



*Aufwändige
Maschinenintegration?*

Angst vor Cyber-Angriffen?

*Überlastetes,
störanfälliges Netzwerk?*



NAT-Gateway/Firewall-Kombination für die Anbindung
von Maschinen in übergeordnete Produktionsnetze

Sicher vernetzt

Seite 6

Helmholz[®]
COMPATIBLE WITH YOU

Titelbild: Helmholz GmbH & Co. KG

WAS KANN SPE UND WIE SIEHT ES AUS?

Trendumfrage zu Single Pair Ethernet

Seite 13

5G – GRUNDLAGEN UND ERSTE ANWENDUNGEN

Mehr Funk-Power für die Industrie

ab Seite 20

WENN DER HACKER DIE SPS ÜBERNIMMT

Produktionsanlagen richtig schützen

Seite 44

Highend-Messtechnik

Präzise, schnell, robust: die ELM-Module



24 Bit
10 kSps pro Kanal
simultan
25 bzw. 100 ppm @ 23 °C

www.beckhoff.de/messtechnik

Mit den EtherCAT-Messtechnikmodulen der Serie ELM wird die hochpräzise, schnelle und robuste Messtechnik integraler Bestandteil der PC-basierten Steuerung von Beckhoff. Direkt integrierbar in das modulare EtherCAT-Klemmensystem lassen sich die ELM-Module mit dem umfassenden Portfolio von über 500 EtherCAT-Klemmen kombinieren.

- schnell: Abtastraten bis zu 50.000 Samples/s
- zeitpräzise: exakte Synchronisierung < 1 μ s
- wertpräzise: Messgenauigkeit von 100 ppm
- proaktiv: integrierte Anschluss- und Funktionsdiagnose in den einzelnen Modulen
- flexibles Stecker-Frontend: LEMO, BNC, Push-in
- Eingangsbeschaltungen: Spannung 20 mV ... 60 V, Strom 20 mA, IEPE, DMS, RTD/TC

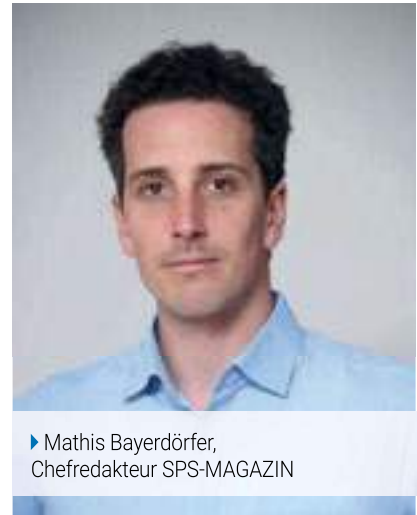


Durchgängige Messkette: von der Datenerfassung bis zur Analyse in der Cloud.

New Automation Technology **BECKHOFF**



Um ihrer Schlüsselrolle bei der Digitalisierung der Fertigung gerecht zu werden, soll die industrielle Kommunikation bitteschön komplett durchgängig, hochperformant, intelligent und flexibel sein. Zudem gilt es, alle Komponenten, Systeme und Maschinen in einem konvergenten Netz zu verbinden. Damit das funktioniert, bedarf es mehrerer noch junger Technologien – einige dieser Player sind schon recht populär und greifbar. Anderen Mitspielern hingegen fehlt es noch an Bekanntheit.



► Mathis Bayerdörfer,
Chefredakteur SPS-MAGAZIN

Hidden Champions für konvergente Netze

Zwischen der durchgängig vernetzten Fabrik und der industriellen Realität liegen heute noch Welten. Selbst hochmoderne Vorzeigestrukturen, die auf der grünen Wiese hochgezogen werden, sind vom Ideal noch einiges entfernt. Das ist zwangsläufig so, weil die nötigen Mitspieler für konvergente Kommunikationsnetze noch gar nicht alle verfügbar sind. Dennoch werden einige schon ausgiebig diskutiert, allen voran die Teamplayer OPC UA und TSN. Während OPC UA auf Applikations-Layer heute bereits verbreitet ist und Konvergenz bis in die oberen Kommunikationsebenen erlaubt, fehlt eine echtzeitfähige Transportschicht. Und weil es ohne Deterministik in der Produktion nicht geht, wird die Ethernet-Erweiterung TSN sehnlich erwartet. Das Zusammenspiel der beiden Standards soll dann einen großen Schritt

in Richtung konvergenter Netze zulassen. Der große Knackpunkt bei der TSN-Standardisierung ist übrigens nicht mehr die Echtzeitfähigkeit, sondern vielmehr das durchgängige Engineering und die Konfiguration von TSN-Netzen. Hier wird zur Zeit an den entsprechenden Substandards noch kräftig gearbeitet.

Einen weiteren Schritt in Richtung Konvergenz erlaubt 5G, denn die fünfte Mobilfunkgeneration soll insbesondere mit großen Datenraten ausreichend Leistung für die smarte Fabrik und das industrielle IoT mitbringen. Auch bei den Latenzzeiten ist 5G schon ziemlich weit vorn. Zudem lassen sich – zumindest in Deutschland – über die Campus-Option Strukturen realisieren, die werks- bzw. standortübergreifend sind, aber nicht am öffentlichen Netz hängen. Insgesamt ist die Einführung von 5G über ein Prototypenstadium jedoch noch nicht hinaus. Entsprechende Beiträge zu 5G finden Sie ab Seite 20 dieser Ausgabe.

Soweit die viel zitierten Player für konvergente Netze. Kommen wir zu den weniger bekannten aber nicht minder relevanten Technologien. Auch 5G wird voraussichtlich nicht alle Wireless-Anforderungen in der Fabrik erfüllen. Minuspunkte sind etwa in Bezug auf die Lizenzen, aber auch auf Latenzen zu erwarten. Deswegen soll zur Echtzeitunterstützung eine neue WiFi-Generation kommen, bei der determinis-

tische Garantien möglich sind und die wie in der Vergangenheit lokal administriert wird. Ein weiterer Hidden Champion, der in der Standardisierung mit rund anderthalb Jahren Versatz zu TSN läuft, ist DetNet. Hierbei handelt es sich um dessen logische Fortsetzung auf den ISO/OSI-Layern 3 und 4. DetNet soll entsprechend für Echtzeit auf IP-Ebene sorgen – also sogar über Fabrikgrenzen hinweg. Ebenfalls als Enabler für wirklich konvergente Kommunikationsstrukturen gehandelt werden Backbone-Netze. Sie unterstützen Echtzeit über große Distanzen mit massiven Datenmengen auf Basis optischer Übertragungslösungen.

Insgesamt ist auf dem Kommunikationsweg der smarten Fabrik noch ein gutes Stück zu gehen. Um nicht zu stolpern, ist es dabei wichtig, die Strecke Schritt für Schritt zurückzulegen. Zudem schadet es ganz sicher nicht, die Technologien, die einem auf diesem Weg begegnen werden, schon früh zu kennen. Als Leser des INDUSTRIAL COMMUNICATION JOURNALS können Sie sicher sein: Wir stellen Ihnen alle Player rechtzeitig vor. In diesem Sinne wünsche ich eine spannende Lektüre.

Mathis Bayerdörfer
mbayerdoerfer@sps-magazin.de



Messen in Zeiten von Corona

Aufgrund des Corona-Virus wird zurzeit eine Messe nach der anderen abgesagt. Was bleibt ist der Bedarf, sich über neue Produkte und Branchenlösungen auszutauschen und einen differenzierten Marktüberblick zu erhalten. Der TeDo Verlag lässt die Messen virtuell erstehen – bequem, direkt und ganz ohne Anreise oder Aufwand für Aussteller und Besucher. Für nähere Infos wenden Sie sich an: mlehnert@tedo-verlag.de



Bild: MS Ultraschall Technologie GmbH

Bild: Helmholz GmbH & Co. KG

6

TITELSTORY

Sicher vernetzt



Als weltweit tätiger Maschinenbauer ist MS Ultraschall Technologie Tag für Tag mit der Anforderung konfrontiert, Maschinennetze sicher in übergeordnete Produktionsnetze zu integrieren. Mit Wall IE von Helmholz – einer Kombination aus Industrial NAT/Gateway und Firewall – wurde eine Lösung für diese Aufgabenstellung gefunden. Trotz unkomplizierter Integration und Inbetriebnahme bieten sie bei der Vernetzung und Absicherung ein flexibel nutzbares Funktionsspektrum.

Titelanzeige: Helmholz GmbH & Co. KG



MARKT - TRENDS - TECHNIK

- 9 Markt- und Branchen-News
- 10 Neue Produkte und Lösungen



PROTOKOLLE UND STANDARDS

- 13 Single Pair Ethernet im Maschinen- und Anlagenbau
- 16 Normiert in die Zukunft mit SPE
- 19 Produktübersicht: OPC UA
- 20 5G-Campusnetze für Produktionsstandorte
- 22 Pilotprojekte für 5G in der Industrie
- 25 Internetplattform für IO-Link-Beschreibungsdateien
- 26 ASI-5: Weiterentwicklung des AS-Interface-Standards



KOMPONENTEN UND LÖSUNGEN

- 28 Integration von Sensoren per IO-Link
- 31 Sensor-Produktion in der Smart Factory
- 32 Fernwartung für Steuerungssysteme
- 33 Marktübersicht serielle Adapter für Ethernet



WIRELESS UND REMOTE

- 38 Industrie 4.0 in der praktischen Anwendung
- 41 Produktübersicht Wireless-Produkte
- 42 Profinet-Gateway für industrielle Heizungsanwendungen



SICHERHEIT

- 44 Schutz vor Cyber-Attacken im IIoT
- 46 Cyber-Kriminalität als Bedrohung für KMU
- 48 Die drei wichtigsten IIoT-Security-Trends 2020
- 49 Neuheiten IT- und Datensicherheit



SERVICE

- 3 Editorial
- 5 Nachrichten-App für alle industrierelevanten Themen
- 50 Vorschau, Inserenten, Impressum

Lichtleiter-Sensorik



Bild: Sick AG

Gateways ermöglichen die direkte Integration von Sensoren in die IO-Link- oder Feldbuswelt. **Seite 28**



Bild: ©ipopba/Fotolia.com



Nachrichten-App für alle industrierelevanten Themen

Wissen, was die Community bewegt!

Seit anderthalb Jahren ist die Nachrichten-App **INDUSTRIAL NEWS ARENA** - kurz **INA** - nun auf dem Markt. Als bisher einzige Fachmedien-App, die die Themen industrielle Automatisierung und IIoT in einer eigenen Sparte aufgreift, wird sie von den Lesern des **INDUSTRIAL COMMUNICATION JOURNAL** rege genutzt. Mit deutlich steigendem Nachrichtenwert und wachsendem Funktionsumfang hat sich die **INA App** zu einem zukunftsweisenden Informationskanal für Automatisierungs- und Netzwerkspezialisten entwickelt.

Mit der App **INDUSTRIAL NEWS ARENA** hat der TeDo Verlag einen einzigartigen digitalen Kanal geschaffen, der alle relevanten Fachinformationen - aufgeteilt nach Themengebieten - bündelt. Hier erfahren User zu jeder Zeit, welche Branchenthemen die Community bewegen. Aktuell umfasst das Angebot acht Fachgebiete wie Automatisierung, Bildverarbeitung, Gebäudetechnik, IIoT, Robotik oder Schaltschrankbau. Neu hinzugekommen sind zuletzt künstliche Intelligenz und Maschinenbau. Alle Inhalte werden von erfahrenen Redakteuren zusammengestellt und hochwertig aufbereitet. Sie lassen sich aus der App heraus jederzeit über Social-Media-Plattformen teilen oder per E-Mail weiterleiten.

Relevante Zielgruppen

An wen richtet sich die industrielle Nachrichten-App? An Anwender und Experten aus dem Bereich Maschinen- und Anlagenbau, an Systemintegratoren und Lösungsanbieter, Geschäftsführer, Fertigungs- und Betriebsleiter, Produkti-

onsleiter, Unternehmensleiter und IT-Verantwortliche. Außerdem adressiert werden Anwender und Konstrukteure aus der industriellen Bildverarbeitung, Entwickler, Hersteller und Anwender von IIoT-Produkten, außerdem Anwender und Experten aus den Bereichen Elektroinstallation und Elektrohandwerk sowie dem Schaltschrankbau.

Kostenloser Download

Die App kann kostenlos im App Store oder auf Google Play heruntergeladen werden. Durch Bedienelemente, die Nutzern bereits aus anderen Anwendungen vertraut sind, lässt sie sich einfach und intuitiv nutzen. Onboarding-Screens erklären schnell und einfach die wichtigsten Features und Bedienelemente. Außerdem informiert ein Erklärvideo über die App und ihre Vorteile. Themengebiete lassen sich in der App gezielt und individuell auswählen. Mit einer Filterfunktion werden nur News gezeigt, die auch den spezifischen Interessen des Nutzers entsprechen.

Zuhören statt lesen

Ein Highlight der App: Die **INDUSTRIAL NEWS ARENA** liest auf Wunsch Nachrichten vor und erleichtert so den Informationszugriff. Mithilfe eines Lesezeichens lassen sich Nachrichten speichern, die besonders interessant sind oder die zu einem späteren Zeitpunkt gelesen werden sollen. Die App ist zudem in der Lage, die gesamte Bookmark-Liste hintereinander vorzulesen, eine sehr praktische Funktion für unterwegs. Besonders wichtige Mitteilungen versendet **INDUSTRIAL NEWS ARENA** auf Wunsch als Push-Nachricht. Bilder, Videos, Bilderstrecken und interaktive Grafiken vertiefen die Nachrichten zusätzlich.

Top-News immer im Blick

Natürlich umfasst die App auch eine zuverlässige Suchfunktion. Mit der Funktion Top10-News erhalten die App-Nutzer, z.B. nach einer längeren Abwesenheit, einen schnellen Überblick über die wichtigsten Nachrichten der letzten Zeit. Der Zeitstrahl zeigt genau an, wann eine Nachricht veröffentlicht wurde. Tagesaktuelle News, informativ aufbereitet und zurzeit besonders wichtig: Garantiert virenfrei! (fiz/bfi) ■



DIE WICHTIGSTEN FEATURES IM VIDEO ERKLÄRT!

► Mit Wall IE von Helmholz lassen sich die Maschinen der Firma MS Ultraschall Technologie unkompliziert und sicher in Produktionsnetze integrieren.



Bild: MS Ultraschall Technologie GmbH

NAT-Gateway/Firewall-Kombination für die Anbindung von Maschinen in übergeordnete Produktionsnetze

Sicher vernetzt

Als weltweit tätiger Maschinenbauer ist die Firma MS Ultraschall Technologie Tag für Tag mit der Anforderung konfrontiert, Maschinennetze sicher in übergeordnete Produktionsnetze zu integrieren. Mit einer Kombination aus Industrial NAT/Gateway und Firewall wurde eine ebenso zuverlässige wie praktikable Lösung für diese Aufgabenstellung gefunden. Trotz unkomplizierter Integration und Inbetriebnahme bieten sie bei der Vernetzung und Absicherung ein flexibel nutzbares Funktionsspektrum.



Ultraschall bringt thermoplastische Kunststoffe durch hochfrequente Schwingungen mühelos zum Schmelzen und sorgt damit in kurzer Zeit für eine sehr feste Verbindung der Fügepartner. Mit gutem Grund setzen deshalb viele Automobilzulieferer, aber auch andere Kunststoffverarbeiter weltweit auf dieses Verfahren. Ein Anbieter in diesem Bereich ist die Firma MS Ultraschall Technologie. Rund 350 Sonder- und Serienmaschinen verlassen deren Fertigung jährlich.

Industrial Ethernet und Cybersecurity

Der Siegeszug von Industrial Ethernet, konkret der Wandel von Profibus zu Profinet, macht dabei selbstverständlich auch vor diesem Maschinenbauer nicht halt. In den letzten Jahren hatten immer mehr Kunden die Anforderung gestellt, die Maschinen bzw. deren Kommunikationsnetze in ein übergeordnetes Produktionsnetzwerk zu integrieren. Technisch klingt das zunächst einmal machbar: Das Maschinennetz, also

das Netzwerk einer Automatisierungszelle mit einer oder mehreren Maschinen, ist dabei als Local Area Network (LAN) zu betrachten, das Produktions- bzw. Firmennetz als Wide Area Network (WAN). Aus Sicht der absolut notwendigen Cybersecurity stellt sich die Situation jedoch deutlich komplexer dar. Denn um Steuerungssysteme und Automatisierungsnetze wirkungsvoll gegen Angriffe von außen zu schützen, muss das Maschinennetz sicher in das übergeordnete Produktionsnetz integriert bzw. von diesem abgegrenzt werden.

Praktikable Lösung

Die Realisierung einer solchen Schnittstelle war bis vor einigen Jahren nur über den Umweg komplexer Firewall-Lösungen möglich. Die sind allerdings für einen solchen Einsatzzweck überdimensioniert, und damit auch entsprechend teuer und kompliziert in der Handhabung. Für MS Ultraschall Technologie war deshalb klar, dass eine praktikable Lösung gebraucht wird. Fündig wurde der Maschinenbauer 2015 auf der SPS-Messe in Nürnberg. Dort stellte das Unternehmen Helmholz erstmals die NAT-Gateway/Firewall-Kombination Wall IE vorstellte.

Leistungsstarker Helfer

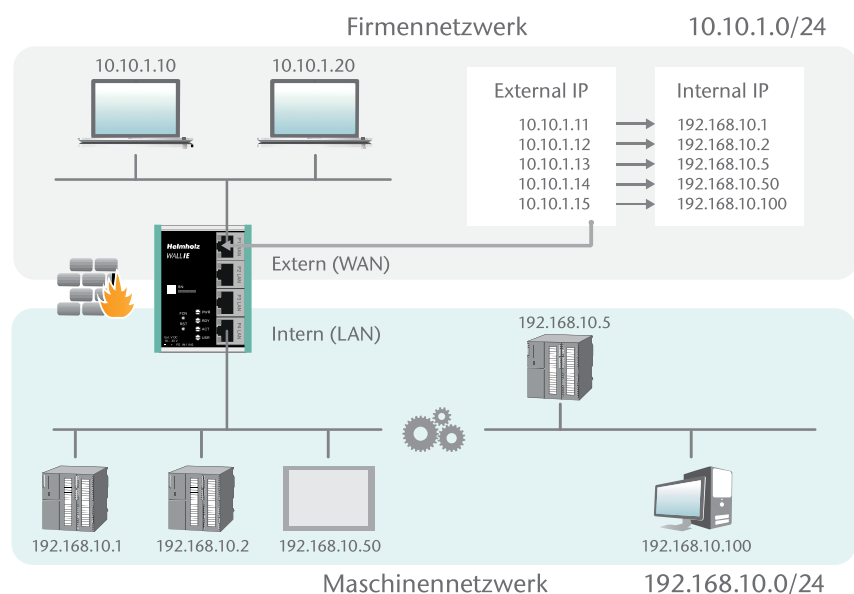
Die robuste und unkomplizierte Ethernet-Komponente ermöglicht eine einfache Integration von Maschinennetzen in das übergeordnete Produktionsnetz. Konkret schützt Wall IE die Netze, indem genau geregelt wird, welcher Teilnehmer mit welchem Gerät kommunizieren und Daten austauschen darf. Wall IE passt sich durch eine individuelle Konfiguration über das Webinterface den jeweiligen Anforderungen des vorhandenen Maschinennetzes an. Die Beschränkung von Zugriffsrechten auf autorisierte Personen stellt dabei eine Grundvoraussetzung für den Schutz der Automatisierungsumgebung dar. Dabei bleiben die hinter Wall IE liegenden Netze bzw. IP-Adressen verborgen und sind von außen nicht sichtbar. Wird das Firmennetz nun durch einen Hackerangriff oder auch nur durch Unachtsamkeit eines Mitarbeiters von einer Schadsoftware oder einem Com-

putervirus bedroht, bleibt das Automatisierungsnetz hinter Wall IE davon unberührt und dementsprechend sicher.

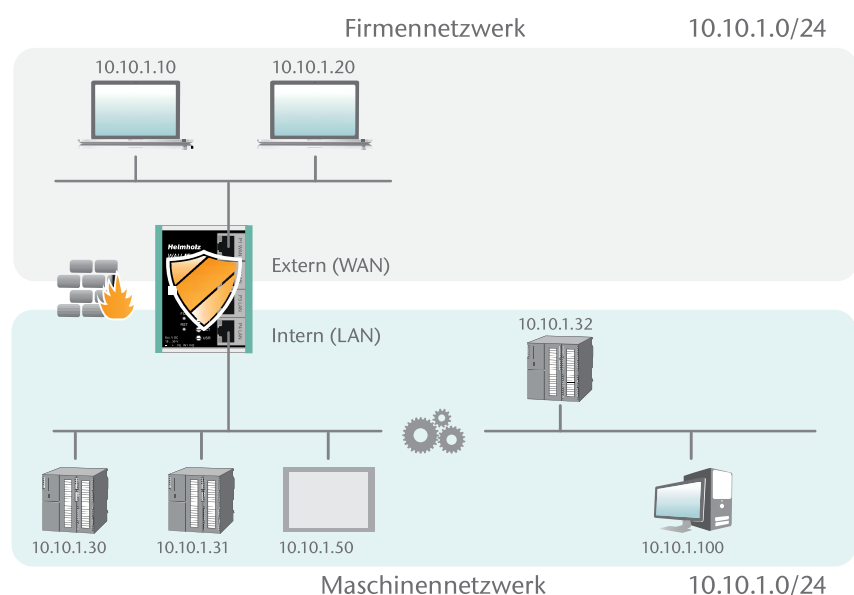
Paketfilter regelt Datenverkehr

Die Voraussetzung dafür schafft eine Paketfilterfunktion: Mit dieser Eigenschaft wird die Sicherheit dahingehend erhöht, dass nur erwünschte Kommunikation stattfindet. Ein unnötiger Datenaustausch wird blockiert. Folglich wird der Zugriff zwischen dem Fabriknetzwerk und dem Maschinennetzwerk passend ausgelegt.

Als Filterkriterien auf Layer 3 und 4 stehen bisher IPv4-Adressen, Protokoll (TCP/UDP), Ports und MAC-Adressen zur Verfügung. Als weitere Besonderheit kann Wall IE im NAT-Betriebsmodus und gleichermaßen auch als Bridge eingesetzt werden. Im Bridge-Betriebsmodus agiert das Gerät als Layer 2 Switch. Im Gegensatz zu marktüblichen Switches ist jedoch auch in dieser Betriebsart eine Paketfilterung möglich. Dadurch kann die Einschränkung des Zugriffs zu einzelnen Bereichen eines Netzwerks erreicht werden, ohne dass hierfür unterschiedliche Netzwerke verwendet werden müssen.



► Basic NAT ist die Übersetzung von einzelnen IP-Adressen und auch ganzer Adressbereiche.



► Im Bridge-Betriebsmodus agiert Wall IE als Switch mit Paketfilter zwischen der Automatisierungszelle und dem Produktionsnetz.



► Nicht nur die zuverlässige Hardware von Wall IE konnte überzeugen, sondern auch die Software und die Philosophie dahinter.

Industrietaugliche Hardware

Wall IE unterstützt Industrial Ethernet mit einer Übertragungsrates bis 100Mbit/s. Die zugrundeliegende Software ist Linux-basiert und wurde komplett von Helmholz selbst entwickelt. Die Hardware ist industrietauglich robust und geeignet für die Montage auf der Hutschiene. Die Konfiguration erfolgt unkompliziert und schnell über ein responsives Webinterface. In die übersichtliche Benutzerführung hat Helmholz die langjährigen Erfahrungen aus der Toolbox TB20 einfließen lassen. Der Online-Zugang ist streng passwortgeschützt und läuft über eine verschlüsselte HTTPS-Verbindung.

NAT-Betriebsmodus

Bei der Verwendung von NAT (Network Address Translation) erlaubt es Wall IE, die IP-Adressen der vorhandenen Maschinen zu belassen, aber die Kommunikation zum Maschinennetz mit eigenen IP-Adressen aus dem Produktionsnetz zu ermöglichen. Im NAT-Betriebsmodus leitet Wall IE den Datenverkehr zwischen verschiedenen IPv4-Netzwerken (Layer3) weiter und nutzt Paketfilter für die Zugriffsbeschränkung auf das dahinterliegende Automatisierungsnetzwerk. Dabei wird die Adressübersetzung mittels NAT unterstützt. Kollisionen, die andernfalls durch die nicht eindeutigen Adressen im Gesamtnetz entstehen würden, sind damit ausgeschlossen. Für die Kommunikation mit anderen Automatisierungszellen kommen statische Routen zum Einsatz. Hierfür muss das Netzwerk sowie die Adresse des dafür zuständigen Routers (Next Hop) konfiguriert werden.

Router-Betriebsmodus

Im Router-Betriebsmodus unterstützt Wall IE zwei NAT-Funktionen: BasicNAT und NAPT. BasicNAT (auch 1:1NAT oder StaticNAT genannt) ist die Übersetzung von einzelnen IP-Adressen und auch ganzer Adressbereiche. Die Übersetzung geschieht ausschließlich auf IP-Ebene, wodurch alle Ports ohne explizite Weiterleitungen angesprochen werden können. Bei NAPT (Network Address and Port Translation, auch 1:NNAT oder Masquerading genannt) hingegen werden nicht nur die IP-Adressen, sondern auch Port-Nummern umgeschrieben. Alle Adressen der Automatisierungszelle werden in eine einzige Adresse des Produktionsnetzwerks übersetzt. Die Absenderadressen von Paketen aus der Automatisierungszelle werden durch diese ersetzt. Das DHCP-Protokoll (Dynamic Host Configuration Protocol) ermöglicht per DHCP-Server auf der LAN- sowie DHCP-Client auf der WAN-Seite eine automatische Vergabe von Adressen und DNS-Namen. Zudem ist nun nicht mehr für jeden einzelnen Port eine eigene Regel erforderlich, denn über Wildcards können ganze Port-Ranges gebündelt werden.

Einfache Integration mit SNAT

Mit der Funktion SNAT (SourceNAT) gibt Wall IE den eingehenden Datenverkehr WAN-seitig transparent an das LAN-Netzwerk weiter. Dabei werden alle ausgehenden Datenpakete mit der Absender-IP-Adresse der Komponente versehen. Somit bleiben die festgelegten Parameter aller LAN-Teilnehmer unverändert und die Eintragung eines Gateways entfällt. Dies ist ein erheblicher Vorteil bei der Integration in bestehende Netzwerkstrukturen. Alle Vorgaben können bei Wall IE anwenderspezifisch definiert und konfiguriert werden. Diesen Mehrwert durch Individualisierung bietet Helmholz seinen Kunden auch als Serviceleistung an. Die bereits anwendungsspezifisch konfigurierte Firewall wird dann einsatzbereit geliefert und muss nur noch mit Spannung versorgt werden.

