufzurüsten. Dies hat viele Vorteile, u.a. eine rechnerisch 40-fache Kommunikationsgeschwindigkeit zusammen mit einem achtfachen Anstieg bei der Datenkapazität. CC-Link IE benötigt keine spezielle Art von Glasfaserkabeln, sondern kann mit einem standardmäßigen 1000base-SX Standard-Glasfaserkabel installiert werden, wodurch die Installations-Kosten deutlich gesenkt werden. In einer großen Fertigungsanlage sind die Einsparungen an Material schon besonders maßgeblich, darüber hinaus ergibt sich ein entscheidender Vorteil aus der Erleichterung und Geschwindigkeit bei der Instandhaltung und Rekonfiguration. Dies wird noch gesteigert durch die verbesserte Diagnosefähigkeit und Vereinfachung der Systemarchitektur. Das Steuerungsnetz in der LCD-Fertigungsanlage hat nun einen einfachen Aufbau:

1. Die wichtigen Systeme wie das ERP und MES verwenden das Industrie-Standardprotokoll HSMS.
2. Shopfloor-Systeme, die Geräte steuern und Anlagen- und Produktionsstandortinformationen bereitstellen, sind auf CC-Link IE ausgerichtet.
3. Datenaustausch zwischen Geräten oder Anlagen-Hardware-Steuerungen basiert ebenfalls auf CC-Link IE oder CC-Link-Feldbus.

Zusammenfassung und Ausblick

Der Plan ist, dass es in naher Zukunft eine vollständige Integration von der Feldgerätebene bis in die Informationsebene des strategischen Managements mithilfe von CC-Link geben wird. Die LCD-Herstellung wird von Produktionsingenieuren in der asiatischen Fertigungsanlage als Möglichkeit gesehen, viele der technologischen Steuerungslösungen zukünftiger Produktionstechniken zu zeigen. Zu den zu erwartenden Trends gehört, dass viele Produktionsstätten nahezu unbesetzt sein könnten. Anstelle von standortspezifischem Personal werden Ferndiagnose und Überwachungstechnik schrittweise zur Norm werden. Netzwerke werden eine entscheidende Rolle in der Verwirklichung dieser Trends spielen und CC-Link steht an der Spitze dieses Vorsprungs.

Wesentliche Vorteile:

- achtfache Erhöhung der Datenkapazität
- einfachere Instandhaltung
- wesentlicher Anstieg der Kommunikationsgeschwindigkeit
- reduzierte Kabel-spezifische Kosten
- verbesserte Diagnosefähigkeit

CLPA und PI kooperieren bei Schaffung einer transparenten Netzwerkinfrastruktur

Bild: CC-Link Partner Association

Die CC-Link Partner Association und Profibus & Profinet International (PI) haben eine enge Zusammenarbeit bei der Förderung und Verbreitung von offenen Netzwerken für Industrieanwendungen angekündigt. Da immer mehr Anwender für die Implementierung von Fertigungssystemen basierend auf Industrie 4.0 oder dem Industrial Internet of Things (IIoT) bereit sind, ist die einfache Integration unterschiedlicher Netzwerke zu einem entscheidenden Faktor geworden. Die digitale Kommunikation über Feldbus oder Industrial Ethernet ist in modernen Fertigungswerken bereits weit verbreitet und ein wichtiger Baustein für eine steigende Produktivität. Die Nachfrage nach intelligenter Kommunikation wird infolge von Megatrends wie Industrie 4.0 und dem IIoT weiter wachsen. Die seit Jahren bestehende heterogene Landschaft der Industrial-Ethernet-Standards führt jedoch zu dem Problem, dass Geräte und Maschinen verschiedener Kommunikationssysteme untereinander nicht zum Datenaustausch in der Lage sind. Daher sind Maschinenbauer gezwungen, ihre Maschinen mit unterschiedlichen Netzwerktechnologien auszustatten, oder Anlagenbetreiber sind bei der Auswahl von geeigneten Maschinen entsprechend stark eingeschränkt. Um dies zu ändern, bedarf es herstellerspezifischer Übergabespezifikationen sowie komplizierter und maßgeschneiderter Wandler. Mit ihrer Kooperation wollen die CLPA und PI eine transparente und einfache bidirektionale Kommunikation zwischen CC-Link IE- und Profinet-Geräten über standardisierte Schnittstellen gewährleisten. Derzeit wird eine gemeinsame Arbeitsgruppe zusammengestellt, in der die entsprechenden erforderlichen technischen Spezifikationen entwickelt werden sollen. Wenn die Arbeiten an den Spezifikationen abgeschlossen sind, wird sie den Mitgliedern beider Organisationen zur Implementierung zur Verfügung gestellt. „Mit der CC-Link Partner Association konnten wir einen gleichwertigen Partner gewinnen, dessen Netzwerke weltweit in zahlreichen Branchen eingesetzt werden“, sagte der Vorstandsvorsitzende von PI, Karsten Schneider. „So profitieren die Anwender von der größtmöglichen Flexibilität, wenn sie ihre IIoT-, Industrie 4.0- oder e-F@ctory-fähigen Systeme gestalten“, erklärte Naomi Nakamura, Global Director von CLPA. „Mit dem kombinierten weltweiten Netzwerk an Vertretungen von CLPA und PI sowie den zahlreichen verfügbaren Geräten von Mitgliedern beider Organisationen können wir für unsere Mitglieder weitere Märkte erschließen. Demzufolge werden CC-Link IE und Profinet noch schneller wachsen.“ ■

Firma: ***CC-Link Partner Association***
www.clpa-europe.com

Spitzenleistung in Tiefziehmaschine mit Melsec L-Serie

Bild: VC999 Packaging Systems

Bild 1: Die Steuerung der Hochleistungs-Tiefziehmaschine der i-Serie von VC999 Packaging Systems übernimmt eine Mitsubishi Electric SPS der Melsec L-Serie. Dazu kommt das Ethernet-basierte industrielle Netzwerk CC-Link IE zum Einsatz – das branchenweit erste und schnellste Ethernet-basierte Gigabit-Netzwerk.

Um möglichst leistungsstarke Anwendungen adressieren zu können, setzte VC999 Packaging Systems bei der Entwicklung ihrer Hochleistungs-Tiefziehmaschine der i-Serie auf ein innovatives, modulares Maschinendesign. Es sorgt für hohe Anlagenflexibilität und eine einfache Bedienung, sodass auf einer Maschine unterschiedliche Kunststoffschalen und Blisterverpackungen produziert werden können. Voraussetzung für eine leichte Montage und Demontage war eine Standardverkabelung zwischen den Maschinensegmenten. Um eine umfassende Gewährleistung übernehmen zu können, waren zudem zuverlässige 'Best-in-Class'-Automatisierungskomponenten notwendig.

VC999 Packaging Systems U.S.A., Teil der Inauen Group, wurde bereits 1986 gegründet. Der Unternehmenssitz befindet sich samt Vertrieb, Fertigung und Service in Herisau, in der Schweiz. Schon früh setzte das Unternehmen den industrieweiten Trend modularer Maschinenkonzepte um und ermöglichte den flexiblen Anlagenauf- und -abbau für den regulären Betrieb sowie für Transport und Reinigung. Das modulare Design der i-Serie umfasst die drei Hauptsegmente Formung, Versiegelung und Auswurf, die jeweils über ein eigenes Gehäuse für die Steuerungen verfügen. Auswahlkriterien für die Steuerungen waren eine einfache Installation, Verkabelung und Anpassung, um den Entwicklungsaufwand für Anlagenbediener und Wartungspersonal zu reduzieren. Um die optimale Lösung zu finden, die die Anforderungen an Verbindungsflexibilität, Hochleistungsbetrieb und zuverlässige Steuerung erfüllt, verglich VC999 mehrere Steuerungsanbieter für die Industrieautomatisierung.

Melsec L-Serie erste Wahl

Die Wahl fiel auf die modulare SPS der Melsec L-Serie von Mitsubishi Electric. Die Steuerung verfügt über ein vielseitiges, Baugruppenträger-freies, erweiterbares Design. Die Datenübertragung läuft über CC-Link IE Field, das branchenweit erste und schnellste Ethernet-basierte Gigabit-Netzwerk. Die standardmäßige Ethernet-Verkabelung über CC-Link IE Field erlaubt eine einfache Anwendung bei hoher Kosteneffizienz, wodurch sich letztlich das modulare Maschinendesign realisieren lässt. Power Motion, Inc., langjähriger strategischer Partner von VC999 und Lieferant von Automatisierungskomponenten, leistete bei der Anbindung der Melsec L-Serien SPS an Mitsubishi Electric MR-J3 Servosysteme sowie an FR-E700-Frequenzumrichter Unterstützung. Die Servomotoren kommen bei der Indexsteuerung des Auswurfs zum Einsatz, während die Umrichter die Zusatzachsen antreiben. Ein weiterer Servomotor hält die Folienspannung am Folien-Einzugssys-

tem aufrecht und sorgt für einen vereinfachten Mechanismus, sodass keine Trapezrollen nötig sind. Das Ergebnis ist ein modulares, leistungsstarkes Design. Tom Fritz, Electrical Engineering Manager bei VC999, erklärt: „Die Tiefziehmaschine der i-Serie läuft auf einer sehr stabilen und bewährten Steuerungsplattform, die dazu beiträgt, unseren Kunden die für sie nötige Flexibilität zu bieten." Das Industriel-Ethernet-Netzwerk CC-Link IE Field verbessert die Gesamtanlageneffektivität der Maschine durch eine besonders hohe Übertragungsgeschwindigkeit und punktet zusätzlich mit reduzierten Verdrahtungs- und Installationszeiten.

Qualität ist Key

Dank der hohen Qualität der Mitsubishi Electric Hardware kann die Tiefziehmaschine der i-Serie mit einer Garantie von zwei Millionen Durchläufen geliefert werden. Diese umfassende Gewährleistung ist ein Beleg für die marktführende Position von VC999 in der Entwicklung hochmoderner Verpackungsmaschinen.

Hinweis:

Erfahren Sie, wie Mitsubishi Electric die Automatisierungsanforderungen von heute erfüllen kann:
de3a.mitsubishielectric.com/fa/de/solutions ■

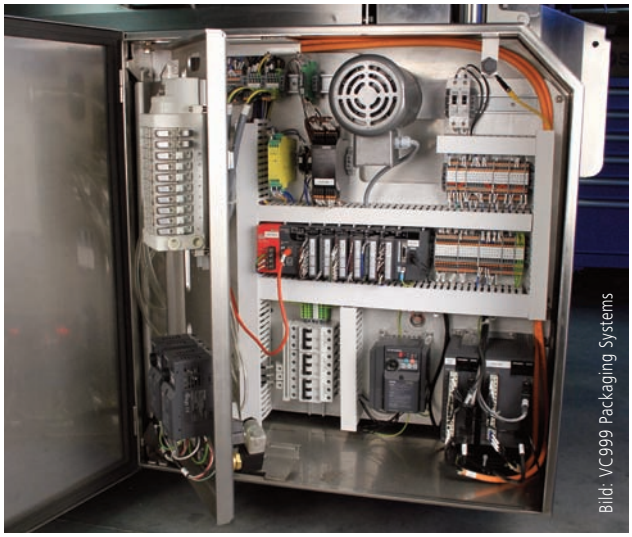


Bild 2: Schon früh setzte das Unternehmen den industrieweiten Trend modularer Designkonzepte um und ermöglichte den flexiblen Anlagenauf- und -abbau für den regulären Betrieb sowie für Transport und Reinigung.

Firma: ***Mitsubishi Electric Europe B.V.***
de3a.mitsubishielectric.com/fa/de/solutions

CC-Link IE und A800-Antriebstechnik modernisieren chinesische Reifenproduktion

Modernisierung für heute und morgen

Seit 2006 befindet sich die chinesische Reifenindustrie in einer rasanten Entwicklung. Basierend auf den statistischen Daten der 'China Rubber Industry Association' stieg die Anzahl produzierter Reifen in China von 112.400.000 im Jahr 2000 auf 630.000.000 in 2014. Das ist mehr als ein Drittel der weltweiten Produktionsmenge und China ist damit der größte Reifenproduzent, -exporteur und -konsument. Neben der Quantität spielt heute die Qualität sowie die Wertschöpfungstiefe eine bedeutende Rolle. Der vorliegende Beitrag erläutert, wie Mitsubishi Electric einen führenden Reifenproduzenten mit einer umfangreichen Automatisierungslösung dabei unterstützt, diese hohen Anforderungen zu bewältigen.

Mit dem Fokus auf der Realisierung umfassender e-F@ctory-Fabrikautomation und der Intregration von Fertigungsautomatisierungs-Produkten bietet Mitsubishi Electric seinen Kunden integrierte Lösungen und Beratung sowie Austausch und erweitertes Post-Sales-Training, Bildung und technischen Support. In dem hier beschriebenen Projekt waren die technischen Vorteile des Automatisierungssystems wegweisend für die Modernisierung bei einem führenden chinesischen Reifenhersteller.

