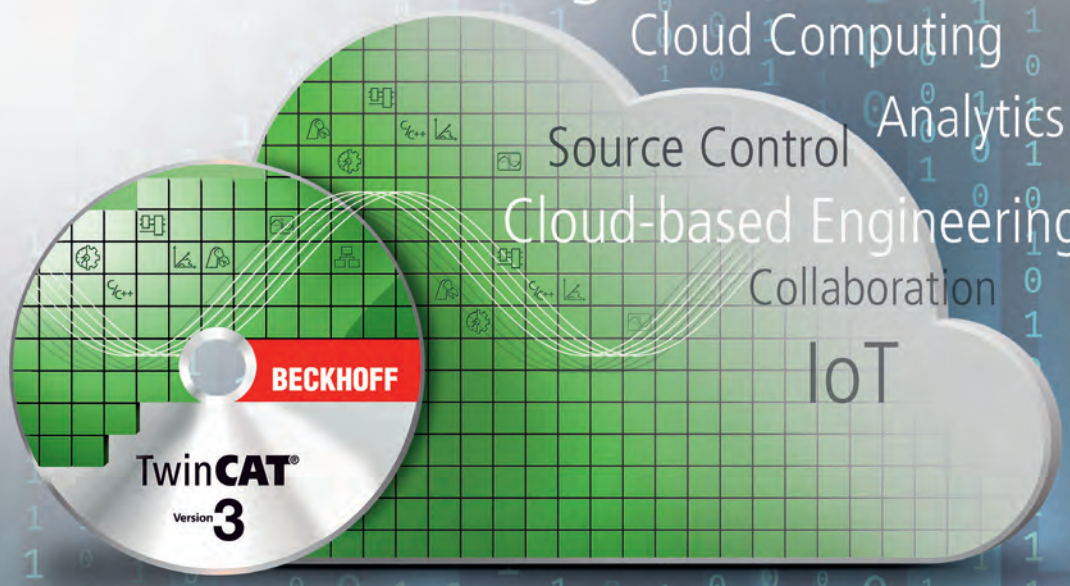
SPS MAGAZIN SONDERAUSGABE 2/2020
www.sps-magazin.de

INDUSTRIAL COMMUNICATION JOURNAL

ETHERNET WIRELESS SECURITY

BECKHOFF



TwinCAT Cloud Engineering als Grundlage hocheffizienter IoT-Automatisierungskonzepte

Smart Engineering direkt in der Cloud

Seite 5

Titelbild: Beckhoff Automation GmbH & Co. KG

FELDBUS-NETZE EINFACH VERBINDEN

mit den Helmholz PROFINET Gateways

Mit unseren PROFINET Gateways ermöglichen wir Ihnen Maschinen direkt auf I/O Ebene miteinander zu verknüpfen. Erzielen Sie einen nahtlosen Datenfluss zwischen Anlagen unterschiedlicher Hersteller – unabhängig von der eingesetzten SPS.

- ✓ **Einfache Inbetriebnahme – keine Programmierung erforderlich**
- ✓ **Konfiguration nur mit GSDML/GSD-Dateien**
- ✓ **Kompakte Bauform zur Hutschienenmontage**

www.helmholz.de

Helmholz®
COMPATIBLE WITH YOU

Einen Cent für die Vernunft

Blinde Zerstörung ist längst nicht mehr das Ziel von Hackern (und war es vermutlich auch nie). Vielmehr ist das unerlaubte digitale Eindringen in Unternehmen ein lukratives Geschäftsmodell mit Umsätzen, die nach Expertenmeinungen diejenigen aus Drogengeschäften mittlerweile übersteigen. Dabei könnte man zumindest den Angriffsvektor E-Mail ganz einfach eleminieren...

Die Vorgehensweise von Cyber-Kriminellen ist hinlänglich bekannt: Per E-Mail-Massenverteilung werden in einer Art brutalem Frontalangriff so lange Office-IT-Systeme befeuert, bis ein Anwender einen Fehler begeht und auf einen Link oder einen Dateianhang klickt, der einen Virus, Trojaner oder einen Ransomware-Lock auslöst. Dies alles passiert täglich und einen endgültigen Schutz dagegen scheint es auch in absehbarer Zeit nicht zu geben. Dabei könnte es so einfach sein: Müsste jeder Teilnehmer am E-Mail-System nur einen Cent für die Zustellung seiner Nachricht bezahlen, wäre der Sumpf schnell trocken gelegt. Erstens, weil diese Angriffe in der Regel über die schiere Masse der E-Mails funktioniert: Angriffs-E-Mails werden millionenfach versendet; Angreifer müssten selbst bei nur einem Cent pro E-Mail schon mal bereit sein, 10.000 Euro auf den Tisch zu legen, um eine Millionen E-Mail-Postfächer anzugreifen. Zudem müssten sie an ein Bezahlsystem angeschlossen sein, das eine entsprechende Identifikationsprüfung voraussetzt. Bei seriösen Unternehmen ist weder die Bezahlung von 0,01 Euro pro E-Mail ein Problem, noch die Identifikation über ein entsprechendes Bezahlsystem. Die Massenweise versendeten Spam- und Malware-E-Mails wären Vergangenheit. Leider ist diese Vorstellung naiv und nicht ansatzweise absehbar. Stattdessen sind Privatleute wie Unternehmen dazu gezwungen, Unmengen an Zeit und Geld in die Sortierung von guter und böser E-Mail-Post zu stecken, von entsprechenden Sicherheitssystemen ganz zu schweigen.

Ist die Malware erstmal im Unternehmen eingeschleust, haben die Angreifer meist die freie Auswahl, welche Daten sie abgreifen oder welche Systeme sie blockieren wollen. Entscheiden sich die Hacker für das Produktionssystem eines Industrieunternehmens, ist guter Rat buchstäblich teuer. Aber auch der direkte Angriff auf Produktionssysteme findet immer häufiger statt: Ein Blick auf die gegenwärtigen Trends bei Cyberangriffen zeigt, dass der Weg ins Unternehmen immer häufiger über schlechter gesicherte OT-Systeme führt. Das jedenfalls sagt Sicherheitsspezialist Tenable, den wir in dieser Ausgabe auf Seite 14 zu Wort kommen lassen. Die gute Nachricht: Immer mehr Unternehmen befassen sich explizit mit der Absicherung von OT-Systemen und können die besonderen Anforderungen der Produktionsumgebungen berücksichtigen. Mit künstlicher Intelligenz ausgestattete Systeme können helfen, Angriffsversuche frühzeitig zu erkennen und zu verhindern. Aber auch Cyberkriminelle haben die KI längst für sich entdeckt. Und so geht der Wettstreit einfach nur in die nächste Runde...

Kai Binder, Chefredakteur SPS-MAGAZIN

Kai Binder
kbinder@sps-magazin.de

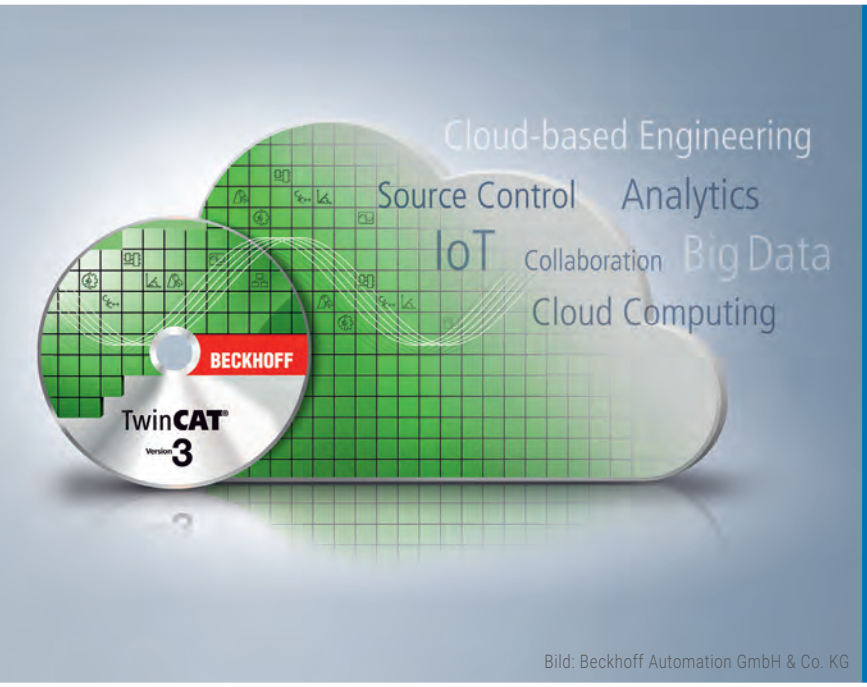


Bild: Beckhoff Automation GmbH & Co. KG

TITELSTORY

5 Smart Engineering direkt in der Cloud

PC-based Control unterstützt als zentrale, offene Steuerungsplattform für alle Maschinenfunktionen optimal die Umsetzung hocheffizienter IoT-basierter Automatisierungskonzepte. Maschinen, Anlagen und Fertigungslinien lassen sich derart miteinander vernetzen, dass Effizienzpotenziale prozessübergreifend ausgeschöpft werden können. Am Anfang steht dabei mit dem neuen TwinCAT Cloud Engineering das einfache Engineering aller Instanzen und Steuerungen direkt in der Cloud.

Mit dem Digital Twin zur Smart Factory

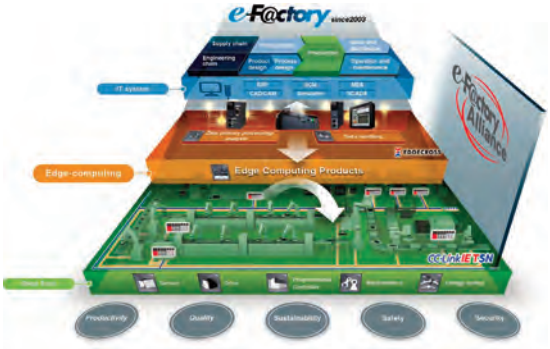


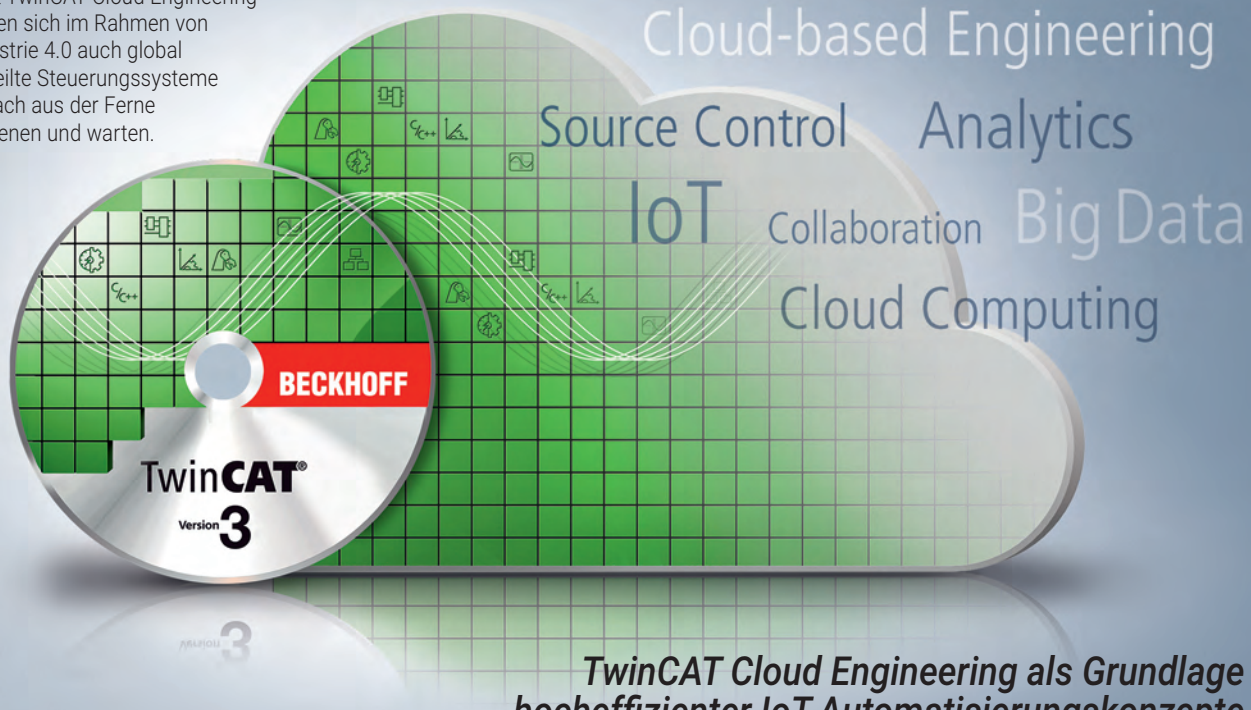
Bild: Mitsubishi Electric Corporation

Die Plattform Contact Elements orchestriert Daten des digitalen Zwillings zwischen den OT- und IT-Systemen.
Seite 22

Inserentenverzeichnis

MARKT – TRENDS – TECHNIK

SERVICE



Mit TwinCAT Cloud Engineering lassen sich im Rahmen von Industrie 4.0 auch global verteilte Steuerungssysteme einfach aus der Ferne bedienen und warten.

TwinCAT Cloud Engineering als Grundlage hocheffizienter IoT-Automatisierungskonzepte

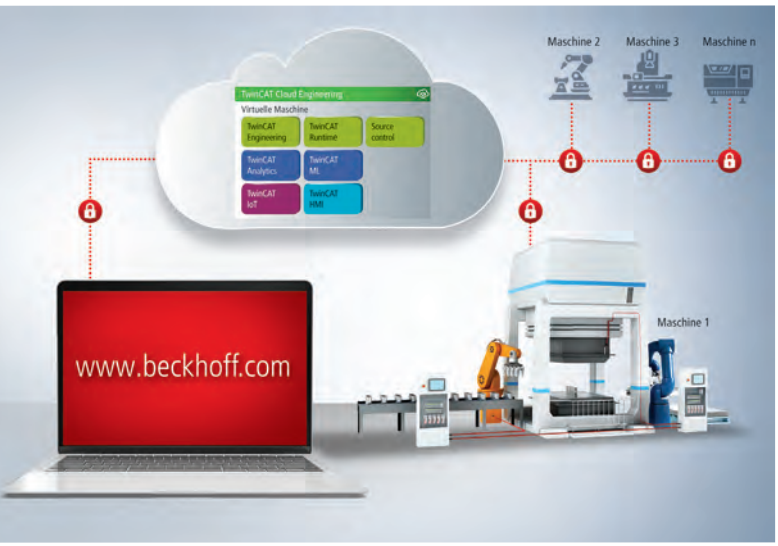
Smart Engineering direkt in der Cloud

PC-based Control unterstützt als zentrale, offene Steuerungsplattform für alle Maschinenfunktionen optimal die Umsetzung hocheffizienter IoT-basierter Automatisierungskonzepte. Maschinen, Anlagen und Fertigungslinien lassen sich derart miteinander vernetzen, dass Effizienzpotenziale prozessübergreifend ausgeschöpft werden können. Am Anfang steht dabei mit dem neuen TwinCAT Cloud Engineering das einfache Engineering aller Instanzen und Steuerungen direkt in der Cloud.

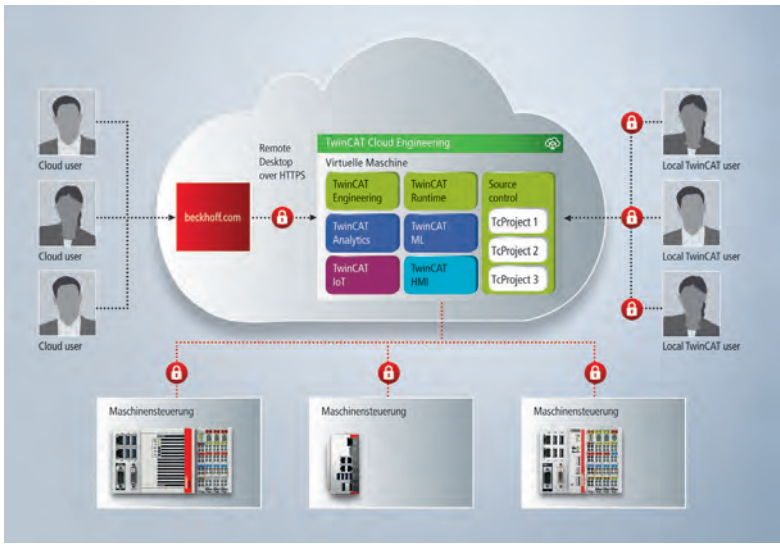
Die effiziente Nutzung von Clouddiensten entwickelt sich im industriellen Umfeld zunehmend zum entscheidenden Wettbewerbsfaktor, denn dies ermöglicht die einfache und skalierbare Umsetzung zahlreicher Anwendungsfälle, die in der Vergangenheit nur mit vergleichsweise hohem Aufwand zu realisieren waren. Die PC-basierte Steuerungstechnik bietet hier eine umfassende Grundlage für die gezielte Nutzung von IoT-Infrastrukturen in der globalisierten industriellen Produktion. Die sichere, skalierbare Vernetzung global verteilter Steuerungssysteme, z.B. zur Realisierung von Big-Data- oder Analytics-Szenarien, ist hierbei nur der Anfang. Im nächsten Schritt müssen diese vernetzten Systeme so einfach wie möglich auch aus der Ferne bedient und gewartet werden können. TwinCAT Cloud Engineering setzt genau an dieser Stelle an. Es ermöglicht eine Instanziierung und Verwendung der existierenden TwinCAT-Engineering- und -Runtime-Produkte direkt in der Cloud.

IoT-basierte Automatisierung optimal unterstützt

Mit PC-based Control unterstützt Beckhoff IoT-basierte Automatisierungskonzepte optimal: Alle Maschinenfunktionen von der PLC über Motion Control und Robotik bis hin zu Vision, HMI und Machine Learning sind auf einer zentralen, offenen Steuerungsplattform integriert. Über die PC-basierte Steuerungstechnik lassen sich Maschinen, Anlagen und Fertigungslinien zudem für eine verbesserte Prozesseffizienz nahtlos miteinander vernetzen. Am Anfang steht dabei TwinCAT Cloud Engineering, das ein einfaches Engineering aller Instanzen und Steuerungen direkt in der Cloud und inklusive direkter Analytics- und HMI-Integration ermöglicht. Die TwinCAT-Entwicklungsumgebung lässt sich zwar schon seit einigen Jahren auch auf einer virtuellen Maschine in der Cloud betreiben, bislang musste der Anwender hierfür allerdings selbst einen Vertrag mit einem Cloudanbieter abschließen und alle TwinCAT-Elemente manuell umsetzen. Mit TwinCAT Cloud Engineering stellt Beckhoff nun ein entsprechendes Komplettpaket zur Verfügung: Der Zugriff auf das TwinCAT Cloud Engineering erfolgt einfach über die Beckhoff-Webseite, das heißt der registrierte Nutzer muss sich lediglich über ein Webportal einloggen und kann dann komfortabel auf seine virtuellen Maschinen zugreifen. Außer einem Webbrowser sind hierfür keine zusätzlichen Softwarekomponenten erforderlich, eine Softwareinstallation entfällt somit. Außerdem kann auf diese Weise rein browserbasiert sogar über bisher



Über das entsprechende Beckhoff-Webportal ist das Engineering aller Instanzen und Steuerungen direkt in der Cloud möglich.