Positive Praxiserfahrungen

MS Ultraschall Technologie liefert inzwischen rund die Hälfte der Sondermaschinen standardmäßig mit der NAT-Gateway/Firewall-Kombination aus, also im Durchschnitt eine Maschine pro Woche. Die Entscheidung für die Lösung von Helmholz hat sich aus Sicht des Maschinenbauers damit längst bestätigt. Nicht nur das Produkt selbst und die zuverlässige Hardware konnte überzeugen, sondern auch die einfache Menüführung der Software und die Philosophie dahinter. Der Anwender sieht anstelle der Ports, die hinter Wall IE verschaltet werden, nur eine einzige IP-Adresse. Damit kommt der Maschinenbauer nach eigenen Angaben gut klar. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/p/29734



Lucia Zimmermann,
Head of Marketing,
Helmholz GmbH & Co. KG
www.helmholz.de

**Produktdetails
online ansehen**





IEC63171-6 veröffentlicht

Ende Januar wurde mit der IEC63171-6 die internationale Norm für Single-Pair-Ethernet-Schnittstellen in industriellen Anwendungen veröffentlicht. Herausgeber ist das IEC Komitee SC 48B Kupfersteckverbinder. Die Norm für das Steckgesicht IEC63171-6 T1 Industrial Style war die erste Norm, welche schon 2016 von Harting für ein Single-Pair-Ethernet-Steckgesicht bei SC 48B eingereicht wurde. Die IEC63171-6 (Industrial Style) ist ein vollständiges Normendokument mit allen notwendigen Spezifikationen und Prüfsequenzen und fließt in aktuelle SPE-Verkabelungsstandards der Normenreihe für strukturierte Verkabelung ISO/IEC11801-x mit ein. Das 2019 gegründete SPE Industrial Partner Network besteht aus bisher 17 Unternehmen.

Harting Stiftung & Co. KG
www.harting.com



Informationssicherheit in der industriellen Automatisierung

Die neue VDI/VDE2182 Blatt 1 beschreibt, wie die Informationssicherheit von automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Schutzmaßnahmen erreicht werden kann. Dazu betrachtet die Richtlinie Aspekte der eingesetzten Automatisierungsgeräte, Automatisierungssysteme und Automatisierungsanwendungen. Sie definiert ein einfaches Vorgehensmodell zur Bearbeitung und Darstellung der Informationssicherheit, das aus mehreren Prozessschritten besteht. Richtlinie VDI/VDE2182 Blatt 1 definiert einfaches Vorgehensmodell zur Bearbeitung und Darstellung der Informationssicherheit. Auf Basis einer zwischen Herstellern von Automatisierungsgeräten und -systemen und deren Nutzern – wie Maschinenbauer, Integratoren und Betreiber – abgestimmten, gemeinsamen Begriffsdefinition beschreibt die VDI/VDE2182 Blatt 1 eine einheitliche, praktikable Vorgehensweise, um Informationssicherheit im gesamten Lebenszyklus von Automatisierungsgeräten, -systemen und -anwendungen zu gewährleisten. In diesem Lebenszyklus sind die Phasen Entwicklung, Integration, Betrieb, Migration und Außerbetriebsetzung berücksichtigt. Die Anwendung des Vorgehensmodells aus Sicht von Herstellern, Integratoren und Betreibern wird in den Richtlinien VDI/VDE2182 Blatt 2, Blatt 3 und Blatt 4 anhand konkreter Beispiele beschrieben. Herausgeber der Richtlinie VDI2182 Blatt 1 „Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell“ ist die VDI-Gesellschaft Mess- und Automatisierungstechnik (GMA). Die Richtlinie erscheint im Januar 2020 als Weißdruck und ersetzt die Ausgabe von Januar 2011.

VDI Verein Deutscher Ingenieure e.V.
www.vdi.de



VDE-Studie zu 5G und KI



Bild: @sdecoret/fotolia.com

Die Studie 'Technologische Souveränität' des VDE analysiert anhand der Wertschöpfungskette des Technologiefelds KI in der Automatisierung und der Schlüsseltechnologie 5G, welche Schritte Politik und Wirtschaft jetzt gehen müssen, um bei der Digitalisierung aufzuholen. Derzeit haben die USA und China die Nase vorn im B2C-Bereich. Beide Länder investieren zudem in die Forschung für künstliche Intelligenz. Noch punkte Deutschland mit seiner Vorreiterrolle in der industriellen Produktions- und Automatisierungstechnik, aber diese Position bröckele bereits in den Bereichen Automobil und industrielle KI, weil die Investitionen im Vergleich zur Konkurrenz zu gering seien: Laut VDE Tec Report sehen 28% der befragten Mitglieder China, Japan und Südkorea bei Industrie 4.0 vor Deutschland. Die Studienautoren formulieren konkrete Handlungsempfehlungen für das zentrale Technologiefeld der Informations- und Kommunikationstechnik. Zugleich stellen die Fachleute Bezüge zu anderen existenziellen Feldern her. „Politik und Wirtschaft müssen ihre Anstrengungen gleichermaßen vervielfachen. Um unsere technologische Souveränität zurückzugewinnen bzw. auszubauen, sind auch massive Investitionen in Aus- und Weiterbildung sowie für die Forschung in Deutschland notwendig“, sagt VDE-Präsident Dr. Gunther Kegel.

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



Lütze tritt Single-Pair-Ethernet-Netzwerk bei



Bild: Friedrich Lütze GmbH

Der Automatisierungsanbieter Friedrich Lütze ist zum Jahresanfang dem SPE Industrial Partner Network beigetreten. Das im Herbst 2019 gegründete SPE Industrial Partner Network ist ein gleichberechtigter Zusammenschluss von Unternehmen, die die Single-Pair-

Ethernet-Technologie als Grundlage für ein schnelles und erfolgreiches Wachstum des IIoT und Industrie 4.0 vorantreiben.

Friedrich Lütze GmbH
www.luetze.com



Drahtlose Echtzeitkommunikation per Licht

Das Fraunhofer IPMS hat Li-Fi und Time Sensitive Networking kombiniert, um die echtzeitfähige und deterministische Datenübertragung drahtlos zu ermöglichen. Damit können mobile Anwendungen wie Industrieroboter oder dynamische Fertigungszellen drahtlos und in Echtzeit via TSN Standard kommunizieren. Li-Fi ist eine Technologie zur drahtlosen Datenübertragung mittels Licht und bietet die Möglichkeit Übertragungszeiten im Mikrosekundenbereich zu realisieren. Zudem ist die Datenverbindung mit Li-Fi zuverlässig und bietet eine gleichbleibende Qualität. Time Sensitive Networking (TSN) erweitert bisherige Ethernet-Standards, um die

deterministische und echtzeitfähige Datenübertragung durch ein gemeinsames Netzwerk. Vor allem im Bereich der modernen Produktion werden hohe Bandbreite und garantierte Zykluszeiten unter einer Millisekunde benötigt. Eine zeitkritische und priorisierte Steuerung der Datenströme ist hierfür unabdingbar. Bisher war die echtzeitfähige Datenübertragung für TSN kabelgebunden. Eine Übertragung mit Funk wäre eine Alternative, unterliegt jedoch klaren Grenzen. Mit heutigen Funkstandards wie 4G, LTE,



WLAN oder auch dem zukünftigen Funkstandard 5G sind geforderte Latenzzeiten aus der Automatisierung im Mikrosekundenbereich nicht erreichbar.

Fraunhofer IPMS
www.ipms.fraunhofer.de

LORA-GATEWAY MIT LTE-FUNKTION

In das Sentries RG186 LoRa-Gateway von Laird wurde seitens M2M Germany der Mobilfunkstandard LTE integriert. Prinzipiell offeriert das Gateway sichere, skalierbare und robuste LoRa-Lösungen für die End-to-End-Steuerung eines privaten LoRaWAN-Netzwerks. Aufgrund der

► Durch die LTE-Integration kann das Gateway flexibel eingesetzt werden.

Integration von LTE erweitert sich das Einsatzspektrum, denn nun ist es möglich auch in entlegenen

Winkeln LoRa-Netzwerke zu installieren und gesammelte Daten entsprechend via Gateway und LTE-Mobilfunk weiterzuleiten. Das Gateway verfügt weiterhin über Dual-Band-WLAN, BT v4.0 (BLE und Classic) und kabelgebundenes Ethernet. Basierend auf den Semtech SX1301/SX1257 Chipsatzdesigns bietet es eine LoRa-Reichweite bis zu 16km und eine vorinstallierte Packet-Forwarder-Software, abgestimmt auf skalierbare, flexible IoT-Netzwerke. Das Gateway verwendet zertifizierte LoRa + BLE-Module der SentriesRM186-Serie.

m2m Germany GmbH
www.m2mgermany.de

Gateways mit frei programmierbaren Schnittstellen

MC Technologies bietet die Gateways der MC100-Familie für 4G-Mobilfunk in einer neuen Version an. Das MC100 GPIO ist Microsoft-Azure-zertifiziert, basiert auf Linux und besitzt frei programmierbare Schnittstellen. Anwender können aufgrund von digitalen, analogen, seriellen und Sensorschnittstellen aus der Ferne diagnostizieren, vorausschauend warten oder Personal informieren. Ei-

gene Anwendungen können Entwickler mit Node-Red über eine grafische Weboberfläche erstellen. Verschiedene Eingabe-, Ausgabe- und Prozess-Nodes lassen sich mit vorkonfigurierten Funktionsblöcken miteinander verbinden.

MC Technologies GmbH
www.mc-technologies.net



Virtuelle serielle Kabel

Das virtuelle serielle Kabel von Coniugo ist kein Kabel im klassischen Sinne, sondern eine virtuelle Verbindung über LTE/4G. Die bei CSD übliche Geschwindigkeitsbegrenzung auf 9.600Bit/s wird somit umgangen. Die Abrechnung erfolgt nicht im Zeittakt, sondern nach Datenvolu-

men. PC und SPS können mit dem System problemlos kommunizieren, ebenso viele fernauslesbare Energiezähler und andere technische Einrichtungen, die die serielle Schnittstelle nutzen. Das virtuelle Kabel Vortex Serial Data Bridge kann sowohl als serielles Kabel konfiguriert werden, als auch als Modem für die Anwahl mit einer Rufnummer. LTE-Funk soll serielle Echtzeitverbindungen für Fernwirkanwendungen problemlos realisieren.



Coniugo GmbH
www.coniugo.com

Outdoor LoRaWAN Gateway für das Internet der Dinge

IP67 Rundumschutz und bis zu 16 simultane Kanäle sind dem neuen UG87 von ICP Deutschland zu Eigen. Damit ist das Gateway in der Lage im Außenbereich eingesetzt zu werden und Daten von Klasse A und Klasse C Geräten in einem Bereich von max. 10km Reichweite zu empfangen und an Rechenzentren weiterzugeben. Im Inneren arbeitet ein 64Bit ARM Cortex-A53 mit 800MHz Taktrate. Das UG87 ist mit 512MB DDR RAM und 8GB eMMC Speicher ausgestattet und verfügt über einen m.2 Slot zur Erweiterung des Speichers mit Sata-basierten SSDs. Der Netzwerkanschluss unterstützt 10/100/1000 Base-T und ist PoE fähig. Als Powered Device verbraucht das UG87 maximal 8,2W. Wer keine PoE Spannung zur Verfügung hat, kann auf 9~48VDC oder 220VAC-Varianten

zurückgreifen. GPS für die Lokalisierung und hochpräzise Zeitsynchronisation stehen standardmäßig zur Verfügung. Optional bietet das UG87 die Möglichkeit Mobilfunk nach 3G/4G-LTE-Standard und Wi-Fi IEEE 802.11 b/g/n/ac nachzurüsten. Das UG87 unterstützt eine Vielzahl an Netzwerkprotokollen wie MQTT, TCP, UDP, VPN Tunnel wie OpenVPN, DMVPN, Zugriffsauthentifizierung wie CHAP, PAP, Firewall Funktionalitäten und Management Optionen. Montiert wird das UG87 entweder direkt an einer Wand- oder an einem Mast und kann in einem Temperaturbereich von -40 bis +70°C betrieben werden. Vom Sensor in die Cloud, mit dem UG87 bieten sich Systemintegratoren vielfältigen Möglichkeiten ihre Daten in die Cloud zu bringen.



ICP Deutschland GmbH
www.icp-deutschland.de

NEUE UNMANAGED SWITCHES FÜR PROFINET UND ETHERNET/IP

Phoenix Contact bringt zwei neue Unmanaged Switches für Ethernet/IP und Profinet auf den Markt. Die Produkte mit der Endung 'PNE' sind für Automatisierungsanwendungen ausgelegt, in denen Daten von Profinet und Ethernet/IP gegenüber anderen Ethernet-Paketen priorisiert werden. Dazu bieten sie nicht nur über dasselbe Multicast-Filtering wie die bisherigen Profinet-Switches (PN-Varianten), sondern unterstützen darüber hinaus die spezielle UDP-Priorisierung des Ethernet/IP-Datenverkehrs. Die Switches ermöglichen dem Anwender eine nahtlose Integration ohne weitere Konfiguration.



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

Industrial NAT Gateway/Firewall

Die robuste und unkomplizierte Ethernet-Komponente Wall IE von Helmholz ermöglicht die Integration von Maschinennetzen in das übergeordnete Produktionsnetz. Konkret schützt die Komponente die Netze, indem sie genau regelt, welcher Teilnehmer mit welchem Gerät kommunizieren und Daten austauschen darf. Das Gateway passt sich durch eine individuelle Konfiguration über das Webinterface den jeweiligen Anforderungen des vorhandenen Maschinennetzwerkes an. Die Beschränkung von Zugriffsrechten auf autorisierte Personen stellt dabei eine Grundvoraussetzung für den Schutz des Automatisierungsnetzwerkes dar. Dabei bleiben die hinter Wall IE liegenden

Netze bzw. IP-Adressen verborgen und sind von außen nicht sichtbar. Wird das Firmennetzwerk nun durch einen Hackerangriff oder auch durch Unachtsamkeit eines Mitarbeiters von einer Viren- bzw. Schadsoftware bedroht, bleibt das Automatisierungsnetz hinter dem Gateway davon unberührt



Helmholz GmbH & Co. KG
www.helmholz.de

Flexible Lösungen für hochleistungsfähige Netzwerke

Kyland Technology hat sein Produktprogramm um die Managed-Ethernet-Switches der neuen Sicom 3000A-Serie erweitert. Diese robusten IPv4/IPv6-fähigen Geräte, die Ethernet/IP, Modbus/TCP und Profinet unterstützen, wurden insbesondere für datenintensive Anwendungen in Bereichen wie der Fabrikautomatisierung, dem Verkehrswesen oder der Stromübertragung und Stromverteilung entwickelt. Insgesamt 20 Ausführungen mit unterschiedlichen Kombinationen aus RJ45-Ports für GBit Ethernet (GE) und Fast Ethernet (FE) sowie Steckplätzen für elektrische und optische SFP-Module, ermöglichen flexible Lösungen für hochleistungsfähige Netzwerke. Die Switches sind als Full-GE-Geräte, mit GE-Uplinks und FE-Ports sowie als reine FE-Geräte erhältlich.



Kyland Technology Co., Ltd.
www.kyland.com

INDUSTRIEGERECHTE FIREWALL MIT MULTI-PORT KONFIGURATION

Belden präsentiert die industriegerechte Firewall Eagle von Hirschmann. Sie bietet zusammen mit dem Hirschmann Security Operating System (HiSecOS) eine Lösung zur sicheren Überwachung der Datenkommunikation und wurde speziell für Anwendungen in der Operational Technology (OT) entwickelt, insbesondere industrielle Netzwerke wie Anlagen der Fabrik- und Prozessautomatisierung. Die aktuelle Version bietet Betreibern verbesserte Leistung und Sicherheit, z.B. durch mehr Portoptionen mit erhöhter Bandbreite und unterschiedlichen Verschlüsselungsfunktionen. Die Systemkonfigurierbarkeit ist für alle Qualifikationsgrade des Personals ausgelegt, mittels einer umfassenden grafischen Bedienoberfläche, einem Firewall Lernmodus und DPI Modulen (Deep Packet Inspection). Um unterschiedlichen industriellen Einsatzszenarien gerecht zu werden, hat die Firewall ein konvektionsgeköhltes Metallgehäuse und bietet somit eine robuste Lösung für den Fertigungsbereich, die die Netzwerkleistung nicht beeinflusst. Davon profitieren vor allem OT-Teams, die in rauen Umgebungsbedingungen des Maschinenbaus und der Produktion tätig sind.



Belden Electronics GmbH
www.belden.com

Direkter Zugriff auf IO-Link-Devices

Schmalz hat den IO-Link-Master SDI-USB entwickelt, der den Zugriff auf Vakuum-Komponenten mit IO-Link-Schnittstelle direkt vom Rechner aus ermöglicht. Eine Verbindung zur übergeordneten Steuerung ist somit nicht mehr notwendig. Dazu wird die Komponente direkt an den IO-Link-Master angeschlossen, der über USB mit einem Laptop verbunden wird. Der Anwender installiert die dazugehörige Software HMI-SDI und kann nun über die entsprechende Maske das Device auslesen sowie parametrieren.



► Das SDI-USB ermöglicht den direkten Zugriff auf Vakuum-Komponenten mit IO-Link-Schnittstelle – unabhängig von der übergeordneten Steuerung.

J. Schmalz GmbH
www.schmalz.com

OPC-UA-Server für Statusinformationen und Alarmer

Bachmann Electronic hat einen integrierten OPC-UA-Alarms-and-Conditions-Server für das Automatisierungssystem M1 auf den Markt gebracht. Alarmer und Statusinformationen aus der Steuerungs- und Feldebene können unabhängig von Hersteller oder Plattform von einer SPS auf andere Maschinen, Bediengeräte, Überwachungssteuerungen oder ERP-Systeme übertragen werden. Das installierbare Modul erkennt kritische Werte oder Statusänderungen ohne eine erforderliche Programmierung. Zusätzlich kann die Steuerungslogik Alarmstatusänderungen über eine API aus dem Steuerungsprogramm auslösen. Alle weitergeleiteten Änderungen an Bediengeräte, Leitstände oder Clients können verschlüsselt werden.

Bachmann Electronic GmbH
www.bachmann.info

Industrielle LTE-Gateways für Remote-Verbindungen



Moxa hat die kompakten Mobilfunk-LTE-Gateways OnCell 3120-LTE-1 vorgestellt. Das Gateway wurde für den Anschluss von seriellen und Ethernet-Geräten an ein Mobilfunk-Netzwerk entwickelt und ermöglicht die Bereitstellung von Anwendungen in verschiedenen IIoT-Fernzugriffsszenarien. Mit ihren Stromsparfunktionen, einer erweiterten Betriebstemperatur von -30 bis 70°C, einer sicheren VPN-Kommunikation und GuaranLink für eine zuverlässige Mobilfunk-Konnektivität gewährleistet das Gateway unterbrechungsfreie Verbindungen über LTE-Netzwerke. Darüber hinaus unterstützen die Gateways die OnCell Central-Manager-Software, um eine Vielzahl

von Gateways über Mobilfunknetzwerke zu konfigurieren und zu verwalten, einschließlich Remote-Neustart und Durchführung von Firmware-Upgrades. Die OnCell 3120-LTE-1 Serie bietet zwei Standby-Modi, um den Stromverbrauch im Leerlauf zu reduzieren, so dass das Gerät mit solarbetriebenen Batterien betrieben werden kann. Der Sleep-Modus reduziert den Stromverbrauch effektiv auf weniger als 2W und unterstützt das Aufwachen per SMS oder nach einem vorkonfigurierten Zeitplan.

Moxa Inc.
de.moxa.com



► Beim Thema SPE im Maschinen- und Anlagenbau stehen sich zwei Anbieterinitiativen gegenüber, das SPE Industrial Partner Network (links) und die SPE System Alliance (rechts).

Single Pair Ethernet im Maschinen- und Anlagenbau

Was kann SPE und wie sieht es aus?

Auf den letzten Messen gab es bereits erste Lösungsansätze und Prototypen für Single Pair Ethernet (SPE) zu sehen. Parallel wurden auch schon zwei Anbietervereinigungen ins Leben gerufen – das SPE Industrial Partner Network und die SPE System Alliance. Beide schreiben SPE großes Potenzial für den Maschinen- und Anlagenbau zu. Das INDUSTRIAL COMMUNICATION JOURNAL hat bei den Sprechern beider Initiativen nachgehakt, welchen Weg sie bei SPE einschlagen wollen.

Bietet SPE in der Produktion die bessere Alternative zu heute genutzten Technologien bzw. Standards?

Frank Welzel, SPE Industrial Partner Network: Das Ziel von SPE ist es, Ethernet da hin zu bringen wo es heute noch gar nicht verwendet wird. Wenn man sich in der Industrie heute die Feldebene anschaut, erfolgt dort die Kommunikation überwiegend über proprietäre Feldbusse oder analoge Signale, wie die 0(4)-20mA-Stromschleife. Hier kann Single Pair Ethernet die Lösung sein, um eine einheitliche offene TCP/IP

basierte Kommunikation zu ermöglichen. Durch die reduzierte Verkabelung von nur noch einem Adernpaar, mit dem man simultan auch Leistungen von bis zu 50W am Gerät übertragen kann, bietet SPE sehr einfach und kostengünstig die Möglichkeit, Ethernet in die Feldebene zu bringen. Vor dem Hintergrund, dass Sensoren immer intelligenter, die Datenraten, und Menge immer größer werden, kann SPE genau die Lösung sein, um alle Geräte in der Feldebene digital miteinander zu verbinden.

**Simon Seereiner, SPE System Alliance**

» **Das Konzept hinter SPE ist eine Erweiterung von Ethernet bis in die Sensorik, also bis in den letzten Winkel des Anlagenfeldes.**



Bild: Weidmüller-Gruppe

Simon Seereiner, SPE System Alliance: Bereits heute ist absehbar, dass herkömmliche Ethernet-Bussysteme den zukünftigen Anforderungen im industriellen Umfeld nur noch bedingt gerecht werden. Durch die Digitalisierung steigt die Anzahl smarter Sensorik, die in Maschinen und Anlagen eingebunden werden und damit auch der Aufwand der Vernetzung. SPE bietet sich hier als Alternative an, denn es steht für eine durchgängige skalierbare und deterministische Vernetzung von der Sensorik bis in die Cloud. Und das in praktisch jeder Anwendung, in der Daten anfallen, ob in der Industrie, in der Logistik oder im Gebäude. Das Konzept dahinter ist eine Erweiterung von Ethernet bis in die Sensorik, also bis in den letzten Winkel des Anlagenfeldes. Ein Vorteil von SPE ist die durchgängige Kommunikation, bei der keine Gateways für die Umsetzung auf andere Protokolle benötigt werden. Der Anwender spart Kosten und Zeit bei der Implementierung seiner Sensoren bis in die obersten Leitebenen. Bisherige Ethernet-Lösungen benötigen zwei bzw. vier Adernpaare, während Single Pair Ethernet nur noch ein Adernpaar benötigt. Mit SPE steht nicht nur eine industrietaugliche, kompakte und einfach aufgebaute Verkabelung bereit, SPE vereinfacht auch den Einsatz an extremen Einsatzorten, an denen eine Verkabelung mit kleinem Außendurchmesser, kleinen Biegeradien und geringem Gewicht unabdingbar ist.

» **Ist die Standardisierung schon so weit, dass man in die Umsetzung konkreter Produkte gehen kann?**

Seereiner: Nur mit Standardisierung auf der physischen Ebene sind Interoperabilität und damit der langfristige Erfolg von SPE gesichert. Der erste SPE-Standard wurde in der IEEE802.3 veröffentlicht. In der IEEE sind bereits die Kanalanforderungen erarbeitet, mit der IEEE802.3cg die 10MBit/s-Variante 10Base-T1, in der 802.3bw geht es bei 100Base-T1 um 100MBit/s und bei 802.3bp um 1000Base-T1 mit 1GBit/s. Durch diese drei

Frank Welzel, SPE Industrial Partner Networks

» **Eine flächendeckende Verbreitung von SPE sollte innerhalb der nächsten fünf Jahre möglich sein.**



Bild: Harting Technologiesgruppe

Steckgesichter, Abmessungen sowie mechanische Eigenschaften. Normungsaktivitäten sind allerdings ein dynamischer Prozess, bei dem neue Normen erarbeitet, eingebracht und diskutiert werden. Dabei werden permanent auch neue Normungsprozesse angestoßen. Naturgemäß neigen in diesem Stadium des Prozesses manche Hersteller dazu, Vorschläge kurzerhand als Vorschrift zu kommunizieren, um ihr Produkt als neuen Standard anzupreisen. Der normative Prozess ist derzeit in Arbeit, aber noch nicht abgeschlossen.

» **Ist sich der Markt bezüglich der elektromechanischen Schnittstellen einig?**

Welzel: Die Unternorm IEC63171-6 ist aus der ersten eingereichten Norm für SPE-Steckgesichter hervorgegangen. Nämlich aus der IEC61076-3-125, einem in sich geschlossenen und vollständigen Normendokuments mit allen notwendigen Spezifikationen und Prüfsequenzen. Weiterhin ist die IEC63171-6 die einzige Schnittstelle aus dieser Reihe, die in allen wichtigen Verkabelungsnormen und Anwendergruppen referenziert wird. Bereits 2018 haben sich ISO/IEC und TIA nach einer internationalen Abstimmung für die IEC63171-6-Schnittstelle für SPE in industriellen Anwendungen ausgesprochen. Das heißt: Wenn Sie normenkonform zu der

ISO/IEC11801-3 verkabeln wollen, müssen Sie den T1 Industrial einsetzen. Auch bei TIA entsteht so eine Verkabelungsnorm mit klarer Aussage zu den einzusetzenden Steckgesichtern. IEEE802.3cg stützt diese Position und referenziert ebenfalls ausschließlich auf die IEC63171-6-Industrial-Style-Schnittstelle. Nachdem diese Norm schon in der Entwicklung war, sind weitere Hersteller auf das Thema SPE aufgesprungen und haben eigene Steckgesichter in die Normung eingebracht, statt gemeinsam die schon in Arbeit befindliche Schnittstelle zu einem Standard zu formen. So entsteht die momentan als unentschieden wahrgenommene Situation des Wettbewerbs. Diese Situation wollen wir eigentlich vermeiden. Die angesprochene Konkurrenzsituation ist aber auch etwas ganz Normales und sorgt dafür, dass sich der Beste durchsetzt – auch in der Normung. Unsere IEC63171-6 wurde Ende Januar veröffentlicht und ist für jeden frei verfügbar, der eine umfassend genormte End-to-End-Verbindung sucht, die vollständig standardisiert ist. Alle 17 Mitglieder des SPE Industrial Partner Network haben sich zur IEC63171-6 committed. Deswegen: normativ ist mittlerweile alles klar.