CC-Link IE in der Anwendung

Von dem in der Reifenherstellung und den Produktionsprozessen involvierten Equipment sind Verbundmaterial-Extrusion- und Kalander-Anlagen die Anlagenteile, bei denen die Übertragungslänge am größten ist und gleichzeitig das höchste Datenvolumen und die größte Anzahl an Stationen aufkommt. Die Präzision bei den hergestellten Halbfabrikaten spielt gleichzeitig eine entscheidende Rolle bei der Qualität des fertigen Reifens,

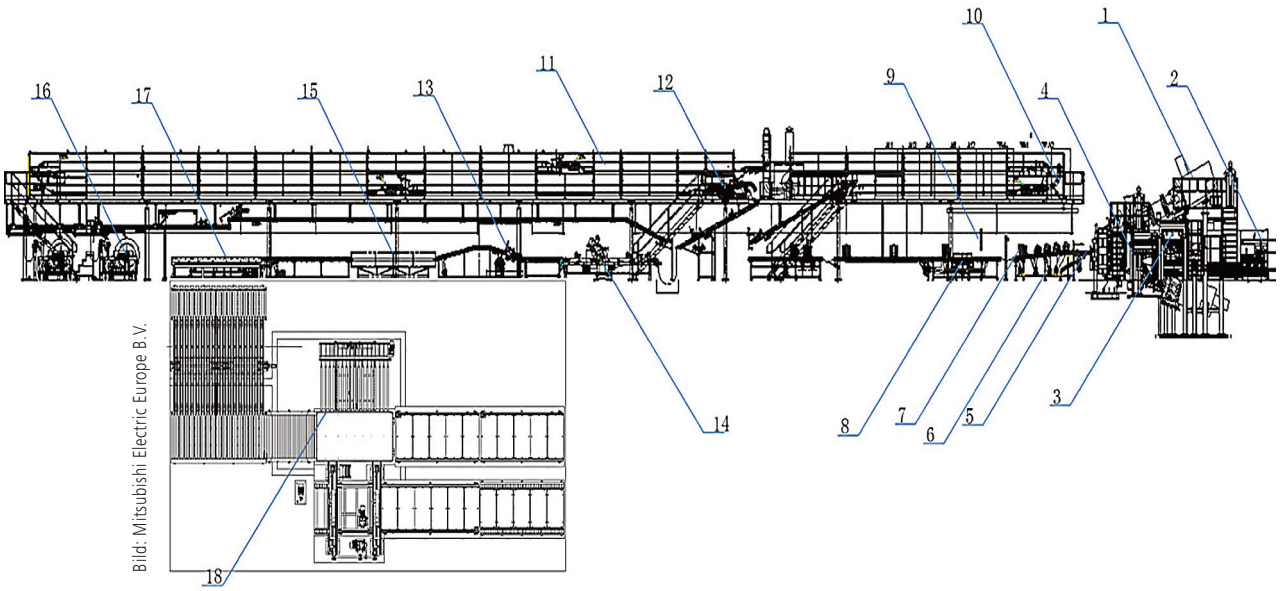


Bild 1: Eine Verbundmaterial-Extrusionsanlage besteht aus zwei Hauptkomponenten, der Extrusionseinheit und einem Kühlband. Die Extrusionseinheit besteht aus dem Extruder (1), der Extrudernase mit Hydraulikdruck-Station (4), der Zuführung (3) und der Wärmeregulierungseinheit (2). Das Kühlband besteht aus der Übertragungsbaugruppe (5), der Aufrolleinrichtung (6), der Markierungseinheit (7), einem Breite-Messgerät (9), einer kontinuierlich-wiegenden Einheit (11), primären und sekundären Ventilatoren (12, 13), Fixlänge-Schneidern (14), Geräten zur Endkontrolle und zum Wiegen (15), Wickelvorrichtungen (16), Sammlern für Abfallprodukte und automatischen Kollektoren.

z.B. bei der Ebenheit und dem dynamischen Gleichgewicht. Die Qualität der Reifen-Halbfabrikate ist die Voraussetzung für die Realisierung der endgültigen Automatisierung und einer hohen Qualität der Endbearbeitung. Daher genießen die Steuerungs- und Antriebssysteme dieser Anlagen eine hohe Aufmerksamkeit. CC-Link IE – das GBit-Ethernet-basierte Netzwerk für die Fertigung – ist hier ideal geeignet, da es die Anforderungen hinsichtlich Geschwindigkeit/Determinismus, Datenübertragungsvolumen, Zuverlässigkeit, Wartungs- und Diagnosefähigkeit sowie Integration anderer Netzwerke spielend erfüllt.

Anforderungen der Kunden

Verbundmaterial-Extrusions- und Kalandrierungs-Produktions-Anlagen sind vorbereitende Verbindungen in der Reifenproduktion. Während der Produktion von Gummireifen werden diese Anlagen zur kontinuierlichen Herstellung von Gummi-Halbfabrikaten einer bestimmten Form (Profile, Seitenwände etc.) genutzt. Genau wie sich die Gummitechnologie und die Automatisierung der Reifenindustrie kontinuierlich weiterenwickeln, werden auch die Voraussetzungen betreffend der Homogenität, Stabilität der Dimensionen und Toleranz von extrudierten und kalandrierten Produkten immer anspruchsvoller. Vor diesem Hintergrund und basierend auf der Industrial Ethernet Gigabyte-Kommunikationsrate gewährleistet das offene CC-Link IE-Netzwerk mit den Frequenzumrichtern A800 eine optimale Steuerung, was in der Anwendung nachgewiesen werden konnte.

Anforderungen aus der Anwendung

Im Extruder und der Kalandrierungsanlage sind die Anforderungen an die Echtzeitkommunikation und die Präzision der Steuerungs- und Antriebstechnik für die Qualität und die Quantität von entscheidender Bedeutung. Im Extruder ist die Stabilität von einzuspeisendem Material der wichtigste Einflussfaktor. Daher ist der Beschickungsvorgang durch einen Drucksensor in der Nase des Extruders gesteuert. Eine Veränderung im Kanaldruck der Extruderspitze kann zum Extruder zurückgeleitet und durch Anpassung der Schneckendrehzahl kompensiert werden. Da jeder Extruder unabhängig gesteuert wird, kann die Stabilität des Gummiausstoßes und des halbfertigen Produktes garantiert werden, wenn der Druck in der Nase stabil gehalten wird. Darüber hinaus können durch ein kontinuierliches Wiegesystem Veränderungen in die Steuerung der Produktionslinie zurückgekoppelt und die Geschwindigkeit angepasst werden. Dadurch ist es möglich, homogene Halbfabrikate mit passendem Qualitätsanspruch des Nutzers zu produzieren. In der Kalander-Anlage sind die Hauptvoraussetzungen eine in jeder Zugzone stabile Materialspannung. Es gibt vier Zugzonen. Dabei handelt es sich um den Stahldraht-Bereich, wo Stahldraht in die Hauptmaschine abgewickelt wird (Spulengatter-Raum), das Hauptzugzonen-Gebiet zwischen der Hauptmaschine und dem Kühlband, die Lagerungs-Zugzone zwischen dem Kühlband und der Traktion sowie die Wicklungszone zwischen der Traktionseinheit und der Wickeleinheit. Für jedes Produkt in der Stahldraht-Zugzone sind die OS- und DS-Seiten im Grunde die selben. In der Haupt- und Lagerungs-Zugzone ist die OS-Seite lockerer als die DS-Seite. In der Wicklungszugzone ist die OS-Seite straffer als die DS-Seite. Die Kalandrierungsspannung ist hauptsächlich durch die Diferenzgröße der Übertragungsgeschwindigkeit der beiden elektronischen Maschinen bestimmt. Daher spielt das Steuerungssystem eine deterministische Rolle in der Spannungsjustierung und es ist eine Voraussetzung, dass die Geschwindigkeit jedes Elektromotors automatisch auf Basis der Fördergeschwindigkeit abgestimmt werden kann – mit automatischer Feinabstimmung basierend auf der tatsächlichen Spannung. Zusätzlich wird der Rollenabstand während des Produktionsprozesses unter Bei-

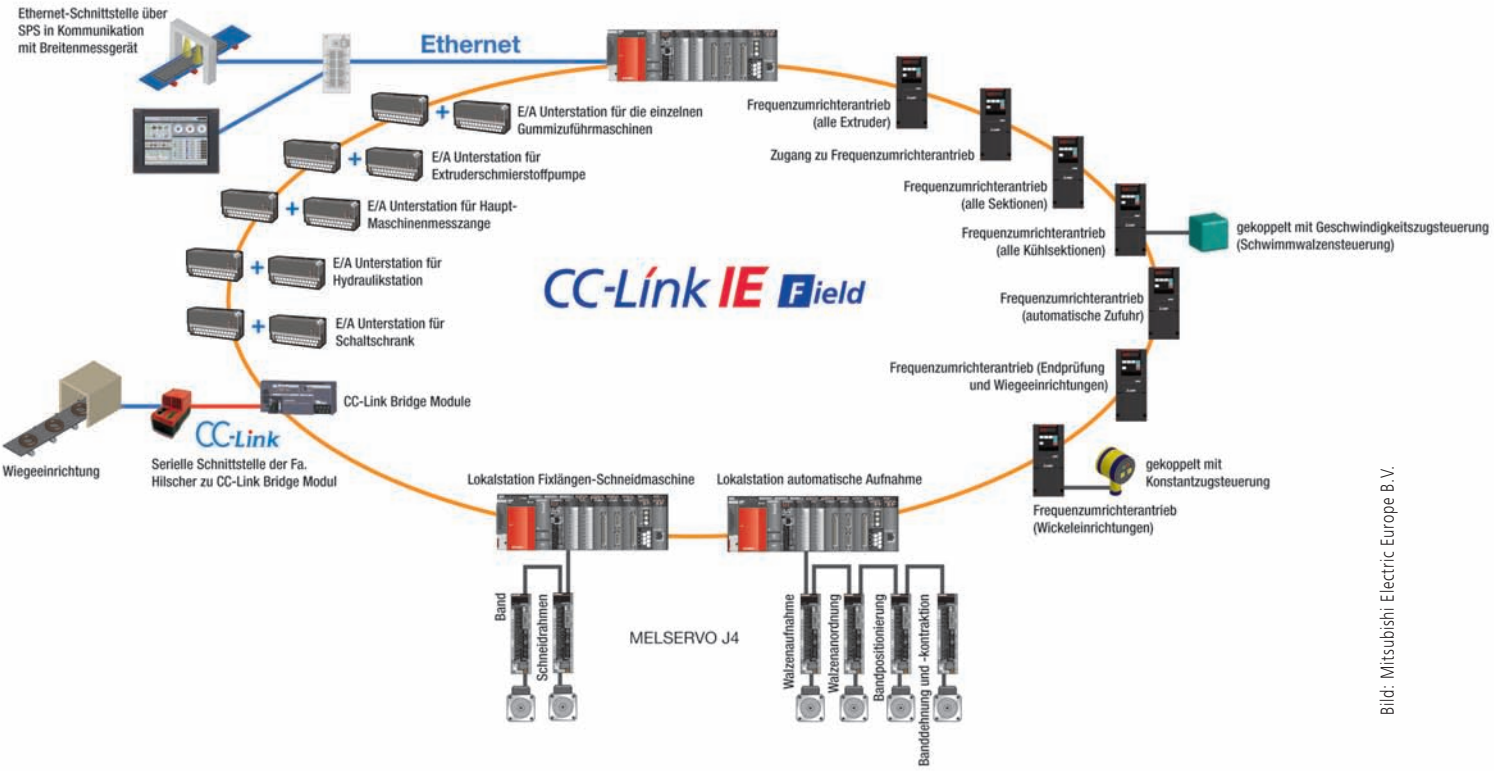


Bild: Mitsubishi Electric Europe B.V.

Bild 2: Diagramm des Extrusionslinien-Systems für Verbundmaterial

behaltung der Konformität von Produktbreite und festgelegter Breite automatisch kalkuliert. Es ist ebenfalls nötig, dass Energie- und Antriebssysteme hochperformante Kalkulation und Reaktionsgeschwindigkeit sowie stabile Netzwerk-Kommunikation mitbringen.

Vorteile von CC-Link IE

Die Kommunikationsgeschwindigkeit von CC-Link IE beträgt 1Gbps. 120 Stationen können in einem einzelnen Netzwerk miteinander kommunizieren, die maximale Anzahl von Netzwerken beträgt 239. Bei Anwendung von Multimode-Glasfasern liegt die maximale Distanz zwischen den Stationen bei 550m. Bei Dual-Loop-Topologien beträgt die maximale Übertragungskapazität 1920Bytes. CC-Link IE ist ein Real-Time-Industrienetzwerk und die Reaktionszeit der Verbindungen kann durch einfache Kalkulation ermittelt werden. Die Automatisierungs-Produkte von Mitsubishi können nicht nur die bestehende Netzwerkkonfiguration in eine Ring-Topologie bringen, wodurch die Auswirkungen von Kommunikationsfehlern reduziert wird, sondern sie unterstützen darüber hinaus Stern- und Linien-Topologien sowie Kombinationen.