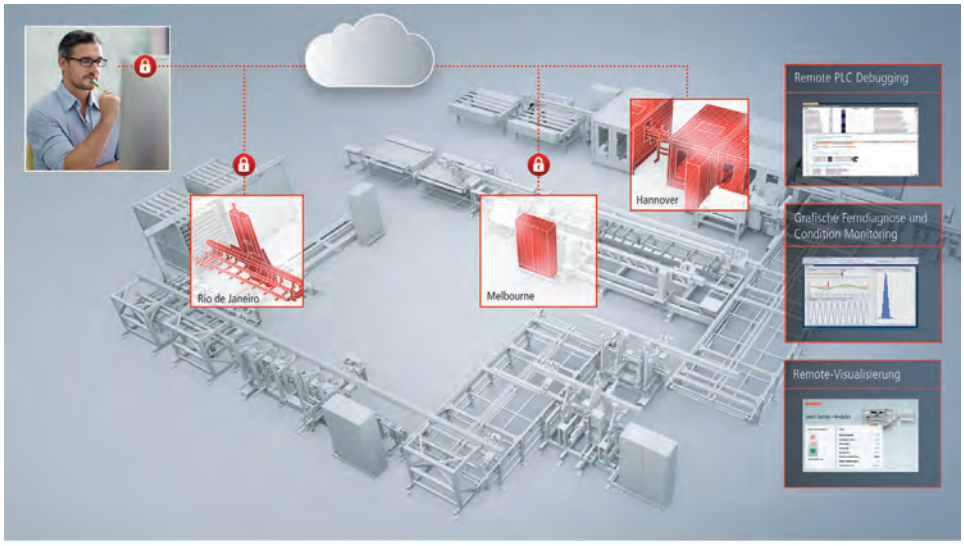
Über die Cloud können auch größere Expertenteams aus lokalen und Cloudnutzern effizient zusammenarbeiten.

nicht geeignete Hardwareplattformen wie z.B. Tablet-PCs mit der TwinCAT-Entwicklungsumgebung gearbeitet werden.

TwinCAT Cloud Engineering für Experten und Einsteiger

TwinCAT Cloud Engineering unterscheidet zwei Benutzermodelle mit spezifischen Abrechnungsmodellen und Funktionsumfängen: **Einsteiger- und Professional-User:** Einsteiger erhalten ein Zeitkontingent, währenddessen sich die Instanz verwenden lässt und alle Funktionalitäten getestet werden können. Der Ablauf des Zeitkontingents erfolgt nur bei laufender Instanz und wird stundengenau ermittelt. Zudem kann der Anwender seine Instanz eigenständig starten bzw. stoppen, was eine effiziente Verwendung des Zeitkontingents ermöglicht. Professional-User haben nach Beendigung des Testzeitraums die Möglichkeit, die Instanz gegen eine monatliche Gebühr weiter zu verwenden. Darüber hinaus erhalten Professional-User Zugang zu einem zentralen Source Control Repository.

TwinCAT dient als Grundlage eines PC-basierten Steuerungssystems und stellt dem Professional-User zahlreiche Möglichkeiten zur Verfügung, um Maschinenprojekte zu realisieren und zu erweitern. Mit dem neuen TwinCAT Cloud Engineering können in diesem Zusammenhang auch existierende TwinCAT-Softwarekomponenten genutzt werden. Somit besteht nun die zusätzliche Möglichkeit, die TwinCAT-Architektur komplett in die Cloud zu transferieren. Die bisherige Möglichkeit, TwinCAT 'on-premise', das heißt lokal auf dem Engineering-PC zu nutzen, bleibt natürlich weiterhin bestehen. Einziger Unterschied gegenüber der konventionellen Vorgehensweise ist nun die Verwendung einer virtuellen Maschine statt eines lokalen Engineering-PC. Dies bietet den Vorteil, dass sich der Anwender nicht an eine neue Softwareumgebung gewöhnen muss, sondern weiterhin in seiner gewohnten Entwicklungsumgebung arbeiten kann. Zudem entfällt die Installation und Vorhaltung unterschiedlicher, auf die individuelle Maschinengeneration zugeschnittener Softwareversionen auf dem eigenen PC. Stattdessen können verschiedene TwinCAT-Cloud-Engineering-Instanzen mit verschiedenen Versionsständen verwendet werden, der Zugriff erfolgt aus der Ferne und je nach Bedarf. Anwender haben so immer die zur Maschine passende Softwareversion zur Hand. Als Projektablage dient ein Source Code Control Repository, auf das direkt aus TwinCAT XAE heraus zugegriffen werden kann.



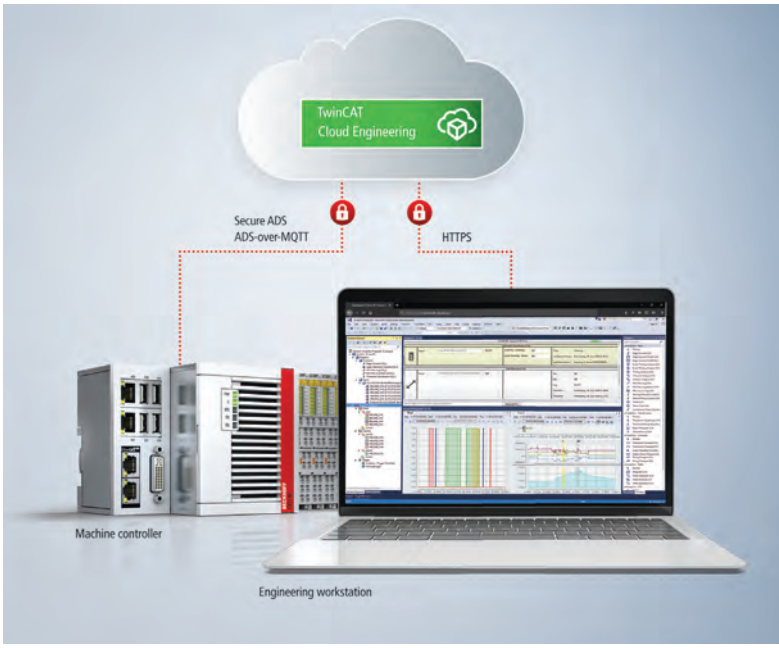
Mit TwinCAT Cloud Engineering vereinfachen sich IT-Integration, Ersteinrichtung sowie Steuerungszugriff, Fehlersuche und Wartung auch bei weltweit verteilten Produktionsanlagen.

Bilder der Doppelseite: Beckhoff Automation GmbH & Co. KG

Aufgrund der gewohnten Automatisierungsumgebung finden sich nicht nur professionelle Anwender wie Maschinenbauer oder Anlagenbetreiber gut in der TwinCAT-Cloud-Engineering-Architektur zurecht. Die TwinCAT-Cloud-Engineering-Instanz bietet auch für Einsteiger eine umfassende und ideale Grundlage, um die ersten Schritte in der TwinCAT-Umgebung zu vollziehen. Programmbeispiele und Video-Tutorials liefern die erforderlichen Hinweise und Informationen, um möglichst schnell mit dem System vertraut zu werden und erste eigene Automatisierungsprojekte zu erstellen. Die Tutorials sind hierbei nach verschiedenen Schwierigkeitsstufen sortiert, sodass sich auch Einsteiger mit Vorkenntnissen wiederfinden. Weiterhin informiert ein integrierter News Feed über TwinCAT-Neuheiten.

Vereinfachte Abläufe und Umsetzung

Über ein frei konfigurierbares Dashboard erhält der Anwender Übersicht über alle erstellten Instanzen. Aus dem Dashboard heraus lässt sich eine webbasierte Remote-Desktop-Verbindung mit der Instanz initiieren. Der Webbrowser dient als alleiniges Werkzeug, um die Verbindung über HTTPS herzustellen. Es werden keinerlei zusätzliche Softwarekomponenten oder Einstellungen in der Unternehmens-Firewall benötigt. Innerhalb der Instanz greift der Anwender über die bekannte TwinCAT XAE Toolchain auf sein Projekt zu und kann dies über ein Git-basiertes System kollaborativ oder als Backup zur Quellcodeverwaltung hinzufügen. Die Kommunikation aus der virtuellen in die physikalische Welt mit einer realen Steuerungshardware kann wahlweise über Secure ADS oder ADS-over-MQTT erfolgen. Die Datenverbindung wird über Sicherheitsmechanismen wie TLS-Verschlüsselung mit Zertifikaten abgesichert.
Die Bereitstellung einer TwinCAT-Cloud-Engineering-Instanz über einen speziellen, automatisierten Prozess dauert nur wenige Minuten. Durch die Integration der Arbeitsoberfläche in den Webbrowser müssen keine zusätzlichen Softwarekomponenten installiert und bedient werden. Der Zugriff kann zudem von beliebigen Betriebssystemen und Endgeräten aus erfolgen. Auch die Anbindung realer Steuerungshardware an die Instanz ist denkbar einfach, da für alle Komponenten derselbe Kommunikationsport verwendet wird. Die Integration in existierende IT-Infrastrukturen wird so vereinfacht.
Da sich pro Instanz mehrere Steuerungen anbinden lassen, sind Remote-Szenarien wie z.B. die Ferndiagnose einer Maschine oder das Debugging eines SPS-Programms möglich. Die Einrichtung eines HMI und der weltweite Zugriff darauf sind durch die in der Cloud ablaufende Visualisierung äußerst einfach. Der Projektaustausch über das Quellcode-Verwaltungssystem erfolgt nahtlos. Lokale TwinCAT-Installationen lassen sich ebenfalls anbinden, sodass die Projekte auch außerhalb der TwinCAT-Cloud-Engineering-Umgebung weiterverwendet und synchron gehalten werden können.
Über moderne Source-Control-Funktionalitäten von TwinCAT können Git-basierte Systeme angebunden und zur Verwaltung des Automatisierungsprojekts verwendet werden. Die TwinCAT-Multi-User-Funktion ermöglicht den einfachen und nahtlosen Zugriff auf das Source Control Repository ohne tiefgehendes Fachwissen des Anwenders.



TwinCAT Cloud Engineering schützt die Kommunikationsverbindung durch etablierte Standardmechanismen und stellt damit sicher, dass sich nur authentifizierte Benutzer und Geräte mit der Instanz verbinden können.

Cloudbasierte Datenanalyse für die Maschinenoptimierung

Mit TwinCAT Analytics bietet Beckhoff die Möglichkeit der punktuellen oder kontinuierlichen Datenanalyse. Hierfür stehen diverse Softwarewerkzeuge und Mechanismen zur Verfügung, die verschiedene Anwendungsfälle abdecken und dem Anwender einen schnellen Start in die Maschinenanalyse ermöglichen. Eine integrierte Code-Generierung ermöglicht die automatische Überführung der erstellten Analysekonfiguration in IEC61131-konformen SPS-Code, der sich dann in eine SPS-Laufzeit einbinden lässt. Dies ermöglicht eine 24/7-Analyse angeschlossener Maschinen.
Parallel zur Code-Generierung wird automatisch ein zugehöriges Analyse-Dashboard generiert. Dieses TwinCAT Analytics One-Click Dashboard basiert auf TwinCAT 3 HMI und ist in HTML5 plattformunabhängig realisiert. Dabei entsteht per einfachem Klick nicht nur das Dashboard an sich, sondern sogar die komplette, bei Bedarf im Nachhinein modifizierbare TwinCAT-3-HMI-Applikation inkl. HMI-Source-Code. Die Webseiten werden über den TwinCAT HMI Server bereitgestellt. Sowohl der TwinCAT Analytics Code als auch das Dashboard lassen sich innerhalb der TwinCAT-Cloud-Engineering-Umgebung verwenden. Durch die globale Erreichbarkeit der TwinCAT-Cloud-Engineering-Instanz kann von berechtigten Anwendern jederzeit und überall auf dieses Dashboard zugegriffen werden. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/1175

Sven Goldstein,
Produktmanager TwinCAT Connectivity & IoT,
Beckhoff Automation
www.beckhoff.de/twincat-cloud-engineering

Spezifikation für OPC UA Safety Release 1.00 fertiggestellt

Die Arbeitsgruppe OPC UA Safety hat die Veröffentlichung der Version 1.00 ihrer Spezifikation für funktionale Sicherheit fertiggestellt. OPC UA Safety basiert auf dem Black-Channel-Prinzip und adressiert die Controller-zu-Controller-Kommunikation über OPC UA Clients/Server. OPC UA Safety berücksichtigt alle Sicherheitsanforderungen, die in den internationalen Normen definiert sind, baut auf den Erfahrungen aus bestehenden Sicherheitsprotokollen auf und befasst sich mit neuen Anwendungsfällen, die sich seit ihrer Entwicklung ergeben haben. So unterstützt der Standard z.B. die Vergabe von Safety-IDs an Serienmaschinen und ermöglicht den Wechsel des Kommunikationspartners während der Laufzeit: Das ist eine wichtige Voraussetzung für moderne Produktionsprozesse mit Losgröße 1, bei denen Maschinen oder Maschinenteile häufig umgruppiert werden müssen.

OPC Foundation
www.opcfoundation.org

Erweiterung der Ethernet/IP-Spezifikation

Die ODVA hat Erweiterungen der Ethernet/IP-Spezifikation angekündigt, um eine verbesserte Netzwerkdiagnose, neue Methoden zur Reduzierung der Bandbreiten- und Ressourcenanforderungen für Geräte sowie die Erweiterung um eine IIoT-Baustein-Infrastruktur bereitzustellen. Die zusätzliche Ethernet/IP-Systemdiagnose vermittelt eine bessere Übersicht über die Anzahl der Verbindungen, die Ressourcennutzung, die Anzahl der Ethernet-Fehler, verpasste Pakete und die gesamte CPU-Auslastung. Die Definition einer skalierbaren Netzwerkdiagnosen-Assembly für Diagnoseverbindungspunkte, die durch andere Objekte definiert werden, führt dazu, dass diese neuen Statistiken bei der Fehlerbehebung im Netzwerk helfen können.

ODVA Inc.
www.odva.org

Entwicklungshilfe für CC-Link IE TSN und CC-Link IE Safety

Mesco bietet CC-Lin-IE-TSN- und CC-Link-IE-Safety-Entwicklungsdienstleistungen für Gerätehersteller von Automatisierungskomponenten. Durch modulare Konzepte und den Einsatz von Design Packages lassen sich TSN-basierte, sichere und nicht sicherheitsrelevante industrielle Kommunikationslösungen mit geringem Aufwand und Risiko implementieren. Das Entwicklungskonzept soll die Produktentwicklung von CC-Link-IE-TSN- und CC-Link-IE-Safety-konformen Slave-Geräten erleichtern und bietet einen schnellen und vereinfachten Einstieg in diese Technologien.

Mesco Engineering GmbH
www.mesco.de

Notfallhilfe gegen Ransomware-Angriffe

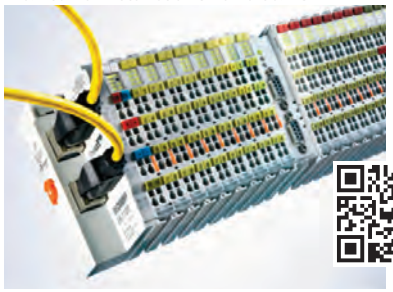
Bild: ©Peter Eggermann/Fotolia.de

Ist ein Cyberangriff auf die Unternehmensinfrastruktur erfolgreich, zählt insbesondere die schnelle Wiederherstellung der betrieblichen Systeme in einen stabilen und sicheren Arbeitsmodus. Der VDMA bietet dafür eine Übersicht von Notfallmaßnahmen und Kontaktdaten zu Behörden und Dienstleistern, die in solchen Fällen unterstützen können. Mit Ransomware-Angriffen können sämtliche Systeme von der Verwaltung über Webserver bis hin zur Produktion lahmgelegt werden. Nahezu jeder Fachverband im VDMA verzeichnet mindestens einen größeren Vorfall bei Mitgliedsunternehmen. Mit dem Notfallhilfe-Papier hat der VDMA gemeinsam mit Experten des Maschinen- und Anlagenbaus aus dem Arbeitskreis 'Informationssicherheit' die Antworten auf grundlegende Fragen nach einer Ransomware-Infektion zusammengeführt.

VDMA e.V.
www.vdma.org

Korrektur: Marktübersicht 'Serielle Adapter für Ethernet'

Bild: Beckhoff Automation GmbH & Co. KG



In der Marktübersicht ‘Serielle Adapter für Ethernet’ in der letzten Ausgabe des INDUSTRIAL COMMUNICATION JOURNALs ist uns bei einem der Produkte ein Fehler unterlaufen. Entgegen der abgedruckten Angaben, unterstützt die serielle Schnittstelle (RS422/RS485) EL6021 von Beckhoff Automation neben Ethercat auch die Industrial-Ethernet-Kommunikationsprotokolle Ethernet/IP, ModbusTCP und Profinet. Durch Scannen des QR-Codes gelangen Sie noch einmal zur korrigierten Version der Marktübersicht. Wir bitten darum, den Fehler zu entschuldigen! **www.i-need.de/?Produkt=11264**

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

Neue Spezifikation

Die IO-Link Community hat zum einfachen Austausch von Daten eine neue Spezifikation veröffentlicht. Diese beschreibt wie von IO-Link Daten über JSON REST und MQTT ausgetauscht werden können. Durch eine zusätzliche Festlegung der Semantik wird nun auch eine einfache Interpretierbarkeit der Daten möglich. Die Spezifikation umfasst sowohl die Definition einer API als REST-Schnittstelle als auch den Datentransport über MQTT. Mit dem standardisierten Austauschformat ergeben sich neue Möglichkeiten, wie z.B. herstellerübergreifendes Engineering oder der globale Zugriff auf Messwerte oder andere Monitoring-Daten. Z.B. können klassische Konfigurations-Tools durch JSON via REST herstellerübergreifend angebunden werden. Darüber hinaus werden auch schlanke Sensor-to-Cloud-Applikationen einfach möglich. So wird sogar die Umsetzung einer cloudbasierten Automatisierungsaufgabe mit herstellerunabhängigen Komponenten möglich.

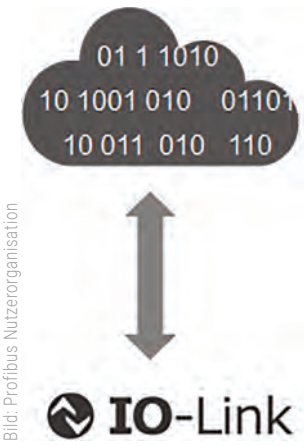


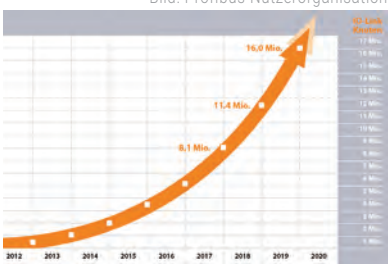
Bild: Profibus Nutzerorganisation

Profibus Nutzer-organisation e.V.
www.io-link.com

Profinet und IO-Link im Aufwind

Auch nach über 30 Jahren seit ihrer Gründung kommen die Technologien von Profibus & Profinet International (PI) im Markt gut an. Die größte Steigerung auf Jahressicht erfuhr in 2019 IO-Link mit 40%. Die Gesamtzahl der installierten IO-Link-Geräte beträgt jetzt mehr als 16 Millionen. Profinet verzeichnete mit der Jahreszahl von 6,4 Millionen installierten Geräten im Markt den bisher größten Jahreswert. Das entspricht einem Wachstum von 25% (Gesamtzahl: 32,4 Millionen Knoten).