Seereiner: Die Aussage, dass der Markt sich bereits auf ein Steckgesicht geeinigt hätte, ist definitiv falsch. Die Steckverbinder gemäß IEC63171-2 und IEC63171-5 sind für den indus-

IEEE-Gremien sind somit drei Datenraten abgedeckt. Die generellen elektrischen Anforderungen an die Schnittstellen sind in der Grundnorm IEC63171 zu finden. Die in den Normenreihen -1 bis -6 definierten Steckverbinder haben unterschiedliche

triellen Einsatz spezifiziert. Dafür investieren die Firmen Weidmüller, Phoenix Contact und Telegärtner bereits in Werkzeuge und wollen demnächst fertige Produkte vorstellen.

Sind noch weitere Herausforderungen zu lösen?

Seereiner: Eine Herausforderung ist es

Menge an Geräten mit SPE-Technik verfügbar sein wird, ist nicht leicht. Wir rechnen mit ersten Geräten zur SPS im November 2020. Eine flächendeckende Verbreitung von SPE sollte dann innerhalb der nächsten fünf Jahre möglich sein. Erste Anwendungen werden in der Bahnindustrie, bei kleinen Robotern und autonomen

Simon Seereiner, SPE System Alliance

» Für Steckverbinder gemäß IEC63171-2 und IEC63171-5 investieren die Firmen Weidmüller, Phoenix Contact und Telegärtner bereits in Werkzeuge.

jetzt, sich nicht nur auf spezifizierte Steckgesichter zu fokussieren. Die SPE System Alliance hat es sich durch die Ausrichtung zu einer branchen- und applikationsübergreifenden Austauschplattform zur Aufgabe gemacht, Unternehmen aus allen zukünftigen SPE-Ecosystemen zusammen zu bringen. Der Blick ist dabei nicht auf Einzelaspekte wie die Anschlusstechnik fokussiert. Ziel ist es vielmehr, Experten aus unterschiedlichen Bereichen zusammenzuführen und gemeinsam die Infrastruktur für das IIoT aufzubauen.

Wann rechnen Sie mit einer flächendeckenden Verbreitung?

Seereiner: Die Vorteile von SPE sind unbestritten. Wir rechnen damit, dass sich in den nächsten zwei bis fünf Jahren die ersten durchgängigen Lösungen etabliert haben und signifikante Stückzahlen erreicht werden. Bis die Technologie den gesamten Automatisierungsmarkt durchdringt, kann es noch sieben bis zehn Jahre dauern. Wenn sich zeigt, dass sich mit SPE im industriellen Umfeld ähnliche Einsparungen erreichen lassen wie beim Einsatz im Automobilbereich, wird die Marktakzeptanz sicherlich schneller von statten gehen.

Welzel: In der Automatisierung benötigt es zweifellos einige Zeit, bis sich ein Technologiewechsel vollziehen kann, da alle benötigten Geräte mit der Technik ausgerüstet werden müssen. Eine verlässliche Abschätzung darüber, ab wann eine ausreichende

Transportsystemen umgesetzt werden, da man in diesen Bereichen zum Teil händierend nach Möglichkeiten zur Miniaturisierung und einer schlankeeren Verkabelung sucht.

Welche Rolle wollen Sie bei der Einführung von SPE in der Industrie übernehmen?

Seereiner: Mit den Playern der SPE System Alliance – wie Moxa, Phoenix Contact, Sick und Microchip, um nur einige zu nennen – haben sich führende Industrieunternehmen vorgenommen, die SPE-Technologie am Markt zu etablieren. Erste marktfähige Produkte werden bereits zur Hannover Messe gezeigt.

Welzel: Das SPE Partner Network ist im Verbund der Technologieführer gleichzeitig Investitionsgrundlage, Produktanbieter und Berater. In unseren Augen ist es wichtig, auch andere Organisatoren als Partner zu gewinnen. Daher haben wir das Partnernetzwerk auch schon bei der PNO vorgestellt und werden dies auch bei weiteren Gruppen machen. Unser Netzwerk freut sich über jegliche Kooperation, um SPE als Technologie nachhaltig zu positionieren. ■

Simon Seereiner ist Head of Product Management Sensor-Aktor-Interface / Industrial Ethernet bei Weidmüller.

Frank Welzel ist Director Global Product Management bei Harting Electronics.



Informationsportal für die Industrie

- ✓ Passende Produkte finden
- ✓ Marktüberblick gewinnen
- ✓ Kompetent entscheiden

Nicht suchen, sondern finden!



Gleich ausprobieren!
www.i-need.de



► Single Pair Ethernet kann mit seinen Möglichkeiten zur DNA des IIoT werden.



Normiert in die Zukunft mit SPE

Quo vadis Ethernet?

Die technologischen Vorteile einer reduzierten Verkabelung treten immer deutlicher zu Tage. Sein Potenzial kann das Single Pair Ethernet (SPE) aber nur als herstellerunabhängiger und normierter Teil einer neuen Netzwerkarchitektur ausschöpfen. Gemeinsam mit Marktbegleitern treibt Phoenix Contact die Entwicklung und Standardisierung von geschützten und ungeschützten Steckgesichtern voran.

Mit den Trends ist es manchmal so eine Sache. Jeder hat schon davon gehört, viele reden darüber, aber kaum einer weiß wirklich Bescheid. Das gilt auch für das Single Pair Ethernet (SPE). Deswegen Vorteile liegen sprichwörtlich auf der Hand und sind bereits vielfach kommuniziert worden: weniger Rohstoffeinsatz bei den Kupferadern, geringeres Gewicht in der Handhabung, kompaktere Kabeltrassen in der Gebäude- und Anlagenverkabelung. All das sind unbestreitbar echte Vorteile – gegenüber dem achtadrigen Ethernet oder der Feldbusverkabelung. Aber in welchen Szenarien kommen diese Vorteile zum Tragen? Was ist wirklich erforderlich, damit SPE zur DNA des Industrial Internet of Things (IIoT) werden kann?

Zukunft der industriellen Kommunikation

Das IIoT ist die Vision einer vollständig vernetzten industriellen Produktion. Alles ist mit Allem verbunden und tauscht fleißig Daten aus: Menschen mit Maschinen; Maschinen mit Roh-, Zwischen- und Endprodukten; Endprodukte mit anderen Endprodukten. Und das alles quer über Branchen und Anwendungsbereiche hinweg. Dabei wird schnell klar, dass nicht nur die Anzahl der Teilnehmer in diesem industriellen Netz der Dinge potenziell unendlich ist. Auch die relevanten Datenmengen wachsen in kaum vorstellbare Dimensionen hinein. Nahezu unendlich viele Teilnehmer und unendlich viele Daten – da könnte man auch

an ein Chaos babylonischen Ausmaßes denken. Man stelle sich nur eine riesige 'Talkrunde' vor, in der jeder einzelne Mensch auf der Erde gleichzeitig in seiner Sprache versuchen würde, sich allen anderen Zeitgenossen mitzuteilen. Undenkbar ohne eine gemeinsame Sprache, ohne gemeinsames Regelwerk und ohne genau definierte Ordnung, wer wann wie lange und mit wem spricht. Das Industrial Internet of Things kennt jedoch eine derartige Ordnung: das Ethernet-Protokoll. Als Kommunikationsprotokoll für den Datenaustausch definiert es exakt die oben genannten Rahmenbedingungen. Bereits seit den 1970er Jahren ist das Ethernet zur firmeninternen und lokal begrenzten Übertragung von Datenpaketen in kabelgebundenen Computernetzwerken (LAN – Local Area Network) etabliert. Bisher drang es jedoch nicht in die letzte Feldebene vor. Vor diesem Hintergrund wurden die bestehende Feldverkabelung, die Geräteschnittstellen sowie die Geräte selbst hardwareseitig für die Feldbus-Kommunikation ausgelegt.

SPE ist heute richtungsweisend

Es zeigt sich also deutlich, dass es sich beim Single Pair Ethernet noch um eine Zukunftsvision handelt – aber auch beim Konzept des IIoT steht das Visionäre ja noch im Vordergrund. Die kommenden drei bis fünf Jahre werden allerdings richtungsweisend für beide Visionen sein. Und in der Tat bedingen sich beide gegenseitig. Denn das Single Pair Ethernet umfasst,



wie aufgezeigt, nicht nur das softwareseitige Kommunikationsprotokoll, sondern auch dessen physikalische Übertragungswege – den so genannten Physical Layer. Ähnliche Definitionen werden nicht nur für das Single Pair Ethernet erarbeitet, sondern auch für andere Anwendungen wie beispielsweise die Funkübertragung (5G), die Datenübertragung in der Prozessindustrie und im Großanlagenbau (APL – advanced physical layer) oder Echtzeitkommunikation (TSN – time sensitive networking). Damit wird schon heute der Grundstein für eine ganz neue Netzwerkarchitektur gelegt.

Erst die Normierung schafft Sicherheit

Ausgangspunkt für die aktuell entwickelten SPE-Normen ist der offene BroadR-Reach-Standard von 2011. Ursprünglich von der Broadcom Corporation entwickelt und an Teilnehmer der Open Alliance SIG lizenziert, beschreibt der Standard physikalische Schnittstellen und Übertragungsmedien in Automobilanwendungen. Im Kern geht es dabei um die Datenübertragung über ein einziges, verdrehtes Aderpaar. Hier liegt also die eigentliche Geburtsstunde des Single Pair Ethernet – wenn auch noch nicht unter diesem Namen. Die IEEE 802.3 hat bezüglich der Normierung der Steckverbinder für das Single Pair Ethernet der ISO/IEC JTC 1/SC 25 WG 3 einen Arbeitsauftrag erteilt, um entsprechende Steckverbinder vorzuschlagen und zu standardisieren. Dabei kommt es darauf an, die entsprechenden MICE-Klassen für die unterschiedlichen Applikationen in Büro- und Industrieumgebung zu berücksichtigen. MICE beschreibt die mechanischen Eigenschaften, die Dichtigkeitseigenschaften, die klimatischen Eigenschaften und die elektromagnetischen Eigenschaften der Steckverbinder und Kabel (MICE-Klas-

sen: Mechanical, Ingress, Climatic, Electromagnetic). Seit 2017 wurden dann in der Normenreihe IEC63171 neue Normen zusammengefasst, die physikalische Schnittstellen für unterschiedliche IP-Schutzarten und damit unterschiedliche Einsatzbereiche in der industriellen und semi-industriellen Automatisierung beschreiben. Die IEC63171 umfasst eine Basisnorm, die alle Steckverbinder erfüllen müssen. Darunter gliedert sich die Norm in aktuell sechs Standardisierungsvarianten mit unterschiedlichen Steckverbindern, die allesamt für das Single Pair Ethernet geeignet und zugelassen sind. Keiner dieser Standards wurde bereits veröffentlicht. Daher kann in Bezug auf deren Definitionsrahmen – die physikalischen Übertragungswege – derzeit auch noch nicht von einem Standard gesprochen werden. Eine Empfehlung der IEEE für zwei dieser Standards in Kombination mit dem entsprechenden Einsatzgebiet – Gebäude- und industrielle Verkabelung – wurde jüngst wieder revidiert. Erst mit Prüfung und Veröffentlichung der endgültigen Norm sowie der breiten Akzeptanz am Markt kann sich hier ein Standard etablieren.



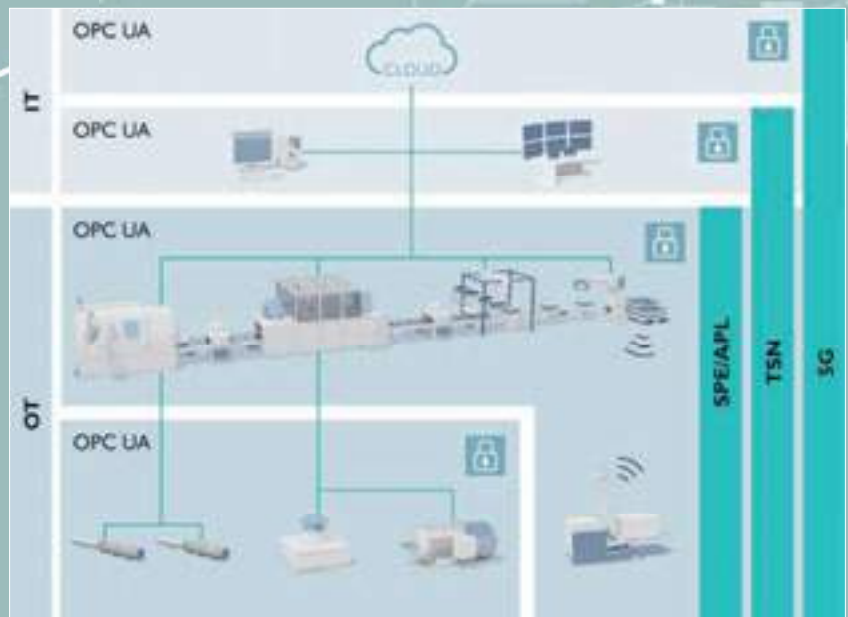
► Einpaarige und vierpaarige MICE-Schnittstellen werden für IP20- und IP6x-Anwendungen konzipiert.



Single Pair Ethernet – auf einen Blick

Das Single Pair Ethernet (SPE) beschreibt die physikalischen Schnittstellen zur einpaarigen Übertragung von Daten und Leistung zwischen unterschiedlichen Kommunikationsteilnehmern.

Das IEEE erarbeitet Normen für unterschiedliche Anwendungen mit Datenübertragungsraten von 10 (802.3 cg), 100 (802.3 bw) und 1000 MBit/s (802.3 bp) sowie für Leitungslängen von 15 bis 1.000 m.



► Neue Kommunikationsstandards sind die Basis für die durchgängige Vernetzung vom Sensor über die Maschine und übergeordnete Systeme bis in die Cloud hinein.

Use Case Factory Automation

Aktuelle Gerätegenerationen, Schnittstellen und Verkabelungskonzepte sind von den Standardisierungsbemühungen also nicht unmittelbar betroffen. Hersteller von Sensoren und Aktoren sowie von Steuerungen und Feldgeräten beschäftigen sich jedoch schon heute im Design-in-Prozess mit der Geräte-Generation, die erst in zwei bis drei Jahren Marktreife erlangt. Die durchgängige Ethernet-basierte Kommunikationsstruktur ist gerade für Hersteller von Feldgeräten schon heute ein wichtiges Argument. Auch die hohen Übertragungsdistanzen von bis zu 1.000 m sowie die Möglichkeit, Daten und Leistung von bis zu 60 W über nur ein Aderpaar (PoDL - Power over Dataline) zu übertragen, sind Schlüsselargumente für SPE in zukünftigen Gerätegenerationen. Phoenix Contact bietet mit seinem Steckverbinderkonzept ein durchgängiges steckkompatibles System an, das kompakt baut und das dem Gerätehersteller erlaubt, möglichst wenig Platz auf der Leiterplatte in Anspruch zu nehmen und damit kleinere Geräte zu bauen. Das Steckverbinderkonzept basiert auf IEC63171-2 für IP20-Applikationen in der Gebäude- und Schaltschrankverkabelung und auf IEC63171-5 für IP67-Applikationen in der Feldebene der industriellen Anwendungen. Außerdem treibt Phoenix Contact die Normierung der entsprechenden Schnittstellen voran. Gemeinsam mit anderen Marktbegleitern – Belden, Fluke Networks, Reichle & De-Massari, Rosenberger, Telegärtner und Weidmüller – entwickelt der Anschluss technik-Spezialist geschützte und ungeschützte Steckgesichter für einpaarige und vierpaarige Leitungen. Darüber hinaus treibt Phoenix Contact das Thema der gesamten SPE-Infrastruktur über die 'SPE System

Alliance' voran, zu der mittlerweile mehr als 15 führende Technologieunternehmen aus verschiedenen Branchen und Anwendungsbereichen zählen, die ihr SPE-Knowhow bündeln und zielgerichtet austauschen. Auch der Wunsch nach Kostenersparnis treibt die Reduzierung auf nur ein Aderpaar maßgeblich voran. Ein im oben erwähnten Konsortium entwickelter Use Case für den Bereich Factory Automation zeigt, dass SPE mögliche Kosteneinsparungen von mehr als 25 Prozent im Vergleich zu modernen modularen Maschinenkonzepten mit sich bringt. Die Kosteneinsparungen liegen nur begrenzt bei den Komponenten, sondern vielmehr in der konsequenten Nutzung der SPE-Technologie. Alle Komponenten der Maschine können dann digital miteinander kommunizieren. Darin liegt der eigentliche Vorteil bei der Kosten-Nutzen-Analyse, denn der Status jeder einzelnen Komponente der Maschine kann jederzeit und von jedem Ort abgerufen werden. Die Vorteile – Gewichtsreduktion der Kabel, Miniaturisierung und Vereinfachung der Anschlusstechnik – kommen erst mit der Durchgängigkeit der gesamten Infrastruktur zum Tragen. Die Netzwerkstruktur in allen Applikationsbereichen, von der Gebäudeautomatisierung über die Fabrikautomation bis hin zur Prozessautomation, wird von dieser Innovation beeinflusst. Niemand sollte in diesem

Kontext außer Acht lassen, dass es sich bereits heute entscheidet, wohin das Ethernet in Zukunft geht. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/36483



Dipl.-Wirt.-Ing. Verena Neuhaus,
Managerin Product Marketing Data Connectors,
Phoenix Contact Deutschland GmbH
www.phoenixcontact.de



IBHsoftec GmbH
64760 Oberzent/Beerfelden | Tel.: +49 6068 3001
info@ibhsoftec.com
www.ibhsoftec.com

IBH Link UA OPC UA Server mit integrierter Firewall



- OPC UA Server für die einfache Anbindung an MES-, ERP- und SAP-Systeme sowie Visualisierungen
- OPC UA Client zur Kommunikation mit anderen OPC Servern
- SINUMERIK® 840D/840D SL Anbindung
- Mitsubishi Electric Roboter- und Steuerungsanbindung
- Rockwell Automation Steuerungsanbindung
- Skalierbare Sicherheitsstufen
- S7-kompatible SoftSPS zur Datenvorverarbeitung integriert
- S7-Steuerungen über S7 TCP/IP oder IBH Link S7++ a ansprechbar
- S5-Steuerungen über IBH Link S5++ ansprechbar
- Komfortable Konfiguration mit dem kostenlosen IBH OPC UA Editor, Siemens STEP7 oder dem TIA Portal
- Administration per Webbrowser
- Historische Daten
- Alarms & Conditions
- Frei definierbarer Adressraum
- MQTT-Anbindung



STEP und TIA sind eingetragene Marken der Siemens Aktiengesellschaft Berlin und München.



Kontron
86156 Augsburg | Tel.: +49 821 4086-0
info@kontron.com
www.kontron.com

KONTRON TSN STARTERKIT

Out-of-the-Box-Lösung für TSN Edge Computing –
von der Entwicklung bis zur Serienreife



- ▶ Vorinstallierte und konfigurierte TSN-Plattform
- ▶ Direkte Integration in das TSN-Netzwerk
- ▶ Echtzeit-Linux und TSN-Beispielanwendungen
- ▶ Kein externer Switch nötig –
4x 10/100/1000/Mbps Ports
- ▶ Hardware und Software im Feld aufrüstbar



Kendrion Kuhnke Automation GmbH
23714 Malente | Tel.: +49 4523 402-0
sales-ics@kendrion.com
www.kendrion.com

SPS als Edge Device

OPC UA fähige CODESYS-Steuerung
für Industrie 4.0 Anwendungen

- Industrie 4.0 / IIoT fähig
- Profinet IRT (IO-Device)
- Modbus TCP / RTU
- CANopen
- EtherCAT
- modular erweiterbar
- Safety integrated
- Data Acquisition



Red Lion Controls
80687 München | Tel.: +49 5795 9421
europe@redlion.net
www.redlion.net/de



FLEXEDGE™

**BIS ZUM LETZTEN TROPFEN!
PRESEN SIE ALLE DATEN HERAUS!**

FlexEdge™ Edge

Automation Plattform - All in One:

- Protokollkonvertierung
- Digitalisierung von Altanlagen
- Einfache Edge-Programmierung mit
Automatisierungssoftware Crimson®
- Modulare Netzanbindung -
Cloud oder On-Premise, 5G ready



Scan & Design
mit dem
FlexEdge™ Builder



Bild: ©WangAnQ/istockphoto.com

5G-Campusnetze für die Industrie Wertvolle Infrastruktur

Kaum eine Fachdiskussion kommt derzeit ohne das Schlagwort 5G aus. Dabei ist die Erwartungshaltung an 5G vielfältig und scheint grenzenlos. Im industriellen Umfeld spielt 5G dabei eine wichtige Rolle als Enabler und Beschleuniger der Digitalisierung und Transformation zur vollvernetzten Industrie 4.0. In Deutschland wurde hierfür in Vorreiterrolle die Möglichkeit geschaffen, 5G-Lizenzen für lokale Campusnetze zu beantragen.

Aber warum sollte ein Unternehmen den auf den ersten Blick beschwerlicheren Weg des eigenen Netzes gehen? Sich mit Fragen der Konzeption, Planung, Beschaffung, Aufbau und Betrieb auseinandersetzen? Es gibt gute Gründe dennoch eine 5G-Campuslizenz zu beantragen. Nach erfolgreicher Beantragung erhält man ein lizenziertes Frequenzband mit exklusiven Frequenzen und somit alleinigen Zugriff auf die volle Netzkapazität im zugewiesenen Frequenzblock. Man muss diese Frequenzen nicht mit anderen Nutzern teilen; die individuelle Nutzung und die volle Kapazität des Spektrums sind garantiert. Aus den individuellen Anforderungen (Use-Cases) können eigene Qualitätsparameter und Redundanzkonzepte abgeleitet und realisiert werden, um die benötigte Verfügbarkeit effizient sicherstellen zu können. Firmendaten bleiben im eigenen Netz und der Eigentümer der Lizenzinhaber behält die Hoheit über seine sensiblen Firmen- und Produktionsdaten.

Kleinere Netze mit weniger Netzelementen lassen sich meist einfacher überwachen und schneller wieder störungsfrei in Betrieb nehmen.

Herausforderungen für den Campus-Netzbetreiber

Angenommen nach entsprechender Abwägung hat sich ein Unternehmen entschlossen Frequenzen zu beantragen und hat diese auch zugeteilt bekommen. Spätestens dann gibt es zahlreiche neue Aufgaben, die als Campus-Netzbetreiber gemeistert werden müssen. Da man vom Betreiber die Netznutzung nicht schlüsselfertig angeboten bekommt, muss man sich selbst um den Aufbau und Betrieb kümmern. Dies fängt bereits der Konzeption und Planung des Netzes als auch der betriebssicheren Funkversorgung an, geht über die Beschaffung, Aufbau und Inbetriebnahme der Systemtechnik



► Wer sich für den Aufbau eines eigenen 5G-Campusnetzes entscheidet, muss sich um den Aufbau und Betrieb selbst kümmern.

Bild: ©skynesher/istockphoto.com / ©sdecoret/stock.adobe.com / ©shotbydave/istockphoto.com / ©FARBAL/istockphoto.com / LS Telcom AG

bis hin zum eigentlichen Netzbetrieb mit Instandhaltung und Überwachung. Da dies in der Regel weder Kernkompetenz noch Kerngeschäft des Lizenzinhabers ist, kann dafür externe Hilfe einbezogen werden - sprich die gesamte Leistung oder Teile davon 'outsourced' werden. Letztendlich muss der Lizenzinhaber im eigenen Interesse sicherstellen, dass seine Frequenzen optimal genutzt, verwaltet und geschützt werden. Nicht zuletzt um einen effizienten Betrieb zu gewährleisten und die Produktionssicherheit zu maximieren.

Betriebssichere Funkkommunikation

Hauptaufgabe und Herausforderung ist die Sicherstellung einer störungsfreien und nicht manipulierbarer Funkumgebung bei gleichzeitiger Bereitstellung ausreichender Kapazitäten für alle erforderlichen Netze, Dienste und Anwendungen. Dabei sind drei Maßnahmen zu empfehlen um eine betriebssichere Funkkommunikation zu gewährleisten: Zuerst ist eine gewissenhafte und professionelle Konzeption und Planung erforderlich. Dabei spielt neben der technisch robusten Planung gerade in der Privatwirtschaft auch die Kosteneffizienz eine wichtige Rolle. Als zweite Maßnahme gilt die Durchführung einer Funk-Inventur. Sowohl das Medium Funk als auch dessen Nutzung sind für das menschliche Auge nicht sichtbar. Um zu wissen, was auf dem eigenen Betriebsgelände 'On-air' ist, ist eine Funkinventur notwendig – vergleichbar mit der Inventur in einem Lager. Eine Funkinventur ist zugleich die Basis der dritten Vorkehrung: Die Einführung einer Frequenznutzungsdatenbank mit Koexistenzanalyse. Dieses Datenbanksystem ist die zentrale Stelle in der alle funkrelevanten Daten und Informationen zusammengeführt und verwaltet werden.

Schutz des Campusnetzes

Nachdem 5G-Lizenzen erfolgreich beantragt wurden, ein eigenes Funknetz geplant als auch aufgebaut hat und nun mit business-kritischen Anwendungen in Betrieb geht sich die Frage, wie die Funkinfrastruktur – welche fraglos ein elementarer Bestandteil des Betriebs ist – nachhaltig geschützt werden kann. Was

kann getan werden, wenn im exklusiven Frequenzband plötzlich unbekannte Nutzer oder Störungen – sei es durch illegale Nutzung, mutwillige Cyberattacken, defekte oder nicht zugelassene Geräte – auftreten? Durch präventives Spektrum-Management wird die Datenbasis aktuell gehalten, man behält Kontrolle über alle Funkangelegenheiten und schützt sich vor bösen Überraschungen. Die kontinuierliche Überwachung des relevanten Frequenzbereichs kann mithilfe einer entsprechenden Anzahl von Messsensoren – verteilt auf dem Betriebsgelände – und einer geeigneten Steuerungs- und Analysesoftware, die Frequenznutzung in den relevanten Frequenzbändern permanent gemessen, gespeichert, kontrolliert und bei Anomalien alarmiert werden. Dies ist vergleichbar mit einer Rauchmeldeanlage, die schnell warnend alarmiert und dadurch großem Schaden zuvorkommt.