Vorteile der Antriebstechnik

Im CC-Link IE-Netzwerk des Reifenherstellers kamen Frequenzumrichter-Antriebe des Typs FR-A800 von Mitsubishi Electric (FR-A800-R2R) zum Einsatz. Hier konnten sie ihre leistungsfähigen Funktionen in der Extrusions- und Kalanderanlage beweisen, schießlich sind Antriebsgenauigkeit und -synchronität sowie Echtzeitfähigkeit von entscheidender Bedeutung für die Produktqualität. Von großem Vorteil waren auch die vorgefertigten Funktionen des FR-A800-Antriebs. Er kombiniert eine spezialisierte Geschwindigkeitsanpassung mit Aufwicklungsfunktionen, wie Geschwindigkeits-Spannungs-Reglung, Drehmoment-Spannungs-Reglung (mit Spannungstest), konstante Zugspannungsreglung (ohne Spannungstest), Rollendurchmesserkalkulation, vorbereitende Rollendurchmesser-Kalkulierung, Rollendurchmesser-Speicher, Wicklersteuerung, automatische Einstellung von Geschwindigkeitszunahme, Short Line Detection, Trägheitskompensation und Aufnahmefunktion der Materiallänge. Da die externen Analogsignale sowie die Steuerungsfunktionen komplett im A800 integriert sind, reduziert dies die Anzahl der SPS-Prozesse sowie die Netzwerkkommunikation.

Fazit

Die Kombination eines CC-Link IE-Netzwerkes und den Produkten von Mitsubishi Electric ergab bei einem der führenden chinesischen Reifenhersteller eine umfassende Lösung. Es konnte gezeigt werden, dass die Kombination von Echtzeitkommunikation auf Basis von CC-Link IE zusammen mit hochgenauer Antriebstechnik eine Lösung ergibt, auf dessen Basis die Anforderungen des Kunden erfüllt werden können und die noch genügend Reserven mitbringt, um auch zukünftigen Anforderungen gerecht zu werden. ■

Open automation network technology leader | CC-Link IE

Das einzige offene Gigabit-Ethernet – bereit für Industrie 4.0

Bereit für Industrie 4.0 mit dem weltweit einzigen **offenen Gigabit-Ethernet.**
CC-Link IE ist das einzige offene Gigabit-Ethernet und hat sich in anspruchsvollen Anwendungen bewährt.

- Maximale Bandbreite für Industrie-4.0-Anwendungen
- Offene Entwicklung und Produkt-Support
- **NEU**: CC-Link IE Field Network Basic verfügbar für 100Mbit Geräte

partners@clpa-europe.com | www.clpa-europe.com

CC-Link IE wird von führenden Automatisierungsanbietern unterstützt:

SCHAEFFLER (LuK, INA, FAG) · BALLUFF · HMS · RENESAS · HARTING · MITSUBISHI ELECTRIC Changes for the Better · COGNEX · molex one company > a world of innovation · CONDUCTIX wampfler · PHOENIX CONTACT · HELUKABEL · Weidmüller · BELDEN SENDING ALL THE RIGHT SIGNALS

CC-Link CLPA PARTNER ASSOCIATION
OPEN AUTOMATION NETWORKS

SPS/IPC/Drives 2016
Halle 2, Stand 2-540

sps ipc drives

CC-Link
CC-Link IE

Integration von Smart Devices über Wireless LAN in das Maschinennetzwerk

Industriespezifische Besonderheiten beachten

Bild: Phoenix Contact Deutschland GmbH

Immer mehr Maschinenhersteller bieten ihren Kunden die Nutzung von Smart Devices – wie Tablets oder Datenbrillen – an den Maschinen an.

Werden Smart Devices wie Tablets, Smartphones oder Datenbrillen an Maschinen verwendet, bieten sie dem Anwender vielfältige Vorteile. Daher stellen immer mehr Maschinenbauer entsprechende Lösungen zur Verfügung. Doch was gilt es bei der Auswahl der notwendigen Access Points zu beachten?

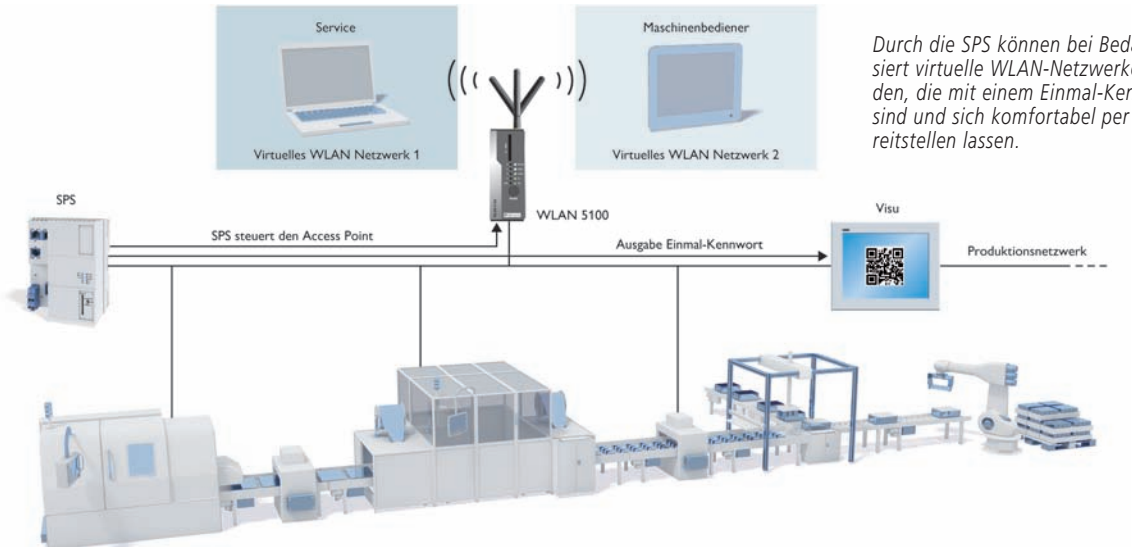
Auf den ersten Blick scheint die kommunikative Anbindung von Smart Devices an die Maschine – meist über Wireless LAN – unkritisch sowie einfach realisierbar zu sein. Dies, weil die jeweilige Anwendung häufig nicht prozessrelevant ist und es keine besonderen Anforderungen an die Echtzeitfähigkeit gibt. Deshalb integrieren einige Maschinenbauer einen simplen WLAN Access Point in ihre Applikation. Selbst wenn das Gerät funktioniert, lässt sich die Aufgabenstellung auf diese Weise nicht umsetzen. Denn Maschinen und Anlagen sind durch Besonderheiten gekennzeichnet, die bei der Erarbeitung des Lösungskonzeptes und der Auswahl der Funkkomponenten unbedingt berücksichtigt werden müssen.

Funktechnologie bereits in die Devices integriert

Smart Devices können für ganz unterschiedliche Anwendungen genutzt werden. Die Geräte kommen beispielsweise immer öfter zur visuellen Onlineunterstützung von Wartungsarbeiten zum Einsatz. Über die in das Smart Device eingebaute Kamera kann der in der Zentrale des Maschinenbauers befindliche Servicetechniker genau das sehen, was der Maschinenbediener vor Ort betrachtet. Auf dem Bildschirm des Gerätes stellt er dem Bediener anschließend Informationen zur Behebung der Störung bereit. Darüber hinaus eröffnen Smart Devices auch während des Maschinenbetriebes zahlreiche Vorteile. Diese reichen von der Anzeige von Betriebsdaten und Warnmeldungen über die Hilfestellung zur einfacheren und schnelleren Einrichtung der Maschine bis zum intelligenten Assistenzsystem, mit dem sich Bedienungsabläufe verbessern lassen. Zum Datenaustausch zwischen Smart Device und Maschine wird in der Regel Wireless LAN verwendet, da diese Technologie weitgehend akzeptiert und bereits in alle Smart Devices integriert ist. Zudem bietet Wireless LAN eine hohe Übertragungsgeschwindigkeit. Das ermöglicht eine flüssige Darstellung der Daten und die Weiterleitung hochauflösender Videodaten. Der Aufbau eines lokalen Wireless LAN-Zuganges zum Maschinennetzwerk erweist sich eigentlich als einfach. Prinzipiell reicht ein im Schaltschrank montierter handelsüblicher WLAN Access Point aus, der um eine außen am Schrank angebrachte günstige Antenne ergänzt wird. Vergibt der Anwender dann noch ein sicheres Passwort für das WLAN-Netzwerk, steht dem Betrieb der Funklösung nichts entgegen.

Konsequenzen eines unbefugten Netzwerkzugriffes

Stellt sich die Frage, ob ein solch gängiger Ansatz genügt, selbst wenn es keine betriebskritische Anwendung ist. Leider agieren viele Betreiber in der beschriebenen Form und beachten daher



Durch die SPS können bei Bedarf automatisiert virtuelle WLAN-Netzwerke aktiviert werden, die mit einem Einmal-Kennwort gesichert sind und sich komfortabel per QR-Code bereitstellen lassen.

Bild: Phoenix Contact Deutschland GmbH

wesentliche Punkte nicht, die später zu einem Sicherheitsrisiko oder Unzufriedenheit des Nutzers führen können. Vor diesem Hintergrund sollten die folgenden Aspekte zwingend bei der Konzeption der Wireless LAN-Lösung und der Auswahl der notwendigen Komponenten berücksichtigt werden:

- sicheres, am besten automatisiertes Passwortmanagement
- durchgängig guter Empfang
- Funkzulassungen für den jeweiligen Aufstellungsort der Maschine.

Üblicherweise handelt es sich bei einem Maschinennetzwerk um ein relativ kleines sowie in sich geschlossenes Netz, zu dem unbekannte Nutzer keinen Zugang benötigen und erhalten. Wird das Maschinennetzwerk jedoch um eine WLAN-Schnittstelle zur Kommunikation mit Smart Devices erweitert, können die unbekannten Nutzer auf das Netz zugreifen. Aufgrund der Funktechnik müssen sie dazu noch nicht einmal vor Ort sein. Denn weil sich Funkwellen lediglich schwer räumlich begrenzen lassen, ist sogar ein Zugriff von außerhalb des Betriebsgeländes möglich. Ein unerlaubtes Eindringen in das Netzwerk kann erhebliche negative Konsequenzen nach sich ziehen. Schäden entstehen dabei nicht nur durch die Störung der Datenübertragung oder die Manipulation von Geräten. Sind Safety-Systeme mit dem Maschinenetz verbunden, könnte sie beeinflusst werden, sodass schlimmstenfalls Personen zu Schaden kommen. Sofern die Maschinen außerdem ungesichert an das Produktionsnetzwerk angekoppelt sind, hat ein Eindringling möglicherweise Zugriff auf sämtliche Maschinen und Systeme dieses überlagerten Netzes. In diesen Fällen reicht die übliche Absicherung des WLAN Netzwerkes mit einem Passwort nicht aus. Beim Einsatz von Wireless-LAN in Maschinennetzen ist ein umfassendes Sicherheitskonzept vielmehr unabdingbar.

Verwaltung der Passwörter als Herausforderung

Die in Maschinen- und Anlagennetzen genutzten Wireless LAN-Systeme werden oftmals über einen gemeinsamen statischen Netzwerkschlüssel geschützt. Der Mechanismus wird als WLAN WPA-PSK (Wi-Fi Protected Access Pre Shared Key) bezeichnet. Erweist sich das Passwort (Netzwerkschlüssel) als sicher, ist die Funkkommunikation ebenfalls nach dem aktuellen Stand der Technik abhör- und manipulationssicher. Die wesentliche Herausforderung bei einem Maschinen-WLAN liegt in der Verwaltung des Passwortes. Verwenden mehrere Mitarbeiter das Funknetzwerk, melden sie sich mit demselben Passwort an. Egal wie sicher dieses gewählt ist: Da das Passwort von allen Nutzern benötigt wird, kennt es ein größerer Personenkreis nach relativ kurzer Zeit. Und weil Passwörter in der Praxis meist nie geändert werden, haben die Mitarbeiter auch dann noch Zugriff auf das Maschinenetzwerk, wenn sie gar nicht mehr dazu befugt sind. Darüber hinaus findet keine Unterscheidung zwischen den einzelnen Nutzern statt. Jeder erhält uneingeschränkten Zugang zum gesamten Netz – gleich ob Servicetechniker oder Maschinenbediener. Die zentrale Frage ist deshalb, wie sichergestellt werden kann, dass lediglich berechtigte Nutzer Zugriff auf das Netzwerk und die dort festgelegten Ressourcen haben. Für jeden Nutzer individuelle Kennwörter und Zugriffsrechte einzurichten – wie im Office-Netzwerk üblich – zeigt sich aufgrund des administrativen Aufwandes und der zusätzlich erforderlichen Infrastruktur als nicht praktikabel und unwirtschaftlich.