Bild: Profibus Nutzerorganisation



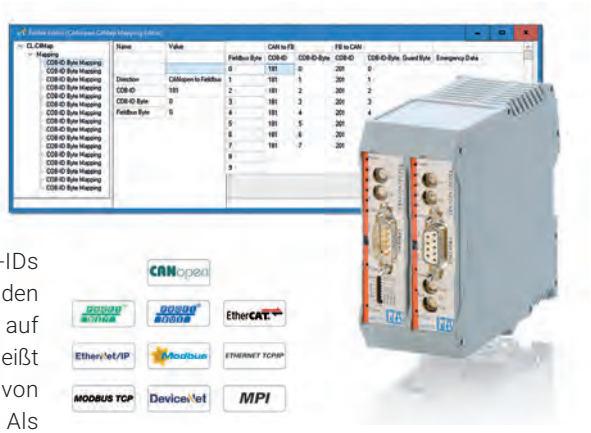
Profibus Nutzerorganisation e.V.
www.profibus.com

Monitoring- und Frühwarnsystem

Das von AIT Solutions entwickelte Netzwerkmanagement-System Herakles ist ein vielfältig einsetzbares Monitoring- und Frühwarnsystem, das die Anforderungen aller wichtigen Use-Cases in den verschiedenen Lebensphasen einer Maschine oder Anlage umsetzt. Es ist speziell für Netzwerke konzipiert, die Profinet einsetzen. Das System verwaltet nicht nur Anlagen, sondern auch die Lebenszyklen aller Einzelgeräte und wird damit zu einem passenden Werkzeug für das Asset Management. Zu den Leistungen des Systems gehören unter anderem die werksweite Zusammenführung aller Assets aus dem Profinet-Netzwerk, die Erkennung von topologischen Veränderungen im Netzwerk, die Berücksichtigung windowsbasierter Systeme, die Verfolgung des Geräte-LifeCycles sowie die Erkennung und Meldung von Konfigurationsveränderungen der Teilnehmer.

AIT Solutions GmbH
www.ait-solutions.de

Neue Funktionen für Gateway-Serie



Deutschmann Automation hat seine Gateway-Serie Unigate CX um neue Funktionen erweitert. Das betrifft vor allem die Bussysteme CANopen und CAN Layer 2. Für CANopen steht ein Mapping für COB-IDs zur Verfügung, das das Abbilden von Daten eines Feldbusses auf einen anderen Feldbus, das heißt das individuelle Kopieren von Prozessdaten, ermöglicht. Als Ausgangsdaten kommen dabei alle von den entsprechenden Feldbussen zur Verfügung gestellten Daten in Frage.

Deutschmann Automation GmbH & Co. KG
www.deutschmann.de

Switches und Router mit Cybersecurity-Funktionen

Die Anybus-Router und unmanaged und managed (Layer 2/Layer 3) Switches von HMS sind in einem Temperaturbereich von -40 bis +75°C einsetzbar. Mehrere Redundanz- und Cybersecurity-Funktionen sollen es Anwendern erlauben, zuverlässige und sichere Netzwerke aufzubauen. Die managed Layer 3 Switches bieten erweiterte Routing-Funktionen sowie die Netzwerksegmentierung und den Schutz sensibler Daten. Die erweiterten Funktionen sollen dabei ein hohes Maß an Sicherheitsfunktionen für die Datenkommunikation zwischen Fertigungs- und IT-Systemen gewährleisten.

HMS Industrial Networks GmbH
www.hms-networks.de

PC-Karten um abgesetzte M12-Netzwerkschnittstelle erweitert

Hilscher hat die PC-Karten der CifX-Familie um eine abgesetzte Netzwerkschnittstelle mit M12-Anschlusstechnik erweitert. Die Nutzung von M12 anstelle von klassischen RJ45-Steckverbindern ermöglicht die Verwendung in rauen Industrieumgebungen. Schutzklassen bis IP67 sind somit realisierbar. Durch die Schnittstelle AIFX-RE\M12 sind unabhängig von der Anschlusstechnik alle bestehenden Komponenten wie Kabel, Firmware, Konfigurationen, Tools und Hardware identisch und aus bestehenden Anlagen und Lösungen wiederverwendbar. Durch den reinen Plug&Play-Austausch lässt sich ein Wechsel von RJ45- auf D-kodierte M12-Steckverbinder in Real-Time-Ethernet-Systemen allein durch eine Gehäuseanpassung realisieren.

Hilscher Gesellschaft
für Systemautomation GmbH
www.hilscher.com

Softwarepaket für interoperable OPC-UA-over-TSN-Kommunikation

Bei der Implementierung von OPC-UA-over-TSN in seine Automatisierungs-Produkte arbeitet B&R mit TTTech Industrial zusammen. Aufgrund der Integration der Edge IP Solution von TTTech Industrial kann B&R seinen Kunden offene, interoperable und schnelle OPC-UA-over-TSN-Kommunikation anbieten. Bei Edge IP Solution handelt es sich um ein integriertes Softwarepaket, das Industrie-PCs, Switches und Feldgeräte mit TSN-Funktionen ausstattet. Die umfassende Implementierung von TSN hat es ermöglicht, die Entwicklungszeit für den Netzwerkteil zu verkürzen. Das Softwarepaket beinhaltet außerdem ein Acceleration-Modul, mit dem die OPC-UA-over-TSN-Produkte von B&R für alle relevanten Automatisierungsanwendungen genutzt werden können, unter anderem auch für die Steuerung von Motion-Anwendungen, die Hochgeschwindigkeit erfordern. Die TTTech-Lösungen decken den gesamten Bereich von TSN-Core-IP- und Embedded-Software bis hin zu automatisierten Netzwerkkonfigurations-Tools für OPC UA over TSN ab.

TTTech Industrial Automation AG
www.tttech.com

CPU/FPGA-BOARD FÜR IOT-EDGE-ANWENDUNGEN

Arrow Electronics hat gemeinsam mit Exor Embedded das GigaSom gS01 entwickelt, ein komplettes Produktionsdesign und Entwicklungskit mit einem leistungsstarken, energieeffizienten System-on-Module für IoT-Edge-Anwendungen. Das System-on-Module kombiniert die Leistung der Intel-Atom-E3900-Prozessorserie mit der Flexibilität des über eine Breitband-Dual-Lane-PCIe-Schnittstelle angeschlossenen Intel-Cyclone-10-GX-FPGA. Das Board ist ein kombiniertes Design aus X86-CPU und Intel-High-Speed-FPGA. Mit der Time-Coordinated-Computing-Technik, der Unterstützung für IEEE 802.1 Time-Sensitive Networking im FPGA-Referenzdesign und ausgerüstet mit einem Echtzeit-IoT-Stack, bietet das Board den für die Verarbeitung synchronisierter und Echtzeit-Smart-Factory-Anwendungen notwendigen Determinismus. Es kann mehrere Geräte wie Industrie-PCs oder HMI-Controller in einem einzigen Modul integrieren.

Arrow Central Europe GmbH
www.arrowce.com

Unmanaged Ethernet Switches

Moxa hat mit den Serien EDS-2000-EL und EDS-2000-ML eine neue Reihe industrieller Unmanaged Ethernet Switches mit 5 bis 18 Ports sowie GBit-Combo-Ports für die zuverlässige Vernetzung von zahlreichen Knoten mit hohen Bandbreiten eingeführt. Die Switches bieten Quality of Service und

Broadcast Storm Protection per DIP-Switch und ermöglichen es den Technikern vor Ort, zuverlässige Netzwerke per Plug&Play zu erweitern. Beide Serien eignen sich für eine Vielzahl von industriellen Anwendungen.

Moxa Europe GmbH
de.moxa.com

Sicherer Ausfallschutz

Die Rex100-Router-Familie von Helmholz wurde jetzt um die neuen Varianten Rex100 LTE+WAN sowie Rex100 WIFI+WAN ergänzt. Alle Router der Serie zeichnen sich durch ihre einfache und schnelle Konfiguration über das MyRex24-V2-Portal sowie durch ihre kompakte und handliche Bauform aus. Die Hardware der LTE- und WLAN-Varianten wurde um eine WAN-Schnittstelle erweitert. Diese zusätzliche Schnittstelle bietet im Zusammenspiel mit dem 4G- bzw. WiFi-Modem eine Fail-Over-Funktion, die als sicherer Ausfallschutz dient.

Helmholz GmbH & Co. KG
www.helmholz.de

Abnormal Condition Detection bei Sicherheitsventilen

Ideation hat mit dem CBM Predictor ein Wireless-iIOT-Gerät für Abnormal Condition Detection vorgestellt. Das Gerät hilft dabei, vorbeugende Wartungsintervalle bei Sicherheitsventilen zu strecken. Auf ein Sicherheitsventil montiert, liefert er zuverlässig Informationen zu Pop (Öffnen und Schließen der Feder) sowie Leak (Leckage des Ventils). Die Informationen werden dabei direkt im Gerät von den Daten der Vibrationsmessung und einem Algorithmus gebildet und gespeichert. Es handelt sich also nicht um einen reinen Sensor, sondern um einen echten Informationsserver. Per Bluetooth 5.0 Low Energy wird der Instandhalter auf seiner Android App über abnormale Zustände der Ventile informiert und die Informationen optional in Richtung Wartungssoftware weitergeleitet.

Ideation AS
IdeationCBM.com

Ethernet-Komponenten

Ausgereifte Technologie, hohe Performance und umfassende Abwärtskompatibilität: Das kennzeichnet die Ethernet-Standards und macht sie auch im Bereich der Industriekommunikation zur Nummer eins. Aber auch die permanente Weiterentwicklung (z.B. TSN) ist ein Wesensmerkmal dieser Technik.

Die Beständigkeit von Ethernet liegt in seiner Wandlungsfähigkeit. Und das ist eine Eigenschaft, die wir in der Automatisierungstechnik sehr gut gebrauchen können. Es ist heute kaum eine Anwendung denkbar, bei der die Auswertung von Prozessdaten für die Betreiber nicht von großem Interesse wären. Die Einbindung von Apparaten, Maschinen oder Anlagen in überlagerte Netzwerke bis hin zur Cloud stellt somit eine Grundfunktion dar, bei der Ethernet die zentrale Basistechnologie liefert. Egal ob große Datenmengen, hohe Performance oder präziser Determinismus: In der Industrial-Ethernet-Familie gibt es für alle Anforderungen gleich mehrere passende Lösungen. Und dank Gateway-Lösungen kann auch das ein oder andere 'historische' Automatisierungsgerät heute an der modernen Ethernet-Kommunikationswelt teilhaben – was will man mehr... *(kbn)* ■

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

Bild: © Thomas/stock.adobe.com

Die aktuellen Security Trends für Industrie- und Steueranlagen

Die Digitalisierung in der Arbeitswelt erlaubt effiziente Arbeitsmethoden und ein flexibles Geschäftsleben. Auch in Industrieunternehmen gibt es eine Vielzahl an neuen Web- und Cloudapplikationen sowie smarten Geräten im Unternehmensnetz. Hinzu kommt die zunehmende Vernetzung von Industrie- und Steueranlagen, die Vorgänge flexibilisiert und optimiert. Doch stellt sich zugleich die Frage, wie Unternehmen Automatisierungsumgebungen, Industrieanlagen und Kritis sichern können. Um die Sicherheit im gesamten, erweiterten Netzwerk zu schützen, sollten die Security-Teams für Industrie- und Steueranlagen die folgenden Entwicklungen und Trends im Auge behalten.

Das Zusammenwachsen von IT und OT eröffnet neue Angriffsvektoren: Weil IT, OT und IoT noch stärker miteinander verschmelzen, vergrößert sich die Angriffsfläche und die Zahl der Vektoren, die überwacht und verteidigt werden müssen. Unternehmen sollten prüfen, ob ihre Systeme trotz Air Gap erreichbar sind und OT-basierte Angriffe damit tatsächlich ein Problem für Sie darstellen. Sie müssen dabei ständig ihre OT-Umgebungen aktuell halten. Um Bedrohungen frühzeitig zu erkennen, sollten Betreiber ihre industriellen Steuerungssysteme (ICS, industrial control systems) auf Netzwerk- und Geräteebene durchgängig monitoren.

OT zu IT-Attacken sind auf dem Vormarsch

Angriffe, die zuerst die IT angehen und sich dann auf OT-Netzwerk ausweiten, sind in den letzten zwei Jahren häufiger aufgetreten. In diesem Jahr werden aber auch Angriffe zunehmen, die von OT-Systemen auf die IT übergreifen. Es ist zu erwarten, dass Hacker gezielt ICS-Geräte in OT-Netzen ins Visier nehmen, um über diesen Weg Zugriff auf die IT zu erhalten und beispielsweise an Kundendaten zu gelangen. Die Hacker nutzen dazu die schlechter gesicherten OT-Umgebungen, da diese einfacher zu kompromittieren sind und sie so leichter die Datenbestände der IT erreichen Security-Teams für IT und OT sollten eng zusammenarbeiten und Informationen miteinander teilen, um derartige Angriffe aufzudecken. Die Verantwortlichen müssen außerdem prüfen, ob Geräte befallen sind, und derartige Angriffe bereits auf der Geräteebene erkennen, bevor sie sich auf das gesamte Netzwerk ausbreiten. IT-Teams werden für OT-Sicherheit zuständig sein: Industrieunternehmen müssen akzeptieren, dass das Thema Sicherheit die OT- und IT-Teams gleichermaßen betrifft. Darüber hinaus werden höchstwahrscheinlich IT-Teams sich auch um die Sicherheit in OT-Umgebungen kümmern müssen. Schließlich haben sie jahrzehntelange Erfahrung darin, Anwendungen und Technologien zu schützen, die mit dem Internet verbunden sind. Die Verantwortlichen für OT-Netze haben sich jahrelang dagegen gewehrt, dass die IT auch Einfluss auf ICS erhält. Dies wird sich mit dem steigenden Bewusstsein für interne und externe Gefahren aber ändern. Wahrscheinlich werden IT-Teams künftig deshalb auf Basis der Anforderungen von OT-Teams die Richtlinien für OT-Security definieren. Traditionell unterscheiden sich die Ansätze für IT- und OT-Sicherheit. Nun ist es an der Zeit, diese miteinander zu verbinden. Industrieunternehmen soll-

ten sich die bewährten Methoden der IT- und OT-Sicherheit aneignen und darauf basierend eine Architektur entwickeln, die Einblick, Sicherheit und Kontrolle bietet.

ICS-as-a-Service

ICS-as-a-Service wird in Zukunft häufiger eingesetzt werden: In den kommenden 12 Monaten setzt sich die Cloud als verlässlicher Weg zur Bereitstellung von OT-Sicherheit durch. Dies gilt vor allem dort, wo physikalische Installationen nicht praktikabel oder möglich sind. OT-Security, die via Cloud realisiert wird, etabliert sich auch in anderen Bereichen der IT-Infrastruktur: Customer Relationship Management (on-premise), Software-as-a-Service, Antivirus-Lösungen (lokal und online) sowie Host- oder Cloud-basierte Endpoint-Detection oder Response-Lösungen. Die Cloud lässt viele Möglichkeiten zum Sichern von Grid-Umgebungen zu, wie z.B. das Teilen von anonymisierten Daten mit anderen OT-Umgebungen. Dies erleichtert es, Angriffe früher zu entdecken und Schwachstellen schneller zu beseitigen. Über die Cloud können Unternehmen OT-Sicherheit auch an Orten einrichten, an denen die Installation zusätzlicher Anlagen nicht umsetzbar ist.

Edge und Fachkräftemangel

Der Netzwerkrand ist stärker gefährdet als der Netzwerkkern: Angreifer werden voraussichtlich vermehrt auf schwächer gesicherte OT-Infrastrukturen abzielen, wie z.B. kleinere Umspannungswerke. Zweigstellen sind in der Regel mit größeren OT-Netzen verbunden. Deshalb besteht beim Angriff auf eine Zweigstelle die Gefahr einer Kettenreaktion. OT-Security-Installationen sollten nicht nur die Hauptniederlassungen abdecken, sondern auch Zweigstellen schützen. OT-Security via Cloud sichert Niederlassungen ab, denen aktuell nicht die gleichen Security-Möglichkeiten wie der Zentrale zur Verfügung stehen. Der Fachkräftemangel wird sich auch auf die OT-Sicherheit auswirken: Derzeit sind etwa 4 Millionen Stellen für IT-Sicherheit unbesetzt. (ISC)², die weltweit größte Vereinigung von Cybersecurity-Profis nimmt an, dass im Jahr 2022 die Situation im Bereich OT-Sicherheit mit 1,8 Millionen unbesetzten Stellen ähnlich sein wird. Tenable geht davon aus, dass bereits in diesem Jahr der Fachkräftemangel bei IT und OT schon Risiken hervorrufen wird. Dies liegt daran, dass die Angestellten derzeit nicht das nötige Fachwissen für IT oder OT haben und auch keine qualifizierten Neukandidaten vorhanden sind. Unternehmen sollten herausfinden, wo bereits jetzt Lücken bestehen und dann das aktuelle Wissen ihrer OT SCADA-Teams und der IT-Security Fachkräfte überprüfen. Wissenslücken werden dann durch entsprechend spezialisierte Schulungen geschlossen. Diese Herausforderungen sind eine gute Gelegenheit, neue Talente aus den Universitäten zu rekrutieren oder Kandidaten mit weniger Erfahrungen anzustellen und diese von Anfang an in IT- und OT-Security zu schulen.

Fazit

Cybersecurity ist mittlerweile einer der wichtigsten Aspekte bei industriellen Steuerungsanlagen. Vollständiger Einblick sowie umfassende Kontrolle und Sicherheit sind nötig, um allen Risiken professionell zu begegnen. Das gilt für sämtliche Anlagen wie Fernbedienungs-Terminals, SPSen, Unterbrecher, Messinstrumente, Motoren und viele andere Gerätearten. Diese Trends werden die Sicherheitsteams in Industrieunternehmen heuer und darüber hinaus beschäftigen. Daher sollten Unternehmen gut darauf vorbereitet sein. ■

Tenable Network Security GmbH
www.tenable.com

Die fortschreitende Automatisierung von Produktionsanlagen macht einfache und zuverlässige Testung unverzichtbar.

Ausfallzeiten bei Industrial-Ethernet-Netzen verhindern

No Downtime

Für Industrieunternehmen ist mangelndes Knowhow bei der Diagnose von Störungen in Ethernet-Netzen mehr als riskant. Schließlich stehen Liefertreue, Produktqualität und das gesamte Unternehmensimage auf dem Spiel.