Fazit

Getrieben durch die Digitalisierung und Industrie 4.0 gewinnen zuverlässige, hochverfügbare und sichere Funknetze enorm an Bedeutung. In Deutschland gibt es neben den 5G-Frequenzen für den nationalen Mobilfunk die Möglichkeit Breitband für lokale Campusnetze zu beantragen. Dadurch können Unternehmen und Organisationen eigene 5G-Netze aufbauen und betreiben. Um eine optimale, effiziente Nutzung der Frequenzen sicherzustellen, muss das eigene 5G-Netz von Beginn an professionell konzipiert und geplant werden. Maßnahmen wie die Einführung einer Frequenznutzungsdatenbank, die Durchführung einer Funkinventur und Koexistenzanalysen sind empfehlenswert, um eine betriebssichere Funkkommunikation gewährleisten zu können. Vorausschauendes Spektrum-Management und permanentes Spektrum-Monitoring als Frühwarnsystem sind die geeigneten Versicherung für den vorbeugenden Funkschutz. ■



Roland Götz, Chief Operation Officer (COO)
und Mitglied des Vorstands der LS telcom AG
Fabian Ludwig, Business Development und Sales Manager
der LS telcom AG
www.lstelcom.com



Pilotprojekte für 5G in der Industrie

Next Generation in der Praxis

Industrial 5G soll die Tür zur umfassenden drahtlosen Vernetzung von Produktion, Instandhaltung und Logistik öffnen. Hohe Datenraten, leistungsfähige Breitband-Übertragung und ultrakurze Latenzzeiten werden dann große Effizienzsteigerung und Flexibilisierung bringen – so heißt es. Doch bisher ist 5G vor allem Theorie. Mit Ausnahme der folgenden Feldversuche und Pilotprojekte, die das INDUSTRIAL COMMUNICATION JOURNAL zusammengetragen hat. (mby)

Entfesselung der Roboter mit 5G

Bei Audi sorgt der neue Mobilfunkstandard in einem Testlabor dafür, dass Produktionsroboter ohne Kabel in die Automatisierung eingebunden werden. Ein Cobot mit Greifer setzt dabei Airbags passgenau in das Lenkrad ein. Ein Vorgang, der künftig jeden Tag vielfach so im Werk ablaufen könnte. Das Besondere ist bei dieser Testanwendung der Augenmerk auf die Personensicherheit. Denn der Roboter muss wireless im Gefahrenfall genauso schnell und sicher stoppen wie in herkömmlichen Fällen. Laut Audi ist mit 5G die Performance der dezentralen Steuerung über Funk genauso gut wie per Kabel. Aus Sicht des Automobilherstellers zeigt das Beispiel, dass 5G unter realen Produktionsbedingungen funktionieren kann. Entsprechend sei die 5G-Technologie bereit für den großen Einsatz, auch wenn es noch ein bis zwei Jahre dauere, bis 5G in Deutschland Realität ist. Die Technik hinter dem mit 5G vernetzten Roboter hat Audi zusammen mit Ericsson entwickelt. Gemeinsam sollen weitere Erkenntnisse für den 5G-Einsatz und neue Szenarien für die Smart Factory definiert werden. Etwa beim Einsatz von fahrerlosen Transportsystemen deren WLAN-Technik heute immer wieder mit abbrechenden Verbindungen und Fehlern kämpfen muss. Der ausschlaggebende Vorteil dafür sei, dass bei 5G erstmals auch der Fokus auf Verfügbarkeit und niedrige Latenzen gelegt werde, die in der Fertigung gebraucht werden. ■



5G in der Schaltschrankproduktion



Rittal hat als eines der ersten Industrieunternehmen die 5G Frequenzuteilung erhalten. Noch in diesem Jahr soll ein privates 5G Mobilfunknetz im neuen Werk in Haiger installiert werden. Erste Pilotprojekte etwa in der Produktionsüberwachung und -analyse sind bereits definiert. So soll die neue Funktechnologie den Datenverkehr deutlich beschleunigen und vereinfachen – etwa beim videobasierten Abgleich von Stückzahlen mit hinterlegten Auftragsdaten und bei der schrittweisen Implementierung von Analytics für eine präventive Instandhaltung. 5G kann Daten mit einer Geschwindigkeit von 10Gbit/s verarbeiten, das ist hundert mal schneller als mit LTE. Nach ersten Teststellungen will Rittal die 5G-Technik sogar in produktionskritische und steuerungsrelevante Aufgaben integrieren. Auch eine Anbindung der Produktion über 5G an das KI-basiertes Edge/Cloud-Rechenzentrum Oncite für echtzeitfähige Verarbeitung und Analyse von Industriedaten ist geplant. Sobald die Hersteller von 5G-Technik die entsprechenden Geräte zur Verfügung stellen, will Rittal die nächsten Schritte gehen. Das Unternehmen erwartet, dass die Installation der Technik für die ersten Teststellungen bis Ende 2020 abgeschlossen ist. ■

Testbed für vernetzte Produktion in Echtzeit

Seit 2017 arbeiten Fraunhofer IPT und Fraunhofer IWU mit mittelständischen Projektpartnern an einer Testumgebung für die vernetzte und standortübergreifende Produktion. In der ersten Phase wurde eine digitale Infrastruktur samt sicherer Cloud-Anbindung realisiert und gemeinsam mit Ericsson eine prototypische 5G-Verbindung errichtet. Im Rahmen der zweiten Phase geht es jetzt in die praktische Erprobung. Zur Datengewinnung werden z.B. Sensoren direkt an der Maschine, am Werkzeug oder am Bauteil angebracht. Die aufgezeichneten Ferti-

gungsdaten zum Zustand der Fräsmaschine und des Bauteils werden aufbereitet, in der Cloud gespeichert, analysiert und in einem Fertigungs-Cockpit visualisiert. Ein weiterer Anwendungsfall beschäftigt sich mit der Datenübertragung aus einer Werkzeugmaschine mittels einer 5G-Verbindung in die Cloud. Am Beispiel einer roboterbasierten Multi-Technologiezelle entwickeln die Partner zudem eine Entscheidungslogik, die die manuelle Planung ersetzen kann und Prozesse hinsichtlich Eingangs- und Zielgrößen aufeinander abstimmt. ■



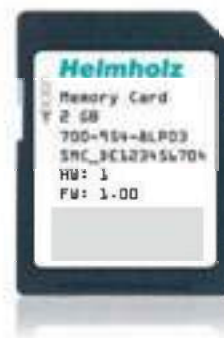
Bild: Fraunhofer-Institut für Produktionstechnologie

**KOSTEN SENKEN
OHNE QUALITÄTSVERLUST.**
Helmholz Speicherkarten – die clevere Alternative!



Helmholz Memory Cards für 1200er/1500er Baureihe

- Sofortige Kosteneinsparung
- Plug and Play
- Für den Einsatz in S7 Steuerungen
- Ab Lager lieferbar



BESTELLDATEN

BESTELL-NR.

Memory Card, 4 MByte	700-954-8LC03
Memory Card, 12 MByte	700-954-8LE03
Memory Card, 24 MByte	700-954-8LF03
Memory Card, 256 MByte	700-954-8LL03
Memory Card, 2 GByte	700-954-8LP03

Einsatzmöglichkeiten: CPU 1200, CPU 1500

Fordern Sie Ihr individuelles Angebot an:

Phone +49 9135 7380-0
E-Mail vertrieb@helmholz.de

Helmholz®
COMPATIBLE WITH YOU



Automobilwerk am 5G-Netz

Im Werk des Elektroautoanbieters e.GO Mobile in Aachen wurden mit Hilfe von Vodafone und Ericsson 5G-Features bereits umgesetzt. Gemäß dem Ansatz von Mobile Edge Computing verarbeiten kleine Echtzeit-Rechenzentren die Daten direkt in der Produktionshalle. Network Slicing sorgt für ein Netz nach Maß – abgestimmt für die Anforderungen der Serienproduktion. Insgesamt 36 Mobilfunkantennen garantieren in der 8.500m² großen Produktionshalle Bandbreiten bis 10Gbit/s und Latenzzeiten unter 10ms. Transportfahrzeuge, Maschinen und Werkzeuge tauschen so nahezu in Echtzeit Informationen aus – über den aktuellen Standort, zum momentanen Batterie-

zustand oder zur geplanten Fahrroute. Sämtliche Produktionsstoffe und Materialien werden direkt nach der Anlieferung über eine spezielle RFID-Schnittstelle automatisch und berührungslos identifiziert und in Echtzeit im Onlinesystem verbucht. Mit der gleichen RFID-Lösung werden Fahrzeuge beim Produktionsstart erkannt. Weil mit der Serienproduktion des Elektroautos auch die Zahl von Montagevorgängen und der Bedarf an Produktionsmaterialien zunehmen, müssen die Systeme zeitgleich immer mehr Daten verarbeiten. Um diese Datenmassen auch zukünftig sicher, zuverlässig und schnell zu bewältigen, wird 5G eingesetzt. ■



Bild: Vodafone GmbH

Erstes privates industrielles Standalone-5G-Netz

Siemens und Qualcomm haben ein eigenständiges privates 5G-Netz in einer realen industriellen Umgebung bei Nutzung des 3,7-3,8GHz-Frequenzbandes implementiert. Siemens stellt dabei die

realen industriellen Testbedingungen und Endgeräte wie Simatic-Steuerungen und I/O-Devices zur Verfügung. Qualcomm liefert das 5G-Testnetz sowie die dazugehörigen Testgeräte.

Das 5G-Netz wurde im Automotive Showroom und Testcenter von Siemens in Nürnberg installiert. Mithilfe von fahrerlosen Transportsystemen werden neue Fertigungsmöglichkeiten und -methoden entwickelt, getestet und präsentiert. Im Automotive Showroom soll die 5G-Technik unter realen Bedingungen getestet und Lösungsansätze für zukünftige Anwendungen im industriellen Umfeld erarbeitet werden. In Deutschland hat die Bundesnetzagentur insgesamt 100MHz Bandbreite im Frequenzbereich für die lokale Nutzung in Industrieumgebungen reserviert. Das gibt Unternehmen in Deutschland die Möglichkeit, Spektrum für einen jährlichen Beitrag zu mieten und innerhalb ihrer eigenen Betriebsstätten exklusiv in einem privaten 5G-Netzwerk zu nutzen. Auf dieser Basis wird im Showroom die neue Mobilfunkgeneration auch im Zusammenspiel mit Industrieprotokollen wie OPC UA oder Profinet evaluiert und getestet. ■



Bild: Siemens AG



Internetplattform für IO-Link-Beschreibungsdateien

Unter einem Dach



► Der IODDfinder steht Nutzern des Web-Frontend kostenfrei zur Verfügung.

Mit mehr als 400.000 Downloads allein im November 2019 und über 12.000 Geräten hat sich der IODDfinder als die Internetplattform für IO-Link-Beschreibungsdateien in nur drei Jahren zu einer festen Größe im Markt etabliert. Sie beherbergt mittlerweile mehr als 7.500 Beschreibungsdateien von rund 80 Herstellern und ist damit die weltweit größte Sammlung an IODDs.

Betrieben wird die Datenbank von den Mitgliedern der IO-Link Community. Jedes Mitglied bekommt bei Eintritt in die Gemeinschaft die Möglichkeit, ein Herstellerkonto im IODDfinder einzurichten, um die Beschreibungsdateien zu seinen Geräten dort hochladen zu können. Die Plattform verfügt über ein Web-Frontend, über das IODDs zu einzelnen Geräten von Menschen gesucht und gefunden werden können. Der eigentliche Mehrwert aber entsteht durch die Programmschnittstellen (APIs), mit deren Hilfe die Gerätehersteller auch eine Vielzahl an IODDs automatisiert hochladen, updaten und verwalten können. Diese Schnittstellen gewährleisten, dass die zentrale Datenbank vollständig und ihr Inhalt stets aktuell ist. Auch das Herunterladen von Beschreibungsdateien kann über die APIs automatisch vollzogen werden. So können z.B. Softwaretools zur Geräteparametrierung oder zur Integration in Automatisierungssysteme über das Internet auf die Datenbank zugreifen. Mittlerweile erfolgt bereits der größte Teil der Downloads

über solche Tools. Jedes IO-Link-Gerät verfügt über eine individuelle Geräte- und eine spezifische Herstellerkennung. Diese beiden Identifikationsnummern (IDs) können die Softwaretools unmittelbar nach dem Verbinden mit einem IO-Link-Geräte auslesen und - sofern sie online sind - ganz automatisch die passende Beschreibungsdatei aus dem Internet herunterladen. Damit wird das Softwaretool in die Lage versetzt, sofort nach dem Download mit dem angeschlossenen IO-Link-Gerät kommunizieren zu können. ■



*Vom (intelligenten) Sensor bis in die Cloud*

Daten-Pipeline

Hohe Datenbreite, kurze Zykluszeiten, verbesserte Integration intelligenter Sensoren und Aktuatoren mit IO-Link sowie Cloud-Konnektivität per OPC UA – ASI-5 bringt frischen Wind in die industrielle Automatisierung.

Bei ASI im Allgemeinen und bei ASI-5 im Speziellen denken viele vielleicht nur an ein gelbes, zweiadriges Profilkabel, an den Geräteanschluss in Durchdringungstechnik oder an Hutschienenmodule im Schaltschrank. Doch der neue Feldbusstandard kann mehr: Eine hohe Datenbreite und kurze Übertragungszeiten machen ASI-5 zu einer Daten-Pipeline, die der Automatisierungstechnik neue Möglichkeiten im Rahmen der Digitalisierung eröffnen kann. Dabei wird Bewährtes nicht über Bord geworfen – vielmehr kommunizieren ASI-5 und ASI-3 im gleichen Netzwerk, so dass Anwender bisherige ASI-3 Lösungen um ASI-5 Module und deren Funktionalitäten erweitern können. Die Vorteile des AS-Interface – etwa der im Vergleich zu anderen Feldbuslösungen deutlich reduzierte Verdrahtungsaufwand, die freie Wahl der Topologie sowie die kostengünstige Integration von Safety auf derselben Infrastruktur – bleiben auch bei ASI-5 erhalten.

Konnektivität für Datenstreaming

ASI-5 könnte zu einem wichtigen Schrittmacher für die digitale Transformation im Maschinen- und Anlagenbau werden. So wird der bisher vergleichsweise eher träge Datenkanal mit ASI-5 zur leistungsfähigen Daten-Pipeline und ermöglicht ein ‚ruckelfreies‘ Datenstreaming. Die Daten-Power von ASI-5 ist darauf ausgelegt, komplexe Steuerungsprozesse in industriellen Anwendungen zu ermöglichen. So können zum einen deutlich mehr Signale kosteneffizient und schnell an einem Ort eingesammelt und angeschlossen werden, denn mit ASI-5 lassen sich jetzt bis zu 384 Ein- und 384 Ausgangsbits in 1,27ms Zykluszeit übertragen. Im Gegensatz zu ASI-3, das mit 167kHz kommuniziert, nutzt die neue AS-Interface Generation dafür den Frequenzbereich zwischen 1 und 10MHz. ASI-5 Netzwerke und ASI-3 Applikationen können so parallel auf einer Leitung betrieben werden, wodurch die von Anfang an angestrebte Abwärtskompatibilität zu allen bisherigen ASI Generationen sichergestellt ist. Zum anderen ist es mit ASI-5 jetzt möglich, intelligente Geräte – beispielsweise IO-Link-Sensoren – noch einfacher in AS-Interface zu integrieren. Genau dafür haben die Entwickler von ASI-5 nämlich schon frühzeitig Profile spezifiziert, die es erlauben, bis zu 32Byte I/O-Daten zyklisch zu übertragen. Praktisch umsetzen lässt

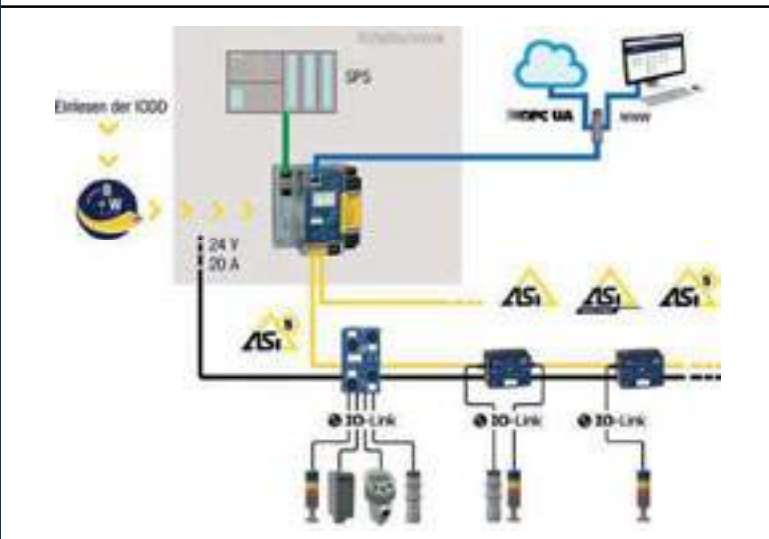
sich das auch schon, beispielsweise mit den ASI-5 Slave / IO-Link Master Modulen von Bihl+Wiedemann. Dies ist der eine Aspekt der verbesserten Konnektivität mit ASI-5 – der andere heißt OPC UA. Diese plattformunabhängige, standardisierte Kommunikationsarchitektur ist in der Lage, Maschinendaten wie Sensordaten, Messwerte oder Regelgrößen zu transportieren und – das ist die für die Digitalisierung relevante Innovation – auch maschinenlesbar semantisch zu beschreiben. OPC UA ist interoperabel und sorgt für industrielle Konnektivität: Größere Mengen an Daten können ohne Einschränkung dorthin transportiert werden, wo aus ihnen wertvolle Informationen gewonnen werden – beispielsweise in Cloud-basierte Applikation des Condition Monitoring oder der Predictive Maintenance. Mit dem OPC-UA-Server, den die Firma Bihl+Wiedemann standardmäßig in ihre neuen ASI-5/ASI-3 Gateways für Profinet, Ethernet/IP oder Ethercat integriert hat, ist somit auch Datenstreaming im Sinne von Edge Computing ohne Umwege parallel zum jeweiligen Feldbus möglich.

Bewährtes Look&Feel

Über 200.000 Arbeitsstunden hat eine Entwicklungsgruppe aus namhaften AS-Interface-Herstellern in das Gemeinschaftsprojekt ASI-5 gesteckt. Von der technologischen Komplexität von ASI-5 bemerkt der Nutzer allerdings nichts – weder bei der Bedienung der neuen Gateways und Digitalmodule noch bei der Nutzung der Software. Was die Projektierung anbelangt, lässt sich ASI-5 grundsätzlich auch ohne Software projektieren – komfortabler, sicherer und schneller erfolgt das Planen, Konfigurieren und Parametrieren von ASI-Netzwerken mit oder ohne Safety allerdings mit Software-Suites: Wer z.B. die



► Einsatzfähige Produkte wie die ASI-5 Slave / IO-Link Master Module von Bihl+Wiedemann sind bereits erhältlich.



► Neue ASI-5 Komponenten können nicht nur in reinen ASI-5 Netzen genutzt, sondern auch in bestehende ASI Applikationen integriert werden.

Safety-Software Asimon360 oder die ASI Control Tools360 für Standardapplikationen schon für ASI-3 einsetzt, kann sie durch ein kostenloses Update fit für ASI-5 Anwendungen machen und dann den Hardware-Katalog mit Produkten von Bihl+Wiede-

mann wie gewohnt nutzen, um das gewünschte Gerät für die Konfiguration auszuwählen. Eine neue Funktionalität ist die On-line Businformation: Mit ihr lassen sich Slaves einfach adressieren sowie Ein- und Ausgänge live parametrieren und überwachen. Das Instrument, das sich auch für eine schnelle Diagnose bei der Inbetriebnahme von Anlagen eignet, zeigt beispielsweise noch nicht projektierte Slaves durch einfache Symbole auf einen Blick für jeden verständlich an. Die Hinweise zur Behebung von Fehlern sind dabei eindeutig und bieten dem Nutzer Hilfestellungen für die nächsten Schritte. Alle Slaves können in der Online Businformation einzeln ausgewählt und angesprochen werden – etwa, um Eingänge zu diagnostizieren, Ausgänge zu setzen oder Parameter zu ändern. Der Anwender erkennt damit unmittelbar, welche konkreten Auswirkungen die aktualisierten Einstellungen haben, und kann die Konfiguration gegebenenfalls sofort anpassen. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/?f1323



Thomas Rönitzsch,
Unternehmenskommunikation,
Bihl+Wiedemann GmbH
www.bihl-wiedemann.de

- Anzeige -

IBH softec

Das Embedded OPC UA Server/Client Gateway

IBH Link UA

- OPC UA Server/Client für die Anbindung an MES-, ERP- und SAP-Systeme, Visualisierungen und Modbus
- SIMATIC® S7-Steuerungen über S7 TCP/IP oder IBH Link S7++ ansprechbar
- SIMATIC® S5-Steuerungen über IBH Link S5++ ansprechbar
- SINUMERIK® 840D/840D SL Anbindung
- S7-kompatible SoftSPS zur Datenvorverarbeitung integriert
- Mitsubishi Electric Roboter- und Steuerungsanbindung
- Rockwell Automation Steuerungsanbindung
- Firewall für eine saubere Trennung der Prozess- und Leitebene
- Skalierbare Sicherheitsstufen
- Komfortable Konfiguration mit dem kostenlosen IBH OPC UA Editor, Siemens STEP7, dem TIA Portal oder per Webbrowser
- Historische Daten
- Alarms & Conditions
- Eigene Informationsmodelle
- MQTT-Anbindung



Per Gateway in die Cloud

Lichtleiter-Sensorik

Drastisch reduzierter Verdrahtungsaufwand, bedienfreundliche Remote-Parametrierung und Datenabfrage über die Steuerung sowie funktionale Mehrwerte für Industrie-4.0-Szenarien – mit den Gateways WI180C für die IO-Link- und Feldbusintegration will diese Vorteile jetzt auch für Lichtleiter-Sensoren und Displacement-Messsensoren erschließen. Die Gateway-Variante für IO-Link erlaubt zudem durch die dezentrale Ausführung von Smart-Task-Funktionen ein effizientes Edge-Computing und Kommunikation bis in die Cloud.



► Die Gateways ermöglichen es, eine Reihe von Sensoren über eine einzige Leitung direkt in die IO-Link- oder in die Feldbuswelt zu integrieren.

Detektions- und Messaufgaben durch Sensoren mit Lichtleiter-Optik oder separatem Optikkopf umgesetzt werden. Die Verstärker- und Auswerteeinheiten werden dabei an abgesetzter Stelle montiert – und bislang häufig einzeln verdrahtet. Die neuen WI180C Gateways ermöglichen es, Lichtleitersensoren WLL180T, Kontrastsensoren KTL180 und messende Displacementsensoren wie die OL1 und verschiedene OD-Produktfamilien von Sick über eine einzige Leitung direkt in die IO-Link- oder die Feldbuswelt zu integrieren. Die Möglichkeit, die Objekte detektierenden, Kontraste erfassenden oder Abstände messenden Sensoren auch im gemischten Betrieb anzuschließen, bietet zusätzliche konstruktive und applikatorische Flexibilität.

Sensoranschluss über Rückwandbus-Stecker

Die Gateways übernehmen die bewährte Stecker-Buchse-Anschluss-technik der einzelnen Sensorbau-reihen. Bis zu 16 Sensoren können auf einer Hut-schiene per Rückwandbus aneinander gesteckt und durch das gleiche Prinzip mit dem Kommunikationsmodul verbunden werden. Das Gateway sammelt alle Sensordaten ein und überträgt diese Daten über ein einziges Kabel entweder an einen IO-Link-Master, z.B. das Sensor Integration Gateway SIG200, oder über ein Feldbusmodul für Profibus, Profinet, Ethercat oder Ethernet/IP weiter an die Maschinensteuerung. Die Sensoren im Busverbund können ihrerseits im Betrieb einzeln mit der IO-Link- oder Feldbuswelt kommunizieren – also Prozess- und Servicedaten übertragen oder Parametrierungsdaten empfangen. Gleichzeitig werden sie dabei mit Energie versorgt. Unter dem Strich minimiert der Anwender durch den Einsatz der Gateways seinen Ma-terial- und Verdrahtungsaufwand – so dass sich deren Einsatz bereits bei wenigen angeschlossenen Sensoren als wirtschaftlich vorteilhaft darstellen kann. Entsprechendes gilt auch im Vergleich mit Lichtleiter-Sensoren mit integrierter IO-Link-Anbindung, die lediglich stand alone eingesetzt werden können und einzeln verdrahtet werden müssen. Hinzu kommen weitere Vorteile.

Sensoren, bei denen Optik und Verstärker getrennt sind, kommen immer dann zum Einsatz, wenn Detektions- oder Messfunktionen nahe am Objekt umgesetzt werden müssen, dort aber kein Platz für die Montage integrierter Standardsensoren vorhanden ist. Häufig geht es in solchen Maschinen generell eng zu, so dass gleich eine Vielzahl von

Material- und Verdrahtungsaufwand – so dass sich deren Einsatz bereits bei wenigen angeschlossenen Sensoren als wirtschaftlich vorteilhaft darstellen kann. Entsprechendes gilt auch im Vergleich mit Lichtleiter-Sensoren mit integrierter IO-Link-Anbindung, die lediglich stand alone eingesetzt werden können und einzeln verdrahtet werden müssen. Hinzu kommen weitere Vorteile.

Individuelle Parametrierung und vereinfachte Bedienung

So können die Lichtleiter-, Kontrast- und Displacementsensoren mit abgesetztem Verstärker von Sick über Bedienelemente am Gerät intuitiv bedient werden. Bei den Lichtleitersensoren und den Kontrasttastern kann die Anzeige im 7-Segment-Display je nach Einbaulage elektronisch um 180° gedreht werden – der Sensor kann also immer richtig herum abgelesen werden. Ist eine direkte Bedienung der einzelnen Verstärker z.B. aufgrund der Einbaulage nicht möglich oder zu umständlich, können die einzelnen Sensoren auch zentral über das Gateway ferngesteuert werden – entweder direkt per IO-Link bzw. per entsprechendem Bus aus der Steuerung heraus oder bei Einsatz des neuen IO-Link Gateways über das Engineering-Tool Sopas. Alle Einstellungen wie beispielsweise Empfindlichkeit oder Schaltschwelle können als Klartext vorgegeben und bei Bedarf für jeden einzelnen Sensor optimiert werden – auch im laufenden Betrieb. So lassen sich beispielsweise bei einem Wechsel von Verpackungsmaterialien oder zu detektierenden Elektronikbauteilen die Sensoreinstellungen bequem und sicher über die Steuerung an die verschiedenen Erfordernisse anpassen. Damit integrieren sich diese Sensoren mit abgesetztem Verstärker jetzt ebenfalls in automatisierungstechnische Bedienkonzepte üblicher Standardsensoren mit IO-Link oder Feldbusanbindung.



