

Besuchen Sie uns auf
der SPS: Halle 7, Stand 230



Einfach in die Cloud? Sicher!

Das ist die digitale Zukunft!

www.wago.com/digitale-zukunft/de

Hacktivismus gefragt

Daten sind das Öl des 21. Jahrhunderts. Ergo: Daten stehlen lohnt sich! In der logischen Konsequenz nehmen Cyber-kriminelle Anstrengungen unweigerlich zu und wirksame Schutzmaßnahmen für Industrieunternehmen werden unerlässlich.

Mit ausreichend Zeit und Mitteln kommen Hacker in jedes System. Die Sicherheit im Informationszeitalter kann also nicht als absoluter Zustand verstanden werden, sondern vielmehr als einer, dem man sich ständig annähern muss. Doch inwieweit kann dabei Unterstützung von oben kommen? Bundesregierung, Ministerien und das BSI geben sich umtriebiger und haben im Rahmen ihrer Sicherheitsstrategie schon verschiedene Initiativen auf den Weg gebracht, z.B. die Sonderstelle ZITIS.

Auch die Bundeswehr hat mit dem Cyber- und Informationsraum (CIR) einen neuen Bereich geschaffen, der sich dem Kampf gegen Cyber-Angriffe widmen soll. Doch in der Praxis stößt man hier auf ein Problem, dass wir aus dem Produktionsumfeld nur zu gut kennen: Auch hier schlägt der Fachkräftemangel in den MINT-Disziplinen zu Buche. So konnten bisher weder ZITIS noch CIR ansatzweise die Wunschzahl an Mitarbeitern einstellen.

Dass sich zudem die meisten jungen Cyber-Spezialisten und White Hacker aus ihrem Selbstverständnis nicht leicht tun, ihre Ex-

pertise zukünftig als Beamte oder Soldaten einzubringen, kommt vielleicht Industrieunternehmen dabei zugute, selbst Cyber-Kompetenz aufzubauen – und ohne die wird es in Zukunft nicht mehr gehen. Natürlich berichtet auch diese Ausgabe des INDUSTRIAL COMMUNICATION JOURNALS wieder vielseitig über Sicherheitsaspekte. Ich wünsche eine interessante Lektüre.



Mathis Bayerdörfer
mbayerdoerfer@sps-magazin.de



Mathis Bayerdörfer, Chefredakteur

- Anzeige -

Zukunftssichere Plattform für die Industrie 4.0



www.odva.org

ODVA®



Bild: Profibus Nutzerorganisation e.V.

TITELSTORY

Mehr Transparenz für die Anlage

Während der Planung oder dem Aufbau einer Maschine oder Anlage können sich zahlreiche Änderungen ergeben. Eine saubere Anlagendokumentation von Anfang an funktioniert in der Realität oft nur unzureichend. Die Asset-Identifikation von Profinet bietet schon eine ganze Reihe an Unterstützung. Ein neuer Service zur Anlagenerfassung kann jetzt Anlagenteile und sogar Baugruppen und Module erfassen, die nicht mit Profinet modelliert wurden.

Open Source für die Automatisierung



Erfahrungsberichte:
Sercos SoftMaster in der Praxis
Seite 20

Bild: Rovema GmbH

Markt-Trends-Technik

- 10 Aktuelles aus der Branche
- 12 Neuheiten und Produktvorstellungen

Protokolle und Standards

- 15 Interview: Die Zukunft von CANopen FD
- 18 Artikelserie FDT und OPC UA (Teil 1/2): Einheitlicher Ansatz
- 20 Artikelserie Open Source (Teil 2/2): Sercos für alle
- 22 Marktübersicht: I/O-Systeme

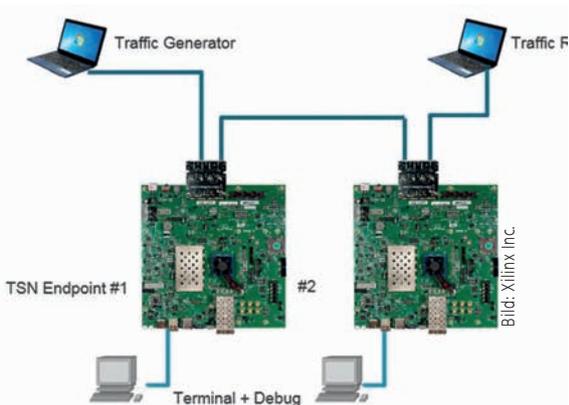
TSN-Faktencheck

- 24 Kommt Zeit, kommt TSN? Experten über TSN
- 26 Elektronikimplementierung von Time-Sensitive Networking