Viele Hersteller nutzen für ihre automatischen Betriebsabläufe als Kommunikationssystem Industrial-Ethernet, das ursprünglich entwickelt wurde, um Computer mit Geräten in der industriellen Fertigung zu vernetzen. Der Datenaustausch in Produktions- und Verpackungsanlagen beschränkt sich zwar nur auf relativ wenige Daten, die aber nahezu in Echtzeit übertragen werden müssen. Beispielsweise ist ein Roboter, der eine Flaschen-Abfüllanlage bedient, darauf angewiesen, dass die benötigten Daten sofort und exakt zum jeweiligen Zeitpunkt des Produktionsschrittes eintreffen. Seit vielen Jahren ist die Automatisierung in der Fertigungsindustrie immer raffinierter geworden und viele Unternehmen nutzen die Vorteile von hochtechnisierten Anlagen. Allerdings sind die Vorteile dieser investitionsintensiven Systeme nur dann gewinnbringend nutzbar, wenn sie störungsfrei funktionieren. Meistens sind moderne Produktionslinien mit unterschiedlichen Überwachungssystemen ausgestattet. Jedoch konzentrieren sich diese eher darauf, akute Probleme bei deren Auftreten zu melden, anstatt bereits im Vorfeld Veränderungen im Industrial-Ethernet-Netzwerk aufzudecken, die möglicherweise erst später zu Störfällen führen können.

Fachkräftemangel

Das größte Problem besteht jedoch darin, dass in vielen Werken keine Techniker arbeitet, die sich mit Industrial-Ethernet auskennen. Wenn eine Störung

Bilder der Doppelseite: Ideal Industries GmbH

Navitek IE ist ein kompakter Handtester zur Inbetriebnahme, präventiven Wartung und Fehlerdiagnose für Profinet- und Ethernet-Standardnetze.

auftritt, muss diese das Produktionsteam oder ein externer Dienstleister beheben. Das kann dazu führen, dass aufwändig getestet und auf Verdacht ein neues Gerät installiert oder die Software aktualisiert wird. Diese Vorgehensweise ist sowohl aufwändig als auch ineffizient. Definitiv wirtschaftlicher ist eine regelmäßige vorbeugende Wartung in der die Funktion aller in der Produktionsanlage installierten Geräte und Komponenten kontrolliert wird, um rechtzeitig Korrekturmaßnahmen ergreifen und Ausfälle vermeiden zu können. Diese Tests müssen kritische Ereignisse, wie die doppelte Vergabe von Namen und IP-Adressen, eine unterbrochene Kommunikation zwischen den Geräten oder zu viele Paketfehler, die unter Umständen den Betrieb der Geräte beeinträchtigen und eine schnelle Fehlerbehebung erfordern, ermitteln. Selbst wenn ein verdächtiges Gerät augenscheinlich noch funktioniert, kann es bereits Probleme geben, die im Rahmen der vorbeugenden Wartung erkannt und behoben werden können.

Vorteil Tester

Der kompakte Industrial-Ethernet-Tester Navitek IE wurde speziell für Produktionsteams entwickelt, die vorbeugende Wartungstests durchführen und die Fehlerdiagnose beschleunigen müssen, da er exakt die Fehlerursache sowie die Fehlerstelle ermittelt. Das Gerät empfiehlt sich besonders für Tests und Fehlerdiagnosen in Profinet-Netzen: Der Tester erkennt sofort, ob das Netzwerk oder das Kabel die Ursache für die Störung ist. Bei einem Kabelproblem zeigt er an, wo sich die Fehlerstelle befindet. Der bedienerfreundliche Tester vereinfacht die Installation, da er nicht nur handlicher als ein PC mit Spezialsoftware ist, sondern ein wirklich kompakter Tester, mit dem komfortabel Berichte erstellt werden können, die als Leistungsnachweis für das überprüfte Netzwerk nutzbar sind. Die gleichen Berichte erlauben auch, die einwandfreie Funktion des Netzwerks und die korrekte Installation der Kabel nachzuweisen. Sollte die Störung anhalten, muss die Fehlerursache also woanders liegen.

Fazit

Die Robotisierung wird weltweit unaufhaltsam fortschreiten, damit Hersteller ihre Produktivität und die Rentabilität weiter steigern können. Deshalb ist es unabdingbar, dass Mitarbeiter mit Industrial-Ethernet-Netzen vertraut sind und diese mit den entsprechenden Messgeräten korrekt testen und warten können. ■

Neuer Mobilfunkstandard für die Industrie

Testfelder für KMU

Vier Testumgebungen für 5G gibt es im Ländle bereits. Nun kommt in Karlsruhe eine weitere hinzu. Alle fünf stehen kleinen und mittelständischen Unternehmen offen, um den neuen Mobilfunkstandard zusammen mit Forschungseinrichtungen zu erproben sowie Produkt- und Geschäftsideen zu entwickeln, die ohne 5G nicht möglich wären. Die Bewerbung um gemeinsame Projekte ist ab sofort möglich.

5G, die fünfte Generation des Mobilfunks, berücksichtigt erstmals die Bedürfnisse der Industrie. So ermöglicht der neue leistungsstarke Mobilfunkstandard die bedarfsgerechte Vernetzung mit hoher Bandbreite, niedriger Latenz und hoher Verbindungsanzahl – und schafft so die Grundlage für Industrie 4.0 sowie das Internet der Dinge. Um zu erforschen, welche neuen Produkte und Geschäftsideen mit 5G möglich werden, werden bereits vier 5G-Testumgebungen in Stuttgart, Mannheim, Reutlingen und Freudenstadt aufgebaut. Eine fünfte kommt nun in Karlsruhe hinzu. Das Ministeriums für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg hat den entsprechenden Förderbescheid über 900 000 Euro an das Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA in Stuttgart verschickt. Wissenschaftler des dortigen Kompetenzzentrums DigITools koordinieren das Forschungsprojekt »Transferzentrum 5G4KMU«. Beteiligt sind außerdem die Projektgruppe für Automatisierung in der Medizin und Biotechnologie PAMB des Fraunhofer IPA, das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, das Reutlinger Zentrum Industrie 4.0, das Centrum für Digitalisierung, Führung und Nachhaltigkeit Schwarzwald (kurz: Campus Schwarzwald) in Freudenstadt – und nun auch das wbk Institut für Produktionstechnik des Karlsruher Instituts für Technologie (KIT).

Fünf Testumgebungen, fünf Forschungsschwerpunkte

Die Forscher am KIT beginnen nun mit dem Aufbau der neuen 5G-Testumgebung. Sobald sie in Betrieb ist, wollen sie diese nutzen, um u.a. Fragestellungen rund um die vorausschauende Instandhaltung von Maschinen und der dafür nötigen Auswertung von Daten durch intelligente Algorithmen zu beleuchten. Weitere Forschungsschwerpunkte liegen beispielsweise in der Lokalisierung von Betriebsmitteln, Augmented-Reality-Brillen und der Interaktion von Mensch und Maschine. Abhängig von ihren Kernkompetenzen setzen die vier bestehenden 5G-Testumgebungen andere Schwerpunkte. So konzentriert sich in Stuttgart das Fraunhofer IPA auf Potenziale von 5G für Fabriken und Produktionssysteme, während sich das Fraunhofer IAO mit Smart Services und Smart Products beschäftigt. In Freudenstadt legt der Campus Schwarzwald den Fokus auf Fragestellungen rund um die Produktion, wobei der Maschinenbau und die Fertigungsindustrie im Mittelpunkt stehen. Am Reutlinger Zentrum Industrie 4.0 stehen Logistik und die Informationsbereitstellung in Unternehmen im Fokus. In Mannheim untersucht die Projektgruppe für Automatisierung in Medizin und Biotechnologie PAMB, welche Möglichkeiten 5G Kliniken und medizinischen Labors eröffnet.

Bewerbung um Quick Checks ab sofort möglich

Alle fünf Testumgebungen stehen kleinen und mittelständischen Unternehmen offen, um den neuen leistungsstarken Mobilfunkstandard 5G zusammen mit den Forschungseinrichtungen zu erproben. Die Zusammenarbeit ist im Rahmen sogenannter Quick Checks möglich. Dabei prüfen die Wissenschaftler von den Unternehmen eingereichte Produkt- und Geschäftsideen auf ihre Machbarkeit. Die Bewerbung um Quick Checks ist ab sofort möglich. Anschließend kann die weitere Zusammenarbeit in Form eines sogenannten Exploring Projects erfolgen. In einem Exploring Project wird gemeinsam mit den Unternehmen ein Konzept entworfen, prototypisch implementiert und im 5G-Netz einer der fünf Testumgebungen erprobt. Die Aufwände der Forschungseinrichtungen für Quick Checks und Exploring Projects werden aus den Mitteln des Transferzentrums 5G4KMU finanziert, sodass teilnehmenden Unternehmen keine Fremdkosten entstehen. Auf der Projekthomepage sind die entsprechenden Bewerbungsformulare zu finden. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/4102

Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA
www.5g4kmu.de

Bild: Rainer Bez / Fraunhofer-Institut IPA

Cisco Cyber Vision entdeckt Cybergefahren für Industrieanlagen in Echtzeit.

Sicherheitsarchitektur für das Industrial IoT

Transparente Sicherheit

Kritische Infrastruktur wie Energie, Transport und Produktion fußt maßgeblich auf Betriebstechnologie (OT). Die Basis dafür bilden Netzwerke. Unternehmen benötigen zunehmend Echtzeit-Zugriff auf die Daten dieser Systeme, um Produktion, Sicherheit und Kostenmanagement zu optimieren. Cisco stellt eine IoT-Sicherheitsarchitektur vor, die eine verbesserte Transparenz für IT- und OT-Umgebungen bietet und industrielle Prozesse schützt.

Cybersecurity-Bedrohungen für kritische Infrastrukturen steigen und stellen eine erhebliche Gefahr für Mitarbeiter sowie ein finanzielles Risiko dar. „Änderungen an Geräten und Verbindungen müssen schnell erkannt, auf Schwachstellen untersucht und bei Bedarf behoben werden, bevor die Sicherheit der Organisation untergraben wird“, erklärt Sid Snitkin, Vice President der ARC Advisory Group. Durch die Zusammenführung von IT und OT in Security Operations Centern will Cisco umfassende Sicherheit mit fortschrittlicher Anomalie-Erkennung und integrierter Bedrohungsanalyse bieten „Unternehmen benötigen vollständigen Einblick in die unterschiedlichsten Netzwerkumgebungen, um ihren industriellen Vorsprung zu sichern, das Risiko von Cyber-Bedrohungen zu senken und ihre Prozesse zu optimieren“, so Liz Centoni, Senior Vice President und General Manager Cloud, Compute und IoT bei Cisco.

Sicherung der industriellen Netzwerkumgebung

Cisco Cyber Vision ist die erste softwarebasierte Sicherheitslösung für die automatische Erkennung von industriellen Anlagen, die über das Cisco Industrial IoT (IIoT) Netzwerk-Portfolio bereitgestellt wird. Sie analysiert den Datenverkehr von vernetzten Anlagen und erstellt Segmentierungsrichtlinien in Cisco ISE und DNA Center, um eine Verbreitung von Bedrohungen in den Betriebsumgebungen zu verhindern. Die Lösung basiert auf der Talos Threat Intelligence und bietet ein Echtzeit-Monitoring von Cybersecurity-Gefahren für industrielle Anlagen und Prozesse, die sich auf die Betriebszeit, Produktivität und Sicherheit auswirken.

Daten-Governance vom Edge bis zur Multi-Cloud

Integriert in Ciscos industrielle Netzwerke vereinfacht Edge Intelligence die Extraktion von Daten am Netzwerkrand. Die Lösung macht die Datenbereitstellung für Multi-Cloud- und On-Prem-Systeme effizienter. Zudem verbessert sie die Wettbewerbsfähigkeit eines Unternehmens sowie das Management der Daten in allen kritischen Aspekten ihres Lebenszyklus. Somit wurde die Komplexität einer Multi-Vendor-, Multi-Daten- und Multi-Asset-Infrastruktur beseitigt. So stellt das Unternehmen einfache IoT-Cybersecurity-Lösungen bereit, die sich auf jedem beliebigen Gateway, Switch oder Router von Cisco verwalten lassen. ■

Jürgen Hahnrath,
Head of IoT Germany,
Cisco Systems GmbH
www.cisco.com

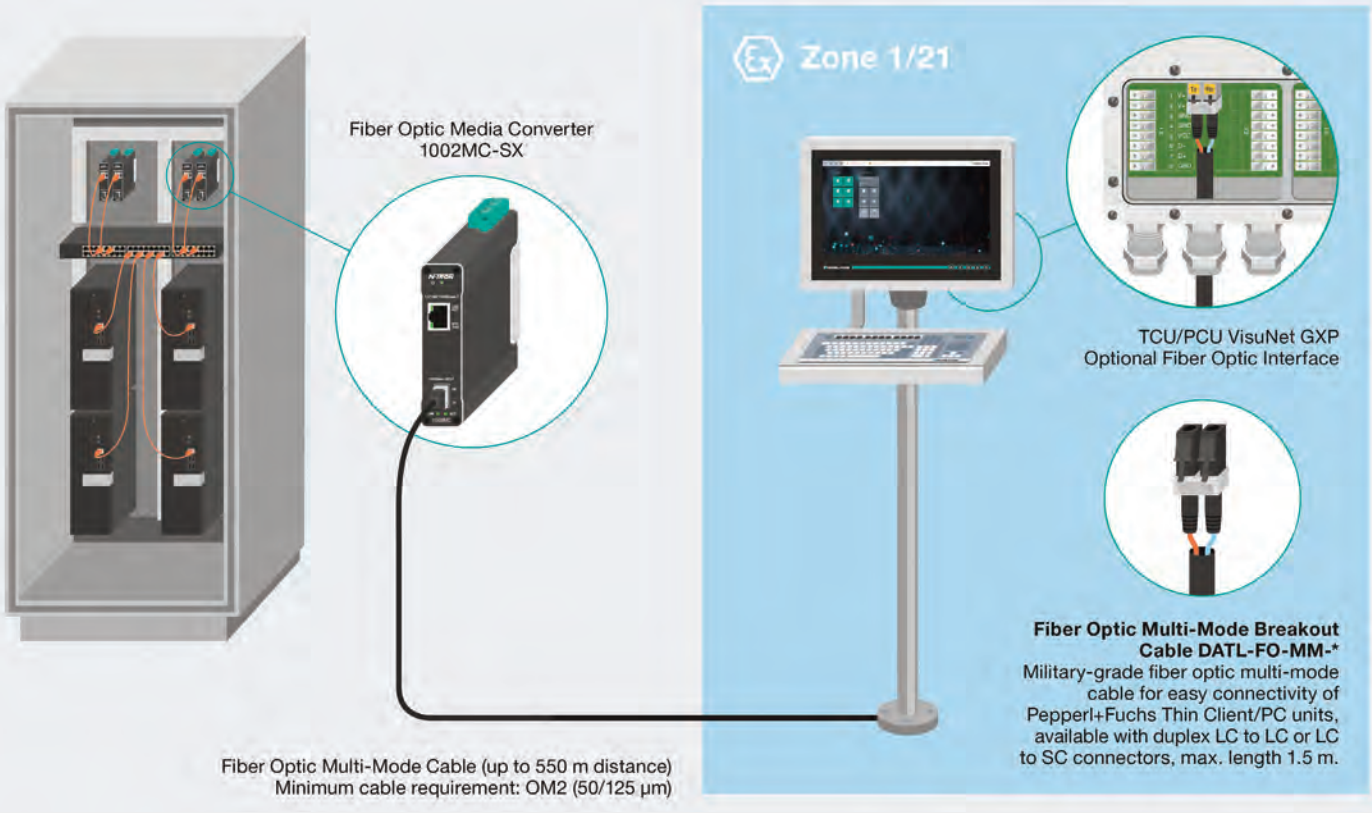
Bild: Cisco Systems GmbH

Schnell, weit und einfach installiert

Lichtwellenleiter im Ex-Bereich optimal umgesetzt

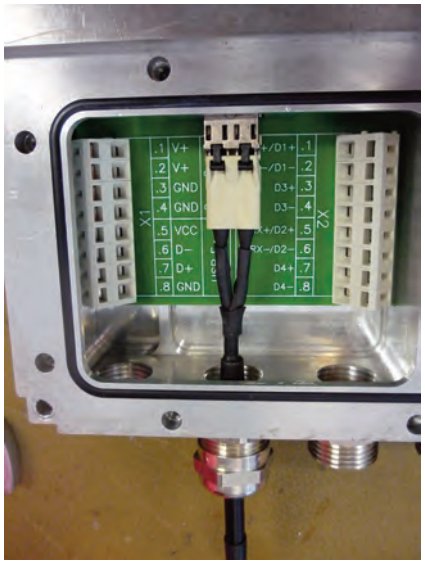
In den meisten Anwendungen werden typischerweise kupferbasierte Kabel an ein vorhandenes oder neu definiertes Netzwerk angeschlossen, doch gerade in sehr großen Industrieanlagen kommt diese Technologie bei langen Übertragungsstrecken aufgrund des Installationskonzeptes oder auch durch Abweichungen der Anforderungen hinsichtlich elektromagnetischer Verträglichkeit (EMV) an ihre Grenzen. Die Alternative bieten hier Lichtwellenleiter (LWL), auch bekannt als Glasfaserverbindungen.

In der Prozessindustrie finden Lichtwellenleiter ihren Einsatz vor allem in der Kommunikation, wenn lange Strecken überbrückt werden müssen. Kommt es zum Anschluss an klassische Bedienstationen, die in explosionsgefährdeten Bereichen installiert sind, ergeben sich besondere Anforderungen. Da gebündeltes Licht eine hohe Energie besitzt und somit eine potentielle Zündquelle darstellen kann, bedarf es einer Bewertung nach Ex-Gesichtspunkten. Hierfür bieten sich nach der IEC Norm 60079-28 unterschiedliche Methoden an. Die wohl populärste Schutzart, die insbesondere bei Bedienstationen eine weite Verbreitung findet, ist die 'optische Eigensicherheit' (engl. Optical Intrinsically Safe 'op is'), die – ähnlich wie die klassische Eigensicherheit – die übertragene Leistung soweit reduziert, dass diese nicht für die Zündung eines explosionsfähigen Gemischs ausreicht. Mit der letzten Fassung der IEC Norm in 2017 wurde eine hilfreiche Neuerung bzgl. der optischen Eigensicherheit eingeführt, die den Einsatz von LWL im Ex-Bereich erleichtert. Kern der in der IEC60079-28 formulierten 'Ausnahme 3' ist, dass nun auch Betriebsmittel, die die Grenzwerte der Laser Klasse 1 der Norm IEC60825-1 einhalten, im explosionsgefährdeten Bereich bis in die Zone 1/21 betrieben werden können. Da Laser der Klasse 1 ebenfalls nur eine reduzierte Leistung für den Schutz des Augenlichts haben dürfen, sind diese Grenzwerte ausrei-



Einfache Plug&Play Installation bis in die Zone 1/21 (z.B. hier Multimode)

Bilder der Doppelseite: Pepperl+Fuchs AG



Enge Anschlussräume sowie die Ex-Anforderung nach einem IP Schutz stellt eine Herausforderung beim Anschluss von LC Steckern dar.