Steuerung des Access Points durch die SPS

Ein automatisiertes Kennwortmanagement, das durch die Maschinensteuerung erfolgt, könnte eine Lösung sein. Dazu ist allerdings ein WLAN Access Point notwendig, der von der Maschinen-SPS über das Netzwerk gesteuert werden kann. Indem die Steuerung nutzergruppenspezifische WLAN-Zugänge (virtuelle Access Points) kontrolliert ein- und ausschaltet sowie verbindungsspezifische Einmal-Kennwörter genutzt werden, lässt sich der drahtlose Zugang zum Maschinennetzwerk sicher gestalten. Um sich mit ihr verbinden zu können, informiert der Anwender die Maschine etwa durch die Anmeldung an einem stationären Bedienterminal. Die Steuerung konfiguriert anschließend einen speziellen WLAN-Zugang (virtuellen Access Point) am Access Point, der durch ein Einmal-Kennwort geschützt ist. Das Einmal-Kennwort wird dem Nutzer über das Bedienterminal in Klartext oder komfortabel als QR-Code zur Verfügung gestellt. Alternativ wäre eine Übermittlung per NFC möglich. Da das Einmal-Kennwort nach der Trennung der WLAN-Verbindung seine Gültigkeit verliert, ist dessen Weitergabe kein Sicherheitsrisiko (Bild 2).

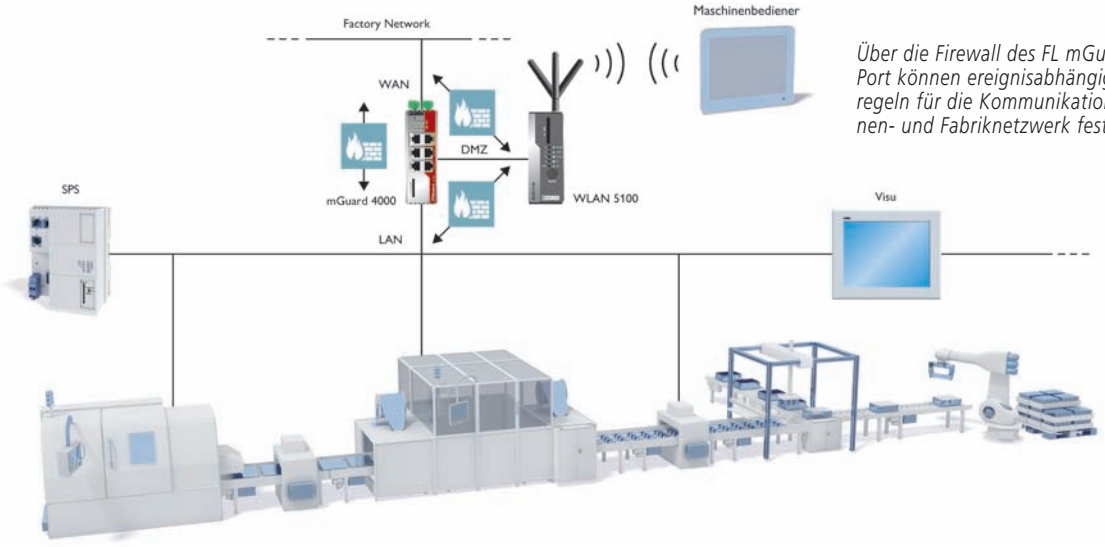


Bild: Phoenix Contact Deutschland GmbH

Über die Firewall des FL mGuard 4000 mit DMZ-Port können ereignisabhängig individuelle Filterregeln für die Kommunikation mit dem Maschinen- und Fabriknetzwerk festgelegt werden.

Firewall mit DMZ-Port bei umfangreichen Filterregeln

Durch verschiedene nutzergruppenspezifische Zugangspunkte (virtuelle Access Points) mit unterschiedlichen Zugangsberechtigungen lässt sich der Zugriff auf die Netzwerkressourcen nutzerabhängig sicher regeln. Beispielsweise kann der Servicetechniker keinerlei Einschränkungen beim Zugang zum Maschinennetzwerk unterliegen, während der Maschinenbediener nur auf den Visualisierungsserver zugreifen kann. Zu diesem Zweck muss der Access Point konfigurierbare Filterfunktionen unterstützen. Sind umfangreiche Filterregeln erforderlich, die sowohl den Zugriff auf das überlagerte Produktions- als auch das Maschinennetz individuell organisieren, bietet sich der Einsatz einer Firewall mit DMZ-Port (Demilitarized Zone – ent- oder demilitarisierte Zone) – wie der FL mGuard 4000 von Phoenix Contact – an. Der WLAN Access Point wird dann an den DMZ-Port angeschlossen. Diese Lösung erweist sich als besonders interessant, wenn der Anwender aus Sicherheits- oder Fernwartungsgründen bereits ein VPN-Firewall-Konzept (Virtual Private Network) auf Basis der Security Appliances FL mGuard in der Maschine verwendet (Bild 3).

MiMo-Antennentechnik für guten Empfang

Die Anforderung, dass die WLAN Access Points überall für einen guten Empfang sorgen sollen, klingt banal, stellt aber in der Praxis ein häufiges Problem dar. Weil die Anwendung nicht prozessrelevant ist, wird versucht die Kosten so gering wie möglich zu halten und daher an der Qualität der verbauten Komponenten – speziell der Antennentechnik – gespart. Eine einfache und dazu an einer funktechnisch ungünstigen Position montierte Antenne führt in Kombination mit der meist reichweitenschwachen Funktechnik der Smart Devices zu einem geringen Empfangssignal in den verschiedenen Bereichen rund um die Maschine. Hier treten nun deutliche Leistungseinbußen und damit längere Ladezeiten der Daten oder sogar Unterbrechungen auf. Selbst wenn die Anwendung nicht prozessrelevant ist, kann eine solche Situation den Nutzer verärgern. Vor diesem Hintergrund sollte schon bei der Planung und Umsetzung auf eine gute Funkleistung der WLAN-Lösung geachtet werden. Eine qualitativ hochwertige und robuste Industrieantenne ist teuer, jedoch langfristig gesehen eine lohnende Investition. Bei der Wahl des WLAN Access Points zeigt sich ein leistungsfähiges Industriegerät gemäß IEEE802.11n mit MiMo-Antennentechnologie (Multiple Input Multiple Output) als eine geeignete Alternative. Die MiMo-Technik sorgt nicht nur für eine Steigerung der Datenrate, sondern im stark reflektierenden metallischen Industrieumfeld zudem für eine höhere Stabilität und Zuverlässigkeit des Funkempfanges. Sie erfordert allerdings den Einsatz von zwei oder mehr Antennen.

Funkzulassung in den Betriebsländern

Darüber hinaus spielt die Funkzulassung eine wichtige Rolle, denn die Maschinen werden oftmals exportiert. Zum Betrieb eines Funksystems müssen die entsprechenden Genehmigungen des jeweiligen Betriebslandes eingehalten werden, die teuer sind. Deshalb verfügen vor allem die preiswerten Funkgeräte lediglich über eine Zulassung für den Betrieb in Europa und Nordamerika. Der Anwender muss bei der Auswahl der WLAN-Komponenten also darauf achten, welche Länderzulassungen vorliegen und ob die Einholung weiterer Genehmigungen bei Bedarf möglich ist. Werden die aufgeführten Aspekte – passendes Sicherheitskonzept, gute Funkleistung und Zulassungen für alle relevanten Betriebsorte – bei der Konzeption der WLAN-Schnittstelle berücksichtigt, steht einer langfristig sicheren Nutzung der Wireless-Lösung nichts im Weg. Es müssen jedoch leistungsstarke industrielle Access Points gemäß IEEE802.11n mit MiMo-Unterstützung verwendet werden, die sich durch die Maschinensteuerung kontrollieren lassen. Der WLAN Access Point 5100 von Phoenix Contact erfüllt die Anforderungen und bietet ferner spezielle Funktionen für den Einsatz an der Maschine. ■

Autor: *Dipl. Ing. (FH) Jürgen Weczerek,*
Product Marketing Network Technology
Phoenix Contact Electronics GmbH
Bad Pyrmont
www.phoenixcontact.de

Halle 10.0
Stand 322C,
Halle 9
Stand 310
sps ipc drives

Schalten, schützen und kommunizieren

Die neue Ära der Energieverteilung

Bild: Schneider Electric GmbH

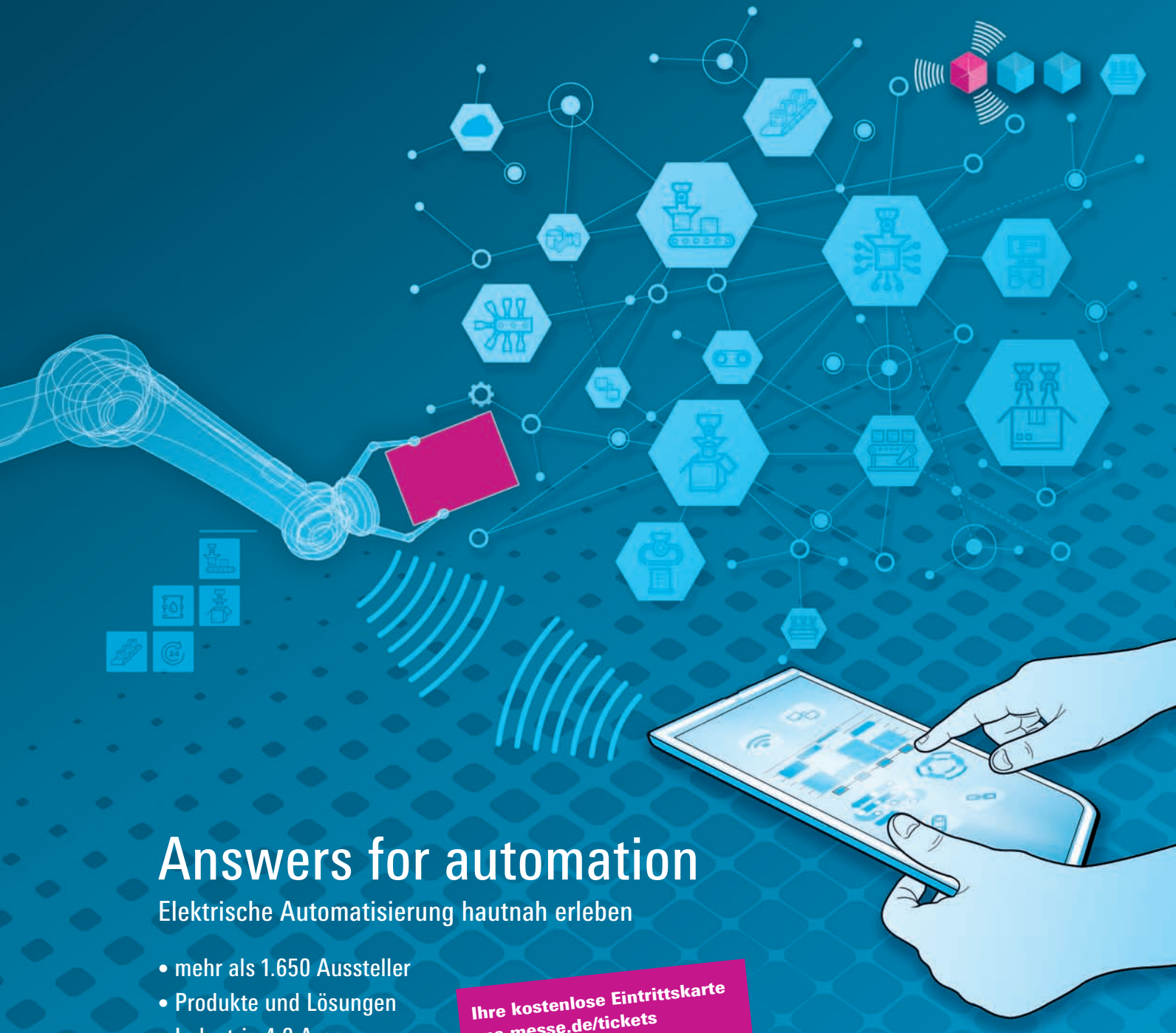
Mit dem Leistungsschalter lassen sich alle kritischen Informationen zu Schutz, Messungen, Diagnostik und Wartung auf einem Mobilgerät abrufen.

Der Leistungsschalter Masterpact MTZ von Schneider Electric bietet integrierte, drahtlose Kommunikationsfunktionen über Bluetooth und NFC.