Komponenten und Lösungen

- 29 Produktübersicht: Industrial-Ethernet-Komponenten
- 31 Neue Switches: Mit IP67 und PoE+ in industriellen Anwendungen
- 32 Brandsichere Brummis: Robuste CAN-Busleitung für Nutzfahrzeuge
- 34 Technologieübergreifende Vernetzung von Werkzeugmaschinen
- 35 Profinet-Switch überwacht und dokumentiert
- 36 Segmentierung des Produktionsnetzes: Drei Ebenen sind keine zuviel
- 38 Kolumne: Keine Bauchschmerzen mit Industrial Ethernet

Elektronikimplementierung von TSN



Netzwerk-Konvergenz für das IIoT: Mithilfe von TSN IT- und OT-Netze zusammenführen
Seite 26

Industrie 4.0 Daten- und Kommunikations- lösungen



Durchgängige HF/UHF-RFID-Lösungen für Datenerfassung und -vorverarbeitung, Identifikation, Rückverfolgung, Serialisierung

Intelligente Sensor- und Verbindungslösungen mit IO-Link-Kommunikation für maximale Flexibilität

Robuste IP67-I/O-Systeme mit dezentraler Intelligenz und Multiprotokoll-Ethernet-Kommunikation zur einfachen IT-Integration

SPS IPC Drives
Wir sind für Sie da!
Halle 7, Stand 250



Tutorialserie Fernzugriff (Teil 3/3)



Mit Basic und Java IloT-Router individuell anpassen
Seite 51

Bild: HMS Industrial Networks AB

Offen aber sicher



Moderne Verschlüsselungskonzepte für industrielle Fertigungsnetze
Seite 62

Bild: ©kruUA/istockphoto.com

Sonderteil CC-Link IE

- 40** Starker Partner für das Netzwerk von Industrie 4.0
- 41** Integriertes Netz für Industrie 4.0
- 43** Gigabit Ethernet: Analysten und Entscheider überzeugt
- 44** Neuheiten rund um CC-Link IE
- 45** Feldgeräte für das 1Gbit-Zeitalter
- 46** CC-Link IE Field Basic
- 47** CC-Link und CC-Link IE in Wort und Bild
- 48** Das Netzwerk für Industrie 4.0
- 49** Partnerschaften und Netzwerk

Wireless & Remote

- 51** Tutorial Fernzugriff auf Maschinen und Anlagen (Teil 3/3): Fernfassung von Daten mit Java und Basic
- 55** Auf dem Weg zum Cloud-Historian: Wenn Grenzen verwischen

Sicherheit

- 58** Zugriff auf Scada-Netze über die Cloud: Entlastung im Wartungsfall
- 60** Schwachstellen in Industrienetzen: Einfallstore schließen
- 62** Verschlüsselung für Fertigungsnetze: Offen aber sicher
- 64** Datenverschlüsselung: Neue Schutzmöglichkeiten
- 65** Industrieanlagen ganzheitlich schützen: Rundumblick für die Sicherheit

Service

- 3** Editorial
- 66** Vorschau, Inserenten & Impressum

CC-Link IE ermöglicht Industrie 4.0 mit offenem Gigabit Ethernet
Seite 39



Bild: CLPA Europe



Prozessabsicherung mit neuer Asset-Management-Funktionalität

Mehr Transparenz für die Anlage

Bild: Profibus Nutzerorganisation e.V.

Mit der neuen Asset-Management-Funktion lässt sich eine Profinet-Anlage noch produktiver gestalten, indem sich alle Komponenten – ob mit Profinet ausgestattet oder nicht – vollständig identifizieren lassen.

Die Bedeutung der sauberen Dokumentation einer Anlage während des Planungsprozesses, der Inbetriebnahme oder auch im späteren Betrieb kann nicht oft genug betont werden. Nicht-stimmige Unterlagen führen jedoch immer wieder zu aufwendigen Aktionen. Viele Anwender setzen daher auf ein automatisiertes Anlagenmanagement, wie es bei Profinet-Komponenten bereits möglich ist. Nun wurde ein neuer Service zur Anlagenerfassung entwickelt, der die bisherigen I&M-Services (Identification & Maintenance) ergänzt. Der Clou: Damit lassen sich auch Anlagenteile – Baugruppen oder Module – erfassen, die nicht mit Profinet modelliert wurden.