Mit dem LWL-Breakout-Kabel bietet P+F ein Zubehör an, um die LC Steckverbinder normkonform nach Ex-Richtlinie zu installieren.

chend um den Anforderungen einer 'optisch eigensicheren' Strecke gerecht zu werden. Daraus resultiert, dass Betriebsmittel, die Laser Klasse 1 erfüllen, ohne ein zusätzliches 'op is' Marking, äquivalent installiert und betrieben werden dürfen. Diesen Normen-Änderung hat sich Pepperl + Fuchs zu nutzen gemacht und ihre Bedienstationen der Serie VisuNet GXP mit optionalen LWL-Schnittstellen (Multimode als auch Singlemode) ausgestattet, welche die Grenzwerte nach IEC60825-1 Laser Klasse 1 erfüllen und somit dem neuesten Stand der Norm, ohne explizite 'op is'-Kennzeichnung entsprechen. Der einfache Aufbau besteht aus einer Bedienstation, beispielsweise dem VisuNet GXP mit optionaler LWL-Schnittstelle, dem angeschlossenen LWL-Kabel und einem Media Konverter, für den Übergang auf ein Kupferkabel. Eine weitere Herausforderung im Ex-Bereich besteht darin die Dichtigkeit der einzelnen Schnittstellen zu gewährleisten und den kompletten Aufbau IP-konform zu gestalten. Eine einfache Durchführung des eckigen LWL-Steckers durch die runden Kabelverschraubungen ist hier schwierig. Gelöst werden kann dies nur mit aufwändigen Spleiß-Vorgängen (verschweißen von zwei Kabelenden) durch Experten, was im engen Anschlussraum kaum möglich ist und somit außerhalb des Gehäuses erfolgen müsste oder mit dem passenden Zubehör. Für die VisuNet GXP Familie bietet Pepperl+Fuchs hier passende Zubehörkabel an, die an die vorkonfigurierte Schnittstelle der Bedienstation angeschlossen werden können. Der mechanische Anschluss wird mit einem LC-Steckverbinder realisiert. Die integrierte Kabelverschraubung sorgt für eine nahtlose Verbindung, sodass der IP66 und der EX-Schutz weiterhin gewährleistet sind. Der aufwendige Spleißvorgang kann somit umgangen werden. Die Steckverbinder werden in einem nächsten Schritt über einen –LC oder –SC Steckverbinder, bei den es sich um die gängigsten Steckverbinder handelt an das installierte LWL-Kabel angeschlossen. Im Beispiel des Multimode Kabels können Distanzen bis zu 550m mit Datenraten von 1GB/s abgebildet werden. Der Übergang zurück auf das Kupferkabel wird durch einen Media Konverter realisiert. Pepperl+Fuchs bietet hier bereits getestete und qualifizierte Konverter an, die die Lichtsignale wieder in elektrische Signale umsetzen. Im Falle von größeren Installationen, können auch passende SFP Module eingesetzt werden, die einen direkten Anschluss an einen Switch ermöglichen. Durch die einzelnen abgestimmten und zertifizierten Komponenten erfolgt eine einfache und schnelle Integration der LWL-Technologie in das vorhandene Netzwerk. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/14546

Pepperl+Fuchs AG
www.pepperl-fuchs.com

Mit dem digitalen Zwilling zur Smart Factory

Digitale Allianz

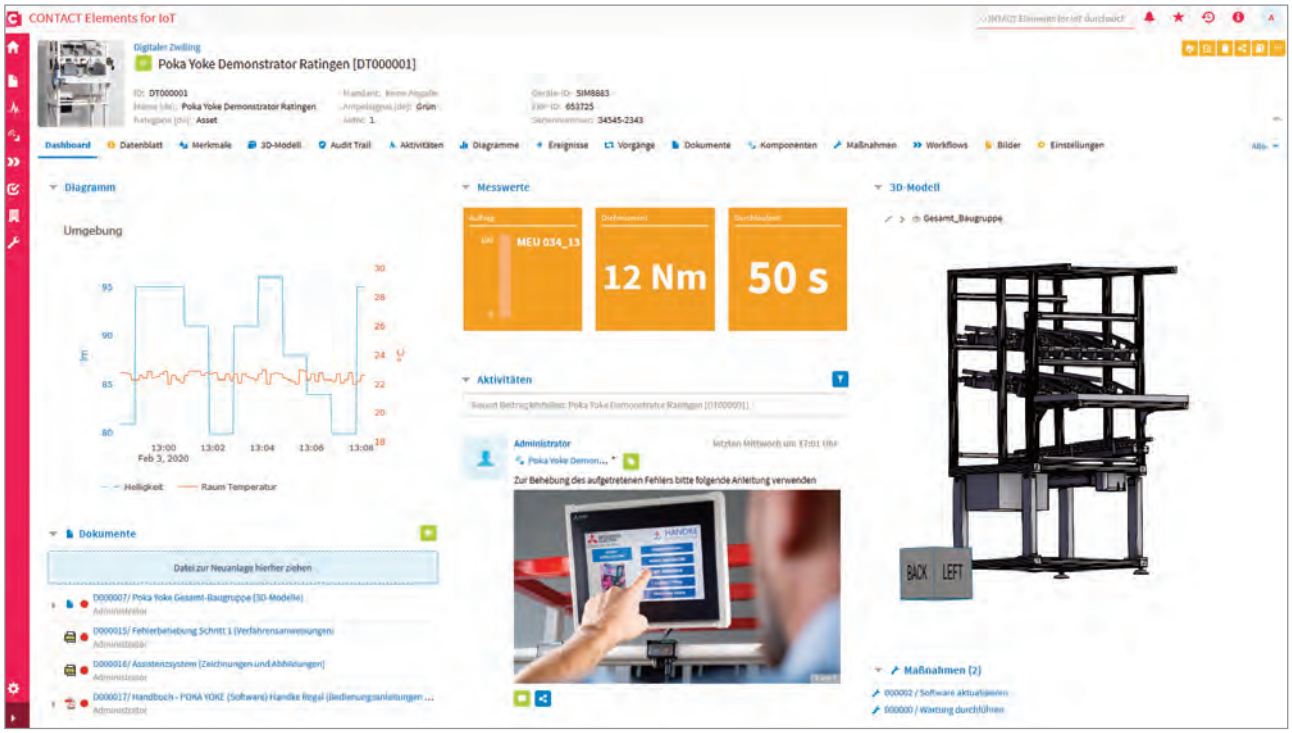


Bild: Contact Software GmbH

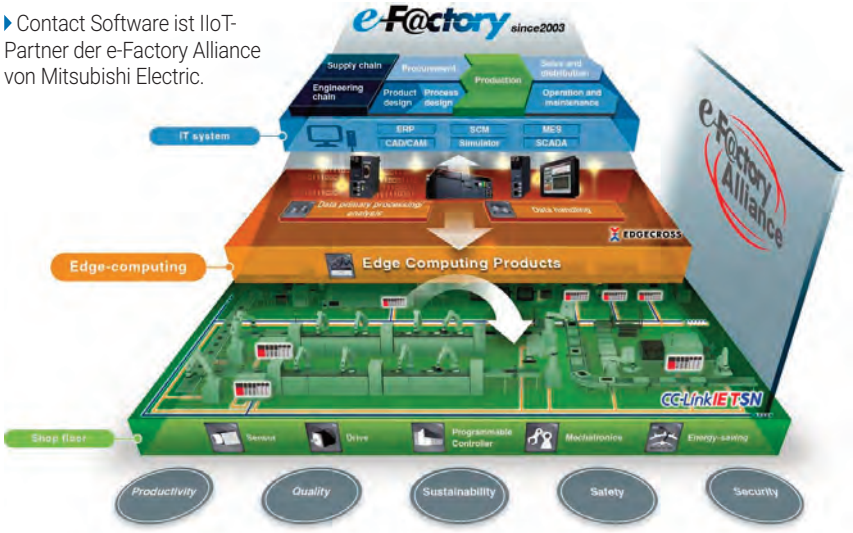
Im Showroom von Mitsubishi Electric wird der digitale Zwilling einer Poka-Yoke-Anwendung gezeigt.

In modernen Produktionsanlagen und Maschinenparks hat die Digitalisierung Einzug gehalten. Von der Optimierung der Fertigung bis hin zu neuen Geschäftsmodellen diskutiert die Industrie viele Szenarien. Im Zentrum steht hier der digitale Zwilling als Bindeglied zwischen realer und virtueller Welt. Sein Einsatz verspricht enorme Vorteile durch die Option, Anlagen in Echtzeit zu überwachen, neue kundenorientierte Dienste zu entwickeln und aus Datenanalysen Rückschlüsse für Prozess- und Produktverbesserungen zu ziehen.

Neuere Anlagen oder Komponenten kommunizieren bereits mit geeigneten Protokollen wie MQTT. Durch die Vernetzung der Produktionsumgebung mittels Gateways und der Verfügbarkeit von Sensoren rund um die Maschinen stehen kontinuierlich Livedaten zur Verfügung. Der digitale Zwilling verwaltet diese Daten, gibt Auskunft über den Betriebszustand der realen Maschine und trägt Informationen aus allen Phasen des Produktlebenszyklus zusammen. Gleichzeitig dient er als Kollaborationsbasis für den Datenaustausch und hilft dabei automatisch zu steuern, wie die Gesamteffizienz des Shop Floors verbessert werden kann.

Anforderungen der Industrie 4.0

Unternehmen betreiben oft mehrere, teils global verteilte Produktionsstandorte. In diesen Fabriken laufen diverse Linien mit Teilprozessanlagen und Komponenten von unterschiedlichen Herstellern. Diese Umgebungen mit allen relevanten Informationen wie Sensordaten, Komponentenstrukturen, Service-Stücklisten und Produktdokumentationen muss der digitale Zwilling abbilden können, um die Gesamtperformance sicherzustellen. Insellösungen verhindern oft noch das effektive Zusammenspiel von operativer Ebene (OT) und strategischen IT-Unternehmenswendungen wie ERP, MES oder PLM. Herausforderung jeder IoT-Lösung ist der reibungslose Datenfluss. Die Contact Elements Plattform bietet eine offene Infrastruktur, die alle Daten des digitalen Zwillings zwischen den OT- und IT-Systemen orchestriert. Ganz gleich, ob dies in Public Clouds wie AWS und MS Azure, einer Private Cloud oder im eigenen Rechenzentrum erfolgt. Der digitale Zwilling wird als konkrete Ausprägung einer ausgelieferten oder auszuliefernden Produktinstanz vom Digital Master abgeleitet. Er



Contact Software ist IIoT-Partner der e-Factory Alliance von Mitsubishi Electric.

Bild: Mitsubishi Electric Corporation

wird je nach Anwendungsfall mit unterschiedlichen Informationen versorgt und steuert die systemübergreifenden Geschäftsprozesse über frei definierbare Workflows, die Fachanwender nach dem No-Code-Prinzip auch selbst gestalten können. Moderne Webtechnologien stellen Daten und Dialoge auf unterschiedlichen Endgeräten passgenau bereit. Von unterwegs oder am Tablet in der Produktion auf aktuelle Aufgaben und Dokumente zugreifen, per Smartphone live diskutieren: Innovative UX-Konzepte und die mobile Verfügbarkeit machen es Anwendern besonders einfach, alle für ihre Arbeit benötigten Informationen auf einen Blick im individuellen Dashboard zu finden und mit anderen zu kommunizieren.

Anwendungen des digitalen Zwillings

Eine Anlage ist mit ihrer 3D-Ansicht inklusive Stückliste mit 'Redlining-Funktion' im digitalen Zwilling abgebildet. Die Stückliste wird ebenfalls zu einer Komponentenstruktur komprimiert, um z.B. wichtige Verschleißteile anzuzeigen. Wird ein Ersatzteil benötigt, kann eine Bestellung im ERP-System automatisch ausgelöst werden. Über die integrierten Chat-Funktionen teilen Mitarbeiter neue Erkenntnisse und setzen diese immer in den Kontext der realen Anlage. Bei der Fernüberwachung interagiert eine Anlage über das Internet mit ihrem digitalen Zwilling. Sensoren erfassen die Zustandsdaten im laufenden Betrieb, die gesammelt, verdichtet und ausgewertet werden. Prozessverantwortliche können auch einzelne Komponenten genauer betrachten und optimieren. Ihr Zustand wird über eine Ampel visualisiert, um einen schnellen Eindruck zu vermitteln. Bei kritischen Abweichungen wird ein Alarm gestartet, der Hinweis geltungssicher abgelegt und Gegenmaßnahmen eingeleitet. Unternehmen können die Datenanalysen für eine Fehlerbehebung, die vorausschauende Wartung oder auch Produktverbesserungen nutzen. Moderne IoT-Plattformen wie Elements for IoT ermöglichen mittels hinterlegter Algorithmen die automatische Auswertung der gesammelten Betriebsdaten am digitalen Zwilling. Über frei definierbare Grenzwerte wird der Idealbereich der entsprechenden Kennzahl für das Unternehmen bestimmt. Die online-berechneten Kennzahlen werden als Reports, die Anwender spezifisch konfigurieren können, in den Dashboards angezeigt. Ist die OEE für eine Anlage oder Linie berechnet, lassen sich durch Vergleiche mit anderen Maschinenparks Qualitäts- oder Performanceunterschiede aufdecken. Bei signifikanten Abweichungen können Anwender Prozess- und Zustandshistorien untersuchen und so Unterschiede begründen. Die Sammlung der Daten erfolgt in einem zentralen System, da sonst unterschiedliche Quellen zur Weiterverarbeitung herangezogen und somit verfälschte Ergebnisse berechnet werden.

Die e-Factory Alliance

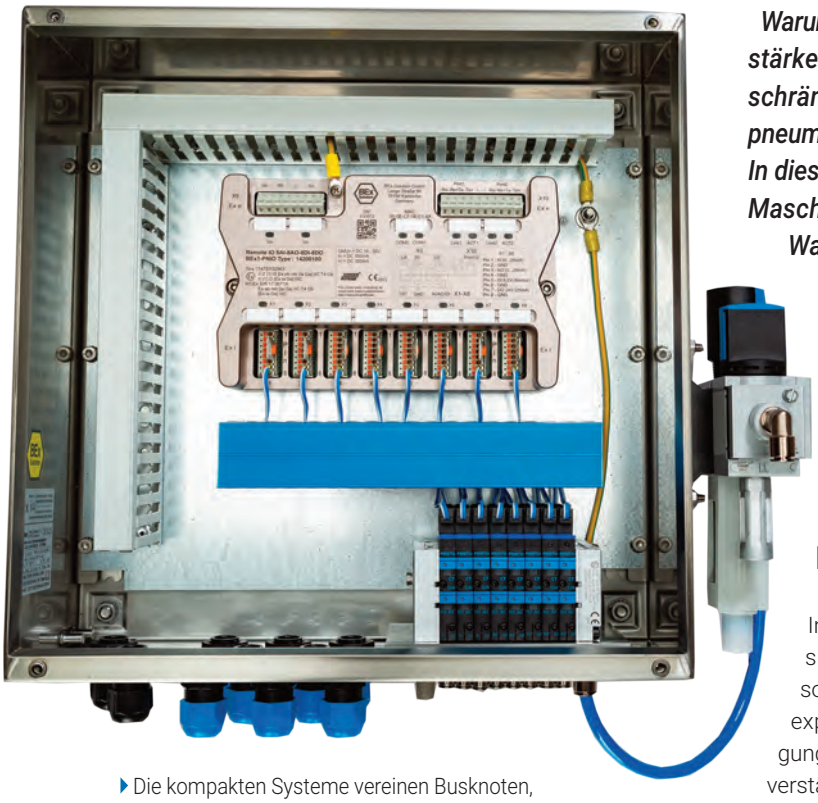
Als Gründer und führendes Mitglied der e-Factory Alliance unterliegen die Produkte des Komponentenherstellers Mitsubishi Electric den Anforderungen der Digitalisierung. Sie müssen sich in die Wertschöpfungskette einbinden lassen und den horizontalen und vertikalen Datenaustausch einfach und intuitiv ermöglichen. Der digitale Zwilling ist dabei das Kernelement für den Datenaustausch. Beginnend vom Design eines neuen Produktes, über die Produktion bis hin zum gesamten Lebenszyklus. Dies beinhaltet die Transparenz von der Bestellung bis zur Lieferung und der Datenaustausch zwischen den Maschinen einer Linie. Bei der Inbetriebnahme und Wartung muss die Durchgängigkeit der Daten von der Programmierung bis zur Simulation durch den digitalen Zwilling gewährleistet sein. Durch die Langlebigkeit der Maschinen, Sensoren und Steuerungen in der Produktion müssen neue und auch extrem alte Komponenten in den Datenstrom eingebunden werden. Hinzu kommen noch die diversen Hersteller. Bei Neugeräten ist OPC UA vorhanden, aber allein beim Blick auf die diversen Feldbusse wird die Integration schon zu einer Herausforderung. Mit der Edgecross Basic Software und dem Edge Computer MeliPC ist dies jedoch einfach zu realisieren. Mittels MQTT können die Daten einfach mit der Contact Elements for IoT Plattform ausgetauscht werden. Dieser Datenaustausch lässt sich bei neueren Geräten, insbesondere der Mitsubishi Komponenten, durch das Time Sensitive Network (TSN) realisieren. Mit CC-LINK IE TSN von CLPA ist dies möglich. Die e-Factory Alliance mit all den verschiedenen Partnern eröffnet dem Kunden eine offene Lösungsplattform. Diese verbindet Sensoren, Steuerungen und Maschinen in der Produktion und ermöglicht den transparenten Datenaustausch in die geschäftliche Wertschöpfungskette. Hierbei kann der Kunde flexibel auf die Bausteine von Contact Software zugreifen, aber auch diverse andere Lösungen von weiteren e-Factory Hardware-Partnern nutzen. ■

Sebastian Creischer,
Barbara Scholvin,
Contact Software GmbH
www.contact-software.com

Remote-I/O-Ventilinsel im Ex-Bereich

Platz für Standards

Warum werden eigentlich immer noch viele Trennschaltverstärker und pneumatische Ventilinseln in großen Schaltschränken verbaut, um die eigensicheren Signale und die pneumatischen Antriebe aus dem Ex-Bereich zu versorgen? In diesem Artikel soll die Aufmerksamkeit der Anlagen- und Maschinenbauer auf ein neues Konzept gerichtet werden. Was ist daran neu und welchen Nutzen bringt es?



Die kompakten Systeme vereinen Busknoten, Trennschaltverstärker, eigensichere I/O-Kanäle sowie die Ventilinsel.