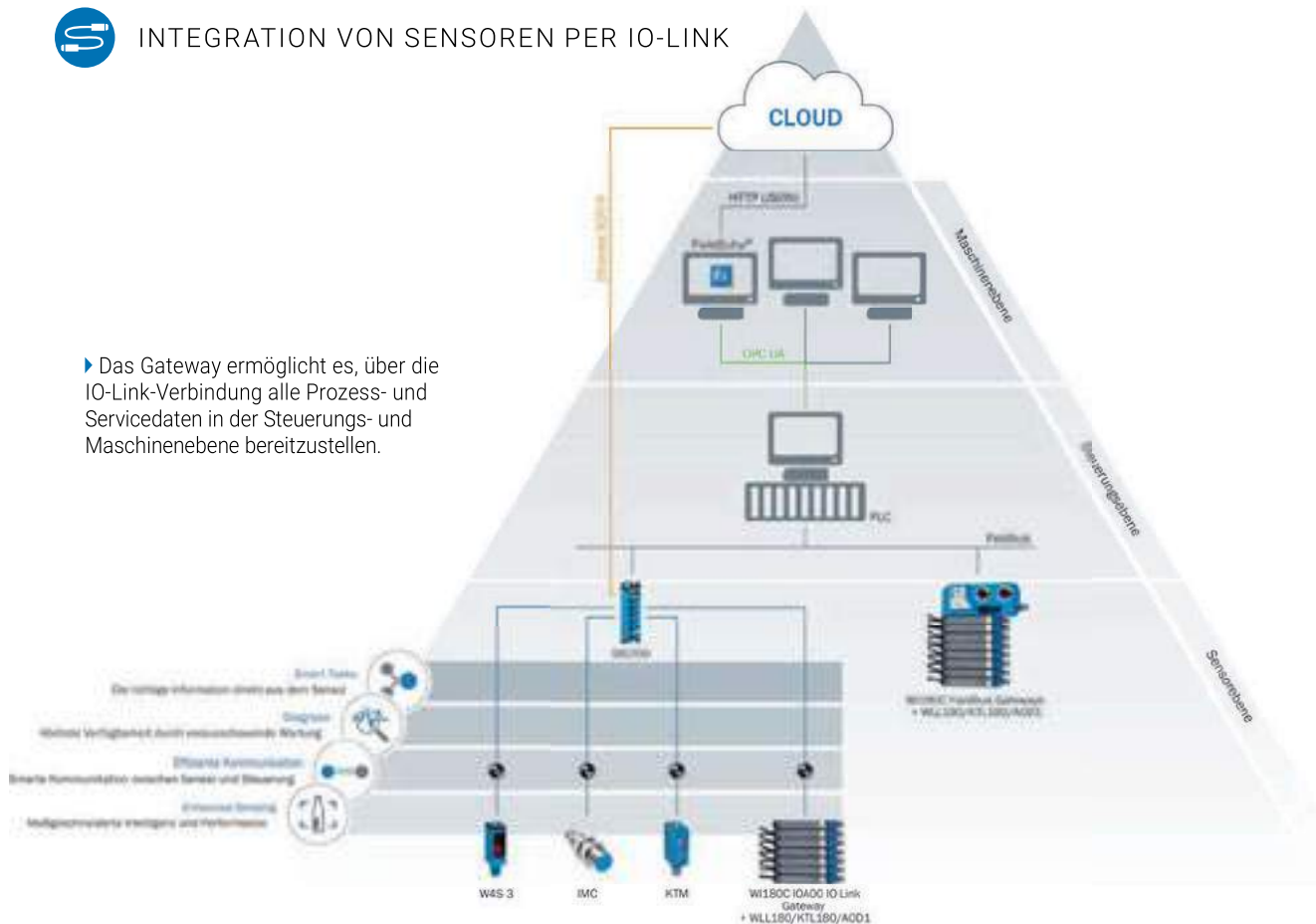
► Bei den Gateways können bis zu 16 Lichtleiter-, Kontrast- und Displacementensoren per Rückwandbus aneinander gesteckt werden.

- Anzeige -

Einfach vom Sensor bis zur Cloud Mit intelligenten Industrial-IoT-Lösungen

Um mit der globalen Digitalisierung mithalten zu können, sind smarte Lösungen gefragt, die bestehende und neue Systeme im Industrial IoT vernetzen und Informationen digitalisieren. In den gewonnenen Daten liegt der Schlüssel zu mehr Produktivität Ihrer Fertigung. Dafür ist eine nahtlose Übertragung vom Sensor bis zur Cloud essenziell. Diese durchgängige Erfassung, Verarbeitung, Kommunikation und Analyse Ihrer Daten ermöglichen unsere IoT-fähigen Produkte und Lösungen. Entdecken Sie, wie smarte Sensoren und Steckverbinder, innovative Komponenten für die gesamte Industrial-Ethernet-Infrastruktur sowie unsere intelligenten Automatisierungs- und Machine-Learning-Lösungen den Mehrwert aus Ihren Daten generieren.

www.weidmueller.de/IIOT



Gateways generieren funktionale Mehrwerte

Die Datenübertragung über die Gateways kann die Maschinenfunktionalität im Kontext von Industrie 4.0 entscheidend erhöhen. So können alle Prozess- und Servicedaten über die IO-Link-Verbindung in der Steuerungs- und Maschinenebene bereitgestellt werden. Bei der Datenübertragung via IO-Link-Gateway und IO-Link-Master ist dies sogar auf direktem Weg bis in die Cloud möglich. Im Fall der Feldbus-Gateways kann die Kommunikation bis in die Cloud über steuerungs-basierte Lösungen umgesetzt werden. Die verbundenen Sensoren liefern individuelle Diagnoseinformationen, die eine Beurteilung der Prozessqualität und des Maschinenstatus ermöglichen. Sendeleistung, Signalstärke, Empfindlichkeit, Schaltschwelle, Kontrastinformationen, Verschmutzungsgrad der Optik – diese und weitere Zustandsinformationen können in regelmäßigen Abständen von der Steuerung oder einer Cloudapplikation abgefragt oder vom Sensor beim Erreichen vorgegebener Grenzwerte selbstständig gemeldet werden. Die Gateways eröffnen jetzt auch beim Einsatz von Sensoren mit abgesetztem Verstärker die Möglichkeit, mit deren Informationen die Performance der Maschine im Betrieb dynamisch und in Echtzeit zu erhöhen und zugleich mögliche Störungen und Ausfallursachen frühzeitig zu erkennen.

IO-Link-Gateway ermöglicht smarte Sensorlösungen

Nicht alleine, dass diese Sensoren dank der neuen Kommunikationsmodule jetzt 'mehr zu sagen haben' als nur Detektionssignale oder Messwerte – das IO-Link-Gateway ermöglicht es zugleich, smarte Sensorlösungen umzusetzen. Denn während auf der einen Seite prozess- und maschinenrelevante Informationen direkt in einen Ethernet-Feldbus oder in die Cloud weitergeleitet werden, wächst auf der anderen Seite der Bedarf, möglichst viele Automa-

tisierungsentscheidungen vor Ort zu fällen. Die Dezentralisierung von ursprünglich in der Steuerungsebene beheimateten Funktionen, das heißt ihre Verlagerung vom Automatisierungssystem in die Feldgeräte, erweist sich immer häufiger als der richtige Ansatz, um Automatisierungsnetzwerke effizienter und performanter zu gestalten. Dieses Edge Computing erfordert dezentrale Rechenleistung und Intelligenz – die das IO-Link-Gateway in Form von integrierten oder optional verfügbaren Smart Tasks bereitstellen kann. Die jeweiligen Auswertungen finden dann vor Ort im IO-Link-Gateway statt – weder die Steuerung noch das Netzwerk werden mit möglicherweise umfangreichen und zeitkritischen Signalen belastet, deren Auswertung prozesskritisch sein könnte.

Mehrwerte für digitalisierte Applikationen

Mit Hilfe des neuen IO-Link-Gateways werden Sensoren zu Smart Sensors. Das Feldbus-Gateway der Serie ermöglicht ihre direkte Integration in die führenden Ethernet-Umgebungen. Beide Gateways sind rückwärtskompatibel und nachrüstbar. Während es für die Sensoren selbst in der Regel eng zugeht in der Maschine, sind die Gateways zugleich für ein weites Anwendungsspektrum geeignet. Die Detektion kleiner Objekte wie beispielsweise Widerständen oder Kondensatoren bei der Handhabung und Montage in der Elektronik- und Solarindustrie gehört ebenso dazu wie die Bahnkantendetektion oder die Detektion transparenter Materialien in Verpackungsprozessen oder die Objektdetektion oder der Aufbau von individuellen Lichtgitter-Lösungen mit Lichtleitersensoren in der Intralogistik. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/20447



Kai Huber,
 Produktmanager Miniature & Fiber Sensors,
 Global Business Unit Presence Detection,
 SICK AG
www.sick.de

Sensor-Produktion in der Smart Factory

Schlaue Sensoren



► Die NT-Fertigung in Tettang zeigt die Potenziale einer Smart Factory.

Die Produkte und Sensoren von IFM werden häufig in Industrie-4.0-Anwendungen eingesetzt. Wie sich Industrie 4.0 umsetzen lässt, demonstriert das Unternehmen in seiner eigenen NT-Fertigung in Tettang. Von der Produktentwicklung über die Montage bis hin zu Verpackung und Logistik werden in dem Werk alle Prozesse gesteuert.

Die Fabrik von Morgen steht bei IFM vor großen Herausforderungen: Sie muss die Produkte unabhängig von deren Komplexität garantiert in der richtigen Qualität, zum richtigen Zeitpunkt und zu den geplanten Kosten nachhaltig herstellen. Basis hierfür ist eine Lean-Struktur, in der die einzelnen Produktionslinien als intelligente Netzwerke fungieren. In einer Produktionslinie können rund 120 Varianten eines Sensors gefertigt werden, wobei die typischen Losgrößen 100 bis 200 Stück betragen. Die schlanke Produktion beginnt aber bereits wesentlich früher – während der Produktentwicklung. Dort arbeitet ein Projektteam, in dem auch Mitarbeiter aus der Produktionsplanung vertreten sind, zusammen, um ein so genanntes Design for Manufacturing zu realisieren. Dabei wird das Poka-Yoke-Prinzip angewendet, um eine fehlerfreie Montage in der Fertigung

sicherzustellen. Außerdem berücksichtigt das Team den möglichen Automatisierungsgrad, Materialfluss-Aspekte und kurze Durchlaufzeiten.

Cloud als Basis

Das Fundament der Produktion ist die IFM Automation Cloud, die u.a. Tracking-Systeme und das so genannte Digital-Production-Order-System beinhaltet. Ziel ist es, die Produktionslinien im Sinne der Overall Equipment Efficiency zu verbessern. So werden etwa die Auftragsinformationen in Echtzeit durch das Produktionsplanungs-System zur Verfügung gestellt, um Reaktionszeiten zu reduzieren. Situationen, bei denen eine Produktionslinie auf den nächsten Auftrag warten muss, werden so ausgeschlossen. Auch im Bereich Intralogistik neue Wege beschritten. So übernehmen Roboter nicht wertschöpfende Transportaufgaben innerhalb der Fertigung. In einem gemeinsamen Pro-

jekt mit dem Robotik-Hersteller MIR werden automatisierte Logistik-Roboter entwickelt, die weitgehend selbstständig arbeiten. Sie sollen in der Lage sein eigene Kommissionieraufgaben zu übernehmen und die Produktionslinien selbstständig zu versorgen. Die Kommunikation mit dem ERP-System ist durch eine SAP-Schnittstelle sichergestellt. Bei der Verpackung der gefertigten Produkte arbeitet das Unternehmen ebenfalls an Verbesserungen. Ein Pick-Control-System, das die Entnahme der einzelnen Komponenten mit 2D- oder 3D-Kameras überwacht, soll den manuellen Prozess absichern und so den Mitarbeiter unterstützen. Die Entwicklungen in Richtung 'Fabrik der Zukunft' sind in Tettang noch nicht abgeschlossen. Die intelligente Vernetzung von Produktentwicklung, Produktion und Logistik wird auch in Zukunft einen hohen Stellenwert einnehmen. Die Digitalisierung der Fertigung ist dabei der nächste logische Schritt, um die Wettbewerbsfähigkeit zu sichern. ■

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



IFM Electronic GmbH
www.ifm.com



► Mit TwinCAT Cloud Engineering lassen sich global verteilte Steuerungssysteme aus der Ferne bedienen und warten.



Cloud Engineering als Grundlage effizienter IoT-Automatisierungskonzepte

Smart Engineering

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 des Prozesses steht TwinCAT Cloud Engineering, das eine Instanziierung und Verwendung der existierenden TwinCAT-Engineering- und -Runtime-Produkte direkt in der Cloud ermöglicht. Der Zugriff erfolgt einfach über die Beckhoff-Webseite, das heißt außer einem Webbrowser sind keine zusätzlichen Softwarekomponenten erforderlich. Registrierte Anwender können auf diese Weise sogar über bisher nicht geeignete Plattformen, wie z.B. Tablet-PCs, mit der TwinCAT-Entwicklungsumgebung arbeiten. Die Ankopplung realer Steuerungshardware an die erzeugten Cloud-Engineering-Instanzen erfolgt über einen sicheren Transportkanal. Dabei profitieren Anwender uneingeschränkt von dezentralen Kollaborationsmöglichkeiten über ein Source Control Repository. Weiterhin bietet die Engineering-Instanz insbesondere für Einsteiger eine umfassende und ideale Grundlage, um die ersten Schritte in der TwinCAT-Umgebung zu vollziehen.

Architektur in der Cloud

Mit TwinCAT Cloud Engineering besteht nun die zusätzliche Möglichkeit, die TwinCAT-Architektur komplett in die Cloud zu transferieren. Einziger Unterschied gegenüber der konventionellen Vorgehensweise ist 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. Die Installation und Vorhaltung unterschiedli-

cher, auf die individuelle Maschinengeneration zugeschnittener Softwareversionen auf dem eigenen PC entfällt. Stattdessen können verschiedene TwinCAT-Cloud-Engineering-Instanzen mit verschiedenen Versionsständen verwendet werden; der Zugriff erfolgt aus der Ferne und nach Bedarf. Als Projektablage dient ein Source Code Control Repository, auf das direkt aus dem TwinCAT Engineering heraus zugegriffen werden kann.

Teamarbeit per Source Control

Über moderne Source-Control-Funktionalitäten können Git-basierte Systeme problemlos angebunden und zur Verwaltung des Automatisierungsprojekts verwendet werden. Die Multi-User-Funktion von TwinCAT ermöglicht hierbei den einfachen und nahtlosen Zugriff auf das Source Control Repository ohne tiefgehendes Fachwissen des Anwenders. Bei TwinCAT Cloud Engineering kann hierzu sowohl ein in die Instanz integrierter Git-Server als auch ein separater, Git-basierter Cloud-Dienst verwendet werden, um die kollaborative Arbeit an mehreren Instanzen mit mehreren Benutzern zu erleichtern. ■

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



Sven Goldstein,
Produktmanager TwinCAT Connectivity & IoT,
Beckhoff Automation GmbH & Co. KG
www.beckhoff.de



Serielle Adapter für Ethernet

Noch sind zahlreiche Geräte in der Automatisierungstechnik mit einer Schnittstelle vom Typ RS232/422/485 ausgestattet. Mit seriellen Ethernet-Adaptoren können diese Geräte an ein Ethernet-Netzwerk angeschlossen werden, indem serielle Eingaben in TCP/IP-Daten umgewandelt werden und umgekehrt.

In der industriellen Produktion ist die Kommunikation auch zwischen nicht kompatiblen Standards unabdingbar. Auch Protokolle unterschiedlicher Hersteller von z.B. Antrieben, Sensoren, Bedienterminals, Barcode- oder RFID-Leser müssen miteinander verbunden werden. Um dies zu gewährleisten bedarf es moderner und flexibler Gateways, Adapter und Konverter. In unserer Marktübersicht zeigen wir eine Vielzahl von Möglichkeiten, die Vernetzung verschiedener Kommunikationsprotokolle zu realisieren. (bfi) ■

Direkt zur Marktübersicht auf
i-need.de
PRODUCT FINDER
www.i-need.de/94



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



Anbieter	B&R Industrie-Elektronik GmbH	Beckhoff Automation GmbH & Co. KG	Beckhoff Automation GmbH & Co. KG	Bihl+Wiedemann GmbH	Bressner Technology GmbH
Produkt-ID	16083	11264	11266	11293	11241
Ort	Bad Homburg	Verl	Verl	Mannheim	Gröbenzell
Telefon	06172/ 4019-0	05246/ 963-0	05246/ 963-0	0621/ 33996-0	08142/ 47284-0
Internet	www.br-automation.com	www.beckhoff.de	www.beckhoff.de	www.bihl-wiedemann.de	www.bressner.de
Produktname	X20CS1020/X20CS1030	EL6021 Serielle Schnittstelle RS422/RS485	KL6021 Serielle Schnittstelle RS422/RS485	AS-i 3.0 RS 232-Master in Edelstahl	Sena LS100 HelloDevice Lite
Serielle Schnittstelle RS232	1			1	1
Serielle Schnittstelle RS422	1	1	1		
Serielle Schnittstelle RS485	1	1	1		
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar	-, ✓				
Maße (BxHxT, in mm)	12,5 x 99 x 85	12 x 100 x 68	12 x 100 x 68	120 x 75 x 83	72 x 25 x 100
Montageart	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	DIN-Rail mount kit, Wandmontage
Anschluss	Klemme	Federklemmtechnik	Federklemmtechnik	9-pol. D-SUB Buchse, Stecker	9-pol. D-SUB Buchse, Stecker
Verwendete Ethernetprotokolle	Powerlink, Ethercat, Ethernet/IP, Modbus-TCP, Profinet	Ethercat	Ethernet, ADS, Ethercat, Modbus TCP, Profinet, Ethernet IP		TCP/IP, UDP/IP, Telnet
Unterstützte Industrial-Ethernet-Kommunikationsprotokolle	OPC-UA	Ethercat	Ethernet, ADS, Ethercat, Modbus TCP, Profinet, Ethernet IP		
Feldbus-Anbindung	Konfigurations-Software	Profibus	Lightbus, CANopen, Devicenet, Profibus-DP, Interbus, Modbus	ASI	
Konfiguration der seriellen Adapter	Automation Studio	über COE	Registerkommunikation	Konfigurations-Software	Serielle Konsole, Konfigurations-Software, Telnet
Programmierbarkeit bzw. Skripterstellung	Automation Studio	über COE	Registerkommunikation	✓	
Statusanzeige, Diagnoseinformationen am seriellen Adapter	System Diagnostics Manager	LED	LED	Power, COM	Power, LAN, COM



					
Anbieter	Bressner Technology GmbH	od Electronic	Deutschmann Automation GmbH & Co. KG	E.E.P.D. GmbH	esd Electronics GmbH
Produkt-ID	11252	11260	11286	34264	30211
Ort	Gröbenzell	Michelstadt	Bad Camberg	Weichs	Hannover
Telefon	08142/ 47284-0	06061/ 73353	06434/ 9433-0	08136/ 2282-0	0511/ 37298-0
Internet	www.bressner.de	www.cdelectronic.de	www.deutschmann.de	www.eepd.de	www.esd.eu
Produktname	Digi Connect ES Serie 4/8/16 ports	S7-LAN-Modul 9352-Lancon	Unigate CL-Ethercat	EM USB Modul RS485	CAN-CBX-COM2
Serielle Schnittstelle RS232	4, 8, 16		on board		✓
Serielle Schnittstelle RS422			on board		optional
Serielle Schnittstelle RS485		1	on board	1x 9-pol. D-SUB (male) (optional: Full Duplex)	optional
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar	1		RS232, 485 und 422 on Board		
Maße (BxHxT, in mm)	23,5 x 26,9 x 4,2	65 x 48 x 17	23 x 100 x 115	93 x 38,5 x 26,6	22,5 x 99 x 114,5
Montageart	Wandmontage	direkte Montage auf der Simatic S7	Hutschienenmontage	Hutschienenmontage, Standgerät	Hutschienenmontage
Anschluss	RJ45	9pol. D-SUB Stecker, Huckepack Diagnosebuch.	Schraubsteckverbinder	9-pol. D-SUB Buchse, Stecker	
Verwendete Ethernetprotokolle	TCP/IP, Telnet, UDP/IP, ARP	TCP/IP, UDP/IP, RFC 1006			
Unterstützte Industrial-Ethernet-Kommunikationsprotokolle			Ethercat		
Feldbus-Anbindung		Profibus-DP, MPI, PPI			CANopen
Konfiguration der seriellen Adapter	Konfigurations-Software, Internet-Browser (Web-based-Management), Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfigurations-Software	Konfigurations-Softw. o. alternativ ü. Scriptsprache dadurch sind die Module frei programmierbar.		
Programmierbarkeit bzw. Skripterstellung			Scriptspr. mit mächtigen Befehlen z.B. Mathematische, Speicherbearbeitungsbefehle, Ablauf		
Statusanzeige, Diagnoseinformationen am seriellen Adapter	Power, LAN, COM	Power, LAN, COM	sowohl für die serielle Seite als auch für die Busseite (busspezifisch)		Power, COM

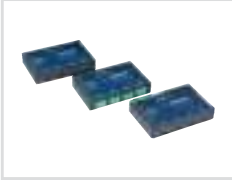
					
Anbieter	Meilhaus Electronic GmbH	MEV Elektronik Service GmbH	Microsens GmbH & Co. KG	Panasonic Electric Works Europe AG	Plug-In Electronic GmbH
Produkt-ID	11223	17016	22811	11232	22799
Ort	Ailing	Hiltter	Hamm	Ottobrunn	Ailing
Telefon	08141/ 5271-0	05424/ 2340-57	02381/ 9452-0	089/ 45354-1000	08141/ 3697-0
Internet	www.meilhaus.de	www.mev-elektronik.de	www.microsens.de	www.panasonic-electric-works.de	www.plugin24.com
Produktname	NetCOM-PLUS Serie und andere	Tibbo DS1100	Ind.-Medienkonv. RS232/Glasfaser MS650142	KS1 Signal Converter	ES-551
Serielle Schnittstelle RS232	1, 2, 4, 8	1	1	1	
Serielle Schnittstelle RS422	1, 2, 4, 8	-			
Serielle Schnittstelle RS485	1, 2, 4, 8	-		1	
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar	1, 2, 4, 8	-			1
Maße (BxHxT, in mm)	je nach Modell	90 x 48 x 25	38 x 116 x 108	25 x 90 x 60	114,5 x 22,6 x 99
Montageart	Wandmontage, DIN-Hutschiene	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage
Anschluss	9-pol. Sub-D, 9-pol. D-SUB Buchse, Stecker	9-pol. D-SUB Buchse, Stecker	9-pol. D-SUB Buchse, Stecker	Schraubsteckverbinder	Schraubsteckverbinder, RJ45
Verwendete Ethernetprotokolle	TCP/IP, Telnet, HTTP, ARP, ICMP, TCP/IP	TCP/IP, UDP/IP, HTTP		TCP/IP	TCP/IP
Unterstützte Industrial-Ethernet-Kommunikationsprotokolle	Ethernet/IP, Modbus-TCP				
Feldbus-Anbindung	CAN-Bus				
Konfiguration der seriellen Adapter	Internet-Browser (Webbased-Management), Konfigurations-Software, Serielle Konsole, Telnet	Serielle Konsole		Konfigurations-Software	Internet-Browser (Webbased-Management)
Programmierbarkeit bzw. Skripterstellung		Tibbo Basic			
Statusanzeige, Diagnoseinformationen am seriellen Adapter	Power, WIFI, RDY	LAN, COM, Power		Power, LAN, COM	Power, LAN, COM



HMS Industrial Networks GmbH 11215 Karlsruhe 0721/ 989777-000 www.hms-networks.de	ICPDAS-Europe GmbH 30950 Reutlingen 07121/ 14324-0 www.icpdas-europe.com	Insta GmbH 11305 Lüdenscheid 02351/ 936-0 www.insta.de	IPC2U GmbH 23282 Langenhagen 0511/ 807-259-0 ipc2u.de	Leine & Linde AB 23763 Hamburg 040/ 3176758-60 www.leinelinde.de	Lenze SE 11301 Aerzen 05154/ 82-0 www.lenze.com
Anybus Communicator	iDS-700 Serie – Device Server	KNX Gateway RS232/485-IP	Profi-2541-SC	CANopen Gateway für EnDat Drehgeber	I/O-System 1000
1 kombiniert RS232, 422, 485	max. 3	1			1 je Modul
1 kombiniert RS232, 422, 485	max. 1				
1 kombiniert RS232, 422, 485	max. 3	1		EnDat	
1 kombiniert RS232, 422, 485		1			Nein
27 x 120 x 75	52 x 95 x 27	REG 4 TE, (ca. 70mm)	33 x 127 x 105	85 x 132 x 29	60,5 x 76 x 100
Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage, Wandmontage	Hutschienenmontage
D-, 9-pol. D-SUB Buchse, Stecker	RJ45, 9-pol. D-SUB Buchse, Stecker	9-pol. D-SUB Buchse, Stecker		M23 oder M12 Stecker	Federklemmtechnik
TCP/IP	TCP/IP	TCP/IP			Ethercat, Modbus TCP, Profinet
Ethernet/IP, Profinet, Ethercat, Modbus-TCP, CC-Link IE Field	Modbus-TCP				Ethercat, Modbus TCP, Profinet
Profibus, Interbus, CANopen, Devicenet, Controlnet, CC-Link, Lonworks	Ethernet	KNX		CANopen	CANopen, Profibus, Devicenet
Konfigurations-Software	Internet-Browser (Webbased-Management), Konfigurations-Software	Konfigurations-Software KNX-Gate2		Konfigurations-Software	über Software
Konfigurationsprogramm		Konfigurations-Software KNX-Gate2			Parametrierung
COM, Power, LAN	Power, LAN, COM	Status-LEDs		Module, Status	LED