Die vierte industrielle Revolution ist in der Schaltanlage angekommen und beeinflusst die Energiewirtschaft. Schneider Electric hat einen Leistungsschalter vorgestellt, der Energieverteilung neu interpretiert und Betreibern von Schaltanlagen ein Werkzeug für den digitalen Wandel an die Hand gibt. Der offene und robuste Leistungsschalter ist Schutz- und Messgerät in einem. Als Lösungsbaustein für Betriebsanalyse, Wartungsmanagement und Fehlerdiagnose sorgt er für eine hohe Anlagenverfügbarkeit. Zudem ist er komplett kommunikationsfähig und vernetzt. Neben den üblichen, kabelgebundenen Kommunikationsarten über Ethernet und Universal Logic Plug (ULP) zeichnet sich der Leistungsschalter durch seine drahtlose Kommunikationsfähigkeit aus. Near Field Communication (NFC) und Bluetooth sorgen für Konnektivität – im Notfall auch ohne Stromversorgung. Das zentrale Steuer- und Auslösesystem Micrologic X verfügt über zahlreiche Schnittstellen, damit der Schalter mit anderen Geräten, übergeordneten Systemen und dem Bediener kommunizieren kann – via Bluetooth, NFC, USB und QR. Neben Schaltzuständen und Betriebsdaten lassen sich so auch Ereignisprotokolle sowie Voralarme direkt vor Ort oder per Fernzugriff ablesen.

sps ipc drives

27. Internationale Fachmesse
für Elektrische Automatisierung
Systeme und Komponenten
Nürnberg, 22. – 24.11.2016
sps-messe.de



Answers for automation

Elektrische Automatisierung hautnah erleben

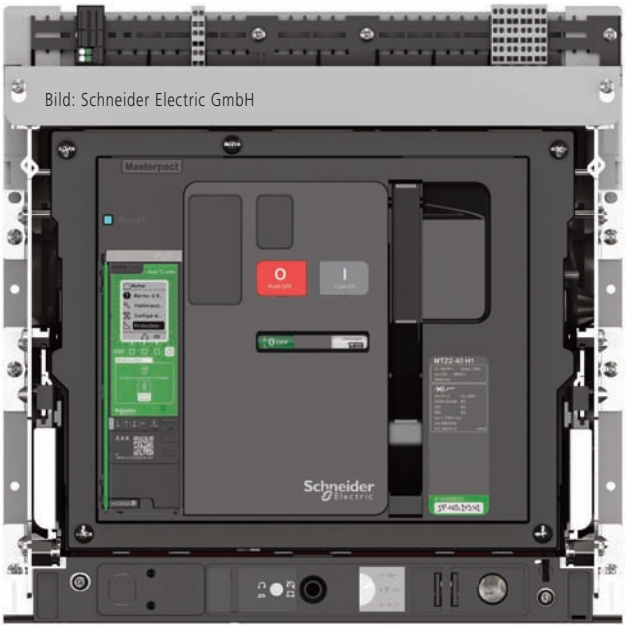
- mehr als 1.650 Aussteller
- Produkte und Lösungen
- Industrie 4.0 Area

Ihre kostenlose Eintrittskarte
sps-messe.de/tickets

mesago
Messe Frankfurt Group

Integrierte Webseiten für direkte Kommunikation

Eine integrierte Ethernet-Schnittstelle (Modbus TCP-Protokoll) macht den Masterpact MTZ netzwerk- und internetfähig. Die IFE (Interface Ethernet)- und im Leistungsschalter integrierte EIFE (Embedded Interface Ethernet)-Schnittstellen können wie üblich über Ethernet an einen PC oder Laptop angeschlossen werden. Neu sind die integrierten Webseiten, die ohne Installation einer separaten Software oder Lizenzierung auskommen: Jeder MTZ hat durch das EIFE-Modul eine eigene IP-Adresse, sodass sich der Leistungsschalter über jeden üblichen Internetbrowser direkt ansprechen lässt. Der Betreiber kann so von nah und fern mit dem Schalter kommunizieren und alle relevanten Mess- und Funktionswerte abrufen. Auf unterster Ebene sorgt eine weitere kabelgebundene Konnektivität für eine Kommunikation der Leistungsschalter untereinander. Hierbei verfügt jeder Leistungsschalter über eine interne Kommunikationsschnittstelle: Ein einfacher ULP-Bus ermöglicht den Austausch von Daten des Leistungsschalters mit gleichartigen Geräten. Digitale Ein-Ausgabe-Bausteine machen periphere Geräte kommunikationsfähig. Das ist beispielsweise praktisch für Hilfskontakte, um Schaltzustände zu kommunizieren. Diese kabelgebundene Kommunikation funktioniert mit einer Übertragungsrate von bis zu einem Megabit pro Sekunde und lässt sich per Plug&Play sofort realisieren.



Der Masterpact MTZ

Mobil vor dem Gerät: Drahtlose Kommunikation

Der Leistungsschalter besitzt zudem die Fähigkeit, drahtlos und berührungslos zu kommunizieren. Das Steuer- und Auslösesystem Micrologic X der neuen Generation ist mit drahtloser Technologie ausgestattet, die Kommunikation per Bluetooth und NFC zulässt. So lassen sich alle kritischen Informationen zu Schutz, Messungen, Diagnostik und Wartung auf einem Mobilgerät abrufen. Eine Bluetooth-Schnittstelle nach dem Bluetooth-Smart-Standard IEEE802.15.1 gestattet es, sämtliche Information berührungslos über jedes handelsübliche Smartphone abzuholen. Steht der Betreiber vor dem Leistungsschalter, kann er über das Mobilgerät Informationen nicht nur abrufen, sondern auch Schutzeinstellungen und Veränderungen vornehmen. Diese Funktion ist als abgesetzte Bedienung zu verstehen, da Bluetooth räumliche Nähe erfordert.

Mit NFC auch ohne Strom Daten abfragen

Eine der Hauptaufgaben eines Leistungsschalters im Störungsfall ist es, die Anlage abzuschalten, um bei Feuer oder Kurzschlüssen Schäden an Mensch und Material zu verhindern. Oft bleibt im Notfall aber auch die Energieversorgung auf der Strecke. Ohne Strom war es bis jetzt unmöglich, die Ursachen der Störung abzufragen. Schaltete der Leistungsschalter ab oder gab es einen Kurzschluss, verging wertvolle Zeit, bis die Störursachen ausgelesen werden konnten. Mit NFC lassen sich die letzten Daten und Infos des Masterpact MTZ drahtlos abfragen. So kann die Ursache für die Störung ausgelesen und analysiert werden – auch wenn die Energieversorgung des Leistungsschalters selbst abgeschnitten ist. Dies kann in Fällen hilfreich sein, wenn Schaltanlagen beispielsweise aufgrund von Kurzschlüssen oder inneren Fehlern derart in Mitleidenschaft gezogen sind, dass sie kaum mehr als solche erkennbar sind. Per Chip lassen sich die relevanten Informationen trotzdem auslesen. So fungiert die NFC-Konnektivität wie eine Blackbox im Flugzeug. Neben NFC sind ULP-, Ethernet- und Bluetooth-Schnittstellen Standard in jedem Masterpact MTZ. Zusätzlich verfügt Micrologic X über eine integrierte Vorrichtung zur proprietären Konnektivität gemäß der Norm IEEE802.15.4. Diese Verbindung ermöglicht die drahtlose Konnektivität des Geräts mit dem kommunikationsfähigen Com'X 510-Modul. Über diese in die Schaltanlage integrierten Energy Server lassen sich so genannte WAGES (Water, Air, Gas, Electricity, Steam)-Daten abrufen. Die Server arbeiten unabhängig voneinander und unterstützen beim Sammeln und Analysieren von Verbrauchsinformationen, z.B. des Luftdrucks aus Kompressoren. Diese interne, drahtlose Kommunikation zwischen Schneider-Electric-Geräten gestattet eine kabellose Nachrüstung in bestehenden Anlagen.

Digitale Module für volle Flexibilität

Die vielfältigen integrierten Kommunikationsschnittstellen sorgen für eine durchgängige Kommunikation vom kleinsten bis zum größten Leistungsschalter, verbinden eine Architektur für alle vernetzten Geräte und helfen so dem Betreiber der Schaltanlage auf dem Weg zur Digitalisierung. Des Weiteren unterstützen digitale Module die geforderte Flexibilität in der Anlage. So lässt sich der Masterpact MTZ in jeder Phase seines Lebenszyklus an geänderte Anforderungen anpassen – während der Konfiguration, bei der Inbetriebnahme, für Änderungen in letzter Minute und bei Erweiterungen auch noch nach Jahren. Die optionale Erweiterung über die Vielzahl digitaler Module bietet außerdem die Möglichkeit, den richtigen Funktionsumfang an die jeweilige Zielgruppe und ihre speziellen Bedürfnisse anzupassen. ■

Autor: *Werner Grewe,*
Offer Manager NS-Leistungsschalter,
Schneider Electric GmbH
www.schneider-electric.de

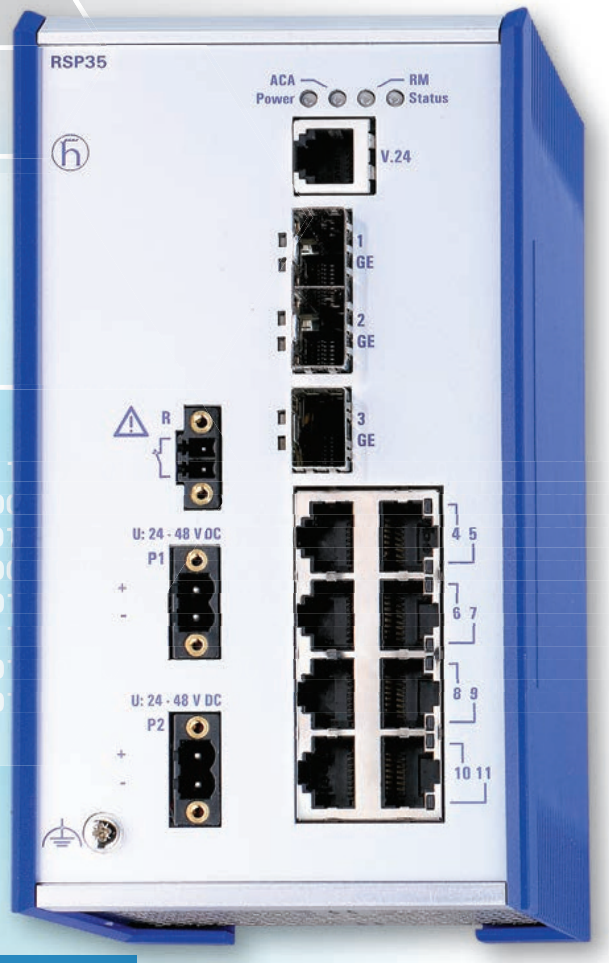
Halle 1
Stand 324
sps ipc drives

INDUSTRIAL COMMUNICATION JOURNAL

icj

ETHERNET WIRELESS SECURITY

TSN 802.1



Moderne Automatisierungsnetze
Cybersicherheit mit TSN

Seite 51

HIRSCHMANN
A BELDEN BRAND

Bild: Belden Electronics GmbH

Moderne Automatisierungsnetze

Cybersicherheit mit TSN

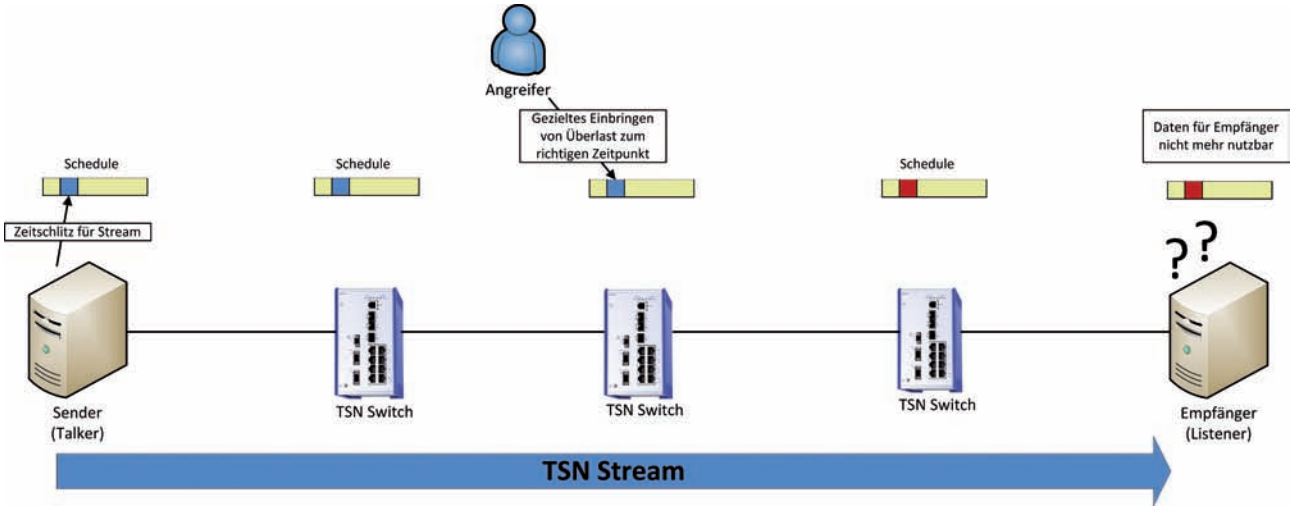


Bild: Belden EMEA Headquarters

Durch Überlastung von Zeitschlitzen kann ein TSN-Stream angegriffen werden.