Während der Planung, aber auch beim Aufbau einer Anlage bzw. einer Maschine ergeben sich oft zahlreiche Änderungen oder Anpassungen. Selbstverständlich sollten diese unmittelbar in die bestehende Anlagendokumentation übertragen werden. In der Realität funktioniert das aber oft nur unzureichend. Meist arbeiten mehrere Firmen mit vielen Leuten an solchen Planungen zusammen – dies ist ohne Tool-Unterstützung per se schon eine große Fehlerquelle. Eine weitere Fehlerursache: Häufig greifen Anlagenplaner auf vorhandene Dokumentationen von ähnlichen Projekten zurück. Dabei kommt es vor, dass zwar aktuelle Geräte ausgewählt, diese aber in der Dokumentation nicht angepasst werden. Während der Inbetriebnahme kommt es dadurch unter Umständen dazu, dass abgekündigte Produkte eingebaut werden müssen, damit die Anlage überhaupt in Betrieb genommen werden kann. Erst später werden diese gegen moderne Geräte getauscht – für

die Betreiber ist dies dreifache Arbeit. Häufig wird daher mit einer Dokumentation gearbeitet, die veraltet ist oder bei der ein Update nicht berücksichtigt wurde. Zudem kommt es oft zu Last-Minute-Änderungen während der Inbetriebnahme. Typisch ist etwa, wenn ein Kabelkanal doch nicht so verlegt werden konnte wie geplant. Dies führt zu weitreichenden Änderungen, deren Dokumentation sehr aufwändig ist und dies zu einem Zeitpunkt, an dem eigentlich kein Anlagenplaner den Kopf dafür frei hat. Die meisten wissen jedoch aus eigener Erfahrung, dass sich diese Unstimmigkeiten durch den gesamten Lebenszyklus einer Anlage ziehen. Spätestens wenn Wartungen oder Reparaturen nicht geplant durchgeführt werden können, weil das falsche Ersatzteil bestellt wurde, wünscht sich wohl jeder eine einfachere und sichere Dokumentation. Viele Anwender wünschen sich daher eine automatische Datenerfassung und -aktualisierung und zwar von allen Komponenten.

Automatisiertes Anlagen-Management

Die Asset-Identifikation von Profinet bietet bisher schon eine ganze Reihe an Unterstützung, so lässt sich die Anlagentopologie erfassen, Geräte, Module und Submodule automatisiert identifizieren. Problematisch ist allerdings der Umgang mit Nicht-Profinet-Komponenten, sprich Baugruppen, Modulen, elektromechanische Komponenten oder Firmware-Komponenten. „Mit den bisherigen Mitteln ist eine Asset-Identifikation von Nicht-Profinet-Komponenten unmöglich. Wir mussten also überlegen, mit welchen Methoden wir diese zusätzlichen Komponenten abbilden“, erklärt Günter Steindl, Principal Engineer bei Siemens und stellvertretender Leiter im Profinet-Arbeitskreis der PNO. „Wir haben kurz überlegt, ob man dies mit bestehenden Verfahren lösen kann. Es war jedoch nicht möglich, daher haben wir uns entschlossen, ein neues Verfahren für eine automatisierte Anlagenerfassung zu entwickeln.“ Mit der Einführung eines Services zur Anlagenerfassung (abgebildet auf den Asset Management Record (AMR)) werden die bisherigen Services zu Identification & Maintenance (I&M) ergänzt. Damit ist ein automatisiertes standortweites Anlagen-Management möglich, und zwar auch von Komponenten, die nicht über Profinet modelliert wurden

Beispiel aus der Praxis

Ein Beispiel aus einer typischen Fertigungsanlage im Automobilbau zeigt, welche Informationen und Daten eine solche automatisierte Anlagenerfassung liefern kann. Die Anforderungen sind hoch: Dabei sollen alle verbauten Geräte, inkl. ihrer verbauten Module, Submodule und nachladbarer Software-Pakete erfassen, unabhängig davon, ob sie nun über Profinet modelliert

wurden oder nur angeschlossen. Zusätzlich sind neben den bereits verfügbaren Geräte- und Netzwerkparametern, sowie I&M-Daten auch Topologieinformationen und Ethernet-Statistikdaten interessant. Derzeit werden verschiedene Tools verwendet, um an diese Daten heran zu kommen. Typisch für eine Anlage in der Automobilindustrie sind viele IO Devices, aber auch zahlreiche I/O-Module, Ventilinseln oder Komponenten für die Sicherheitstechnik. Es werden aber auch Ethernet-Geräte zur Energiemessung oder zur Netzwerkd Diagnose eingesetzt. Welche Informationen werden nun aber benötigt? Wichtig ist etwa, ob wirklich alle geplanten und bestellten Geräte verbaut wurden, da es zunächst nicht auffallen würde, wenn z.B. ein Gerät zur Netzwerkd Diagnose fehlt. Die Anlage würde trotzdem laufen. Auch für die Verkabelung wünschen sich die Anwender detaillierte Informationen, etwa, ob die Ports richtig ausgelegt wurden. Hier wird in der Regel die geplante Ethernet-Topologie in die Tools eingelesen und mit der Ist-Topologie verglichen. Sind die dokumentierten Daten nicht korrekt, ist die Fehlersuche schwierig. Ein anderes Beispiel sind Prozessgeräte, die in der Regel aus Zuführeinheit, Panel, Zentraleinheit und Profinet-Anschaltung bestehen. „Bei dem Prozessgerät wird heute jedoch nicht die Firmwareversion des Prozessgerätes eingelesen, sondern nur die der Profinet-Anschaltung angegeben. Das hilft einem nicht weiter, da diese für die Funktion nicht entscheidend ist. Bei Schaltnetzteilen oder Bediengeräten werden die Firmware-Stände häufig überhaupt nicht erfasst“, so Steindl. Bei über 1.000 Robotern und 1.000 Prozessgeräten in einer typischen Fertigungsanlage in der Automobilindustrie die jeweils gültige Software-Version zu ermitteln und die Anlagendokumentation mit der Anlage konsistent zu halten, ist damit schlichtweg nicht möglich.