Pro-face Deutschland GmbH 11239 Solingen 0212/ 25826-0 www.pro-face.de	Process-Informatik Entwicklungsgesellschaft mbH 23402 Wärschenbeuren 07172/ 92666-0 www.process-informatik.de	Process-Informatik Entwicklungsgesellschaft mbH 23403 Wärschenbeuren 07172/ 92666-0 www.process-informatik.de	Quinx AG 32744 Reinach +41 62/ 76700-40 www.quinx.ch	Rockwell Automation GmbH 11292 Düsseldorf 0211/ 41553-0 www.rockwellautomation.de	Schneider Electric GmbH 11254 Ratingen 01805/ 753575 www.se.com
GP4201TM	S7-LAN - TCP/IP für jede Simatic S7	S5-LAN++ - TCP/IP an jede Simatic S5	Netzwerkadapter DITB-702W	1761-NET-ENI, 1761-NET-ENIW	ETG100, ETG1000, ETG3000
		1x 15-polig (je nach Ausführung)	1	1	
1x RS232, 422, 485			1	Nein	1
98 x 55 x 57	65 x 43 x 17 (wie ein Profibus-Anschlussstecker)	42 x 15 x 65		52 x 118 x 65	
Wandmontage, Hutschienenmontage	dir. Montage auf MPI/Profibus-Schnittst. d. Steu.	dir. Aufstecken auf 15-polige PG-Schnittstelle	Wandmontage	Wandmontage, Hutschienenmontage	Hutschienenmontage
9pol. D-SUB Stecker	9pol. D-Sub Stecker und Buchse	dir. Montage auf 15-polige PG-Schnittst. d. SPS	9pol. D-SUB Buchse, Stecker	Mini-DIN	9pol. D-SUB Buchse, Stecker, RJ45
TCP/IP, UDP/IP	HTTP, RFC 1006, TCP/IP, UDP/IP, ARP, DHCP	TCP/IP, UDP/IP, RFC 1006	TCP/IP, UDP/IP, Telnet, HTTP, ICMP, WPA, WEP, SNMP, AutoIP, DHCP, TFTP	TCP/IP	TCP/IP, HTTP
Modbus-TCP, S7-Ethernet, MM-ASCII, Omron, Mitsubishi, usw. weit. Ethernet Treiber verfügbar.	RFC1006, S7-TCP/IP kompatibel zu CP343-1	RFC 1006, TCP/IP S5 (wie CP143-TCP), TCP/IP S7 (wie CP343-1)		EtherNet/IP	Modbus-TCP
	Profibus, MPI	TTY-Schnittstelle, optional RS232			
Über Konfigurationssoftware GP-Pro EX	integrierter Web-Browser oder Konfigurationstool TIC	Konfigurations-Software	Quinx DNC-In-The-Box	Konfigurations-Software	Konfigurations-Software
Speicherbefehle in umfangreicher Scriptsprache verfügbar					
Power, LAN	Betriebszustand, Linkstatus, Kommunikation	Power, LAN, Kommunikation/ Betriebszustand, LAN (Link-/Data-Status)	Power, LAN	Power	



					
Anbieter	Sigmatek GmbH & Co KG	Spectra GmbH & Co. KG	Spectra GmbH & Co. KG	Sphinx Computer Vertriebs GmbH	Sphinx Computer Vertriebs GmbH
Produkt-ID	22847	11233	11278	11255	11256
Ort	Lamprechtshausen	Reutlingen	Reutlingen	Laudenbach	Laudenbach
Telefon	+43 6274/ 4321-0	07121/ 14321-0	07121/ 14321-0	06201/ 75437	06201/ 75437
Internet	www.sigmatek-automation.com	www.spectra.de	www.spectra.de	www.sphinxcomputer.de	www.sphinxcomputer.de
Produktname	ISE 031	I-7188En	I-7530	NPort 5230	NPort 5400 Series
Serielle Schnittstelle RS232	✓	max. 7	1	1	4
Serielle Schnittstelle RS422		1	1	1	4
Serielle Schnittstelle RS485	✓	max. 4	1	1	4
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar	✓	max. 8	1	1	4
Maße (BxHxT, in mm)	12,5 x 103,5 x 72	72 x 123 x 33	72 x 33 x 118	67 x 22 x 100,4	67 x 22 x 100,4
Montageart	Hutschienenmontage	Wandmontage, DIN-Schienenmontage	Wandmontage, DIN-Schienenmontage	Wandmontage, Hutschienenmontage	Wandmontage, Hutschienenmontage
Anschluss	Federzugklemme	Schraub-Steckklemme	9-pol. D-SUB Buchse, Schraub-Steckklemme	Schraubsteckverbinder	9-pol. D-SUB Buchse, Stecker o. Schraubsteckv.
Verwendete Ethernetprotokolle	Varan	TCP/IP, UDP/IP, ICMP, ARP		TCP/IP, UDP/IP, Telnet, HTTP, BOOTP, ICMP, DHCP, DNS, SMTP, SNMP	TCP/IP, UDP/IP, Telnet, HTTP, BOOTP, ICMP, DHCP, DNS, SMTP, SNMP
Unterstützte Industrial-Ethernet-Kommunikationsprotokolle	Varan				
Feldbus-Anbindung			CAN Bus		
Konfiguration der seriellen Adapter	Engineering Tool Lasal	Internet-Browser (Webbased-Management), Konfigurations-Software	Internet-Browser (Webbased-Management), Konfigurations-Software	Internet-Browser (Webbased-Management), Konfig.-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfig.-Software, Serielle Konsole, Telnet
Programmierbarkeit bzw. Skripterstellung					
Statusanzeige, Diagnoseinformationen am seriellen Adapter	Power, COM	Power, LAN, COM	Power, LAN, COM	Power, LAN, COM	Power, LAN, COM
					
Anbieter	W&T Wiesemann & Theis GmbH	Wachendorff Prozesstechn. GmbH & Co. KG	Wachendorff Prozesstechn. GmbH & Co. KG	Wago Kontakttechnik GmbH & Co. KG	Wago Kontakttechnik GmbH & Co. KG
Produkt-ID	14276	11279	30556	11299	17300
Ort	Wuppertal	Geisenheim	Geisenheim	Minden	Minden
Telefon	0202/ 2680-110	06722/ 9965-20	06722/ 9965-20	0571/ 887-0	0571/ 887-0
Internet	www.WuT.de	www.wachendorff-prozesstechnik.de	www.wachendorff-prozesstechnik.de	www.wago.com	www.wago.com
Produktname	USB-Server Gigabit 2.0	Pegelwandler HD6703825-25-B2	Pegelwandler HD67038-25-A1	Serielle Schnittstelle RS232/RS485 (750-652)	Ser. Schnittst. RS232/RS485 (750-652/040-000)
Serielle Schnittstelle RS232		1	1	1	1
Serielle Schnittstelle RS422				1	1
Serielle Schnittstelle RS485		1	1	1	1
Ser. Schnittstelle: RS232, RS485 o. RS422 einstellbar		Nein		1	1
Maße (BxHxT, in mm)	105 x 75 x 22	71 x 95 x 60	23 x 120 x 107	12 x 65 x 100	12 x 65 x 100
Montageart	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage	Hutschienenmontage
Anschluss	USB-Buchse Typ A	1x RS232 (9-polig Sub-D-Stecker)	1x RS232 (9-polig Sub-D-Stecker)	Cage Clamp	Cage Clamp
Verwendete Ethernetprotokolle	TCP/IP, UDP/IP, HTTP, ARP, BOOTP			TCP/IP, UDP/IP, HTTP, BOOTP/DHCP, SNMP, SNTP, DNS, FTP	TCP/IP, UDP/IP, HTTP, BOOTP/DHCP, SNMP, SNTP, DNS, FTP
Unterstützte Industrial-Ethernet-Kommunikationsprotokolle				Profinet, Modbus/TCP, Ethernet/IP, Sercos III, BACnet, KNX IP, Ethercat	Profinet, Modbus/TCP, Ethernet/IP, Sercos III, BACnet, KNX IP, Ethercat
Feldbus-Anbindung	Ethernet			Profibus DP, Modbus, LonWorks, Lightbus, Interbus, Devicenet, CANopen, BACnet, usw.	Profibus DP, Modbus, LonWorks, Lightbus, Interbus, Devicenet, CANopen, BACnet, usw.
Konfiguration der seriellen Adapter	Internet-Browser (Webbased-Management), Konfigurations-Software	kostenlose Konfigurations-Software SW67038 zur Parametrierung des Gerätes	kostenlose Konfigurations-Software SW67038 zur Parametrierung des Gerätes	Wago-I/O-Check oder GSD-/GSDML-Dateien	Wago-I/O-Check oder GSD-/GSDML-Dateien
Programmierbarkeit bzw. Skripterstellung		kostenlose Konfigurations-Software SW67038 zur Parametrierung des Gerätes	kostenlose Konfigurations-Software SW67038 zur Parametrierung des Gerätes	Registerkommunikation	Registerkommunikation
Statusanzeige, Diagnoseinformationen am seriellen Adapter	Power, LAN, COM	4x LED: Signalanzeige für Versorgung und Kommunikation	4x LED: Signalanzeige für Versorgung und Kommunikation	LED	LED

MARKTÜBERSICHT SERIELLE ADAPTER FÜR ETHERNET

			
SSV Software Systems GmbH 11229 Hannover 0511/ 40000-13 www.ssv-embedded.de	VS Vision Systems GmbH 11271 Norderstedt 040/ 528401-0 www.visionssysteme.de	VS Vision Systems GmbH 25411 Norderstedt 040/ 528401-21 www.visionssysteme.de	W&T Wiesemann & Theis GmbH 11302 Wuppertal 0202/ 2680-110 www.WuT.de
IGW/900	NetCom Plus 811	NetCom Plus 213	Com-Server ++
1	8		
1		2	1
22,5 x 90 x 118	196 x 44 x 147	115 x 73 x 25	22 x 75 x 105
Hutschienmontage	Hutschien-, Wandmontage, Rackmount	Wandmontage, Hutschienmontage	Hutschienmontage, Wandmontage (optional)
Schraubsteckverbinder	9-pol. D-SUB Stecker	9-pol. D-SUB Stecker	9-pol. D-SUB Buchse, Stecker
TCP/IP, UDP/IP, Telnet, HTTP	TCP/IP, UDP, Telnet, PPP, DHCP, ICMP, HTTP, LPD, SNMP V1/2c/3, DNS, openVPN	TCP/IP, UDP/IP, Telnet, HTTP, ARP, ICMP, BOOTP	TCP/IP, UDP/IP, Telnet, HTTP, ARP, ICMP, BOOTP, Wake-on-Lan
CANopen			Ethernet
Internet-Browser (Webbased-Management), Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfig.-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfig.-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfig.-Software, Serielle Konsole, Telnet
frei programmierbar über C, C++ o.ä.			Paketierungsoptionen
Power, LAN, COM	Power, LAN, COM	Power, LAN, COM	Power, LAN, COM

			
Weidmüller GmbH & Co. KG 11225 Detmold 05231/ 1428-259 www.weidmueller.de	Weidmüller GmbH & Co. KG 22775 Detmold 05231/ 1428-259 www.weidmueller.de	Welotec GmbH 22772 Laer 02554/ 9130-16 www.welotec.com	Welotec GmbH 22774 Laer 02554/ 9130-16 www.welotec.com
IE-CS-2TX-2RS232/485	IE-GW-MB-2TX-1RS232/485	Serieller Geräteserver - SE5002-S55is	Serieller Geräteserver - SE5002
2	1		
2	1		
2	1		
2	1	2	2
36 x 140 x 105	29 x 124,5 x 89,2	90 x 63 x 45	90 x 63 x 45
Hutschienmontage	Hutschienmontage	Wandmontage, Hutschienmontage	Hutschienmontage, Wandmontage
2x 9-pol. D-SUB Stecker für RS232, 422, 485	RS232: 9-pol. D-SUB Steck., RS422/485: Steckv.	5-pol. Terminal Block (3,81mm)	9-pol. D-SUB Buchse, Stecker
ICMP, IP, TCP, UDP, DHCP, BOOTP, Telnet, Rtelnet, DNS, SNMP, HTTP, SMTP, SNTP, IGMP	TCP/IP, UDP, Modbus-TCP, HTTP, DHCP, BOOTP, SNMP		ICMP, TCP (UDP)/IP, DHCP Client, SNMP, SMTP, HTTP, Telnet
	Modbus-TCP	ICMP, TCP (UDP)/IP, DHCP Client, SNMP, SMTP, HTTP, Telnet	
	Modbus/RTU, Modbus/ASCII		
Internet-Browser (Webbased-Management), Konfigurations-Software, Serielle Konsole, Telnet	Internet-Browser (Webbased-Management), Konfigurations-Software, Telnet	Web Page, Telnet, Serial console, Windows utility	Web Page, Telnet, Serial console, Windows utility
Spannungsvers. 1 u. 2, Ethernet-Schnittstelle, Übertragungsgeschw. 10 o. 100MBit/s, usw.	Spannungsvers. 1 u. 2, Ethernet-Schnittstelle, Übertragungsgeschw. 10 o. 100MBit/s	LAN, RUN, COM1Tx, COM2Tx, COM1Rx, COM2Rx	LAN, RUN, COM1Tx, COM2Tx, COM1Rx, COM2Rx

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 12.03.2020



Alles auf einen Blick

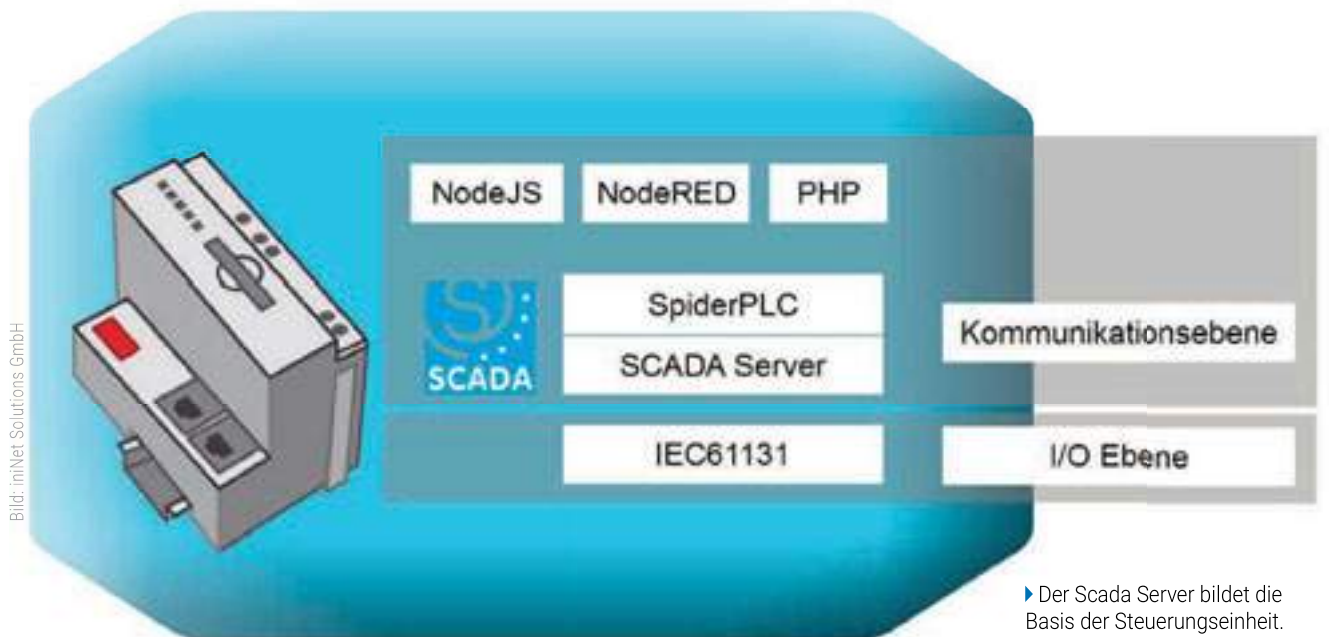


Die **marktführenden Fachmedien des SPS-MAGAZINs** erreichen jedes Jahr mehr als 1,2 Millionen Kontakte und informieren bestens über aktuelle Entwicklungen der Automatisierungstechnik sowie zur digitalen Transformation.

sps-magazin.de

Industrie 4.0 in der praktischen Anwendung

Von der Stange



Das Referenzarchitekturmodell Ram 4.0 führt die wichtigsten Aspekte von Industrie 4.0 zusammen und soll als zentrale Orientierungshilfe dienen. Bei näherer Betrachtung erweist es sich jedoch – trotz Vorteilen gegenüber der klassischen Automatisierungspyramide – an vielen Stellen als zu abstrakt. Anhand eines Fallbeispiels soll dies im Folgenden konkretisiert werden.

Das Referenzarchitekturmodell Ram ist in eine dreidimensionale Architektur gegliedert, welche als Rahmenwerk fungiert und für unterschiedlichste Produktionsanforderungen die Zukunft bilden soll. Dieses Modell soll auch die klassische ein- bis zweidimensionale Automationspyramide ersetzen. Während bei der bekannten Automationspyramide auf jeder Ebene konkrete Produkte, Protokolle oder Aufgabenstellungen problemlos eingefügt werden können, ist das Ram-Modell an vielen Stellen mehr als abstrakt. Hier muss noch intensiv an neuen Definitionen, Standards sowie Produkten gearbeitet werden. Schaut man sich die verschiedenen Schichten des Modells genauer an, entsteht schnell der Eindruck, dass sich die Automationshersteller von den unteren Schichten nach oben arbeiten, während sich die IT entgegengesetzt von oben nach unten bewegt. Von daher ist es nicht verwunderlich, dass die drei Schichten 'Functional', 'Information' und 'Communication' bislang in Punkto Standards sowie Tools am wenigsten Substanz zu bieten haben. Doch denkt man an die Automationspyramide zurück, wird schnell klar, dass zwischen der Automationswelt und IT schon immer

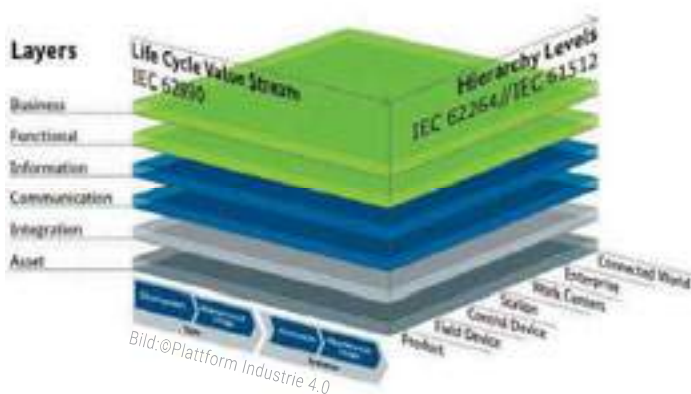
die größten Herausforderungen lagen. Das heißt zwei Welten treffen aufeinander – und dieses Problem gilt es zu lösen.

Automationspyramide nicht zeitgemäß

Was bedeutet Industrie 4.0 konkret? Kurz zusammengefasst: Anwender möchten möglichst viele ihrer Prozesse digitalisieren. Und dies auf verschiedenen Ebenen: Betrieb, Beschaffung, Dokumentation, Logistik, Audit Trail, Vertrieb sowie in vielen weiteren Bereichen. Damit dies alles umgesetzt werden kann, müssen im Vorfeld sämtliche Prozessanwendungen erfasst sowie analysiert werden.

Das Fallbeispiel

Digitalisierung ist am einfachsten, wenn ein Unternehmen, ausschließlich ein Produkt herstellt. In diesem Fallbeispiel kann die Automation für genau eine Aufgabe programmiert werden. Dies entspricht einer klassischen Aufgabenstellung jeder SPS-Programmierung. Für die weitere Digitalisierung



► Das Referenzarchitekturmodell soll Unternehmen als Basis zur Entwicklung zukünftiger Produkte und Geschäftsmodelle dienen.

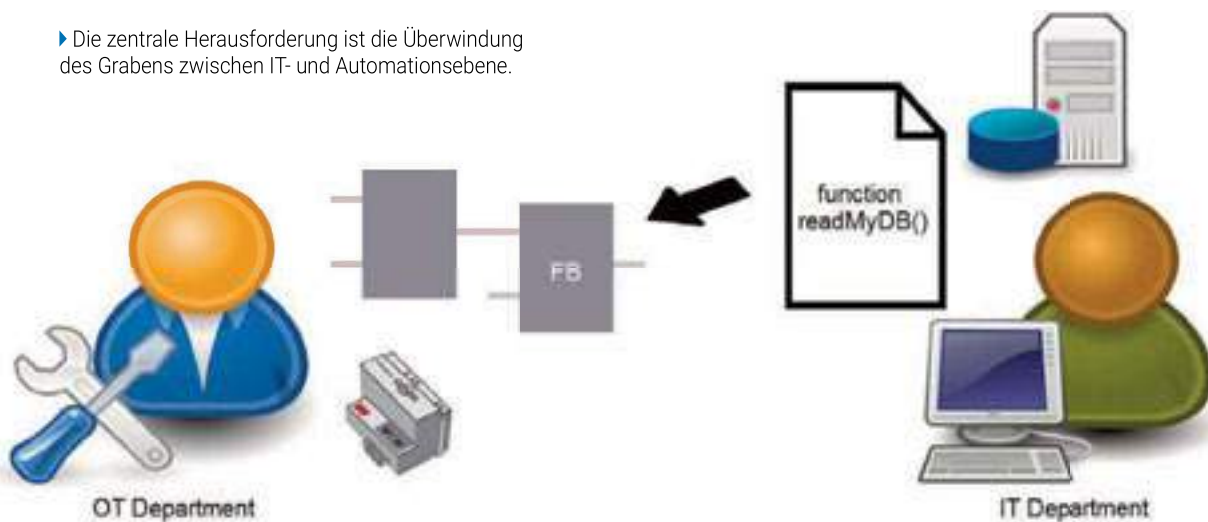
werden beispielsweise Schnittstellen zur Produktionsplanung, Logistik oder Qualitätssicherung benötigt. Durch die möglichen Kombinationen ergibt sich eine beliebige Komplexität. Ferner hat diese Art von Architektur grundsätzliche Design-Fehler: Durch die teilweise Nachbildung der Automationsprozesse in der Leitebene entsteht an dieser Stelle eine Redundanz. Auf das alte Produktionsverfahren übertragen, wäre dies vergleichbar, wie wenn anstatt Facharbeitern ungelernte Hilfskräfte eingestellt werden würden. Jeder einzelne Arbeitsschritt müsste detailliert vorgegeben und kontrolliert werden. Und die Personen, welche diese Schritte kontrollieren müssen, kommen aus der Planung und Buchhaltung. Es entstünde so zu sagen sehr viel teurer Leerlauf. Bezogen auf die Software-Architektur sowie praktische Umsetzung hat dies hier zwei Auswirkungen: Die Quasi-Nachbildung der Produktionsebene in der Leitebene findet auf einem recht abstrakten Niveau statt. Das Debugging ist enorm schwierig, weil weitestgehend im Blindflug programmiert wird. Dies führt zu hohen Entwicklungskosten. Noch kritischer wird es allerdings im weiteren Lebenszyklus dieser Lösung, da das System so komplex ist und Änderungen über die Jahre immer schwieriger werden. Diese Redundanz kann nur dann beseitigt werden, wenn die Produktionsprozesse ausschließlich auf der Automationsebene programmiert werden. Die Leitebene legt fest, welche Aufträge bearbeitet und welche Produkte gefertigt werden sollen. Sie erteilt auch die Anforderungen an die Produktionsmittel, Produktionszeiten, Stücklisten, Testprotokolle und vieles mehr. Dies bedeutet auch, dass die Leitebene festlegt, was produziert werden soll – wie es aber produziert werden soll, bestimmt die Maschine. Deshalb wird auf der Produktionsebene ein möglichst objektorientierter Ansatz verfolgt, im Sinne einer Orientierung an der Maschine als mechatronische Einheit. Das heißt die jeweiligen Produktions- und Steuerungseinheiten holen sich die Aufträge von der Leitebene, kommunizieren mit den für die Produktfertigung notwendigen Subsystemen, allozieren diese und liefern ihnen den Link auf die Vorgaben aus der Leitebene. Der Materialbedarf bzw. -verbrauch wird an ein Logistiksystem gemeldet und der Produktionsstatus zurück an die Leitebene. Jedes Objekt beschäftigt sich ausschließlich mit seiner eigenen Aufgabe. Das bedeutet, dass zu jeder Steuerung nicht nur die I/O-Ebene für die klassische Automation programmiert wird,

sondern eben auch die Kommunikationsebene für die Einbindung in das I4.0 Netzwerk der Firma. Für jedes anschließend darauf gefertigte Produkt wird möglichst 'klassisch' in IEC61131 auf der I/O-Ebene der Automationssysteme programmiert. Also genau so, wie es bei einer Serienanfertigung eines einzelnen Produktes gemacht wird. Das garantiert eine effiziente Entwicklung, eine unkomplizierte Wartung und einen hohen Freiheitsgrad für zukünftige Erweiterungen. Eine Modularisierung von Produkten ist in den meisten Unternehmen längst Standard. Es ist nun zusätzlich ein Mechanismus gefordert, der das passende SPS Programm für zu fertigende Produkt aktiviert. Die Steuerungseinheit führt Test, Messreihen oder Protokolle selbst aus. Auch Formulare oder Typenschilder werden automatisch erstellt. Sollte eine Arbeitsstation nicht vollautomatisch sein, so ist die Steuerungseinheit in der Lage, Arbeitsanweisungen für einen Arbeiter beispielsweise auf einem lokalen Display anzuzeigen.