Es gibt zahlreiche und unterschiedliche Konzepte für die Planung von explosionsgefährdeten Anlagen, wie die Optimierung der Zoneneinteilung, die Reduktion des Ex-Bereiches oder den Wunsch alles über Kabelwege aus der Ex-Zone in einen zentralen Schrank herauszuführen. Die Krux ist jedoch, dass die Kalkulation der Verkabelung oftmals nicht im Leistungsumfang des Anlagen- und Maschinenbauers liegt. Logisch betrachtet, der Aufwand und die Kosten entstehen woanders, jedoch lösen sie sich nicht in Luft auf. Ein Lösungsansatz innerhalb der Schnittmenge der Gewerke muss gut argumentiert werden. Klar ist, dass bereits viele Anlagen, insbesondere in der Chemie, schon lange mit Ex Remote-IO-Systemen ausgerüstet sind. Dort sind die großen und modularen Remote-IO-Schränke etabliert. Ein anderes Konzept für den Ex-Bereich lautet: Kleine Remote-IO-Ventilinseln verteilt innerhalb einer Anlage platzieren, anstatt zentrale oder große dezentrale Lösungen aufzubauen. Das Ziel ist es, die eigensicheren Signale vor Ort einzusammeln und die pneumatischen Antriebe über kurze Pneumatikleitungen dezentral zu versorgen. Von dort erfolgt die Kommunikation direkt über Profinet zur Steuerung.

Problematik des Ex-Bereichs

Neu entwickelte Lösungen aus dem nicht-Ex-Bereich werden meistens zeitverzögert für den Ex-Bereich ertüchtigt und zertifiziert. Bei Produkten für die Zone 2/22 mag das sehr rasch gehen. Jedoch bei Geräten für die Zone 1/21, die auch Sensorik aus der Zone 0/20 versorgen, sind neue und neuartige Produkte meistens nur mit erheblichem Aufwand über die verschiedenen Hersteller realisierbar.

Neue Lösung

In Partnerschaft mit Festo und Exepd hat BEx eine 3-in-1-Lösung entwickelt, die als Ergebnis eine betriebsbewährte sowie zertifizierte kompakte Remote-I/ O-Ventilinsel für den explosionsgefährdeten Bereich in der Zone 1/21 zur Verfügung stellt. Die kleinen Boxen vereinen Busknoten, Trennschaltverstärker, eigensichere I/O-Kanäle sowie die Ventilinsel und sollen kurze Wege zu den Sensoren und den pneumatischen Stellgliedern garantieren. Druckluft, Spannungsversorgung und Profinet anschließen, fertig! Jetzt werden viele sagen, ja aber, was ist mit dem Softwareaufwand. Diejenigen, die bereits Erfahrung haben, wissen das macht Arbeit und kostet viel Zeit und Geld. Da sind wir wieder bei dem großen Thema der Ressourcen. Bei der Entwicklung des neuen Konzepts wurde besonders darauf geachtet, dass das Remote IO Modul selbst nicht konfiguriert werden muss. Über 64 I/O Bytes erfolgen Kommunikation sowie I/O Settings. Anwendungsbereiche sind Lackieranlagen, pharmazeutische und chemische Industrie, Schüttgutanlagen, Misch-/Mahlanlagen, industrielle Heiz-/Kühlsysteme, Kläranlagen, uvm.

Funktionen

Die Ankopplung ist über Profinet oder Modbus TCP/IP möglich. Es können bis zu 16 Stück 3/2-Wegeventile oder bis zu acht Stück 5/2- oder 5/3-Wegeventile konfiguriert werden, aber auch Kombinationen daraus. Für die Stellungsrückmelder stehen 16 Namur-Eingänge zur Verfügung. Das Modul ist ebenfalls mit analogen I/Os ausgestattet, 4 bis 20mA Ex-i-Signale werden mit eingesammelt. ■

Karl Vogel,
CMO,
BEx-Solution GmbH
www.bex-solution.com

Bild: BEx-Solution GmbH

In der Elektronikfertigung von IFM wurden die Absaugeinrichtungen auf eine zustandsorientierte Wartung umgestellt.

Zustandsorientierte Wartung mit Industrie 4.0

Smart observiert

Wie Industrie 4.0 erfolgreich eingesetzt werden kann, demonstriert IFM in seinem Werk in Tettnang. Das Beispiel einer Filterüberwachung in der Sensorproduktion verdeutlicht die Vorteile der zustandsorientierten Wartung. Zum Einsatz kommen dabei Sensoren mit IO-Link-Kommunikation sowie der LR Smartobserver.

Industrie 4.0 verspricht unter anderem größere Effizienz und höhere Verfügbarkeit in Produktionsanlagen. Eine mögliche Strategie bei der Umsetzung ist es, zunächst mit Teilprojekten zu starten, die sich später Stück für Stück erweitern lassen. Voraussetzung ist allerdings die Verwendung entsprechend skalierbarer Systeme. Diese Vorgehensweise hat IFM im Werk Tettnang an Maschinen und Arbeitsplätzen in der Elektronikfertigung verfolgt. Dort sind zahlreiche Absaugvorrichtungen installiert, die über Rohrleitungen an eine zentrale Absauganlage angeschlossen sind. Sowohl an der zentralen Absauganlage als auch an den einzelnen dezentralen Absaugvorrichtungen sind Filter installiert, die Staub und Partikel zurückhalten. Sind die Filter zu stark verschmutzt, sinkt der Luftdurchsatz, und der sichere Betrieb der Maschine ist nicht gewährleistet. Eine Wartung der Absauganlage, die einen ausreichenden Luftdurchsatz sicherstellt, ist also zum unterbrechungsfreien Betrieb der Fertigung unabdingbar.

Austausch der Filter

Der Austausch der Filter wurde in der Vergangenheit in regelmäßigen Wartungsintervallen durchgeführt. Dabei werden die Filter häufig entweder zu früh gewechselt, wenn sie noch kaum verschmutzt sind, oder zu spät, was im schlimmsten Fall zu einem kostspieligen Produktionsausfall führen kann. Im Rahmen eines Industrie-4.0-Projekts wurde auf eine zustandsorientierte Wartung umgestellt. Dazu wird der Verschmutzungsgrad der Filter kontinuierlich gemessen, um so den passednden Zeitpunkt für die Wartung zu ermitteln. An den dezentralen Filtern wurden Druckluftzähler vom Typ SD0523 installiert, die an ein IO-Link-Mastermodul vom Typ AL1302 angeschlossen sind. Zur Auswertung der Messwerte aus den Strömungswächtern kommt das Linerecorder-System des Herstellers zum Einsatz - eine Lösung, die sämtliche Aufgaben vom Einsammeln und Konsolidieren der Daten aus dem Feld über die Datenübertragung bis hin zu Auswertung, Analyse und Visualisierung ermöglicht. Das System besteht aus verschiedenen Software-Tools, die eine einfache Datenübertragung von den einzelnen Sensoren in übergeordnete Systeme ermöglichen. Auf dem IO-Link-Mastermodul arbeitet der so genannte IoT Core, der die Prozesswerte zur Verfügung stellt. Die Auswertung findet dann im übergeordnete LR Smartobserver statt. Mit der webbasierten Bedienoberfläche lassen sich die Messwerte darstellen, Grenzwerte festlegen und das Alarmmanagement konfigurieren. Über eine Anbindung an das SFI-System (Shop Floor Integration) werden bei Grenzwertverletzungen direkt Instandhaltungsaufträge im SAP-System ausgelöst.

Einfache Erweiterung möglich

Das Beispiel zeigt, wie sich eine typische Industrie-4.0-Anwendung auch bei bestehenden Anlagen realisieren lässt. Sensoren, die über IO-Link kommunizieren, und das Linerecorder-System ermöglichen eine reibungslose Kommunikation von der Maschine bis hinauf in das ERP-System. Solche Anwendungen lassen sich nachträglich ohne Probleme erweitern, da das System flexibel skalierbar ist. ■

Direkt zur Übersicht auf i-need.de
www.i-need.de/f/5500

Oliver Bucher,
Abteilungsleiter Anwendungsberatung Industrie 4.0,
IFM Electronic GmbH
www.ifm.com/de

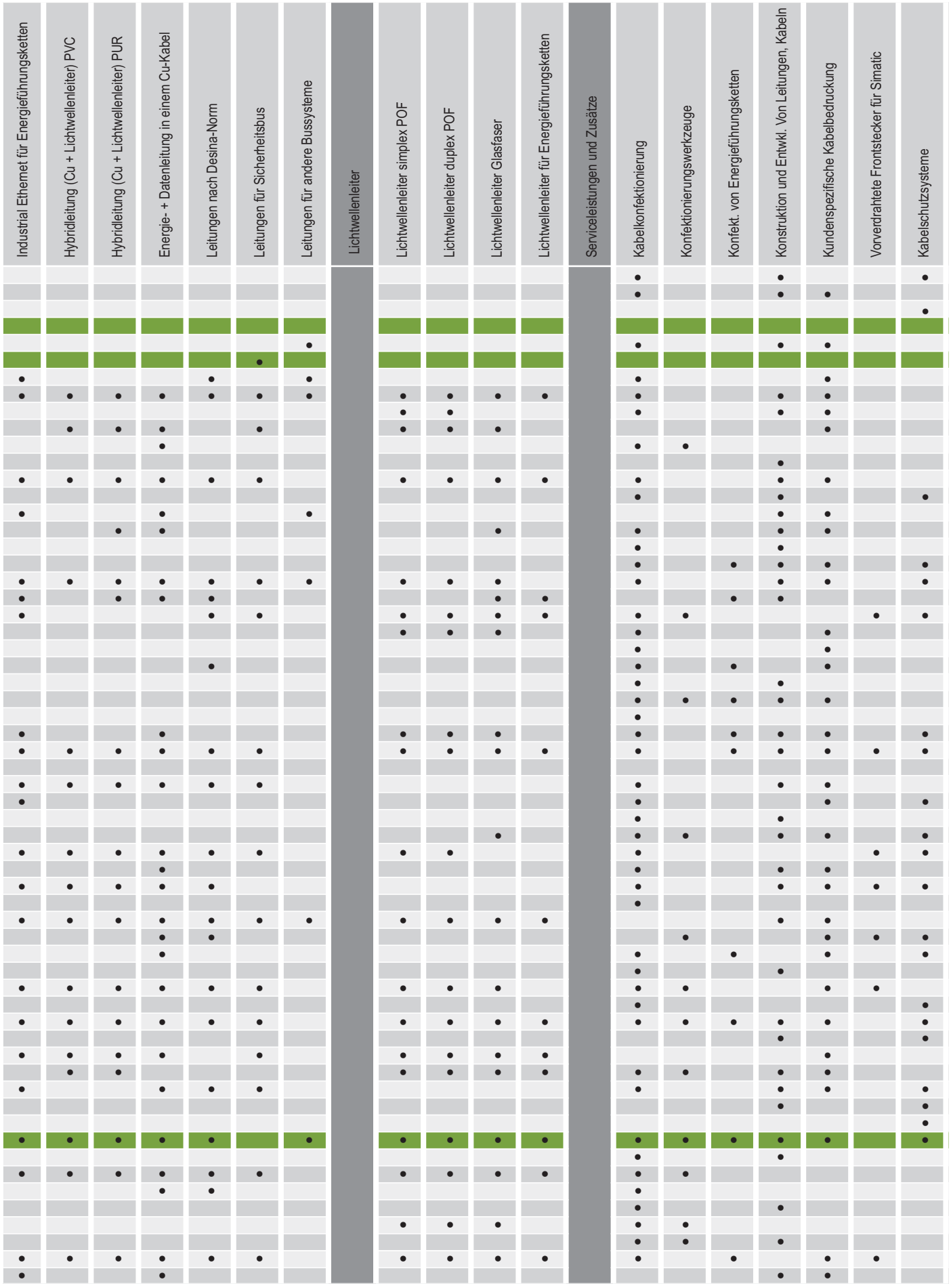
Bild: IFM Electronic GmbH

Kabel und Verbindungstechnik

Welches Kabel gibt es von welchem Hersteller bzw. bei welchem Lieferanten? Unser Marktspiegel gibt auf diese Frage in schneller und übersichtlicher Weise Antworten.

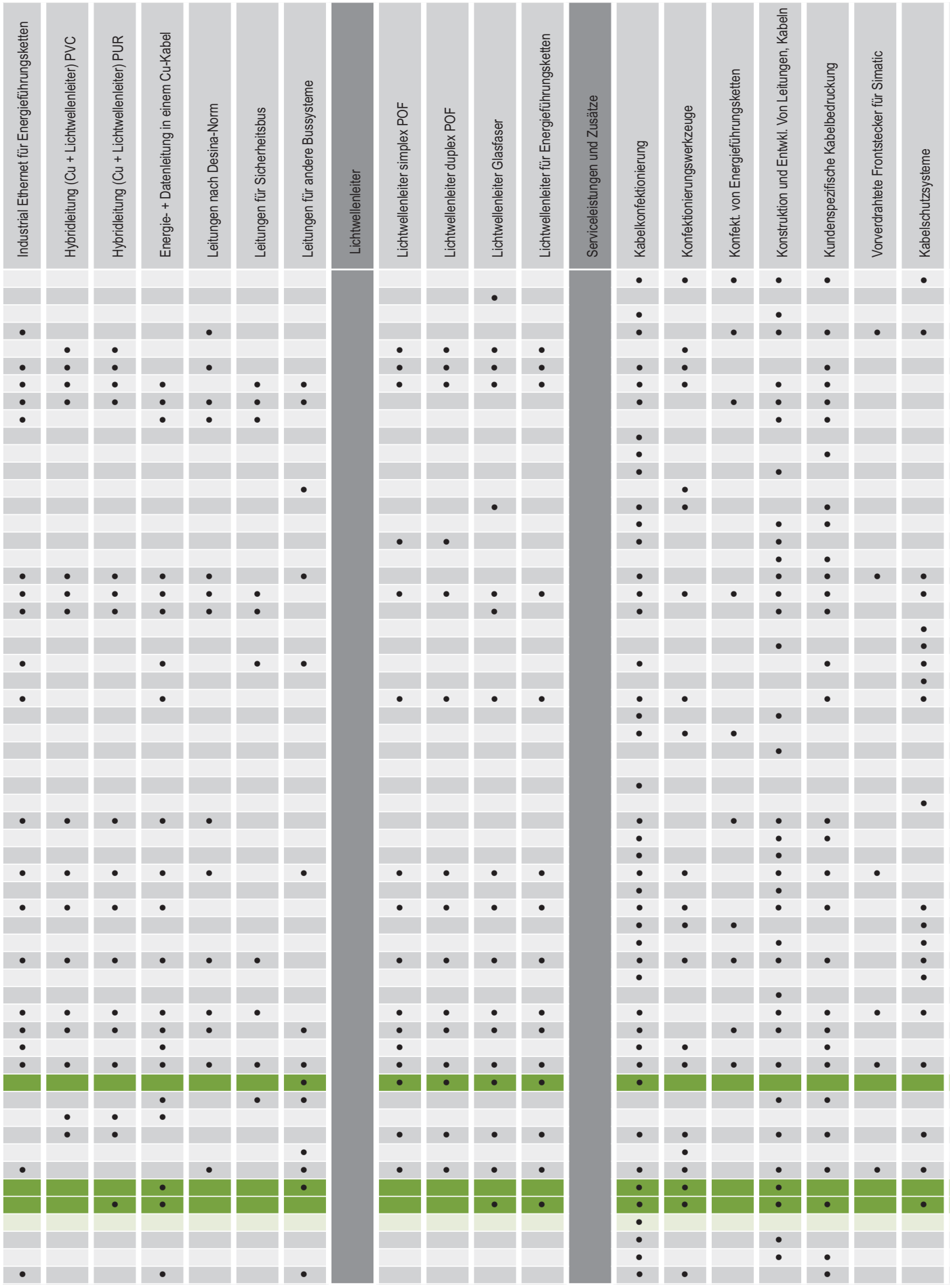
Das Kabelsortiment von 120 Herstellern und Anbietern haben wir kurz und bündig auf den nächsten vier Seiten zusammengefasst. Ausgewertet haben wir die wichtigsten Kabel für den Maschinen- und Anlagenbau und die allgemeine Automatisierungstechnik mit dem Schwerpunk Kommunikation. Mehr gibts auf www.i-need.de *(kbn)* ■

Anbieter	Internet-Adresse	Feldbusleitungen	Sensor-/Aktor-Leitung	ASI-Sensor-/Aktor-Leitung	CAN / Devicenet	Devicenet für Energieführungsketten	Interbus	Profibus	Profibus PA	Profibus für Energieführungsketten	Profibus außen- und erdverlegbar	Industrielles Fast-Ethernet-Kabel
Acal BFi Germany GmbH	www.acalbfi.de											
Adapt Elektronik GmbH	www.adapt.de		•									
Agro AG	www.agro.ch											
Automation24 GmbH	www.automation24.de		•									
Axon Kabel GmbH	www.axon-cable.com											
B&R Industrie-Elektronik GmbH	www.br-automation.com		•		•			•				•
Balluff GmbH	www.balluff.de		•		•	•		•		•		
bda Connectivity GmbH	www.bda-connectivity.com		•	•	•	•	•	•	•	•	•	•
Beck Kabel- u. Gehäusetechnik GmbH	www.beck-kabelkonfektion.de						•	•				
Belden Wire & Cable	www.beldencables-emea.com		•	•	•		•	•	•		•	•
BKL Electronic Kreimendahl GmbH	www.bkl-electronic.de											•
Black Box Deutschland GmbH	www.black-box.de											
Böhm Kabeltechnik GmbH	www.boehm-kabel.de		•	•	•	•	•	•	•	•	•	•
Börsig GmbH Electronic-Distributor	www.boersig.com											
Braunkabel GmbH	www.braunkabel.de		•		•							•
Brugg Kabel AG	www.bruggcables.com											
CobiNet GmbH	www.cobinet.de											
Codico GmbH	www.codico.com											
ConCab Kabel GmbH	www.concab.de		•	•	•	•	•	•	•	•	•	•
Conductix-Wampfler GmbH	www.conductix.de				•	•		•		•		•
Conrad Electronic SE	www.conrad.biz		•	•	•	•	•	•		•	•	•
Contrinex Sensor GmbH	www.contrinex.de		•					•	•		•	
CPL GmbH	cpl-gmbh.de											
DD Kabelkonfektion Dropulic GmbH	www.dropulic.de		•		•		•	•	•	•		
Diamond GmbH	www.diamond.de											
Druseidt Elektrotechnische Spezialfab.GmbH & Co KG	www.druseidt.de											
EasyLan GmbH	www.easylan.de											
Elektrosil Systeme der Elektronik GmbH	www.elektrosil.com		•	•	•	•	•	•	•			•
Eltec GmbH	www.eltec-gmbh.de		•	•	•	•	•	•		•	•	•
Erni Electronics GmbH	www.erni.com		•		•			•				•
Ernst & Engbring GmbH	www.eue-kabel.de		•	•	•	•	•	•	•	•		•
Escha Bauelemente GmbH	www.escha.de		•		•	•		•				•
esd Electronics GmbH	www.esd.eu		•		•							
EVE GmbH	www.eve.de											
fct Electronic GmbH	www.fct-electronic.de		•		•		•	•	•	•	•	•
Festo AG & Co. KG	www.festo.de		•	•								
Friedrich Lütze GmbH	www.luetze.com		•	•	•	•	•	•	•	•	•	•
FRS GmbH & Co. KG	www.frs-online.de											
Gebauer & Griller Kabelwerke GmbH	www.griller.at		•	•	•	•	•	•	•	•	•	•
Gogatec GmbH	www.gogatec.com		•		•	•		•	•	•		•
GSN Greatecs GmbH & Co. KG	www.gsn.sg		•	•	•		•	•	•			•
H&H Components GmbH	www.2h-components.de											
Harting Deutschland GmbH & Co.KG	www.harting.com		•		•			•				•
HellermannTyton GmbH	www.HellermannTyton.de											
Helukabel GmbH	www.helukabel.com		•	•	•	•	•	•	•	•	•	•
Hopf Vertriebsgesellschaft mbH	www.hopf-online.de											
Hradil Spezialkabel GmbH	www.hradil.de				•							•
Huber+Suhner GmbH	www.hubersuhner.de											
Hummel AG	www.hummel.com		•	•	•	•	•	•	•	•	•	•
IBH Elektrotechnik GmbH	www.ibh-elektrotechnik.de											
Icotek GmbH	www.icotek.de											
Igus GmbH	www.igus.de		•	•	•	•	•	•	•	•		•
In-Akustik GmbH & Co. KG	www.in-akustik.de											
Indu-Sol GmbH	www.indu-sol.com		•	•	•	•	•	•	•	•	•	•
Industrieservice Hoppe oHG	www.ish-industrieservice.de						•	•	•	•		
Interkabel GmbH	www.interkabel.de											
ipf Electronic GmbH	www.ipf.de		•									
J.S.T. Deutschland GmbH	www.jst.de											
Kabeltec GmbH	www.kabeltec.de		•	•	•	•	•	•	•	•	•	•
Kabeltronik Arthur Volland GmbH	www.kabeltronik.de		•	•								•



Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 25.05.2020

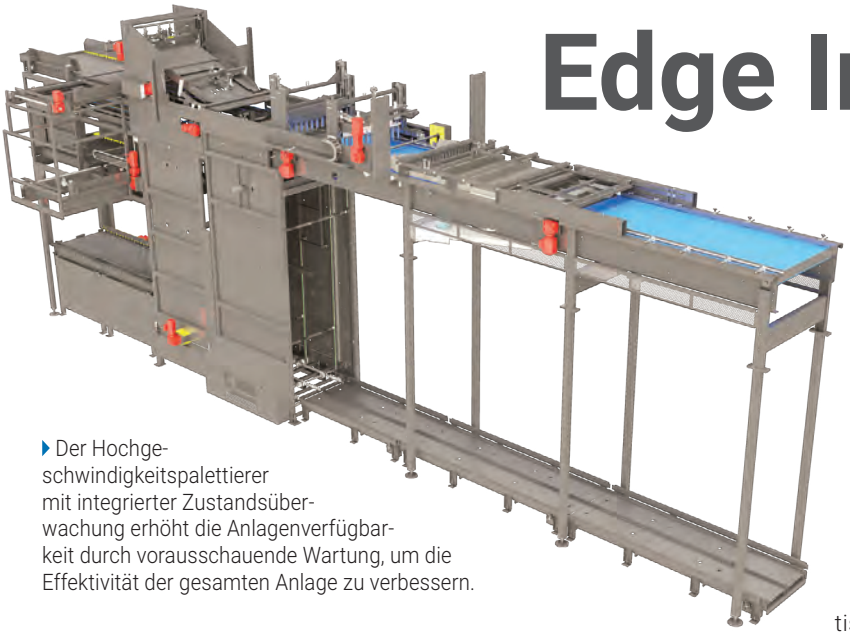
Anbieter	Internet-Adresse	Feldbusleitungen	Sensor-/Aktor-Leitung	ASI-Sensor-/Aktor-Leitung	CAN / Devicenet	Devicenet für Energieführungsketten	Interbus	Profibus	Profibus PA	Profibus für Energieführungsketten	Profibus außen- und erdverlegbar	Industrielles Fast Ethernet-Kabel
Kemmler Electronic GmbH	www.kemmler-electronic.de											
Klaus Faber AG	www.faberkabel.de		●	●			●	●	●		●	●
Komtech Kommunikationstechnik GmbH	www.komtech.de											
Lacon Electronic GmbH	www.lacon.de		●	●	●	●	●	●		●		●
Laser 2000 GmbH	www.laser2000.de											
Leoni Fiber Optics GmbH	www.leoni-fiber-optics.com						●	●	●	●	●	●
Leoni Kerpen GmbH	www.leoni-industrial-projects.com				●			●	●	●	●	●
Leoni Special Cables GmbH	www.leoni-industrial-solutions.com		●	●	●	●	●	●	●	●	●	●
Letronic e.K.	www.letronic.de		●	●	●	●	●	●	●	●	●	●
Lindy-Elektronik GmbH	www.lindy.de											
Lumberg Automation, (Belden)	www.lumberg-automation.com		●	●	●		●	●				●
MC Technologies GmbH	www.mc-technologies.net											
Meilhaus Electronic GmbH	www.meilhaus.de											
Metz Connect GmbH	www.metz-connect.com											
MIL-Kabel-Systems GmbH	www.mil-kabel-systems.com											
MKU Metrofunk Kabel-Union GmbH	www.metrofunk.de							●				
Muckenhaupt & Nusselt GmbH & Co. KG - Kabelwerk	www.munu-kabel.de											
Murrelektronik GmbH	www.murrelektronik.com		●	●	●		●	●		●		●
Mütron Müller GmbH & Co.KG	www.muetron.de		●	●	●	●	●	●	●	●	●	●
Nexans Deutschland GmbH	www.nexans.de		●	●	●	●	●	●	●	●	●	●
Norres Schlauchtechnik GmbH & Co. KG	www.norres.com											
Omerin	www.groupe-omerin.com											
Pepperl+Fuchs AG	www.pepperl-fuchs.com		●	●	●	●	●	●	●	●		●
Pflitsch GmbH & Co. KG	www.pflitsch.de											
Phoenix Contact Deutschland GmbH	www.phoenixcontact.com		●		●		●	●	●	●	●	●
Plastro Mayer GmbH	www.plastromayer.de											
Preising GmbH & Co. KG	www.preising.net											
Prysmian Kabel und Systeme GmbH	www.drakact.de											
Ratioplast-Optoelectronics GmbH	www.ratioplast.com											
Reichle & De-Massari GmbH	www.rdm.com											
Reiku GmbH	www.reiku.de											
SAB Bröckskes GmbH & Co. KG	www.sab-kabel.de		●		●	●	●	●	●	●	●	●
Schaltag AG	www.schaltag.ch											
Secomp GmbH	www.secomp.de											
Siemens AG	www.siemens.com			●				●	●	●	●	●
Signum Computer GmbH	www.signum-vision.com											
Sommer Cable GmbH	www.sommercable.com							●				●
Stecker Express GmbH	www.stecker-express.de		●	●			●	●				
Straschu Elektro-Vertriebs-GmbH	www.straschu.de											
TE Connectivity	www.te.com		●	●	●	●	●	●	●	●	●	●
Telegärtner Karl Gärtner GmbH	www.telegaertner.com											
Telemeter Electronic GmbH	www.telemeter.info											
Thorsten Beulecke Kabelvertrieb	www.beulecke.de		●	●	●	●	●	●	●	●	●	●
Tsubaki Kabelschlepp GmbH	www.kabelschlepp.de		●		●	●	●	●	●	●		●
Hans Turck GmbH & Co. KG	www.turck.com		●	●	●	●		●	●	●		●
U.I.Lapp GmbH	www.lappkabel.de		●	●	●	●	●	●	●	●	●	●
UBF EDV Handel und Beratung	www.ubf.de											
Vogtländisches Kabelwerk GmbH	www.voka.de		●		●		●	●	●		●	●
W.L. Gore & Associates, Inc.	www.gore.com				●			●				
W+P Products GmbH	www.wppro.com											
Wago Kontakttechnik GmbH & Co. KG	www.wago.com		●		●			●				●
Weidmüller GmbH & Co. KG	www.weidmueller.de		●	●	●	●		●	●	●		●
Wieland Electric GmbH	www.wieland-electric.com		●	●				●				
WireMasters GmbH & Co	www.wiremasters.de											
Wisi Communications GmbH & Co.KG	www.wisi.de											
Woertz Systemhaus MBA AG	www.woertzonline.de											
XBK-Kabel Xaver Bechthold GmbH	www.xbk-kabel.de											
Yamaichi Electronics Deutschland GmbH	www.yamaichi.eu											●



Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 25.05.2020

Edge-basierte Lösung für Maschinenzustandsüberwachung

Edge Integration



Der Hochgeschwindigkeitspalettierer mit integrierter Zustandsüberwachung erhöht die Anlagenverfügbarkeit durch vorausschauende Wartung, um die Effektivität der gesamten Anlage zu verbessern.

Emerson und Arrowhead Systems gaben kürzlich ihre Partnerschaft zur Entwicklung einer Lösung für die nächste Generation der Maschinenzustandsüberwachung bekannt. Im Ergebnis erhalten etwa Hochgeschwindigkeitspalletierer eine integrierte Zustandsüberwachung.

Diese Lösung soll die Verfügbarkeit von Hochgeschwindigkeitspalettierern, die beim Stapeln von Behältern zur Anwendung kommen, erhöhen. Die Maschinenzustandsüberwachung kann aber auch für den Einsatz mit anderen Primärprodukten angepasst werden. Der Busse SJI Viper Hochgeschwindigkeitspalettierer für Massengut und der Alpha Turbo Hochgeschwindigkeitsentpalettierer werden mit der Zustandsüberwachung von Emerson ausgestattet, die kritische Parameter von Bewegungs- und Pneumatiksystemen wie Luftstrom, Druck, Unterdruck, mechanische Betätigungsgeschwindigkeiten und Motorvibrationen in Echtzeit überwacht. Somit erhalten Kunden eine Lösung, die eine höhere Effektivität der gesamten Anlage (OEE) ermöglichen kann. Die Systemanalyse- und Zustandsinformationen werden über einen lokalen Data Historian an der Anlagenperipherie verarbeitet und können sowohl auf dem lokalen Bedieninterface als auch auf einem Tablet oder Smartphone angezeigt werden. Somit erhalten Betreiber ein leicht zugängliches Hilfsmittel zur Überwachung des Anlagenzustands. „Diese Lösung bietet den schnellsten und anpassungsfähigsten Weg zur Steigerung der OEE und letztlich zur Erhöhung der Produktionseffizienz Ihres gesamten Anlagenbetriebs", sagte Dana Greenly, Direktor für Geschäftsentwicklung von Lebensmittel- und Getränkeverpackungen des Geschäftsbereichs Emerson Automation Solutions.

Überwachung in Echtzeit

Das Herzstück des neuen Edge-basierten Systems ist die PACSystems RX3i CPL410, welche alle Sensordaten für einfachen Zugriff, bildliche Darstellung und schnelle Analyse zusammenführt. Die Lösung kann für alle Palettiersysteme von Primärprodukten oder auch für komplette Verpackungsanlagen angepasst und skaliert werden. Durch die Maschinenzustandsüberwachung in Echtzeit und einen schnellen Zugriff auf Diagnosefunktionen können durch Maschinenausfälle bedingte reaktive Wartungsmaßnahmen praktisch eliminiert werden. Stattdessen ermöglicht eine vorausschauende Wartung die Planung von Instandsetzungsmaßnahmen bei potenziellen Problemen, die andernfalls die OEE der Verpackungsanlage beeinträchtigen würden. Emersons Automatisierungslösungen unterstützen Betreiber von Verpackungsanlagen bei der Erhöhung der Flexibilität durch die Fähigkeit zur Anpassung an zahlreiche Verpackungsgrößen und -komplexitäten, die Reduzierung von Verlusten durch Verbesserung der Produktivität, der Produktqualität und des Abfallaufkommens sowie die Erhöhung der Bediener- und Produktsicherheit ohne Einschränkung des Durchsatzes. Dies ermöglicht die Ausschöpfung des vollen Potenzials von Verpackungsanlagen durch Bewältigung der aktuellen Herausforderungen in der Verpackungsindustrie: Flexibilität, Zuverlässigkeit, Verunreinigungen und Abfälle sowie Sicherheit. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/39080

T&G Automation GmbH
www.tug.at

Bilder: T&G Automation GmbH

Instandhaltung von Feldbussen und Industrienetzwerken

Permanentüberwachung statt Feuerwehreinsätze

Beim Auto ist die Sache klar: "Einmal alle 30.000km oder alle zwei Jahre" – so oder so ähnlich lauten die Empfehlungen von Fahrzeugherstellern für die Intervalle der regelmäßigen Inspektionen. Aber wie sieht das eigentlich bei Feldbussystemen und Industrienetzwerken in industriellen Prozessen aus? Ist deren Instandhaltung wirklich vernachlässigbar? Wenn nein, wieviel ist nötig? Dieser Frage geht der folgende Beitrag nach.

Obwohl die Wartungsintervalle bei Autos auf langjährigen Erfahrungswerten basieren, sind auch sie nur Richtwerte. Zusätzlich können zwischen den Intervallen betriebsabhängig weitere kleine Arbeiten nötig sein, etwa die Prüfung des Reifendrucks, Kühlwasser auffüllen oder Ähnliches – alles im Sinne einer ungestörten Fahrt und dem guten Gefühl beim Fahrer, nicht in der nächsten Sekunde mit einer Funktionsstörung rechnen zu müssen. Zu diesem guten Gefühl trägt maßgeblich die bei Autos inzwischen weit entwickelte Onboard-Diagnose (Bild 1) bei. Sie informiert rechtzeitig über Anomalien, stellt eine Diagnose und gibt im besten Fall sogar noch eine Handlungsempfehlung, um Abhilfe zu schaffen. Während dieses Prinzip auch bei mechanischen Komponenten in Maschinen und Anlagen der Industrie mittlerweile gang und gäbe ist, wird die Funktion von Feldbussen und Industrienetzwerken noch viel zu oft ohne Überprüfung vorausgesetzt.

Ein Praxisbericht über Zustand und Wartung industrieller Netzwerke

Die Messingenieure des Thüringer Technologieunternehmens Indu-Sol GmbH werden jährlich zwischen 400 und 700 Mal von Kunden aus den verschiedensten Industriezweigen gerufen. Der Grund: Immer häufiger treten in Produktionsanlagen 'mysteriöse' Ereignisse sporadisch und nicht reproduzierbar auf, die die Abläufe zumindest punktuell stören. Ein Komponententausch hilft wenn überhaupt nur kurzfristig. Über eine messtechnische Analyse der Datenkommunikation lassen sich jedoch allerhand Symptome ermitteln: Ab-

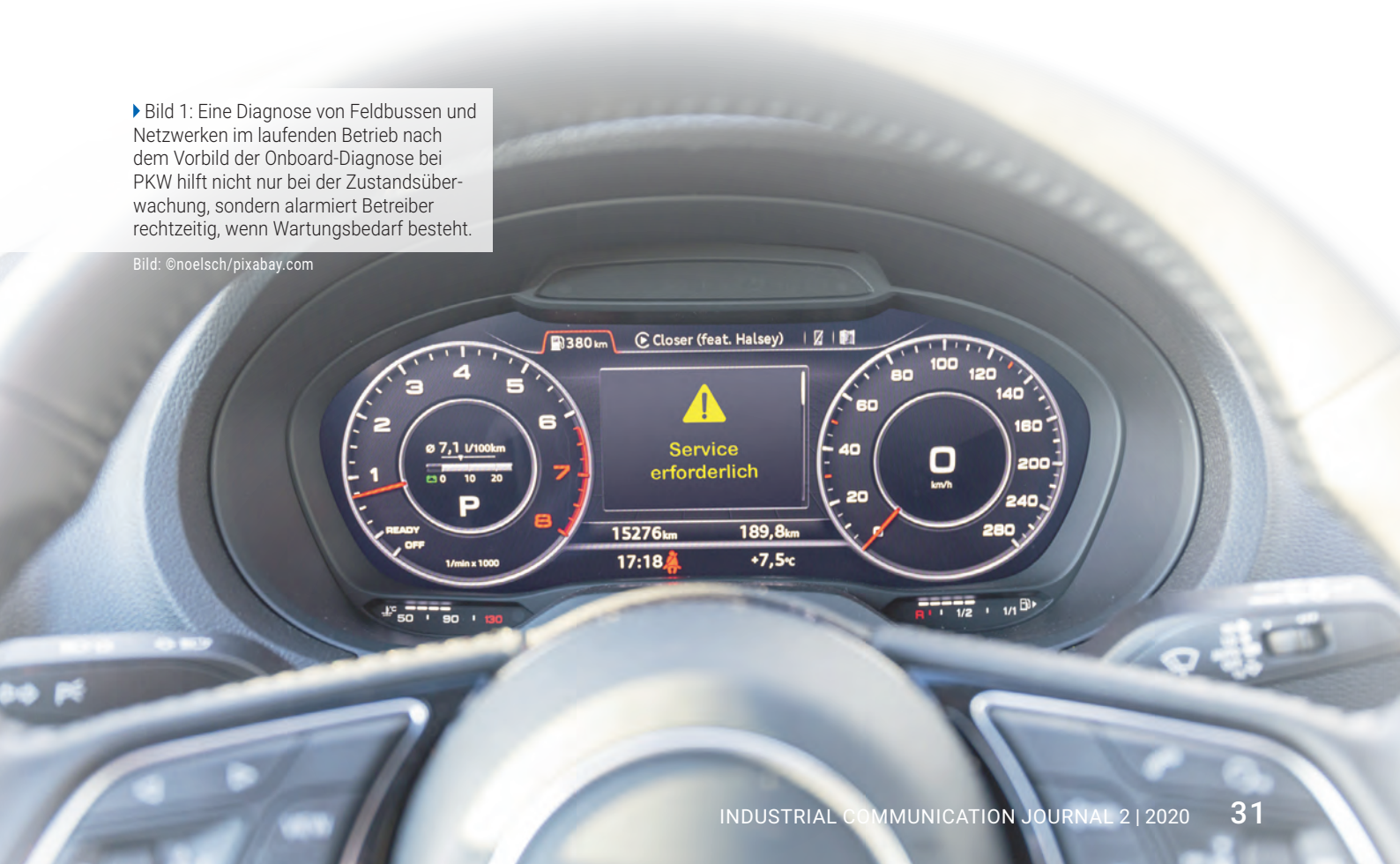


Bild 1: Eine Diagnose von Feldbussen und Netzwerken im laufenden Betrieb nach dem Vorbild der Onboard-Diagnose bei PKW hilft nicht nur bei der Zustandsüberwachung, sondern alarmiert Betreiber rechtzeitig, wenn Wartungsbedarf besteht.

Bild: ©noelsch/pixabay.com

geschliffene Kontakte, veraltete Firmware von Geräten oder auch eine elektromagnetisch unverträgliche Maschinen- und Anlageninstallation wirken sich nachteilig auf die Kommunikationsqualität und damit den Maschinen-/Anlagenbetrieb aus.