Bild: Profibus Nutzerorganisation



Im Zuge des Verfahrens für automatisierte Anlagenerfassung entstand u. a. eine neue Spezifikation, eine praxisnahe Guideline und die Zertifizierung wurde angestoßen.

Bild: Profibus Nutzerorganisation

Vorteile im praktischen Betrieb

Ganz anders würde sich die Situation mit einem automatisierten Asset Management darstellen. Denn die immer aktuelle Maschinendokumentation bringt erhebliche Vorteile für den Anlagen- bzw. Maschinenbauer, etwa bei der Abnahme: Vor der Übergabe an den Kunden wird über die Asset-Management-Funktion der Ist-Zustand erfasst, mit dem erlaubten Soll-Zustand verglichen und im „Gut Fall“ als Teil der Maschinendokumentation abgelegt. Oder wie es Steindl praktisch ausdrückt: „Sie müssen nicht mehr durch die Anlage kriechen und Kabel, Ports und Baugruppen zählen.“ Im Betrieb wird regelmäßig über die Asset-Management-Funktion der Ist-Zustand mit dem erlaubten Soll-Zustand verglichen. Im „Gut Fall“ wird der Ist-Zustand als Teil des Änderungsmanagements abgelegt und dient als Vergleichsgrundlage für täglich bzw. wöchentlich laufende Anlagen-Scans. Auch für den Rückruf von Komponenten oder Versionen wurden Ideen eingebracht. Bisher kann man in solchen Fällen die Komponenten in einem Betrieb noch nicht automatisch abfragen. Wenn ein Geräteelieferant nun aber weiß, dass ein Gerät in überschaubarer Zeit Schwierigkeiten machen könnte, ist es mithilfe der automatisierten Anlagenerfassung einfach möglich, die betroffenen Komponenten im Rahmen des Anlagen-Scans zu identifizieren und den Aufwand für einen Austausch zu beziffern, bzw. diesen Austausch besser zu planen. Steindl nennt einen realen Fall, der in einer elektromechanischen Komponente auftrat: Eine Baugruppe hatte Kontaktfedern, die in einer Umgebung mit aggressiven Gasen in der Luft stärker als definiert korrodierten. Damit war ein stabiler Anlagenbetrieb nicht mehr möglich (sporadische Kontaktfehler). Dieser Fehler betraf jedoch nur eine kleine Charge von Baugruppen, die zu tauschen waren. Nur mit Hilfe der Asset-Management-Daten ließen sich die betroffene elektromechanische Komponente in der Anlage finden, ohne alle möglicherweise betroffenen Stationen zerlegen zu müssen, um die Typschilder zu prüfen. Ähnliche Vorteile zeigen sich bei der Lageroptimierung. Mit den Informationen aus den Anlagen-Scans können nicht mehr benötigte Komponenten ermittelt oder Ausgäbe-

stände korrigiert werden. „Mit der Ist-Erfassung lassen sich ältere oder nicht benötigte Ersatzteile einfach aus den Listen herausnehmen“, so Steindl. Interessant sind die Funktionen auch für den Abgleich bei Qualitätsschwankungen in der Produktion. So lassen sich die Produktionsdaten über den tagesaktuellen Anlagen-Scan Daten abgleichen, um etwa den Einfluss von Komponenten auf die Produktionsqualität zu erkennen oder auszuschließen. Werden Komponenten identifiziert, können diese aus dem Produktionspfad entfernt (diese Maschine bis zur Reparatur nicht mehr nutzen) oder schnellstens getauscht werden. Produkte, die mit Hilfe dieser Komponente produziert wurden, können bei Bedarf überprüft werden.