Die pragmatische Umsetzung

Die Basis für den Aufbau der Steuerungseinheit bildet der SpiderControl Scada Server. Diese Software ist nahezu für alle Betriebssysteme (Windows Standard, embedded Compact, Linux, embedded Linux, Raspian oder Android) verfügbar und wurde bereits auf aktuelle Geräten vieler namhafter SPS Hersteller portiert, die offene Steuerungen anbieten, wie z.B. Wago PFC, Phoenix PLCNext, Siemens IoT2040, industrielle RaspberryPi oder auch Industrie Router wie z.B. die MRX Serie von Insys. Ist der Scada Server auf die SPS integriert, kann dieser direkt mit der lokalen SPS Applikation oder mit abgesetzten Automationskomponenten kommunizieren. In diesen Scada Server ist die SpiderPLC eingebunden, welche eine einfache Programmierung von Funktionsplan über den Browser ermöglicht. Das Besondere daran: Die Funktionsbausteine führen nicht nur einfache Logik aus, sondern können zusätzlich Funktionen aus externen Scripten der wichtigsten aktuellen Hochsprachen, wie u.a. JavaScript (NodeJS, NodeRED), PHP, Python oder .Net aufrufen. Hierzu wird zusätzlich eine Runtime für die Ausführung der benötigten Script-Sprachen auf der SPS installiert. Diese wird im Hintergrund gestartet und wartet darauf, dass sie eine Anfrage für die Ausführung einer Funktion aus SpiderPLC empfängt. Damit wird es möglich, den SPS Code direkt mit den Daten und Funktionen aus der Leitebene zu verknüpfen. Zur Anbindung an die IT Ebene können die Informatiker den Code zur Kommunikation mit deren Applikationen in der Hochsprache ihrer Wahl zur Verfügung stellen. Dieser Code wird über einen Funktionsbaustein gekapselt und in die Automation eingebunden. Die vorher beschriebene Architektur kann beispielsweise wie folgt umgesetzt werden: Um einen Auftrag an eine Produktionseinheit zu übergeben, kann das MES die notwendigen Informationen dazu z.B. in eine Datenbank schreiben, über ein Rest API im Intranet ablegen, oder es gibt ein Software API zum Zugriff auf die entsprechende MES Software. Der Software Ingenieur, der sich im MES auskennt, hat nun mehrere Möglichkeiten. Er kann ein PHP Script erstellen, welches die entsprechenden Felder aus der Datenbank liest. Oder er liefert ein JavaScript, welches sein Rest API auslesen kann. Oder er hat eine .Net Funktion, welche ein API direkt in seine MES Applikation implementiert.

Die zentrale Herausforderung ist die Überwindung des Grabens zwischen IT- und Automationsebene.



Jetzt kann der SPS Programmierer die vom MES Spezialisten gelieferte Script-Funktion aus einem Funktionsbaustein in der SpiderPLC aufrufen. Damit das Script die passenden Daten aus dem MES finden kann, werden alle notwendigen Parameter aus der SPS auf den Funktionsbaustein übertragen. Dazu muss die SPS angeben, für welches Produktionsmittel sie einen Auftrag abfragen will ('wer bin ich'). Das Script wiederum schreibt die Daten dann in den Namespace des Scada Servers. Somit kann man auch größere Datenstrukturen mit einem Aufruf übergeben und auch wieder zurückbekommen. Die SPS weiss nun, was sie als nächstes produzieren soll. Über einen weiteren Funktionsbaustein kann SpiderPLC mit der Produkt-ID ein PHP Script aufrufen, welches aus einer SQL-Datenbank Produktinformationen zu diesem Objekt ausliest. Das Script erteilt Auskunft über Stücklisten, involvierte Subsysteme, Referenzen auf Dokumente, Testprotokolle, etc. und wird von einem Informatiker zur Verfügung gestellt, der mit der Wartung der Produkt-Datenbank vertraut ist. Dieser Informatiker weiss, welche Parameter er von der SPS bekommen muss, damit er den gewünschten Datensatz findet. Den abgefragten Datensatz kann er als Antwort in ein XML Format packen, welches indessen vom Scada Server verstanden und in seinen internen Namespace abgebildet wird. Danach alloziert die SPS die in den Produktionsprozessen involvierte Subsysteme, z.B. ein System welches für die Produktion das notwendige Material aus einem Lager entnimmt sowie für den Weitertransport konfektioniert. Die direkte Kommunikation kann durchaus über ein Feldbus Protokoll erfolgen. Förderlich wäre evtl., wenn die SPS eine Referenz auf die benötigten Datenbank Datensätze an das Subsystem weitergibt. Das Subsystem, das die benötigten Teile auf einen Transportträger konfektioniert, erstellt bei Bedarf einen Datensatz, wie die Teile angeordnet sind. Der Roboter, der dann die Teile vom Transportträger in die CNC Maschine fördert, kann dadurch mit sehr unterschiedlichen Konstellationen umgehen, weil die SpiderPLC ihm mitteilt, welches Teil an welcher Position liegt. Nun werden auf der SPS die für die Fertigung des gewünschten Teiles erforderlichen Programme (in IEC61131) aufgerufen. Diese geben über einen Datenpunkt ein Signal, wann die Sequenz abgeschlossen ist. Somit können die Teile ausgeführt und der Status des Auftrags im MES mutiert werden. Testprotokolle werden zeitgleich an einer anderen Station in

Empfang genommen und durchgeführt. Die Messungen werden in Registern der SPS abgelegt und über die SpiderPLC wird ein PHP Script aufgerufen, welches diese Variablen als Parameter übergibt sowie beispielsweise mit der FPDF PHP Library ein PDF Dokument erzeugt. Da die Daten parallel dazu in einer Datenbank abgelegt werden, ist die Produktion jederzeit zurück verfolgbar. Zudem wird stets eine aktuelle Statistik über die Qualität der Produktion geführt, welche Rückschlüsse über den Anlagenzustand und andere produktionsrelevante Parameter erlaubt. Da für diese Aufgaben z.B. oftmals Python verwendet wird, ergibt sich der Übergang zum Machine Learning nahezu von selbst. Python Funktionen können analog über Funktionsbausteine direkt aus SpiderPLC aufgerufen werden.

Fazit

Anhand dieses Fallbeispiels lässt sich zeigen, wie einfach gängige Abläufe auf Basis der SpiderPLC/Scada-Infrastruktur umgesetzt werden können. Der entscheidende Vorteil besteht darin, dass die Programmierung von I4.0-Anwendungen unkompliziert mit dem eigenen Personal realisiert werden kann. Ohne große anfängliche Investitionen kann man an einer einzelnen Maschine damit beginnen, die Verbindung mit der Leitebene zu schaffen. Erfahrungsgemäß werden im Anschluss daran Schritt für Schritt weitere Komponenten – nach dem gleichen System – eingebunden. Das Risiko für das Scheitern des Projekts mit daraus resultierenden Folgekosten ist hierdurch weitestgehend eliminiert. Das klassische Problem in Hinblick auf die Überwindung des Grabens zwischen der Automationsebene und IT wird hier ebenfalls gelöst, da beide Seiten in den technologischen Domänen bleiben können: Die IT liefert alle relevanten Schnittstellen in einer für sie bekannten Programmiersprache. Die Automationsebene verwendet diese als Funktionsbaustein in einer Funktionsplanprogrammierung, welche über das Scada und seine Treiber Zugriff auf alle Automationskomponenten hat. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/5814



Peter Brügger, Geschäftsleitung,
iniNet Solutions GmbH
www.ininet.ch



Wireless-Produkte

Die Netzwerkkommunikation ist ein Schlüssel für die selbst organisierende Produktion im Sinn der Industrie. Industrielle Funksysteme spielen eine entscheidende Rolle bei der Umsetzung solcher Konzepte, denn sie bieten die Möglichkeit, Produktionsprozesse effizienter und flexibler zu gestalten.

Verbindung über WLAN oder Bluetooth zur Kommunikation in der Fabrik haben sich inzwischen bereits weitestgehend etabliert: Unternehmen setzen heute schon auf moderne drahtlose Lösungen. So ist nicht verwunderlich, dass der Blick bereits nach vorne geht. Der neue Mobilfunkstandard 5G steht am Horizont und verspricht neue Benchmarks zu setzen, was Latenzzeiten und Frequenzkapazitäten betrifft. Heute schon erhältliche Wireless-Lösungen können Sie online über die Suchmaschine i-need.de finden. (bfi) ■

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

WACHENDORFF

Wachendorff Prozesstechnik
65366 Geisenheim | Tel.: +49 6722 9965-544
beratung@wachendorff.de
www.wachendorff-prozesstechnik.de



Ewon Flexy 205

- Aufzeichnung, Alarmierung und Visualisierung für datenbasierte Geschäftsmodelle
- Direkte Anbindung von SPS'en und Feldgeräten
- Kostenfreies zentrales Benutzer- & Gerätemanagement mit Fernwartungsportal Talk2M
- Einfache Inbetriebnahme und Integration in die IT-Landschaft
- Sicherheit gemäß führender Standards

www.wachendorff-prozesstechnik.de/ewon



DIGITALE TRANSFORMATION & INDUSTRIE 4.0

**INDUSTRIAL
MANAGEMENT
NEWS**

TECHNIK // ARBEITSWELT // GESELLSCHAFT

INDUSTRIAL MANAGEMENT NEWS

Das Magazin für die digitale Transformation

Technik, Arbeitswelt, Gesellschaft –

INDUSTRIAL MANAGEMENT NEWS

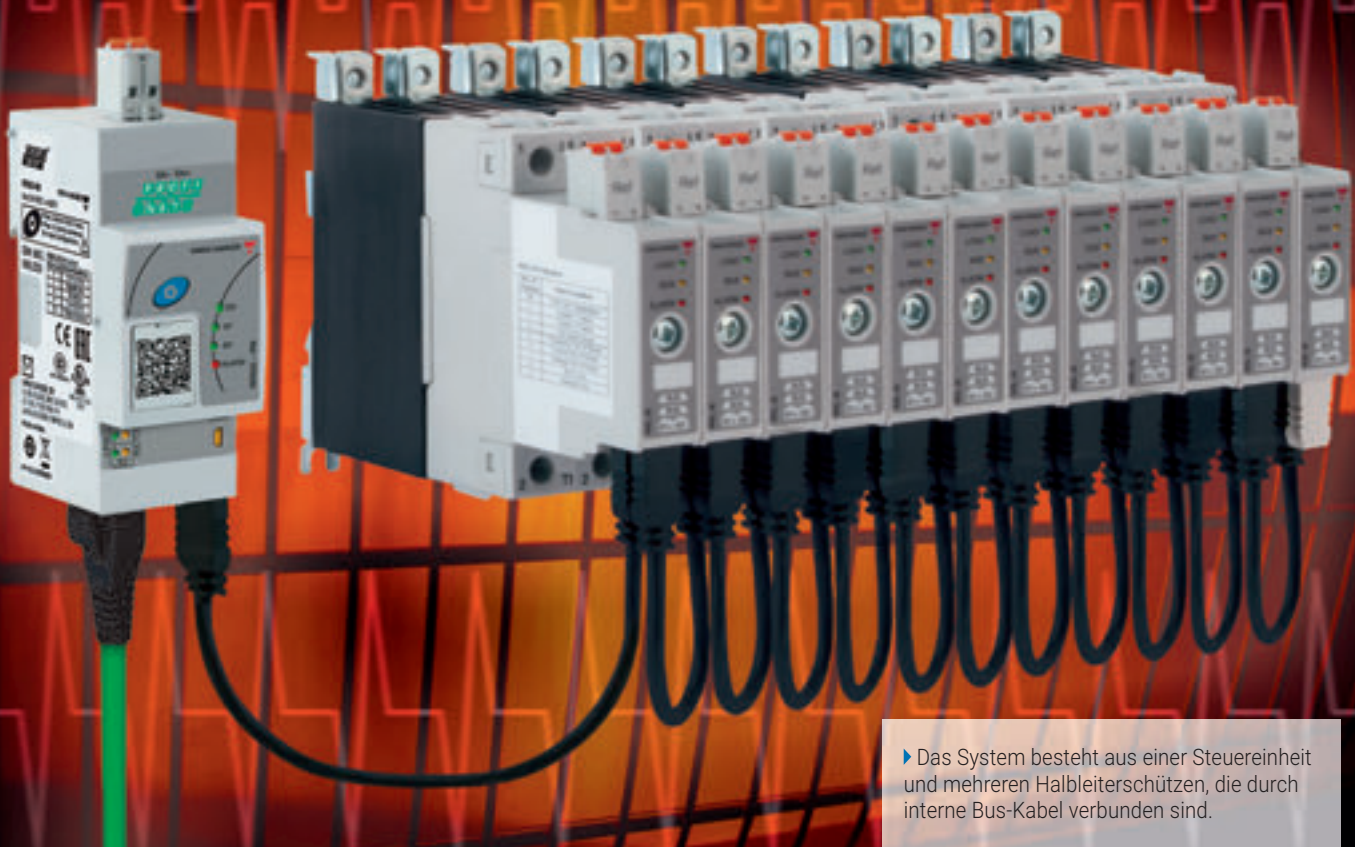
zeigen das ganze Bild!

Verständlich, umfassend und übersichtlich zusammengestellt. So sichern Sie sich Ihren Wissensvorsprung!



Jetzt **KOSTENFREI** abonnieren:
www.i40-magazin.de/anmelden





► Das System besteht aus einer Steuereinheit und mehreren Halbleiterschützen, die durch interne Bus-Kabel verbunden sind.

Heizungssteuerung über Profinet

Voll im Griff

Bei industriellen Heizungsanwendungen ist die zuverlässige, präzise und reproduzierbare Regelung der Temperatur entscheidend für die Qualität des Endproduktes. Mit dem NRG-System hat Carlo Gavazzi eine Produktlösung entwickelt, mit der der Anwender via Profinet-Schnittstelle Heizlasten präzise und schnell schalten kann. Zusätzlich hat er Zugriff auf die Messwerte und die Funktionen der Schaltkomponenten im Lastkreis und kann bei Fehlern frühzeitig korrigierend eingreifen.

Infrarotheizungen werden immer häufiger in Fertigungsprozessen in der Industrie eingesetzt. So kommen moderne Klebe- oder Lackierprozesse nicht mehr ohne gezielte Erwärmung oder Aushärtung durch Infrarotstrahler aus. Fehlfunktionen bei einem NIR Halogen Infrarot-Strahler oder einer Infrarotheizung werden jedoch meist erst sichtbar, wenn das produzierte Teil nicht den Qualitätsvorgaben entspricht. Hier ist es oft schwierig oder kostspielig, einen geschlossenen Regelkreis aufzubauen, der die Funktion der Heizung permanent überwacht. Große Heizflächen oder komplizierte Formen mit einer Vielzahl von kleinen Heizpatronen können aus Kostengründen nur partiell über einen Temperaturfühler überwacht werden. Der Ausfall einer einzelnen Hei-

zung wird ebenfalls oft erst am Ergebnis erkannt. Diese Ausfälle in den industriellen Heizprozessen lassen sich durch eine frühzeitige Erkennung von Fehlern und Funktionsstörungen reduzieren. Grundlage für die vorausschauende Wartung ist die ständige Erfassung und Analyse der Daten der verschiedenen Anlagenkomponenten. Bei elektronischen Schaltelementen wird dafür ein integriertes Diagnose- und Überwachungssystem benötigt. Diese Überwachungsmöglichkeit stellt das NRG-System von Carlo Gavazzi zur Verfügung. Es beruht auf den Halbleiterschützen der Serie RGC1A, die um eine Kommunikationsschnittstelle erweitert wurden, so dass die Messwerte der Last und der Funktionen der Module in Echtzeit erfasst und an die Steuerung übermittelt werden können.



Aufbau des modularen Systems

Ein NRG-System setzt sich aus einer Steuereinheit und bis zu 32 Schaltmodule zusammen, die über einen internen RS485-BUS kommunizieren. Die Module liefern die Daten der überwachten Prozessvariablen. Das NRG-CT stellt als Gateway die Verbindung zwischen den Modulen und der SPS her und ermöglicht die Kommunikation. Proprietäre interne -BUS-Kabel, die die Kommunikations-, Versorgungs- und Autokonfigurationsleitungen tragen, verbinden den Controller mit der ersten und diese mit den weiteren Modulen in der BUS-Kette; an den letzten Anschluss wird ein Abschlusswiderstand angeschlossen. Angeboten wird die Steuereinheit zunächst mit Feldbus-Schnittstelle für Modbus. Inzwischen wurde eine neue Version NRG-CT PN mit Industrial-Ethernet-Schnittstelle für Profinet IO ergänzt. Beide Systeme bieten die Möglichkeit, über den internen BUS jedes einzelne Halbleiterschütz in der Kette anzusteuern und zu schalten. Die Halbleiterschütze der Serie bilden die Schaltelemente und Überwachungssysteme. Neben einem Netzanschluss und einem Anschluss für die Heizungslast weisen sie einen Anschluss für das Referenzsignal L1 oder N für die Spannungsmessung sowie zwei Anschlüsse für den internen BUS auf. Über einen Port wird das erste Halbleiterschütz in der BUS-Kette des Subsystems mit der Steuereinheit verbunden, der zweite Port dient dem Anschluss der folgenden Halbleiterschütze. Die Implementierung erfolgt per Auto-konfiguration, die eine schnelle Einrichtung bei Erstintegration oder Austausch erlaubt und Fehleinstellungen vermeidet. Eine fehlerhafte Konfiguration ist dabei ausgeschlossen. LEDs auf der Frontseite der Module zeigen den Status von geschalteter Last, Kommunikation und Alarm an. Über die Blinksequenz lässt sich die Art des Alarms erkennen, so dass sich Fehler wie Lastverlust, ein offener Lastkreis durch Netzausfall (beispielsweise Sicherung ausgelöst), Unterbrechung oder Kurzschluss des Thyristors unterscheiden lassen und sich die Fehlersuche vereinfacht.



► Die Steuereinheit agiert als Profinet-Gateway eines Subsystems mit maximal 32 Halbleiterschützen.

Überwachung über Profinet

Die Funktion der Halbleiterschütze wird durch die Kommunikation mit dem NRG-CT PN überwacht. Sie sammelt über die Kommunikationsschnittstelle der Halbleiterschütze die Daten der überwachten Messgrößen in Echtzeit und übermittelt sie an die SPS. Überwacht werden Strom, Spannung, Frequenz, Leistung, Energieverbrauch der Last und Betriebsstunden. Als Diagnosedaten der Halbleiterschütze und der geschalteten Last stehen Informationen zu Netzverlust, Lastverlust, Lastabweichung und Übertemperatur, einem Kurzschluss im Lastkreis des Halbleiterschützes und seinem Zustand außerhalb der eingestellten Grenzwerte zur Verfügung. Erfasst werden zudem für jedes Schaltgerät die Anzahl der Schaltungen, die Betriebszeit und der Stromverbrauch. Damit lassen sich die Betriebsstunden und der Leistungsverbrauch der geschalteten

Heizung genau erfassen. Mit Überwachung allein ist es bei Heizanwendungen nicht getan. Via Profinet kann über den Controller als Master jedes einzelne Halbleiterschütz in der Kette über den internen BUS angesteuert und netzsynchron im Spannungsnulldurchgang ein- oder ausgeschaltet werden. Neben der direkten Steuerung kann der Anwender zwischen weiteren Betriebsmodi wählen, mit denen er für jedes Halbleiterschütz und damit jeden Heizungskanal im System definierte Stellgrößen mit einer Auflösung bis zu einer Halbwelle vorgeben kann. Die Betriebsmodi entlasten die SPS und verringern den Kommunikationsaufwand über Profinet.

Fazit

Das NRG-System mit Profinet-Schnittstelle unterstützt Fertigungsbetriebe, die industrielle Heizungsanwendungen nutzen, bei der Ausrichtung auf Industrie 4.0. Mit dem System kann der Anwender Daten in Echtzeit im laufenden Betrieb auslesen, die ihm die Früherkennung von Störungen und die vorbeugende Wartung zur Verhinderung von Stillstand- und Ausfallzeiten ermöglicht. Eindeutige Diagnosen vereinfachen und beschleunigen dabei die Fehlersuche.

Über die Profinet-Schnittstelle können sie die Halbleiterschütze zudem direkt über den BUS steuern. So wird eine sehr hohe Regelgüte und eine konstant hohe Qualität der Endprodukte erreicht.

Die exakte Messung der Energiekosten jedes Produktionsprozesses verbessert die Ermittlung der Stückkosten. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/1824



Michael Schultze,
Marketing Manager,
Carlo Gavazzi GmbH
www.gavazzi.de



Wenn der Hacker die SPS übernimmt

Mehr als die Hälfte der deutschen Industrieunternehmen hat durch Cyber-Attacken finanzielle Schäden erlitten, so eine Studie des VDMA. Dass die Zahl solcher Angriffe abnimmt, ist nicht in Sicht. Daher wird es immer wichtiger, Industrial Networks und Operational Technology (OT)-Umgebungen zu schützen. Dabei helfen Ansätze, die auch beim Schutz von Büronetzwerken Verwendung finden.

Auf rund 103 Milliarden Euro schätzt der Digitalverband Bitkom die Schäden, die deutsche Unternehmen durch Cyber-Angriffe im letzten Jahr verzeichneten. Mehr als ein Fünftel der Firmen war von Datenspionage betroffen. In 17 Prozent der Unternehmen sabotierten Angreifer Produktionsanlagen und Informationssysteme. Zu vergleichbaren Ergebnissen kommt der VDMA in der Studie Cyber-Risiken im Maschinen- und Anlagenbau von 2019. Demnach führten bei der Hälfte der Unternehmen Cyber-Attacken zu finanziellen Schäden. Als Ursache dafür werden zum einen Produktionsausfälle angeführt, zum anderen waren bei fast einem Drittel der Unternehmen Hacker-Angriffe dafür verantwortlich. Mithilfe von Erpresser-Software (Ransomware) die Daten auf IT- und OT-Systemen zu verschlüsseln und erst nach Zahlung eines Lösegelds wieder freizugeben – oder auch nicht. Hierbei kann es im schlimmsten Falle dazu kommen, dass die Produktion der betroffenen Firma wochenlang stillsteht und somit enorme finanzielle Schäden entstehen. Für staatliche motivierte Hacker und Cyber-Kriminelle sind Industrial Networks, Industrial Control Systems (ICS) und OT-Umge-

bungen lukrative Ziele. So können Angreifer Produktionsdaten, die sie bei ihren digitalen Raubzügen erbeuten, vor allem im Dark Web zu Geld machen. Denn für Mitbewerber sind solche Informationen durchaus von Interesse. Sie können beispielsweise Rückschlüsse auf Produktionstechnologien sowie die Art und Zahl der produzierten Güter ziehen.

II.0 und IoT machen Angriffe einfacher

Angreifer profitieren bei ihren Aktionen davon, dass Ansätze wie Industrie 4.0 und das Internet of Things die Grenzen zwischen Büronetzwerken (IT) und OT aufgeweicht haben. Doch nur dadurch lassen sich Konzepte wie Predictive Maintenance und das Monitoring sämtlicher Produktionsprozesse in Echtzeit umsetzen. Bei der vorausschauenden Wartung erfassen Sensoren an Maschinen Daten und geben diese an Edge Devices oder Edge Data Center weiter, die in der Nähe der Anlagen platziert sind. Diese Devices führen eine Vorverarbeitung der Daten durch und übermitteln sie an IT-Systeme externer Rechenzentren, wie z.B. das Data Center des Maschinenherstellers. Dort



erfolgt dann eine detaillierte Auswertung der Informationen. Mittlerweile kommen bei solchen Analysen verstärkt Big Data & Analytics-Anwendungen sowie IoT-Plattformen zum Zuge, die über eine Public Cloud bereitgestellt werden. Dies liefert Cyber-Kriminellen und Saboteuren unterschiedliche Angriffspunkte, um Zugriff auf Steuerungssysteme und Maschinen zu erhalten: direkt über den Ursprung beim Maschinenhersteller, das Netzwerk des Industrieunternehmens oder die Cloud-Provider. Hinzu kommt, dass die Absicherung von OT-Umgebungen keine triviale Aufgabe ist. Ein Grund ist, dass solche Komponenten mit dem Ziel entwickelt wurden, eine hohe Verfügbarkeit und Betriebszeit zu gewährleisten. Dem Schutz vor Cyber-Attacken wurde nie wirklich eine hohe Priorität beigemessen. Zudem ist ein beträchtlicher Teil dieser Systeme bereits seit zehn und mehr Jahren im Einsatz, also einer Zeit, in der Technologien wie Industrie 4.0 und IoT noch in den Kinderschuhen steckten. Daher weisen die Software und Übertragungsprotokolle von Steuerungen und anderen OT-Komponenten häufig Schwachstellen auf, die sich nur mit einem beträchtlichen Aufwand – im schlimmsten Fall sogar gar nicht mehr – beseitigen lassen. Das gilt beispielsweise für Systeme, die auf veralteten Betriebssystem-Versionen basieren, etwa der Windows-XP-Version für Embedded Systems.

Schutzmaßnahmen

Doch trotz dieser Herausforderungen ist es durchaus möglich, OT-Umgebungen und ICS wirkungsvoll vor Cyber-Angriffen zu schützen, ohne über eine umständliche Komplettumstellung auf andere Systeme nachzudenken. Dabei kommen mehrere Ansätze in Betracht, die u.a. bereits zur Absicherung von Verwaltungs- und Office-Netzwerken genutzt werden. Dazu zählt der Einsatz von komplexen Passwörtern und Identity and Access Management(IAM)-Tools. Dies stellt sicher, dass nur befugte Mitarbeiter Zugang zu solchen Netzwerken und Systemen erhalten. Zu den wichtigsten Abwehrmaßnahmen zählt, nur denjenigen Anwendungen – aber auch Anwendern – Zugang zu Steuerungssystemen und Industrial Network-Komponenten zu gewähren, die explizit dazu autorisiert wurden. Umsetzen lässt sich dies mithilfe von Sicherheitslösungen für Embedded-Systeme in Verbindung mit einem „Whitelisting“. Das ist eine Aufstellung von Applikationen, die auf den Embedded-Systemen ausgeführt werden dürfen. Programme, die sich nicht auf dieser Liste finden, werden blockiert. Ein Vorteil von Whitelisting ist, dass sich dadurch auch Zero-Day-Attacken unterbinden lassen. Das sind Cyber-Angriffe, bei denen Hacker Schwachstellen in Programmen ausnutzen, die noch nicht bekannt sind oder innerhalb einer OT-Landschaft nicht gefixt werden können.

Monitoring in Echtzeit

Eine weitere Abwehrmaßnahme ist der Einsatz von IT-Security-Plattformen, die Netzwerke und Systeme in Produktionsumgebungen kontinuierlich auf verdächtige Aktivitäten hin untersuchen. Ein solches Monitoring übernehmen Security Information and Event Management (SIEM)-Lösungen. Diese Tools

sind in der Lage, sowohl IT- als auch OT-Umgebungen von Industrieunternehmen zu überwachen. Sobald sie verdächtige Aktivitäten identifizieren, alarmieren sie die IT-Security-Verantwortlichen, so dass diese darauf mit angemessenen Maßnahmen reagieren können. Zusätzlich zu den SIEM-Tools ist die Implementierung von Data Loss Prevention (DLP)-Lösungen sinnvoll, welche Hardware und Software kontrollieren. Über sie kann z.B. die Verwendung bestimmter Anwendungen eingeschränkt werden. Darüber hinaus machen sie ebenfalls auf unerlaubte Programme oder Hardware und die Exfiltration von Daten aufmerksam. Mit einer solchen Lösung ist es möglich die Brücke zwischen physischer und digitaler Welt zu schlagen und Industrie- und Büronetze vor Cyber-Angriffen als auch den Aktivitäten von illoyalen eigenen Mitarbeitern („Insidern“) zu schützen. Das Monitoring erfolgt in Echtzeit, sodass Gefahren umgehend erkannt werden. Das ist notwendig, um den Schaden durch Angriffe auf ein Minimum zu reduzieren.