Mit Time-Sensitive Networking (TSN) bieten sich neue, offene Ethernetstandards als Kommunikationsbasis für Industrie 4.0- und IIoT-Netze an. Hierdurch entstehen auch Herausforderungen für die Cybersicherheit, die sich allerdings mit bewährten Sicherheitsmechanismen beherrschen lassen.

TSN besteht aus mehreren Standards, die von den IEEE-Arbeitsgruppen 802.1 und 802.3 spezifiziert werden. Ein Teil von ihnen ist bereits veröffentlicht, andere befinden sich noch in der Vorbereitung. Die mit ihnen neu eingeführte Technologie stellt zusätzliche Anforderungen an ein Netzwerk. Zu diesen gehört die Verfügbarkeit einer gemeinsamen Zeitbasis. Das gemeinsame Verständnis von Zeit auf allen Geräten ist notwendig, um Daten-Frames deterministisch übertragen zu können, also mit einer klar definierten Zeitobergrenze für die Ende-zu-Ende-Latenz (Verzögerung) und mit geringem Jitter (Schwankungen). Zur deterministischen Datenübertragung wird bei TSN die Zeit mittels des TDMA-Verfahrens (Time Division Multiple Access) in Perioden unterteilt. Innerhalb dieser Perioden werden wiederum für einen Datenstrom Zeitschlitze reserviert. Diese Reservierungen finden bei sämtlichen Netzwerkteilnehmern entlang des Übertragungspfades statt. So wird von einem Endgerät durch das Netzwerk bis zum anderen Endgerät ein virtueller Kanal gebildet. Dieser ist eng an die internen Uhren der beteiligten Netzwerkteilnehmer gekoppelt. Um eine hohe Präzision bei der Zeitsynchronisation zu erreichen, wird daher bei TSN üblicherweise das Precision Time Protocol (PTP) gemäß IEEE1588 verwendet.

Zeit als Angriffsvektor

Um heute gängige Ethernetnetzwerke lahmzulegen, sind Denial-of-Service-Angriffe ein häufig eingesetztes Mittel. Dabei wird das Netzwerk solange mit Daten geflutet, bis es überlastet ist. Weil TSN auf der Verfügbarkeit von Zeitdaten basiert, eröffnen sowohl das PTP-Protokoll als auch das TDMA-Verfahren neue Angriffsvektoren. So ist es mit TSN beispielsweise bereits ausreichend, einen einzelnen Zeitschlitz gezielt zu überlasten. Neben dem zielgerichteten Überlasten bestimmter Zeitschlitze ist das für die Zeitsynchronisierung genutzte Protokoll IEEE1588 selbst ein Angriffsziel. In vielen Automatisierungsnetzen wird bereits heute PTP eingesetzt. Deshalb wird es auch in vielen Anwendungen für die Synchronisierung der TSN-Uhren zum Einsatz kommen. PTP selbst besitzt allerdings keine eingebauten Sicherheitsmechanismen und verlässt sich vollständig auf Security-Lösungen, die im Netzwerk zum Angreifer dahinter liegen. Ohne Netzwerksicherheit könnte ein Angreifer daher mit gefälschten PTP-Datenpaketen die Funktion der zentralen Zeitquelle, des Grandmasters, kapern. Einmal übernommen, kann der falsche Grandmaster starke Zeitschwankungen in das Netz einbringen, um die Synchronität der Zeitschlitze auf den einzelnen Geräten zu sabotieren. Weiterhin kann er einen Zeitsprung in das Netzwerk einbringen, was empfindliche Endanschaltungen dazu veranlassen kann, die Arbeit einzustellen und in einen sicheren Zustand überzugehen. Was bedeutet dies nun für die Cyber-Sicherheit in TSN-Netzen?

Schutz des Netzwerkes

Der Zeitaspekt wirkt sich neben der zusätzlichen Angriffsfläche auch auf die Anwendbarkeit bestimmter Sicherheitsmaßnahmen aus. Wenn etwa eine Firewall Datenpakete nicht in Echt-

zeit untersuchen kann, weil die Software bis in die Nutzlast hineinschaut (Deep Packet Inspektion, DPI), werden die Pakete verzögert übertragen. Wenn dies nicht von vornherein berücksichtigt wird, kollidieren die Daten mit Zeitschlitzen, für die sie nicht bestimmt waren. Eine Möglichkeit, dies in den Griff zu bekommen, sind Firewallkonzepte, die verzögerungsfrei arbeiten. Eine andere Möglichkeit besteht darin, die zusätzliche Verzögerung im Netz transparent zu machen, so dass sie in die Berechnung des Ablaufplanes des TDMA-Verfahrens mit einbezogen werden kann. Das trifft auch auf Switche zu, die auf Hardwareebene Sicherheitsmechanismen wie Access Control Lists (ACL) unterstützen und den Datenverkehr zustandslos filtern. Obwohl das sehr schnell geschieht, resultiert daraus doch eine geringe Verzögerung. In normalen Ethernetnetzen gibt es dadurch keine Auswirkungen. Bei TSN-Netzwerken, in denen es bei der Datenvermittlung um Mikrosekunden oder weniger geht, kann die Datenkommunikation indessen gestört werden. Dennoch sind solche bewährten Sicherheitsmechanismen bei TSN anwendbar, jedoch muss die zusätzliche Verzögerung – ebenso wie bei den Firewalls – von vornherein in die Berechnung der Latenz einfließen.

Unterschiedliche Fälle berücksichtigen

Abhängig von den Anforderungen der Endanwendung hinsichtlich Übertragungslatenz und Zykluszeit kann eine große Verzögerung, selbst wenn sie sichtbar gemacht wird, möglicherweise nicht toleriert werden. Daraus folgt, das man unter Berücksichtigung der Anforderungen von TSN zwei unterschiedliche Fälle betrachten muss: Zum einen Mechanismen, die direkt auf dem TSN-Kommunikationspfad wirken und zum anderen Mechanismen an den Grenzen eines TSN-Kommunikationspfades. Sicherheitsmechanismen auf dem Kommunikationspfad dürfen nur eine geringe zusätzliche Übertragungslatenz aufweisen. An den Grenzen der Kommunikationspfade können Verzögerungen hingegen oftmals toleriert werden. Diese Vorgehensweise deckt sich mit der bewährten Vorgehensweise der Zonen und Leitungen (Zones and Conduits), und fügt dieser Betrachtungsweise eine zusätzliche Komponente hinzu. Die Unterteilung eines Netzwerks in Kommunikationszonen dient dazu, verschiedene Bereiche gegeneinander abzuschotten und nur die absolut notwendige Kommunikation zuzulassen. Dieser Ansatz bezog sich bislang ausschließlich auf die Cybersicherheit. Neben dem Ansatz des Kommunikationsbedarfes (need to communicate) entsteht in TSN-Netzwerken die zusätzliche Ebene des Zeitbedarfs (timing of communication).

Zuverlässige und sichere Lösungen für wachsende Datenmengen

Das Unternehmen Belden ist ein weltweit tätiger Anbieter von Signalübertragungslösungen und bietet ein umfassendes Produktportfolio, das auf die Anforderungen unternehmenskritischer Netzinfrastrukturen in den Branchen Industrie- und Gebäudeautomation sowie Broadcast zugeschnitten ist. Mit Lösungen für die zuverlässige und sichere Übertragung stetig wachsender Datenmengen für Steuerungs-, Audio- und Videoinformationen, die für moderne Anwendungen benötigt werden, will Belden eine Schlüsselrolle bei der globalen Veränderung hin zu einer vernetzten Welt übernehmen. Das Unternehmen mit Hauptsitz im US-amerikanischen St. Louis wurde 1902 gegründet und betreibt Fertigungsstätten in Nord- und Südamerika, Europa und Asien.

Bewährtes Securitykonzept

Diese beiden Konzepte lassen sich sehr gut miteinander vereinbaren, da der Kommunikationsbedarf und der Zeitbedarf oft an den gleichen Ende-zu-Ende Kommunikationsbeziehungen zwischen Endgeräten festgemacht werden kann. So können beispielsweise DPI-Firewalls an den Übergängen zwischen Kommunikationszonen platziert werden, während innerhalb der Zonen auf dem TSN-Datenpfad zustandslose ACL-Paketfilter eingesetzt werden. Auf diese Weise wird, neben Zones and Conduits, zugleich ein weiteres bewährtes Sicherheitskonzept umgesetzt, nämlich Defense in Depth und Diversität. Bei diesem Konzept, das auf eine tief gestaffelte Verteidigung aus-

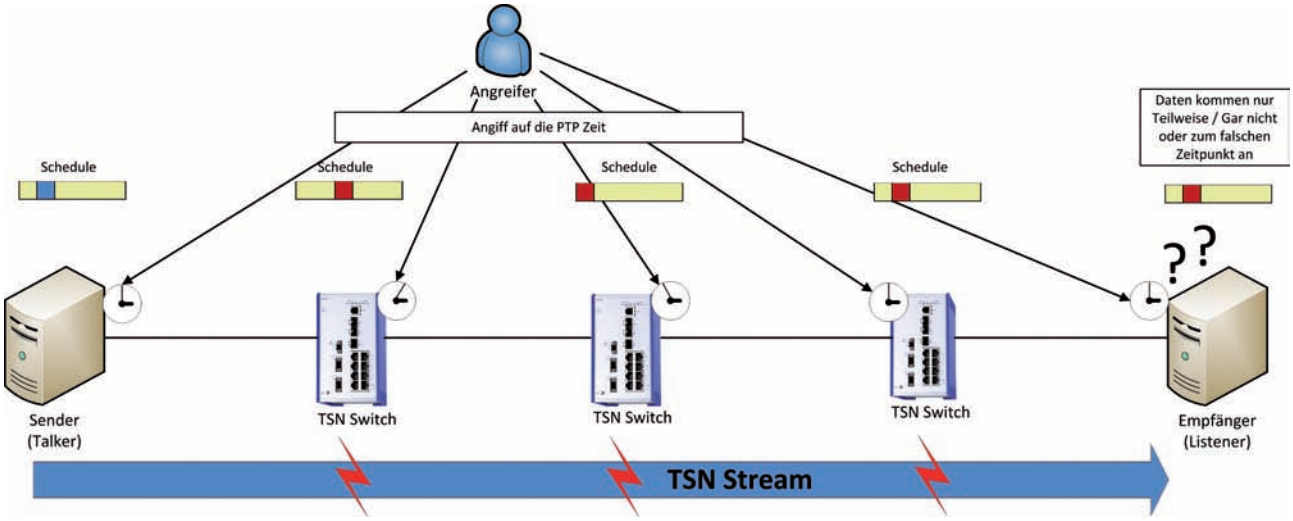


Bild: Belden EMEA Headquarters

Manipulierte Uhren sorgen für Datenverluste auf dem Kommunikationspfad.