Zusammenfassung und Ausblick

Um solche Herausforderungen baldmöglichst auf elegante Art zu lösen, wurde das neue Verfahren für eine automatisierte Anlagenerfassung entwickelt. Dabei wurden von Anfang an die Technologie-Provider miteinbezogen. In diesem Rahmen entstanden im April 2016 eine neue Spezifikation, eine praxisnahe Guideline und die Zertifizierung wurde angestoßen. Nun sind sowohl die Profinet-Spezifikation als auch die Topology and Asset Discovery (TAD)-Guideline verfügbar. Letztere steht kostenlos auf der PI-Homepage zum Download bereit und gibt viele praktische Hinweise. Damit sollten nicht nur Tool-Hersteller die neuen Funktionen schnell und einfach integrieren können. Weiter sind erste I/O-Devices verfügbar und auch die I/O-Controller sind bereits mit den neuen Asset-Management-Funktionen ausgestattet. Die Technologie-Provider bieten seit Anfang 2017 passende Profinet-Stacks an und geben gerne Auskunft. Mit der neuen Asset-Management-Funktion lässt sich eine Profinet-Anlage noch produktiver gestalten, indem sich alle Komponenten, ob mit Profinet ausgestattet oder nicht, vollständig identifizieren lassen. ■

Autor: Sabine Mühlkamp,
freie Journalistin,
Profibus Nutzerorganisation e.V.
www.profibus.com



Halle 2
Stand 539

Sercos Monitor in neuer Version vorgestellt

Die Nutzerorganisation Sercos International stellt eine neue Version des Sercos Monitors als kostenlosen Download zur Verfügung. Das Diagnose-Tool wird kontinuierlich weiter entwickelt, um Anbietern und Anwendern eine umfassende und detaillierte Analyse des Datenverkehrs in Sercos-III-Netzen zu ermöglichen. Die Sercos Monitor Version 3.3.3 beinhaltet eine Vielzahl funktionaler Erweiterungen, aber auch Verbesserungen der Benutzerfreundlichkeit beispielsweise durch Einführung von Drag&Drop-Mechanismen. Neue Features sind unter anderem verbesserte Analysemöglichkeiten für den HotPlug, die Weiterentwicklung der Oszilloskopfunktion, Signalexport während der Aufzeichnung und eine erweiterte S/IP-Unterstützung.

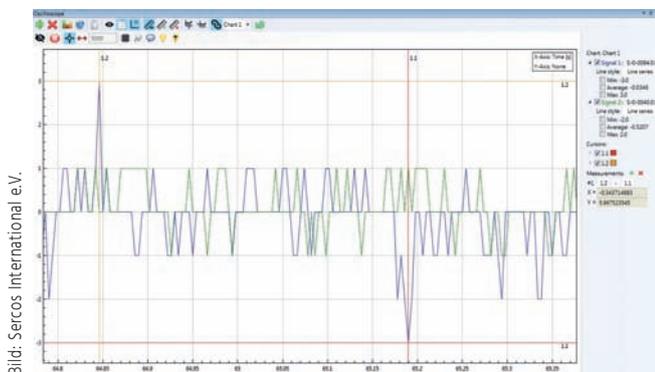


Bild: Sercos International e.V.

Der Sercos Monitor kann in der neuen Version auch als reine Konsolapplikation ohne grafische Oberfläche bedient werden.

Sercos International e. V.
www.sercos.de



Halle 2
Stand 440

Neuer Profidrive-Profiltester verfügbar

Der Profidrive-Profiltester ist ab sofort in Version 5 verfügbar. Das Profinet-basierte Tool prüft die Konformität eines Antriebs zum Profidrive-Profil. Dazu stellt es verschiedene Testfälle für bestimmte unterstützte Anwendungsklassen zur Verfügung. Zudem können Geber und deren Konformität mit dem Encoder-Profil getestet werden. Der neue Profidrive-Profiltester bietet eine neue Benutzeroberfläche, einen Geschwindigkeits- und Positionsinterpolator, schnellere azyklische Datenkommunikation sowie die Filterung von Testskripten nach Anwendungsklassen. Zudem wird isochroner Echtzeitbetrieb unterstützt.

Profibus Nutzerorganisation e. V.
www.profibus.de



Halle 2
Stand 539

Auszeichnung für TSN-Testbed

Das TSN-Testbed des IIC wurde auf dem IoT Solutions World Congress 2017 in Barcelona mit dem Testbed Award ausgezeichnet. 2016 hatte das Konsortium ein erstes TSN Testbed bei National Instruments in den USA aufgebaut. Dieses Jahr wurde entschieden, in Deutschland eine zweite Version des Testbeds aufzubauen, um für die schnell wachsende europäische Community eine räumlich nahe Testmöglichkeit zu schaffen. Bosch Rexroth stellt dafür die Räumlichkeiten und die Infrastruktur zur Verfügung. Die Jury bewertete dieses neu aufgebaute TSN-Testbed als bestes von elf nominierten Testbeds. Inzwischen

finden am Rexroth-Standort Erbach regelmäßig Plug-Feste statt. Aktuell erarbeitet das Unternehmen gemeinsam mit Partnern im IIC TSN Testbed die Grundlagen für eine einfache, anwenderfreundliche Konfiguration.