Die Cloud nicht vergessen

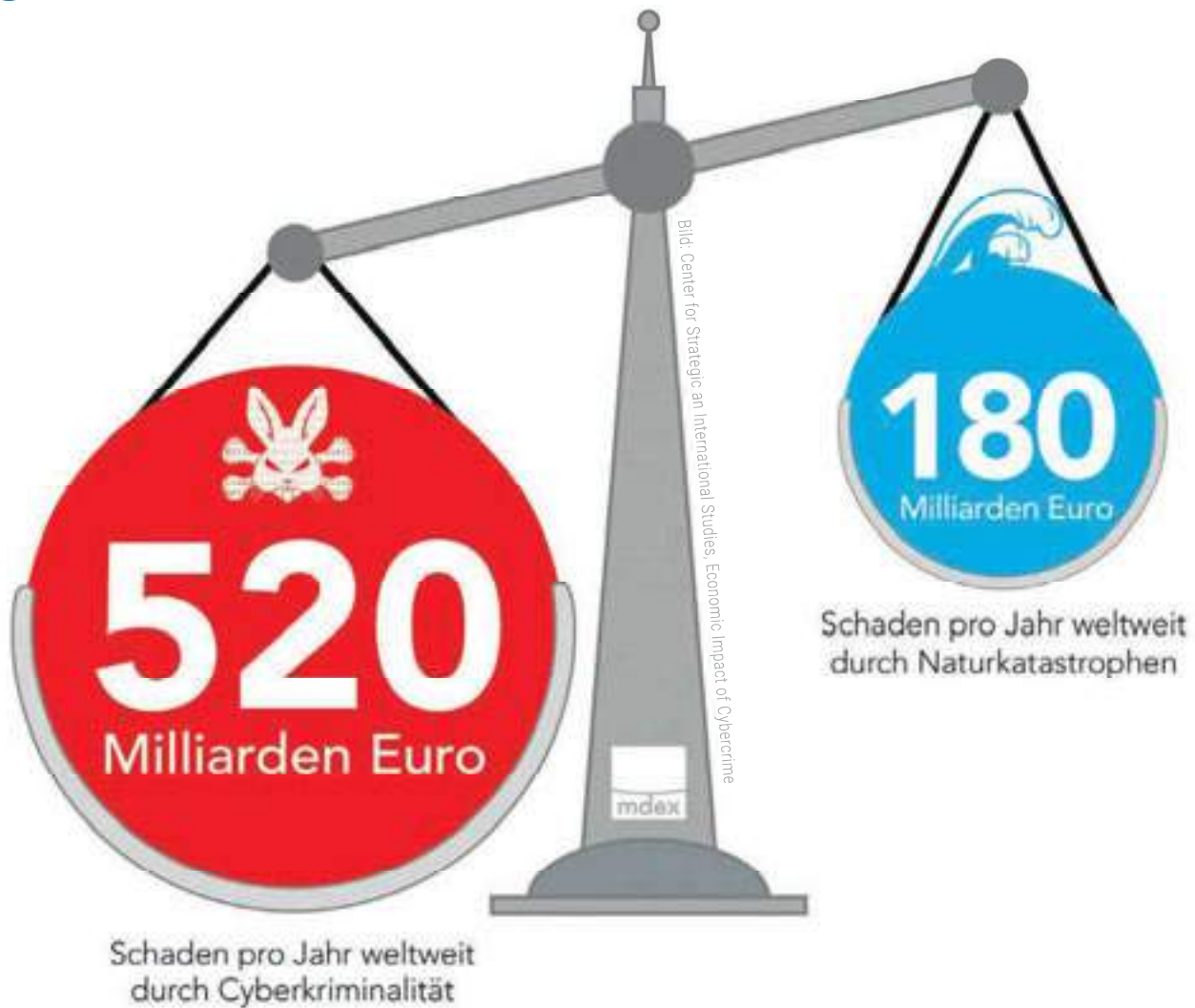
Ein umfassender IT-/OT-Security-Ansatz muss zudem die Cloud miteinbeziehen. Denn es ist absehbar, dass cloud-basierte IoT- und IIoT-Plattformen massiv an Bedeutung gewinnen. Über solche Plattformen können Unternehmen nach Angaben der Marktforscher von IoT Analytics künftig auch Applikationen auf Basis von Künstlicher Intelligenz nutzen, etwa in Bereichen wie Predictive Maintenance und Qualitätssicherung. Um zu vermeiden, dass sich solche Cloud-Anwendungen zu einem Sicherheitsrisiko entwickeln, bietet sich der Einsatz einer Cloud Access Security Broker (CASB)-Lösung an. Sie ermöglicht es dem Unternehmen, den gesamten Datenverkehr zwischen Cloud-Anwendungen sowie Endsystemen und Nutzern zu überwachen. Dadurch werden nicht autorisierte und böswillige Aktivitäten transparent und können unterbunden werden. Außerdem erkennt es beispielsweise, ob ein Unbefugter einen USB-Stick an eine Steuerung oder eine SCADA-Komponente (Supervisory Control and Data Acquisition) ansteckt, um Daten „abzusaugen“.

Sicherheit in OT-Umgebungen ist machbar

Sicherlich erfordert es einen gewissen Aufwand, neben der IT-Infrastruktur auch die OT-Umgebung vor Cyber-Angriffen zu schützen. Doch mittlerweile gibt es eine Reihe von Lösungen, mit denen Unternehmen Produktionsumgebungen gegen solche Attacken umfassend absichern können. Denn Unternehmen, die das Thema OT-Sicherheit auf die leichte Schulter nehmen, gehen ein hohes Risiko ein. Zu den finanziellen Schäden kommt häufig der Verlust von Kunden, weil diese das Vertrauen in den Hersteller verloren haben. Und darauf zu hoffen, dass das eigene Unternehmen von Hacker-Angriffen verschont bleibt, ist sicherlich keine gute Idee. ■



Hans-Peter Bauer,
Vice President Central Europe,
McAfee LLC
www.mcafee.com/de



Schutz vor Ransomware

Internet of Horrors

Das größte unternehmerische Risiko liegt heutzutage nicht etwa in Nachfrageverschiebungen oder Naturkatastrophen, sondern in der Gefahr von Cyberangriffen. Und die kriminellen Banden hinter Viren, Trojanern und Ransomware rüsten laufend auf. Neue Angriffsstrategien erfordern eine angepasste Sicherheitsstrategie, die die Produktion und die IT ganzheitlich gegen Eingriffe von außen abschirmt. Gerade KMU müssen die nächste Verteidigungslinie aufbauen und Anomalien in der IT-Kommunikation so schnell wie möglich erkennen.

Viren sind so alt wie die ersten Computerprogramme. Allerdings hat sich in den letzten Jahren der Bereich der professionellen Cyberkriminalität durch Erpressungssoftware ('Ransomware') zum lukrativen Geschäftsfeld entwickelt. Mit zunehmenden Verständnis für die vernetzte Produktion haben Cyberkriminelle ein ebenso simples wie perfides Geschäftsmodell gefunden, indem sie betriebswichtige Daten verschlüsseln und diese Daten erst gegen Lösegeldzahlung wieder entschlüsseln.

Geschäftsmodell Ransomware

Zwar warnt z.B. das Bundesamt für Sicherheit in der Informationstechnik generell vor Lösegeldzahlungen. Doch die Erpresser



► Ein Drittel der von Cyberangriffen betroffenen Unternehmen wurde von ehemaligen Mitarbeitern vorsätzlich geschädigt



handeln in der Regel rational und wissen genau, wen sie eigentlich angreifen. Daher sind Lösegeldforderungen selten Phantasiezahlen, sondern so kalkuliert, dass der Verlust durch den Betriebsstillstand oder der Wiederherstellungsaufwand größer ist als die Geldforderung, die noch dazu über Bitcoins anonym und sofort bezahlt werden kann. Bislang waren insbesondere stark vernetzte Großkonzerne ins Visier von Cyberkriminellen geraten. Doch inzwischen haben viele Großunternehmen ihre Maßnahmen bei der IT-Sicherheit massiv erhöht. Daher wenden sich Ransomware-Angriffe mehr und mehr mittelständischen Unternehmen und Behörden zu, die potenziell weniger in Sicherheitsmaßnahmen investieren.

Aufwand für Cyberkriminelle erhöhen

Ähnlich wie bei Wohnungs- und Hauseinbrüchen ist ein 100-prozentiger Schutz gegen Schadprogramme und Hacker kaum zu garantieren. Dennoch kann ein durchdachtes und ganzheitliches Sicherheitskonzept das Risiko eines erfolgreichen Cyberangriffs beträchtlich verringern und den möglichen Schaden begrenzen. „Wie in normalen Wirtschaftsbereichen arbeiten auch Cyberkriminelle gewinnorientiert“, erklärt Dennis Paul, IoT-Bereichsleiter bei Mdex. „Je umfangreicher die Schutzmaßnahmen sind, desto größer ist auch die Wahrscheinlichkeit, dass sich Hacker leichtere Opfer suchen. Dies belegt die zunehmende Anzahl an Cyberangriffen auf kleinere und mittelständische Betriebe. Diese bringen zwar einzeln betrachtet geringere Erlöse durch Erpressung, können aber durch die existenzielle Gefährdung einem besonderen Handlungsdruck ausgesetzt werden.“ Zwingende Voraussetzung für einen sicheren Produktionsablauf bleibt die organisatorische und technische Grundsicherung. Die erforderlichen organisatorischen Maßnahmen zielen darauf ab, eine Verhaltens- und Bewusstseinsänderung bei den Mitarbeitern herbeizuführen. Nach einer Erhebung der Bitkom sagt ein Drittel der von Cyberangriffen betroffenen Unternehmen, dass sie von früheren Mitarbeitern vorsätzlich geschädigt wurden. Ein knappes Viertel (23 Prozent) sieht die Verantwortung bei ehemals im Betrieb beschäftigten Personen, die sich aber nicht absichtlich falsch verhalten hätten. Immerhin 14 Prozent der befragten Unternehmen sehen die Schuld bei derzeitigen Mitarbeitern, die aus Unkenntnis gehandelt haben. Die Verbreitung von Ransomware kann nämlich auf ganz

einfachen Wegen erfolgen, etwa durch das Einstecken eines USB-Sticks oder über das Anschließen eines Service-Laptops. „Die organisatorischen Maßnahmen sind erforderlich, um die Belegschaft auf die Gefahren durch Ransomware, aber auch durch Industriespionage zu sensibilisieren“, sagt Dennis Paul. „Dazu gehören eindeutige Arbeitsanweisungen, das Vier-Augen-Prinzip, eine lückenlose Dokumentation und die Einhaltung von Sicherheitsstandards wie z.B. ISO27001.“ Wirklich effektiv ist jedoch lediglich eine Kombination verschiedener Maßnahmen, und dazu zählt die möglichst lückenlose Abschottung der Produktion zum Internet mit Firewalls, geschlossenen Benutzergruppen und Verschlüsselung.

Inkubationszeit als Schwachstelle

Die Eigenart von Ransomware besteht häufig darin, nach der Infektion zunächst einmal unerkannt zu bleiben und gezielt nach weiteren Systemen im Netzwerk zu suchen, die ausnutzbare Sicherheitslücken aufweisen. Diese Inkubationszeit ist typisch für Ransomware, da der Virus zunächst versucht, maximale Verbreitung im System zu erreichen. Gleichzeitig werden dadurch eine Vielzahl an neuen Kommunikationsbeziehungen aufgebaut, die vorher nicht definiert sind und als Anomalie erkannt werden können. Es gibt also ein Zeitfenster, in dem ein befallenes System noch gerettet werden kann, falls der Angriff rechtzeitig erkannt wird. Im Rahmen der Anomalie-Erkennung durch Deep Packet Inspection wird der Datenverkehr ständig in Echtzeit kontrolliert und bei Abweichungen von den vorher definierten und erlaubten Kommunikationsbeziehungen Alarm ausgelöst. Anhand der Kommunikation kann zudem ausgemacht werden, welches System von dem Virus befallen wurde. Im besten Fall kann hier also – eine entsprechend schnelle Reaktion vorausgesetzt – der Befall weiterer Systeme sowie eine Verschlüsselung des befallenen Systems verhindert werden. Im schlimmsten Fall muss nun lediglich der betroffene Industrie-PC neu aufgesetzt werden, ein kostspieliger Produktionsausfall lässt sich noch verhindern ■



Dennis Paul,
Mdex GmbH
www.mdex.de



Die drei wichtigsten IIoT-Security-Trends 2020

End-to-End-Security

Im Internet der Dinge und seiner industriellen Ausprägung, dem IIoT, steckt unglaubliches Wachstumspotenzial. Marktforscher sind sich nur darüber uneins, wie schnell die Verbreitung voranschreiten wird. Unstrittig ist: Die Vernetzung muss sicher erfolgen. Doch welche Sicherheitsaspekte gilt es in diesem Jahr für das Umsetzen und Betreiben von IoT- und IIoT-Anwendungen besonders zu berücksichtigen?

Die Marktforscher von IDG sehen in fünf Jahren rund 41 Milliarden IoT-Devices im Einsatz, und diese gilt es abzusichern. Für dieses Jahr zeichnen sich drei Entwicklungen in der IT-Security ab, die für das IoT- und IIoT-Umfeld besonders relevant sind.

1. Größere Angriffsfläche

Das rasante IoT-Wachstum vergrößert die potenzielle Angriffsfläche für Cyberkriminelle, Angriffsszenarien gibt es genügend. So lassen sich Mirai-Botnetze für DDoS Attacken nutzen. Vorstellbar ist auch das sogenannte Reverse-Engineering von Firmware und Betriebssystemen, bei dem der Quellcode zurückgesetzt wird. Über einen gefälschten LoRa-Access-Point verbinden sich Geräte auf eine Fake-Infrastruktur, auf der Cyberkriminelle Passwörter für die echte Infrastruktur abgreifen wollen. 2020 werden wir den ersten großen Sicherheitsvorfall im IoT-Umfeld erleben, was auch an dem Wettbewerbsdruck liegt, unter dem Hersteller IoT-Technik entwickeln und ausliefern. Dabei passieren Fehler.

2. Mehr Cloud-Services und Managed PKI

2020 ist mit einer deutlichen Zunahme von Cloud-Security-Angeboten zu rechnen, die sich auch auf das Segment Public Key Infrastructure (PKI) auswirken werden. Eine PKI bildet die Grundlage für durchgängige Ende-zu-Ende-Sicherheit, indem die Certificate Authority (CA) das Vertrauen zwischen Systemen auf Basis digitaler Zertifikate herstellt. Eine PKI setzt eine starke Authentifizierung, Datenverschlüsselung sowie digitale Signaturen durch und verhindert so Identitätsmissbrauch. Mit der Technologie lassen sich viele Zugriffssteuerungssysteme realisieren, unter anderem der sichere Zugang zu einer IoT-Umgebung. Im Zusammenspiel mit einem zentralen Device Management würden beispielsweise

Fake-Devices auffliegen und könnten nicht dazwischenfunken - oder im schlimmsten Falle Daten und Informationen ausleiten bzw. manipulieren. Die anstehende Veränderung betrifft das Betreibermodell. So geht im IoT- und IIoT-Umfeld der Trend zur Managed PKI. Hierbei erfolgt der Zugriff auf digitale Zertifikate, ohne eine CA im eigenen Netz einrichten und betreiben zu müssen.

3. Industrie 4.0 startet durch

In den vergangenen Jahren hat die Fertigungsbranche ihre Hausaufgaben zu Industrie 4.0 gemacht. Im Durchschnitt ist vierte Maschine in der deutschen Fertigungsindustrie mit dem Internet verbunden. Mehr als die Hälfte der Unternehmen (53 Prozent) nutzt spezielle Anwendungen für Industrie 4.0, ein weiteres Fünftel (21 Prozent) plant dies, schreibt der IT-Branchenverband Bitkom. In diesem Jahr wird das produzierende Gewerbe einen gewaltigen Schritt nach vorn machen, ihre Produktionsumgebungen weiter vernetzen und neue Geschäftsmodelle umsetzen. Unternehmen sind gut beraten, für jede geplante Anwendung in der Industrie 4.0 die IT-Sicherheit von vornherein mitzudenken. In der Praxis bewährt sich hierfür insbesondere, ein PKI mit einer zusätzlichen Autorität für digitale Identitäten zu kombinieren. Auf diese Weise erhalten hergestellte Komponenten bereits im Fertigungsprozess eine digitale Identität. Im Jahr 2020 geht es für IoT-Geräte-Hersteller, Sicherheitsspezialisten, MSP und Anwender vor allem darum, an der End-to-End-Security vom IoT-Gerät bis zur IoT-Plattform zu arbeiten. ■



Andreas Philipp,
Business Development Manager,
PrimeKey Labs GmbH
www.primekey.com



Security-Modul für IPCs mit Windows 7



Mithilfe des Security-Moduls mGuard von Phoenix Contact können Anwender eine Security-Lücke bei Industrie-PCs mit dem Betriebssystem Windows 7 schließen, für

das Microsoft seit dem 14. Januar 2020 keine Sicherheits-Updates mehr zur Verfügung stellt. Angreifer hätten so die Möglichkeit, in Produktionsrechner einzudringen. Das Modul verfügt über einen patentierten Stealth Mode, der dafür sorgt, dass keine Änderungen am System durchgeführt werden müssen – weder an der Netzwerkinfrastruktur noch

am Rechner. Es kann nachträglich in ein bestehendes Netzwerk integriert werden. Weiterhin werden MAC- und IP-Adresse des zu schützenden Systems automatisch übernommen. Die Netzwerkkonfiguration bleibt ebenfalls unverändert.

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

Plattform für sichere IIoT-Anbindung

HMS Networks stellt eine Sicherheitsplattform für die Produktfamilie Anybus CompactCom vor, die Zertifikatsverwaltung und TLS-Verschlüsselung unterstützt. Vertrauliche Daten wie private Schlüssel werden zur Stärkung der Integrität und Identität des Produkts auf einem separaten Sicherheits-Chip gespeichert. Daten, die vom Modul an die Cloud-ebene gesendet werden, werden mithilfe von OPC UA Secure Channels signiert und verschlüsselt. Die Autorisierung und Authentifizierung der Anwender erfolgt über OPC UA Sessions. Sicherer Zugriff und sichere Dateiübertragung sollen durch TLS über HTTPS und WebDAV gewährleistet sein. Über die Benutzer- und Rollenverwaltung können verschiedene Zugriffsrechte definiert werden.



HMS Industrial Networks GmbH
www.hms-networks.de

MEHRERE SICHERHEITSFUNKTIONEN IN EINEM GERÄT

Liss Appliances vereinen wichtige Sicherheitsfunktionen auf nur einem Gerät. Damit sind sensible Unternehmensnetzwerke



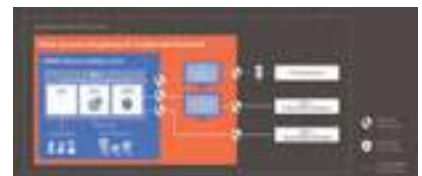
optimal vor Viren, Hackern sowie unerwünschten E-Mails und Webinhalten geschützt. Das Modulsystem beinhaltet unter anderem eine mehrstufige Firewall, Intrusion Detection, einen Virens scanner und VPN-Router, Spam- und Web-Inhaltsfilter sowie https-Filter. Die Geräte garantieren laut Hersteller kundenindividuelle Lösungen bestehend aus optimaler Hardwareplattform und bedarfsgerechter Zusammenstellung der Funktionen. Ein VPN-Modul ist standardmäßig in den Security Appliances enthalten. Hochverfügbarkeit lässt sich durch Kombination von zwei Geräten im Failover-Modus realisieren. Bei höheren Ansprüchen an Performance und Ausfallsicherheit besteht die Möglichkeit des Clustering.

Lantech Communications Europe GmbH
www.lantechcom.de

Security-Maßnahmen planen

Anlagenbetreiber sind dafür verantwortlich, dass ihre Sicherheitssysteme (engl. Safety Instrumented Systems, SIS) relevante Safety- und Security-Normen erfüllen. Oft fehlt jedoch neben Zeit und Ressourcen die erforderliche Systemkenntnis, um die richtigen Maßnahmen hierfür zu identifizieren. Die Hima Paul Hildebrandt bietet jetzt einen SIS Security Check an. Anlagenbetreiber erhalten dadurch einen Überblick über den Status ihrer Safety-Einrichtungen sowie über Security-Risiken und -Schwachstellen, denn prozesstech-

nische Anlagen werden immer komplexer. Der SIS Security Check wird von Safety-Spezialisten durchgeführt, die speziell in Automation-Security geschult sind. Sie führen vor Ort eine grundlegende Überprüfung der Security-Policies und -Maßnahmen durch. Dabei prüfen sie die SIS sowie SIS-nahe Komponenten und gleichen diese mit Security-Empfehlungen ab. Am Ende des Assessments erhalten Anlagenbetreiber einen Bericht einschließlich spezifischer Optimierungsempfehlungen. Dieser bildet die Basis für künftige Ri-



sikoanalysen und Maßnahmen. Die Umsetzung dieser unterstützt Anlagenbetreiber dabei, relevante Normen wie IEC62443 und IEC61511 Edition 2 einzuhalten und das Sicherheitsrisiko für ihre Produktionsanlagen zu minimieren.

Hima Paul Hildebrandt GmbH
www.hima.com



Vorschau Industrial Communication Journal 2020

	Protokolle und Standards	Komponenten und Lösungen	Wireless und Remote	Sicherheit	Industrielle Kommunikation 4.0
Ausgabe 1 (April) ET: 26.03.2020 RS: 27.02.2020	Profibus und Profinet AS-Interface Single Pair Ethernet (SPE)	OPC UA als Backbone für die smarte Fabrik Kommunikationslösungen für die Antriebstechnik Serielle Adapter für Ethernet <i>mit Marktübersicht</i>	Industrielle Mobilfunk-Standards und -Lösungen	Redundante Kommunikation (PSP, HSR etc.) Plagiats- und Knowhow-Schutz Sicher kommunizieren mit FSoE	Industrial IoT & digitale Transformation Cloud & Big Data M2M & PDM Datendurchgängigkeit Security Ethernet TSN & OPC UA
Ausgabe 2 (Mai) ET: 19.05.2020 RS: 21.04.2020	Ethercat Modbus TCP/IP CC-Link	Kabel- und Verbindungstechnik <i>mit Marktspiegel</i> Lichtwellenleiter & Optic Fibre (LWL)	Machine-to-Machine-Kommunikation (M2M) MQTT und AMQP	IT-Sicherheitsgesetz Sicher kommunizieren mit OpenSafety	Industrial IoT & digitale Transformation Cloud & Big Data M2M & PDM Datendurchgängigkeit Security Ethernet TSN & OPC UA
Ausgabe 3 (Oktober) ET: 07.10.2020 RS: 09.09.2020	Ethernet/IP Varan CAN/CANopen	Power over Ethernet (PoE und PoE+) Installations- und Datenmanagement	WLAN für die Industrie <i>mit Marktübersicht</i> Funk in der Feldebene	Antiviren-Software für die Industrie Sicher kommunizieren mit Profisafe Security <i>mit Marktübersicht</i>	Industrial IoT & digitale Transformation Cloud & Big Data M2M & PDM Datendurchgängigkeit Security Ethernet TSN & OPC UA
Ausgabe 4 (November) ET: 18.11.2020 RS: 21.10.2020	Ethernet Powerlink Sercos IO-Link	Diagnose und (Fern-)Wartung IO-Systeme mit Feldbus/ Ethernet-Ankopplung <i>mit Marktübersicht</i>	NFC und Bluetooth	Sicherheit mit RFID Zugriffsschutz und Firewalls Sicher kommunizieren mit CIP Safety	Industrial IoT & digitale Transformation Cloud & Big Data M2M & PDM Datendurchgängigkeit Security Ethernet TSN & OPC UA

ET: Erscheinungstermin, RS: Redaktionsschluss

Insertentenverzeichnis

Beckhoff Automation GmbH & Co. KG	2	Phoenix Contact Deutschland GmbH	52
Helmholz GmbH & Co. KG	Titel, 23	Red Lion Controls BV	19
IBHsoftec Gesellschaft für Automatisierungstechnik mbH	19, 27	Wachendorff Prozesstechnik GmbH & Co. KG	41
Kendrion Kuhnke Automation GmbH	19	Weidmüller GmbH & Co. KG	29
Kontron S&T AG	19		

Impressum

VERLAG/POSTANSCHRIFT:
 Technik-Dokumentations-Verlag
 TeDo Verlag GmbH®
 Postfach 2140, 35009 Marburg

Tel.: 06421/3086-0, Fax: -380
 E-Mail: info@sps-magazin.de

Internet: www.sps-magazin.de

LIEFERANSCHRIFT:
 TeDo Verlag GmbH
 Zu den Sandbeeten 2
 35043 Marburg

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

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

WEITERE MITARBEITER:
 Tamara Gerlach, Susan Jünger,
 Lena Krieger, 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 Mediadata 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.

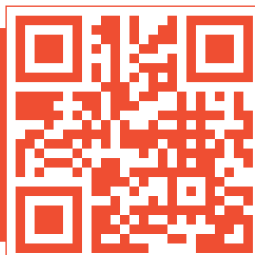
DIE APP ZUM SPS-MAGAZIN

ALLE WICHTIGEN AUTOMATISIERUNGS-NEWS VON A BIS Z SOFORT ERFAHREN!



Mit der kostenlosen App erfahren Sie alle relevanten Themen aus der Automatisierungstechnik sofort. Features wie die Vorlesefunktion, Push-Nachrichten, Bookmark-Listen und die einfache Navigation machen das Lesen zu einem neuen Erlebnis.

**JETZT KOSTENLOS
DOWNLOADEN!**



Laden im
App Store

JETZT BEI
Google Play



powered by: **SPS
MAGAZIN**



DC 05-20.000.1.1



Durchgängig bis zum letzten Meter

Steckverbinder für das Single Pair Ethernet

Phoenix Contact präsentiert kompakte Geräte- und Kabelsteckverbinder für das einpaarige Ethernet. Die normierten SPE-Schnittstellen eignen sich ideal für die effiziente Datenübertragung in der Fabrik- und Prozessautomatisierung. Die anwendungsgerecht optimierte Verkabelung bildet die Basis für die zukunftssichere Vernetzung vom Sensor bis in die Cloud.

Mehr Informationen unter phoenixcontact.com/spe