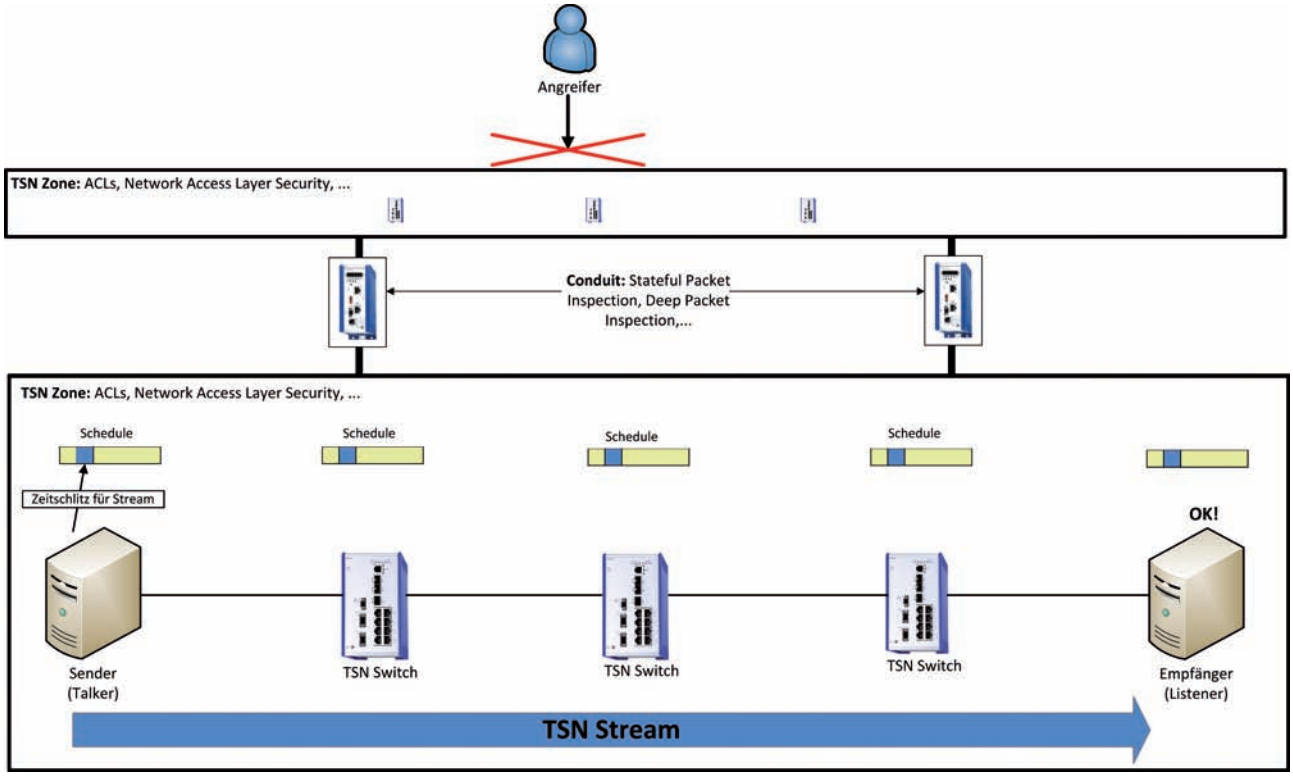


Bild: Belden EMEA Headquarters

Time-Sensitive Zones and Conduits

gerichtet ist, werden mehrere unterschiedliche Security-Mechanismen hintereinander geschaltet, um das Netzwerk zu schützen. Hierzu müssen aber die bewährten Firewall- und Filtermechanismen noch durch zusätzliche Funktionen auf Layer 2 ergänzt werden. Auf der einen Seite sind dies die klassischen Sicherheitsmechanismen auf der Ebene des Netzwerkzuganges (Network Access Layer Security), wie beispielsweise IEEE802.1X, die in Switchen und Routern implementiert sind und den direkten Zugriff auf das TSN-Netz schützen, auf der anderen Seite werden aber auch in der TSN-Spezifikation Mechanismen für diesen Zweck vorbereitet.

Layer-2-Security

Um auch Angriffe auf der Ebene 2 des OSI-Schichtenmodells zu verhindern, sind im Zuge der TSN-Standardisierung bereits erste Maßnahmen in der Entwicklung. Eine davon ist das Ingress Filtering and Policing, das in dem zukünftigen Standard IEEE802.1Qci spezifiziert wird. Bei diesem Verfahren werden die Datenpakete schon am Eingang des Netzwerkes überprüft, ob sie zu einem reservierten Datenstrom passen. Wenn dies nicht der Fall ist, werden die Pakete herausgefiltert und zurückgewiesen. Zusätzlich können Mechanismen wie MACsec (Media Access Control Security) verwendet werden, mit dem sich Datenströme zwischen zwei Netzwerkteilnehmern verschlüsseln lassen. Aber auch diese Sicherheitsmechanismen können, selbst wenn sie auf Hardware-Ebene arbeiten, in TSN-Netzwerken Auswirkungen auf die Ende-zu-Ende-Latenz haben, das heißt, eine minimale Verzögerung in den Kommunikationspfad einfügen. Um diesen zusätzlichen Versatz zu berechnen, müssen die Sicherheitsmechanismen – unabhängig davon, ob sie soft- oder hardwarebasiert sind – einkalkuliert werden. Das ist sozusagen der springende Punkt bei Cybersicherheit in TSN-Netzen innerhalb der Kommunikationszonen. Wenn er beachtet wird, steht einem reibungslosen Betrieb nichts im Wege.

Fazit

TSN gilt als universelle Ethernetweiterentwicklung. Durch hohe Bandbreiten und Dienste in Echtzeit schafft dieser neue Standard die Voraussetzung für moderne Automatisierungsnetze der Zukunft. Da TSN kein herstellerspezifisches Verfahren ist, kann es in der Automatisierung vielseitig eingesetzt werden. Um Cybersicherheit in TSN-Netzwerken zu gewährleisten, muss das Rad aber nicht neu erfunden werden. Denn die Securitymechanismen, die heute schon in der Industrie eingesetzt werden, reichen vollkommen aus, auch wenn durch die strikten Echtzeitanforderungen ein neuer Aspekt hinzukommt, der sich aber nahtlos in die bestehenden Konzepte einfügt. Obwohl die Spezifikation von TSN, noch nicht abgeschlossen ist, lassen sich die veröffentlichten Standards daher bereits sicher nutzen. Da die weiteren Schritte in den IEEE-Arbeitsgruppen 802.1 und 802.3 vorbereitet werden, ist zudem sichergestellt, dass die künftigen Sicherheitsmechanismen für TSN-Netzwerke mit Standardethernet kompatibel sind. ■

Autor: *Dr. René Hummen,*
Senior Researcher Future Technologies
Belden IIT – Core Networking
www.belden.com

Autor: *Dr. Oliver Kleineberg,*
Manager Advance Development
Belden IIT – Core Networking
www.belden.com

Zeit für Umsetzung ist knapp bemessen

Sicherheit per Gesetz

Seit letztem Sommer fordert das IT-Sicherheitsgesetz von den Betreibern kritischer Infrastrukturen verbindliche Maßnahmen zur Gewährleistung der Informationssicherheit. Während die Vorgaben der branchenspezifischen Mindeststandards nicht immer eindeutig sind, liegen die konkreten Umsetzungsfristen dagegen bereits vor: Bis zum 31. Januar 2018 sollen die Forderungen des IT-Sicherheitsgesetzes erfüllt sein.

Das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz (IT-SiG) fordert von Betreibern kritischer Infrastrukturen (Kritis) die Umsetzung noch zu definierender branchenspezifischer Mindeststandards für die Informationssicherheit. Betroffen sind Unternehmen aus Bereichen, die für das Fortbestehen von Gesellschaft und Wirtschaft als unverzichtbar erachtet werden.

Vorgehen zur Einführung eines Informationssicherheit-Managementsystems

Meldepflicht an BSI

Ein wichtiger und von Experten schon lange eingeforderter Punkt ist dabei auch die nun durch das IT-SiG geforderte Meldepflicht: IT-Störungen, die zu einem Ausfall oder einer Beeinträchtigung geführt haben oder führen können, müssen demnach an das BSI gemeldet werden. Bemerkenswert ist zum einen, dass es keine Positivliste von Unternehmen gibt, die unter das Gesetz fallen. Bei den meisten wird es unstrittig sein, aber auf welche Unternehmen das IT-SiG in Grenzbereichen anzuwenden ist, kann nur im Einzelfall entschieden werden. Hierfür werden in einer zusätzlichen Rechtsverordnung, die Ende des Jahres erscheinen soll, Schwellenwerte definiert. Anhand dieser müssen alle Unternehmen selbst prüfen, ob sie zu Kritis zählen oder nicht. Gelegentlich genannte Zahlen von 2.000 meldepflichtigen Betreibern erscheinen weit untertrieben, andere Untersuchungen kommen auf bis zu 18.000 Unternehmen. Auch inhaltlich bleiben die Vorgaben vage. Es wird tatsächlich schwierig sein, a priori gesetzlich zu definieren, was branchenspezifische Mindeststandards umfassen. Umso mehr, als sich gerade das Feld der IT-Sicherheit überaus dynamisch entwickelt.

Spezielle Situation für den Energiesektor

Für die Energiewirtschaft ergibt sich eine spezielle Situation, denn bereits 2011 wurde im Energiewirtschaftsgesetz die Ausarbeitung eines IT-Sicherheitskatalogs (IT-SK) durch die Bundesnetzagentur festgelegt. Er stellt nun den branchenspezifischen Sicherheitsstandard für die Energiewirtschaft dar und ist schon jetzt für sämtliche Strom- und Gasnetzbetreiber verpflichtend – unabhängig von der Größe oder der Anzahl der angeschlossenen Kunden. Kernforderung des Katalogs ist die Etablierung eines Informationssicherheits-Managementsystems (ISMS) gemäß ISO27001. Bis zum 31. Januar 2018 müssen die Betreiber der Bundesnetzagentur die Umsetzung des IT-Sicherheitskataloges durch die Vorlage eines ISO27001-Zertifikats nachweisen. Berücksichtigt man wie viel Zeit allein für die Ressourcenabschätzung, Mittelanforderung und Umsetzungsentscheidungen benötigt wird, so ist das eine durchaus knappe Frist und für einige Unternehmen eine echte Herausforderung.

Ressourcen- und Know-how-Mangel bei KMU

Oftmals besitzen vor allem kleinere Unternehmen kaum die notwendigen Ressourcen oder Know-how, um ein ISMS selbstständig zu etablieren. Für sie kann es sinnvoll sein, einen externen Dienstleister hinzuziehen und nur einen Teil der Arbeit selbst durchzuführen. So können beispielsweise die IT-Sicherheitsanalyse oder auch die geforderten regelmäßigen internen Audits einem Dienstleister überantwortet werden. Alternativ kommt auch eine vollständig externe Lösung in Betracht, bei der ein Dienstleister das ISMS betreibt und kontrolliert sowie die Sicherstellung der Einhaltung der Regularien bis hin zur Kommunikation mit der Bundesnetzagentur übernimmt. In jedem Fall sollten sich betroffene Unternehmen und jene, die bereits abschätzen können, dass sie ggf. zu Kritis zählen, zeitnah mit dem Thema befassen und zumindest erste Abschätzungen zu den benötigten Ressourcen durchführen. ■

Autorin: ***Dr. Katja Siegemund,***
Business Consultant Energie
QSC AG, Hamburg
www.qsc.de

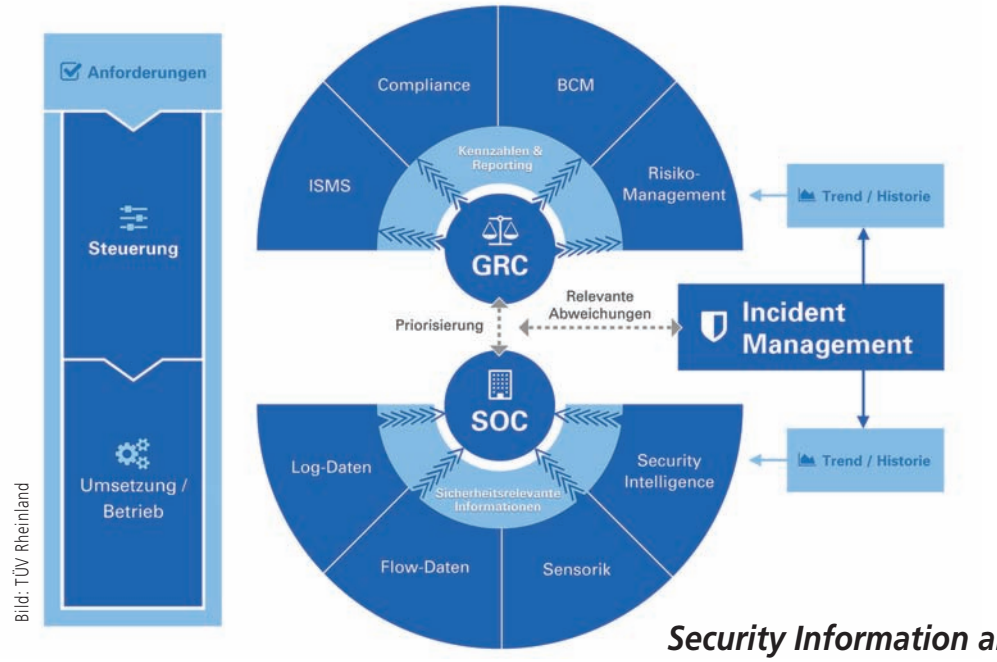


Bild: TÜV Rheinland

Security Information and Event Management

Stolperfallen vermeiden bei der SIEM-Einführung

Ein störungsfreier und reibungsloser Betrieb der IT-Infrastruktur ist einer der Eckpfeiler für den Erfolg der immer stärker vernetzten Industrie. In höchstem Maße schützenswert sind digitale Assets sowie Betriebsablauf und Produktivität. Weil kein Unternehmen eine lückenlose Cyberabwehr aufweist, kommt reaktiven Maßnahmen eine wachsende Bedeutung zu – produzierende Unternehmen sollten deshalb auf ein SIEM-System setzen.