Bild: Bosch Rexroth AG

Das TSN-Testbed des IIC hat den Testbed Award auf IoT Solutions World Congress in Barcelona gewonnen.

Bosch Rexroth AG
www.boschrexroth.com



Halle 7
Stand 450

Viertes AutomationML-PlugFest

Im Oktober 2017 kamen rund 50 Anwender und Entwickler von 29 Unternehmen und Forschungseinrichtungen zum AutomationML PlugFest zusammen. Die Teilnehmer aus Deutschland, Finnland, Frankreich, Japan, Schweden, Tschechien und den USA waren zu Gast in Berlin bei der Firma Inpro. Das PlugFest bot den Teilnehmern neben Vorträgen von Anwendungsexperten die Möglichkeit, selbst Lösungen zu programmieren sowie bestehende Lösungen zu testen und Entwurfsdaten zwischen diesen auszutauschen. Hierbei standen erfahrene Trainer zur Seite, um gemeinsam Konzepte zur einfachen, schnellen Umsetzung von Werkzeugschnittstellen sowie zur gemeinsamen Definition von Semantiken zu besprechen und zu testen.

AutomationML e. V.
www.automationml.org



Halle 6
Stand 230

SPS IPC Drives 2017: Jahres-Highlight für elektrische Automatisierung

Die SPS IPC Drives ist Treffpunkt Nummer 1 für elektrische Automatisierung in Europa. Vom 28. bis 30. November informieren Automatisierungsanbieter aus aller Welt in Nürnberg über Produkte, Innovationen und Trends der Branche. Die Messe bietet eine Plattform für die Suche nach den richtigen Lösungen für Automatisierungsaufgaben. Das Thema Industrie 4.0 entwickelt sich von der Vision zur Realität und ist erneut ein Schwerpunktthema der Messe. Neben themenbezogenen Sonderschauflächen, Vorträgen, vielen Produkten und Applikationsbeispielen zur digitalen Transformation erhält die Halle 6 eine inhaltliche Neuausrichtung, die verstärkt auf die Herausforderungen in der Fertigungstechnik eingehen wird. Die Messe bietet zudem einen kompletten Marktüberblick und zeigt alle Komponenten bis hin zu kompletten Systemen und integrierten Automatisierungslösungen.

Mesago Messe Frankfurt GmbH
www.mesago.de/sps

Äußerst präzise. Äußerst schnell.

Die neue Messtechnik-Generation
der Beckhoff EtherCAT-Klemmen.



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

sps ipc drives



Halle 7,
Stand 406

www.beckhoff.de/EL3751

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

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

New Automation Technology

BECKHOFF

Modulares Feldbussystem mit Powerlink

Bild: SMC Pneumatik GmbH



Die SI-Einheit von SMC verfügt über die Schutzart IP67.

Die SI-Einheit der Serie EX600 von SMC unterstützt jetzt auch den Ethernet-Powerlink-Standard. Die vollständig modular aufbaubaren Kommunikationsplattformen der Serie lassen sich mit digitalen und analogen Eingangs- und Ausgangsmodulen, einer Zählfunktion für die Betriebszyklen sowie einer Selbstdiagnosefunktion ausstatten. Bis zu neun I/O-Module lassen sich mit der Einheit verbinden. Mit der Schutzart IP67 ist sie auch für den dezentralen Einsatz geeignet. Durch die Möglichkeit, die Kommunikationsplattform mit dem Kommunikationsstandard Powerlink auszurüsten, erhalten Anwender große Freiheit in der Wahl ihrer Netzwerktopologie. Mit Powerlink lassen sich Topologien wie Stern, Ring oder Linie sowie Kombinationen realisieren. Außerdem läuft die Kommunikation in Echtzeit. Neben Powerlink unterstützt die Plattform auch gängige Feldbus- und Industrial-Ethernet-Protokolle wie Profinet, Profibus, Ethernet/IP, Ethercat oder DeviceNet.