Der Vortex-Report

Die aktuellen Erkenntnisse aus den Messeinsätzen des jeweils zurückliegenden Jahres veröffentlicht Indu-Sol im sogenannten Vortex-Report. Im vergangenen Jahr rückten die Messingenieure insgesamt 437 Mal aus – nur etwa jeder zweite Einsatz davon war geplant, also eine vorbeugende Messung oder regelmäßige Inspektion analog zum PKW. Die andere Hälfte setzt sich aus Fehlersuchen zusammen, also Reaktionen auf bereits spürbar eingetretene Qualitätsverschlechterungen in den Automatisierungsprozessen, die die Betreiber weder erklären noch selbst beheben konnten. Von 185 Fehlersuchen waren sogar 123 sogenannte SOS-Einsätze: Hier musste der Service-Techniker aufgrund einer schwerwiegenden Störung am besten sofort vor Ort sein, da sonst anhaltende Produktionsstillstände drohten! Dabei fällt auf, dass bei Fehlersuchen in Profibus-Netzwerken mehr als jeder zweite Einsatz als SOS deklariert werden musste, im Profinet nur jeder fünfte. Bei Profinet hat sich also - lernend aus den Erfahrungen mit Profibus - die Erkenntnis der vorbeugenden Wartung mit regelmäßigen bis permanenten Messungen durchgesetzt.

Ist Langlebigkeit planbar?

Dennoch gab ein gutes Drittel der Teilnehmer eines Indu-Sol Webinars im Oktober 2019 an, keine gezielte Netzwerkinstandhaltung zu betreiben. Nur in 7% der Fälle ist sie dieser Umfrage zufolge ein eigener Budgetposten. Eine dauerhafte Zustandsüberwachung von Feldbussen und Industrienetzwerken ist also noch immer kein Standard, obwohl sie die Lebensadern der Maschinen und Anlagen sind. Immerhin planen zumindest die Teilnehmer des oben benannten Webinars überwiegend mit einer Maschinen-/Anlagenverfügbarkeit von mindestens 95% und das in vielen Fällen für mindestens 20 Jahre – viel länger also, als die meisten Autos auf den Straßen unterwegs sind. Um dieses Ziel zu erreichen, gehört eine dauerhafte Zustandsüberwachung von Anfang an in jeden Feldbus bzw. jedes Netzwerk. Bei Profinet-Neuanlagen setzt sich dieser Gedanke immer stärker durch und es wird bereits bei der Inbetriebnahme eine Abnahmemessung durchgeführt. Mit dieser lässt sich die Qualität der Anlagenerrichtung nachweisen und sicherstellen, dass die Anlage mit 100% Funktionsreserve an den Start geht. Außerdem ist die aktuelle Topologie dokumentiert, wodurch eventuelle spätere Änderungen im Netzwerkaufbau identifiziert werden können. Dies gewinnt nicht zuletzt in Bezug auf die immer stärkere Vernetzung und den damit in Zusammenhang stehenden höheren Sicherheitsanforderungen an Bedeutung. Eine dauerhafte Zustandsüberwachung ab dem ersten Telegramm sorgt für eine bedarfsgerechte und kostenschonende Instandhaltung.

Automatisierte Überwachung, Meldung im Bedarfsfall

Mit dem von Indu-Sol entwickelten System zur Permanenten Netzwerküberwachung (PNÜ) lassen sich Feldbusse und Netz-

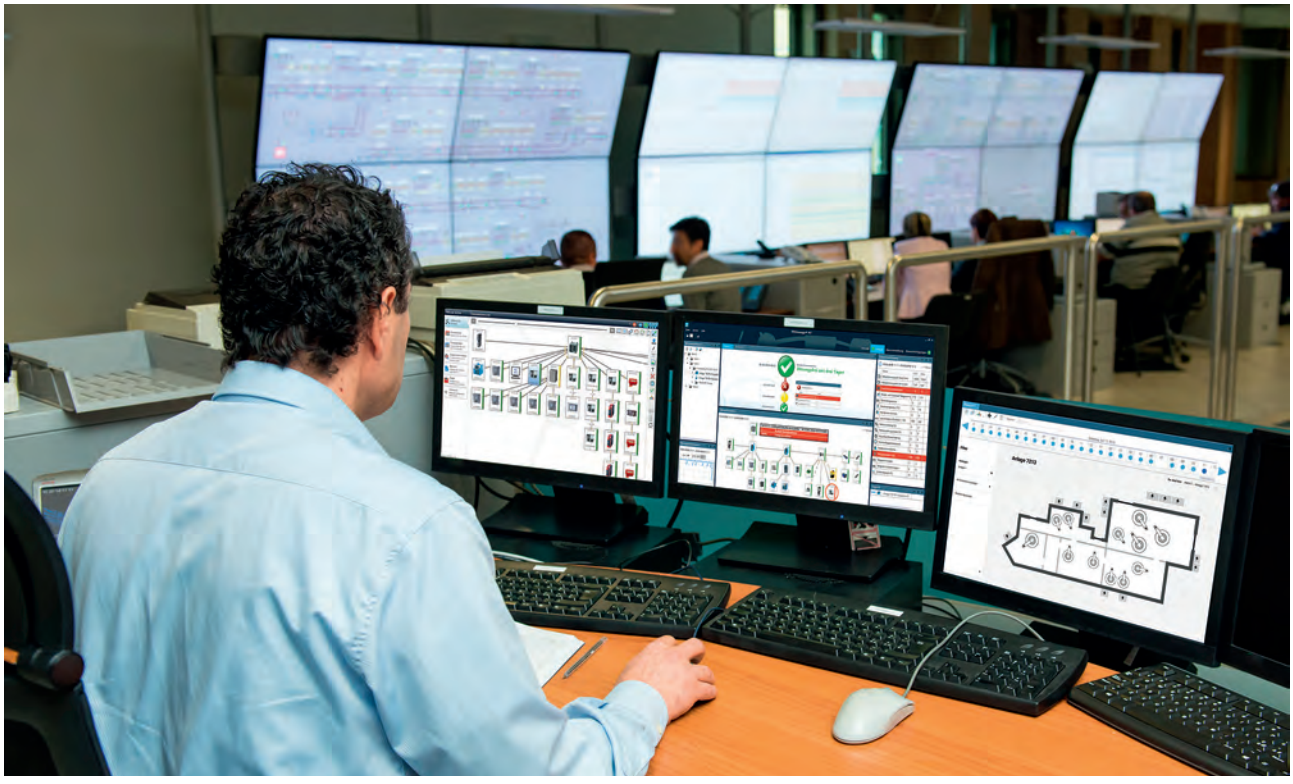


Bild: ©viappy/fotolia.de

Bild 2: Alles im Blick: Mit der Monitoring-Software PROmanage NT lassen sich die Netzwerktopologien (linker Monitor), der Netzwerkgesamtzustand bis hin zu Einzelgeräteinformationen (Mitte) und deren Verortung im Hallenlayout (rechts) zentral überwachen.

Bild: Indu-Sol GmbH

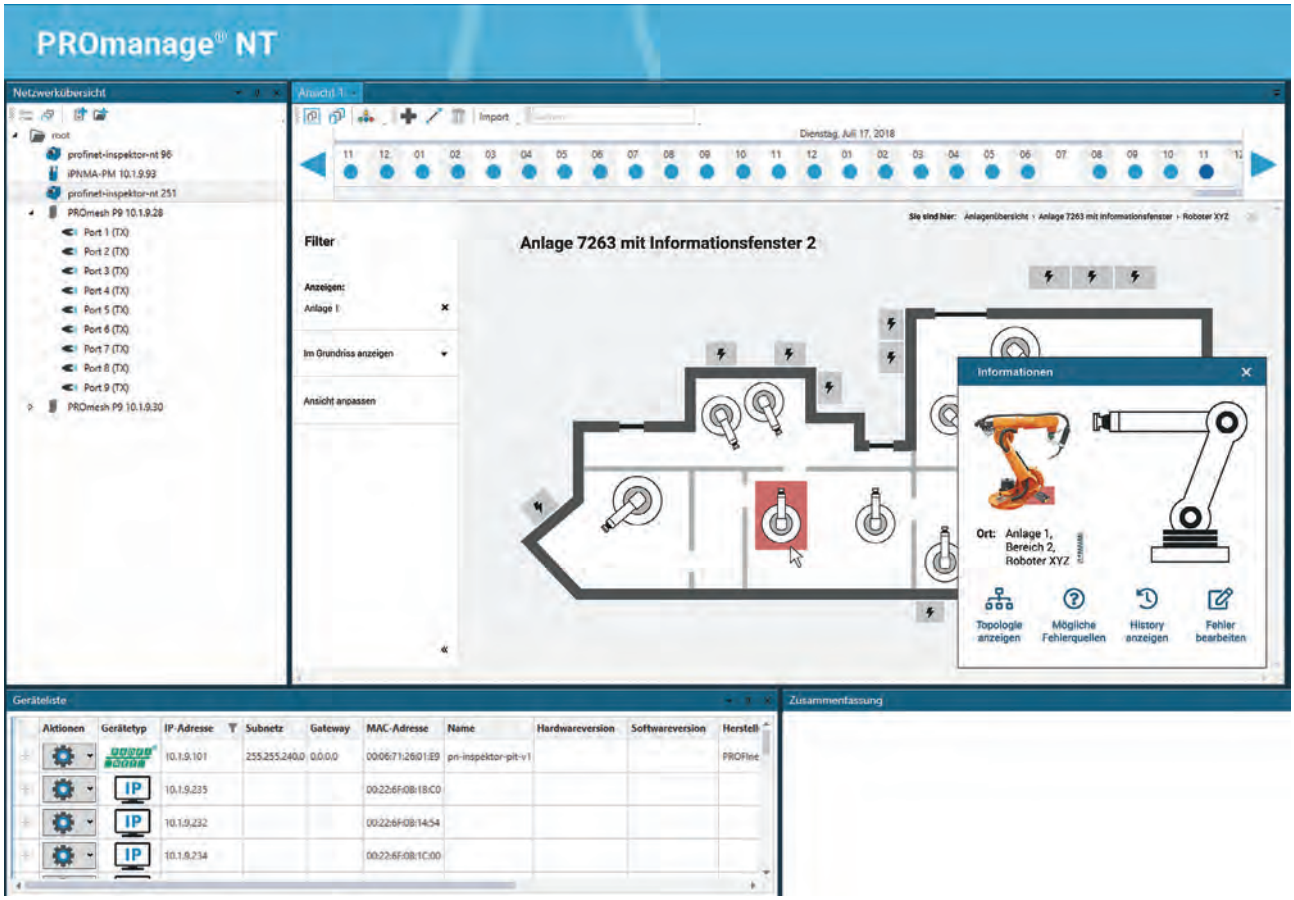


Bild 3: In PROmanage NT können Diagnosedaten aus einzelnen Netzwerken in der Topologie bzw. dem Hallenlayout verortet werden. Unterlegung der Diagnoseergebnisse in Ampelfarben zeigen sofort, ob und wo Handlungsbedarf besteht.

werke dauerhaft rückwirkungsfrei überwachen, um bei Bedarf sofort eine Aussage über den jeweiligen Zustand treffen zu können. Dazu ermitteln passive Datensammler, sogenannte INspektoren, die nötigen Qualitätswerte aus den einzelnen Netzwerken und alarmieren vorbeugend, sobald kritische Veränderungen auftreten. In ethernetbasierten Netzwerken können das zum Teil auch die Switches leisten, sofern sie managebar sind. Die zentrale Monitoring-Software PROmanage NT liest die Diagnosedaten der INspektoren sowie die Portstatistiken der Switches aus und bündelt diese auf einem zentralen Server. So entsteht selbst in weit verzweigten Strukturen ein leicht erfassbarer Gesamtüberblick (Bild 2). Bei Bedarf lässt sich die Analyse mit wenigen Klicks bis auf das einzelne Gerät zurückverfolgen, welches die Meldung abgesetzt hat.

Promanage NT

In PROmanage NT können Betreiber sich diese Informationen mit topologischen Darstellungen und Hallenlayouts (Bild 3) zu einer zentralen Datenbank kombinieren, die sich selbst aktualisiert, bei kritischen Ereignissen vorbeugend meldet und mit Hilfe von Künstlicher Intelligenz präzise Diagnoseinformationen auf den Punkt bereitstellt. Die Anfangsinvestitionen in diese Lösung amortisieren sich schnell, da statt der noch heute üblichen intervallbasierten Instandhaltung nun eine bedarfsgerechte Wartung möglich wird. So wird etwa auch ein vorzeitiger Gerätetausch vermieden, da die Zustandsüberwachung anzeigt, wenn Handlungsbedarf besteht.

Fazit

Durch eine automatisierte, permanente Zustandsüberwachung von Feldbussen und Industrienetzwerken wird die Verfügbarkeit von Anfang an maximiert und Instandhaltungsaufwände bleiben auf ein notwendiges Minimum beschränkt. Dank der präzisen Zustandsinformationen aus den Einzel-Netzwerken kann der Betreiber entscheiden, ob er die Wartung selbst vornimmt oder einen Netzwerk-Spezialisten hinzuzieht. Bereits bei der Konzeption des Netzwerks wird also die Basis für einen stabilen Maschinen- und Anlagenbetrieb gelegt. Eine Festschreibung von Qualitätskriterien und Überwachungslösungen in der firmeneigenen technischen Lieferspezifikation (Lastenheft) schafft aufseiten der Betreiber die notwendigen Qualitätsstandards. Mit diesem Rüstzeug im Gepäck lassen sich die Herausforderungen einer vernetzten Zukunft gut gewappnet angehen. ■

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

Fiktives Unternehmen entlarvt reale Bedrohungen

Honeypot

Trend Micro stellt die Ergebnisse eines über sechs Monate laufenden Honeypots vor, der eine industrielle Fabrik imitierte. Die fiktive Operational-Technology-Umgebung zog Betrüger und andere finanziell motivierte Cyberkriminelle an.

Die sechsmonatige Untersuchung ergab, dass ungesicherte Industrieumgebungen in erster Linie Opfer von herkömmlichen Cyberangriffen sind. Der Honeypot wurde für das Mining von Kryptowährungen kompromittiert sowie durch zwei unterschiedliche Ransomware-Attacken ins Visier genommen. Zudem wurden seine Rechenkapazitäten für betrügerische Aktivitäten genutzt.

Auch KMU betroffen

„Zu oft wurde die Diskussion über Cyberbedrohungen für industrielle Steuerungssysteme (Industrial Control Systems, ICS) auf hochentwickelte Angriffe durch staatliche Akteure beschränkt, die darauf abzielen, wichtige Prozesse zu sabotieren. Diese stellen zwar zweifellos ein Risiko für die Industrie 4.0 dar, aber unsere Untersuchungen belegen, dass alltägliche Bedrohungen wahrscheinlicher sind", so Udo Schneider, Security Evangelist bei Trend Micro. „Betreiber kleinerer Fabriken und Industrieanlagen sollten daher nicht davon ausgehen, dass Kriminelle sie in Ruhe lassen werden. Das Fehlen von grundlegenden Schutzmaßnahmen kann die Tür zu relativ einfachen Ransomware- oder Cryptojacking-Angriffen ermöglichen, die letztendlich schwerwiegende Folgen haben können."

Falsches Unternehmen, echte Angriffe

Um die auf ICS-Umgebungen gerichteten Angriffe besser zu verstehen, hat Trend Micro Research für diese Untersuchung ein äußerst realitätsnahes, industrielles Prototyping-Unternehmen geschaffen. Der Honeypot bestand aus realer ICS-Hardware und einer Mischung aus physischen Hosts und virtuellen Maschinen zum Betrieb der Fabrik, die mehrere speicherprogrammierbare Steuerungen (SPS), Human-Machine-Interfaces (HMIs), separate Roboter- und Engineering-Workstations sowie einen Dateiserver umfasste. Betreiber vernetzter Produktionsanlagen sollten – neben weiteren Best Practices für die Cybersicherheit – die Anzahl der offenen Ports minimieren und die Zugangskontrolle verschärfen. Darüber hinaus kann die Implementierung von Cybersicherheitslösungen für Fabriken, wie sie Trend Micro anbietet, dazu beitragen, das Risiko von Angriffen weiter zu verringern. ■

Trend Micro Deutschland GmbH
www.trendmicro.com

Impressum

VERLAG/POSTANSCHRIFT:
Technik-Dokumentations-Verlag
TeDo Verlag GmbH®

Postfach 2140, 35009 Marburg

Tel.: 06421/3086-0, Fax: -380
E-Mail: info@tedo-verlag.de
Internet: www.industrial-communication-journal.net

LIEFERANSCHRIFT:
TeDo Verlag GmbH
Zu den Sandbeeten 2
35043 Marburg

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

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

WEITERE MITARBEITER:
Bastian Fitz, Tamara Gerlach, Susan Jünger, Lena Krieger, Lukas Liebig, Kristine Meier, Melanie Novak, Florian Streitenberger, Natalie Weigel, Sabrina Werking

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

ANZEIGENDISPOSITION:
Christina Jilg
Tel. 06421/3086-0
Es gilt die Preisliste der Mediadaten 2020.

GRAFIK & SATZ:
Julia Marie Dietrich, Tobias Götze, Fabienne Heßler, Kathrin Hoß, Ronja Kaledat, Patrick Kraicker, Ann-Christin Lölkes, Cara Richter, Nadin Rühl

DRUCK:
Offset vierfarbig
Dierichs Druck+Media GmbH & Co. KG
Frankfurter Straße 168, 34121 Kassel

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

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

ISSN 0935-0187
Vertriebskennzeichen G30449

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

Industrial Exhibitions
We connect professionals

Vernetzen - Informieren - Weiterkommen

DIE VIRTUELLEN FACHMESSEN

GLEICH MAL AUSPROBIEREN!

11.05.– 05.06.2020

- Automatisierung
- Antriebstechnik
- Sensorik
- Industrie 4.0
- Kommunikation

19.05.– 16.06.2020

- Bildverarbeitung
- Embedded Vision (inkl. AI)
- 3D Messtechnik
- Komponenten
- Systeme & Lösungen

08.06.– 17.07.2020

- Cobots & MRK
- Roboterzellen & Integration
- FTS & mobile Roboter
- Greifer & Werkzeuge
- Automation & Handling

Powered by: SPS MAGAZIN · robotik UND PRODUKTION · IT&Production · Anlagenbau Industrie und Gebäude SCHALTSCHRANKBAU · inVISION · GD GEBÄUDEDIGITAL · IoTDESIGN

OPC FOUNDATION

Registration:
https://opcfoundation.org/opcday

OPC DAY
INTERNATIONAL
IT meets Automation
JUN 22 – 25, 2020
TWO HOURS A DAY
DIGITAL EVENT

Join the free of charge digital event "OPC Day – International"

Learn about

- → OPC Foundation in the world – status / adaption / strategy
- → OPC UA technology – status and roadmap for v1.5
- → OPC UA Security – new features like ECC
- → Compliance working group – new test categories
- → Field Level Communications
  - PubSub TSN – status and results
  - UA over Ethernet-APL initiative
  - Controller-to-Controller (C2C) – deep dive
  - OPC UA Safety – Part 15
- → Modeling:
  - Updates on OPC UA for Devices extensions
  - Collaborations: Overview
  - Harmonization working group – status & strategy
  - Announcement: New group "UA for Cloud Library"

NEW Available on June 22, 2020

EXPERTS PODCAST

Listen to influencers on technology, security and solutions:
https://opcfoundation.org/podcast/