Viele produzierende Unternehmen nutzen heute die Möglichkeiten, die sich aus der rasant fortschreitenden Digitalisierung ergeben. Diese Entwicklung birgt aber nicht nur großes Geschäftspotenzial, sondern auch Gefahren. Vor allem dann, wenn die IT-Sicherheitsstrategie und -Maßnahmen der neuen Situation nicht angemessen angepasst werden. Denn Anzahl und Qualität der Angriffe nehmen zu, signaturbasierte Abwehrlösungen sind gegen die immer höherqualifizierten Attacken machtlos. Viele Angriffe sind so raffiniert, dass sie unter Umständen erst viel später oder gar nicht erkannt werden. Das Ergebnis: mangelnde Widerstandsfähigkeit des Unternehmens, Einschränkungen der Produktivität bis hin zum Risiko eines Totalausfalls. Wesentlicher Eckpfeiler einer ganzheitlichen und effektiven IT-Securitystrategie ist ein SIEM (Security Information and Event Management). Moderne Lösungen loggen, analysieren und verwerten in Echtzeit alle relevanten Informationen aus Netzwerk, Betriebssystem, Middleware und Applikationen. Durch die Korrelation von Log-Meldungen unterschiedlicher Systeme lassen sich Angriffsmuster aus der Vergangenheit ebenso erkennen wie neue Anomalien, die für das Unternehmen eine Gefahr darstellen könnten. Auf Basis aussagekräftiger Informationen bleibt das Unternehmen handlungsfähig. Wird ein Angriff erkannt, können sofort Gegenmaßnahmen ergriffen werden. Bei der Einführung und im Betrieb eines SIEM lauern allerdings einige Stolperfallen, die sich – ist man sich ihrer bewusst – systematisch vermeiden lassen.

Stolperfalle 1

Viele Unternehmen definieren die Ansprüche an ihr SIEM-System unzureichend und wählen zuerst die Technologie aus. Möglicherweise erfüllt die ausgewählte Lösung allerdings nicht die Erwartungen, die in sie gesetzt werden. Deshalb gilt es, zuerst Ziele und Strategie zu definieren, dann das Tool auszusuchen. Folgende Fragen sind hilfreich: Was soll das System leisten? Wo befinden sich die wirklich schützenswerten Bereiche im Unternehmen? Welcher Netzwerkverkehr und welche Informationen sind kritisch? Denn jederzeit alles überwachen zu wollen, ist weder realistisch noch zielführend. Weiterhin ist hierbei auch die Frage zu klären, ob das SIEM-System sowohl die gängigen Office-IT-Log-Protokolle wie auch die gängigen Produktionsnetz- und Scada-Log-Protokolle unterstützt.

Stolperfalle 2

Ein neu eingeführtes SIEM beinhaltet in der Regel eine Vollkonfiguration bzw. die vom Hersteller festgelegten Regeln, die oft zu 90 Prozent generisch sind. Das kann die Trefferquote verfälschen – und das Vertrauen in die Glaubwürdigkeit von Alarmen stark negativ beeinflussen. Das serienmäßige Regelwerk also am besten erst komplett abschalten und dann sukzessive aktivieren und an die Gegebenheiten im Unternehmen anpassen. Je nach Umgebung kann diese erste Phase des SIEM-Einsatzes aufwendig und

zeitintensiv ausfallen, aber die Mühe lohnt sich. Vor allem lassen sich so unnütze Datenhalden vermeiden.

Stolperfalle 3

Viele Unternehmen bauen SIEM-Lösungen auf, ohne eine Strategie dafür zu besitzen. Damit die SIEM-Lösung ihr volles Potenzial entfalten kann, muss eine SIEM-Strategie entwickelt werden, die im besten Falle auf einem risikobasiertem Ansatz beruht, d.h. es sind vorher realistische Bedrohungsszenarien festzulegen. Viele Unternehmen rechnen z.B. mit der Kommunikation mit potentiell schadsoftware-verseuchten Zielen, mit Angriffen von Innentätern wie Privilege Escalation, verdächtigem Netzwerkverkehr oder sonstigen unerwarteten Ereignissen.

Stolperfalle 4

In welcher Quantität und Qualität das SIEM Daten loggt, spielt für die Aussagekraft der Ergebnisse eine entscheidende Rolle. Ist das Loglevel zu niedrig angesetzt, sammelt das System nicht genügend Informationen. Unregelmäßigkeiten oder ein potenzieller Angriff könnten unentdeckt bleiben. Ist das Loglevel zu hoch, überlastet die erzeugte Datenmenge unter Umständen die vorhandenen Ressourcen. Dies kann bei Produktionsnetzen besonders bedrohlich werden, da hier die Netzwerkbandbreite oftmals um ein Vielfaches geringer ist als in der Office-IT, und zu Verzögerungen und Ausfällen in der Produktion führen kann. Obwohl in Echtzeit erkannt, finden die Informationen ihren Weg durch die IT-Infrastruktur nur mit Verzögerung bzw. werden stark zeitverzögert ausgewertet – ggf. zu spät, um einen Angriff abzuwehren. Bei der Planung gilt es deshalb immer die Skalierbarkeit der IT-Infrastruktur im Auge zu behalten und wenn nötig, die Kapazitäten anzupassen. Entsprechende Protokollierungs-Policies, basierend auf Usecases, regeln dabei das anforderungsgerechte Log-Volumen an der Quelle.

Stolperfalle 5

Der erfolgreiche SIEM-Einsatz basiert zu einem großen Teil auf dem Know-how der Mitarbeiter, die in der Lage sind, Ergebnisse auszuwerten, zu qualifizieren und deren Kritikalität einzuschätzen. Fehlen dem Unternehmen die nötigen Kenntnisse im eigenen Haus, empfiehlt sich die Unterstützung durch externe Spezialisten – sei es für einzelne Aufgabenstellungen oder insgesamt für die Einführung und den Betrieb des Systems. Diese Experten müssen sich sowohl mit den technischen Details und den Prozessen in der Office-IT sowie auch in der Produktions-IT auskennen.

Stolperfalle 6

Das SIEM darf nicht als Insellösung betrieben werden. Seine Stärke kann das System nur ausspielen, wenn es fest in der Unternehmensstruktur verankert ist. Es empfiehlt sich, das System mit der GRC-Lösung (Governance, Risk and Compliance) des Unternehmens zu koppeln. Diese Informationen helfen dem System, Bedrohungen zu priorisieren und kritische Bereiche konsequent zu überwachen. Gleichzeitig nutzt das GRC die SIEM-Reports, um die Entscheider im Unternehmen über den aktuellen Stand der IT-Sicherheit zu unterrichten.

Stolperfalle 7

Eine weitere Gefahr besteht darin, keine Workflows rund um das SIEM zu definieren. Die Verwendung eines SIEM geht weit über die IT-Abteilung hinaus. Für den Fall eines Cyber-Angriffs gilt es klare Prozesse, Verantwortlichkeiten und Schnittstellen zu anderen Abteilungen festzulegen. Wichtig ist, dass die Eindämmung schnell geschehen kann, dass die Entscheidungskompetenzen verfügbar sind bzw. klare Regelungen schnelle Entscheidungen ermöglichen.

Stolperfalle 8

Eine konfigurierte SIEM-Lösung wäre in der Lage, ein genaues Profil des einzelnen Mitarbeiters zu generieren: wann er wo welches Gerät benutzt hat oder auf welche Daten er zugreift. Dieses Wissen kann beim Identifizieren eines Insiderangriffs oder gestohlener Identitäten nützlich sein, aber auch schnell die Mitarbeiterrechte verletzen. Deshalb müssen die informationellen Grundrechte der Mitarbeiter jederzeit gewahrt sein. Es gilt, Datenschutzbeauftragte und Betriebsrat frühzeitig in die Planung eines SIEM mit hinzuziehen, um auch in punkto Compliance auf der sicheren Seite zu sein.

Stolperfalle 9

Sind Unternehmen zu sehr auf die Enterprise und Office-IT fokussiert, wird schnell vergessen, dass die Produktionsumgebungen meist sehr viel anfälliger gegen Angriffe sind. Dies hängt mit den Updatezyklen zusammen. Bei Produktionssystemen sind das oft Monate bis Jahre. Außerdem ist es für einen Angreifer oft nicht schwierig vom Office-Netz in das Produktionsnetz zu gelangen, da die Hürde hier gering ist. Das macht es einem Angreifer relativ einfach, sich durch beide Netzsegmente zu bewegen. Deshalb sollten produzierende Unternehmen auch die abgeschotteten Produktionsnetze mit in den Fokus nehmen. Um diesem Umstand Rechnung zu tragen, ist bereits bei der Auswahl des SIEM-Systems darauf zu achten, dass die Lösung auch Log-Formate des Produktionsnetzes unterstützt. Findest sich kein SIEM-System, das sowohl Office-IT als auch Produktions-IT unterstützt, empfiehlt es sich, zwei getrennte Systeme aufzubauen.

Fazit

Die SIEM-Einführung ist ein komplexer Prozess, der viel Vorbereitung erfordert, wenn das System erfolgreich und nachhaltig arbeiten soll. Dennoch lohnt sich der Aufwand, weil die Vorteile klar überwiegen. Mehr noch: Ohne entsprechende SIEM-Tools steht die Security Intelligence eines Unternehmens auf wackligen Beinen. ■

Autor: *Alan Scheidler,*
TÜV Rheinland
www.tuv.com/Informationssicherheit

Autor: *Thomas Mörwald,*
TÜV Rheinland
www.tuv.com/siem

Vorschau

Ausgabe 1/2017 erscheint am 27.03.2017

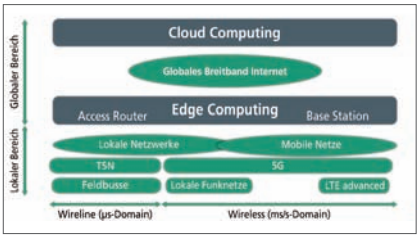


Bild: Fraunhofer

Bild: Nexans Deutschland GmbH

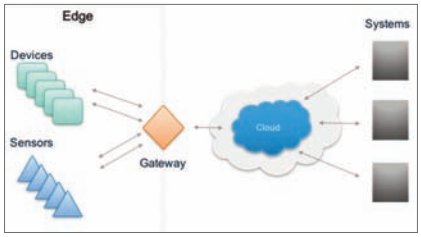


Bild: Techtarget

Die wachsende Komplexität zu bewältigen ist die Aufgabe einer Kommunikations-Referenzarchitektur für das IIoT. Das Fraunhofer ESK hat zusammen mit dem IKT-Anbieter Huawei ein Whitepaper verfasst, in dem eine solche Referenzarchitektur skizziert wird.

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

Ein IoT-Gateway überbrückt die Kommunikationslücke zwischen IoT-Geräten, Sensoren, Ausrüstung, Systemen und der Cloud. Der Informationsaustausch zwischen Komponenten, Gateway und Cloud muss sicher sein, um Datenmanipulation oder uneingeschränkten Zugang zu verhindern.

Inserentenverzeichnis

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:
Frauke Itzerott, Anja Giesen, 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 Krebs

ANZEIGENDISPOSITION:
Michaela Preiß
Tel. 06421/3086-0

Es gilt die Preisliste der Mediadaten 2016.

GRAFIK & SATZ:
Jana Berger, Anja Beyer, Marcus Boeck, Tobias Götze, Moritz Klös, Timo Lange, Ann-Christin Lölkes, Julian Parsch, Verena Vornam, Laura Jasmin Weber, Linnéa Winter

DRUCK:
Offset vierfarbig
Brühlsche Universitätsdruckerei GmbH & Co KG
Am Urnenfeld 12, 35396 Gießen-Wieseck

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

Weidmüller

Mehr Performance, weniger Komplexität
u-remote ist das flexible I/O-System für Ihre Anlagen
Let's connect.

Sie brauchen ein I/O-System, das Ihnen schnelles und flexibles Arbeiten ermöglicht. Eins, das Sie bei der zunehmenden Dezentralisierung von Anlagen nicht im Stich lässt. Das besonders kompakte u-remote-System, bestehend aus IP20- und IP67-Komponenten, eröffnet bei der Automatisierung maximale Vorteile und einen flexiblen Einsatz. Und das Beste: Mit Weidmüller als Partner haben Sie gleich eine Komplettlösung an der Hand.

Erleben Sie u-remote mit Ethernet POWERLINK live auf der SPS IPC Drives in Halle 9, Stand 9-351!

www.u-remote.net

sps ipc drives
Besuchen Sie uns in
Halle 7, Stand 404

INDUSTRIENETZE SCHÜTZEN UND VERBINDEN!

WALLIE – Industrial Ethernet Bridge und Firewall

WALLIE, die Industrial Ethernet Bridge und Firewall, integriert Ihre Maschinennetze auf einfache Weise in das übergeordnete Produktionsnetz. Ein Paketfilter schützt die Netze vor unerlaubtem Zugriff, sollen identische IP-Adressbereiche realisiert werden fungiert WALLIE als Bridge.

- Integration von Maschinennetzen in das übergeordnete Produktionsnetz
- Bridge-Funktionalität für identische IP-Adressbereiche
- NAT (Basic NAT, NAPT und Portforwarding)
- Zugriffsbeschränkung durch Paketfilter
- Industrietaugliche Bauform zur Hutschienenmontage

www.helmholz.com

Helmholz®
COMPATIBLE WITH YOU