SMC Pneumatik GmbH
www.smc.eu

Firewall für dezentrale Anlagenstrukturen

Der Zweck der Firewall Wall IE von Helmholz ist es, Maschinen- und Schaltschrankbauer effizient und zeitsparend bei ihrer täglichen Arbeit zu unterstützen. Das Unternehmen bietet Anwendern die individuelle und projektspezifische Konfiguration der Firewall darüber hinaus als Serviceleistung an. Diese bekommen so die für das jeweilige Projekt konfigurierte Firewall bereits einsatzbereit geliefert. Das Gerät samt fertiger Netzwerkkonfiguration muss anschließend nur noch auf der Hutschiene befestigt und die Spannung angelegt werden. Die kleine smarte Firewall wurde speziell für die Anwendung in industriellen Automatisierungsnetzwerken entwickelt. Ihre Baugröße ist auch für die Verwendung in einer dezentralen Anlagenstruktur geeignet. Denn der Schutz von Automatisierungsnetzen in unterschiedlichen Anwendungsszenarien ist ein wesentlicher Bestandteil der digitalen Welt von heute.



Bild: Helmholz GmbH & Co. KG

Helmholz liefert die Firewall Wall IE einsatzbereit konfiguriert aus.

Helmholz GmbH & Co. KG
www.helmholz.de

 **Halle 7**
Stand 404

Elektronikplattform um IO-Link-Modul erweitert

Emerson hat seine Asco-Numatics-Feldbus-Elektronikplattform der Baureihe 580 um das Kommunikationssystem IO-Link erweitert. In Verbindung mit den Ventilinseln der Baureihe Asco Numatics500 bietet das neue IO-Link-Modul eine kosteneffiziente und zuverlässige Lösung zur Steuerung von Magnetventilen. Denn eine direkte, digitale Datenübertragung mittels einer modernen Steuerung und ereignisgesteuerte Diagnosemöglichkeiten über ein IO-System sind wichtige Voraussetzungen für die vorausschauende Wartung im Rahmen von Industrie 4.0. Die IO-Link-Module sind mit allen Ventilinseln der Serien 501, 502 und 503 kompatibel. Diese liefern bei einer Baubreite von 11, 18 und 26mm einen Durchfluss von 400 bis 1400l/min. Erhältlich ist darüber hinaus auch eine Grundplatte, über die sich zwei verschiedene Drücke gleichzeitig verarbeiten lassen. Dadurch vereinfacht sich die Installation, verschiedene Ventile und Pneumatik-elemente lassen sich über eine Ventilinsel steuern.



Bild: Asco Numatics GmbH

Das neue IO-Link-Modul dient der Steuerung von Magnetventilen.

Asco Numatics GmbH
www.asconumatics.de

 **Halle 2**
Stand 539

Echtzeitdaten vor Ort analysieren



Bild: Bosch Rexroth AG

Mit dem Data Analytics Server präsentiert Bosch Rexroth eine schlüsselfertige Analyse- und Monitoring-Lösung für Neu- und Bestandsmaschinen. Erfasste Echtzeitdaten lassen sich damit maschinennah speichern, auswerten und übersichtlich visualisieren. Predictive Maintenance und andere I4.0-Use-Cases lassen sich schnell und einfach mittels regelbasierter Aktionen über die Web-Oberfläche des Servers erstellen. Die herstellerunabhängige Kommunikation mit Sensoren, Steuerungen und übergeordneten IT-Systemen erfolgt über die offenen Standards OPC-UA und PPMP. Im Paket mit dem IoT Gateway des Unternehmens erzielt der Server hohe Konnektivität, z.B. bei der nachträglichen MES-Anbindung nichtvernetzter Bestandsanlagen.

Bosch Rexroth AG
www.boschrexroth.com

 **Halle 7**
Stand 450

Gigabit-Ethernet-Switches für die Wandmontage



Bild: StarTech.com Ltd.

Die vier Ethernet-Switches von StarTech.com verfügen über Schutzart IP30.

StarTech.com hat vier neue Gigabit-Ethernet-Switches für industrielle Zwecke auf den Markt gebracht. Jeder der Switches ist für die Wandmontage geeignet und mit zusätzlichen Eigenschaften ausgestattet, wie intelligentem Layer-2-Management, das Nutzern mehr Flexibilität und Kontrolle beim Verwalten ihrer Netzwerke gibt. Die Switches ermöglichen die Erweiterung der Netzwerke durch den Anschluss von bis zu acht RJ45-Geräten. Mit den 8-Port-Switches können bis zu acht Benutzer über eine LAN-Verbindung Dateien und Geräte gemeinsam benutzen, indem die vorhandene Netzkapazität mit zusätzlichen Ports erweitert wird. Das stellt eine geeignete Lösung für viele Kommunikationsanwendungen dar. Das robuste und kompakte Design eignet sich für raue Industrieumgebungen. Die Schutzart der Metallgehäuse beträgt IP30.

StarTech.com Ltd.
www.startech.com

Kompakte I/O-Module mit Isolierung auf Spannungsversorgungsseite

Die kompakte Bauform der I/O-Module Tiny ModusRT von ICPDAS sorgt für eine einfache Installation auf kleinem Raum. Die Kommunikation erfolgt entweder über das ModbusRTU-Protokoll oder über das einfache DCON-Protokoll (ASCII) des Unternehmens. Die 20 verschiedenen Modulvarianten sind mit analogen und digitalen Ein- und Ausgängen sowie Relaisausgängen ausgestattet. Die große Auswahl sorgt für hohe Flexibilität und bietet für viele Applikationen eine passende Lösung. Die Konfigurationsoptionen der Einschaltwerte und die Einstellung der Safe Values sorgen für einen stabilen Betrieb der Anwendung, auch bei möglichen Störungen. Zusätzliche Sicherheit verschafft die Isolierung auf Spannungsversorgungsseite.



Bild: ICPDAS-Europe GmbH

Die TM-Serie von ICPDAS hat einen Temperaturbereich von -25 bis +75°C.

ICPDAS-Europe GmbH
www.icpdas-europe.co

- Anzeige -



sps ipc drives
Nürnberg, 28. - 30.11.2017
Halle 7, Stand 115



IBH Link S7++

IBH Link S7++ HS

Ethernet / MPI® / Profibus-Konverter für SIMATIC® S7-200® / 300® / 400®



Die kostengünstige Alternative zum CP-Kommunikationsprozessor oder zum IE/PB Link.

- CommDTM frei verfügbar
- Master Klasse 2 für azyklische Dienste (DPV1)
- Parametrierung von Feldgeräten und Antrieben (DPV1)
- S7-Verbindungen (RFC1006) direkt und geroutet, auch für Bedienpanels
- SPS <> SPS Kommunikation, auch über Subnetzgrenzen hinweg
- Windows 10 Unterstützung
- TIA Integration
- Hochsprachen-Zugriff
- Online auf SIMATIC® S5 über SINEC L2



MPI®, SIMATIC®, S7-200®, S7-300® und S7-400® sind eingetragene Warenzeichen der Siemens Aktiengesellschaft, Berlin und München. © 2017 IBH softec, ein Tochterunternehmen der Microsoft Corporation in den USA und/oder anderen Ländern.

Lüfterlose Computer für die Prozessautomation

Bei den lüfterlosen Computern der PICE3800-Serie von Plug-In Electronics handelt es sich um rechenstarke und robuste Rechner für die industriellen Anforderungen im Bereich der Prozessautomation. Die Serie ist als IoT-Edge-Server-Lösung für industrielle Unternehmen konzipiert, die mit hochleistungsstarken Multi-Core-Prozessoren der sechsten Intel-Generation ausgestattet ist. Die Bauweise eignet sich durch die Skalierbarkeit für die Beaufsichtigung von Sensoren, die laufend große Mengen an Daten für die Bewegungssteuerung speichern sowie für die Durchführung von CAD-/CAM-Anwendungen bei der Darstellung von Grafiken und Animationen zur Überwachung von Prozessen im Zusammenhang mit Produktionsanlagen. Intel HD Graphics Engine ermöglicht es zudem 2D- und 3D-Visuals durchzuführen, um unterschiedliche Geschwindigkeiten und Präzisionsanforderungen zu erfüllen.



Die lüfterlosen Computer von Plug-In Electronic sind mit bis zu vier USB3.0-Ports und drei GbE-LAN-Ports ausgestattet.

Plug-In Electronic GmbH
www.plug-in.de

Industrie-4.0-Gateway in digitaler Fabrik



In der digitalen Fabrik von Membrain werden an verschiedenen Stationen des Shop Floors beispielhaft Anwendungen gezeigt.

Membrain hat ein neues Industrie-4.0-Gateway vorgestellt. Der Kommunikationsserver MembrainRTC (Real-Time Communicator) bildet dabei das Herz der Anwendung und ist zugleich eine flexible und kostengünstige Lösung zur Integration unterschiedlicher Systeme. Die unmittelbare Anbindung und Integration z.B. von Maschinensteuerungen, Scannern oder RFID-Readern sorgt dabei dafür, dass sich beliebige, zum Teil vollautomatische Anwendungen, realisieren lassen. Durch die Integration weiterer Komponenten wie elektronische Steuerung, Fördertechnik, Waagen, Drucker oder Ampeln lassen sich relevante Informationen direkt an das führende

ERP übermitteln. Das führt unmittelbar zu vereinfachten, beschleunigten und sicheren Abläufen. In einer digitalen Fabrik auf der Unternehmens-Website zeigt das Industrie-4.0-Gateway, wie sich vom Wareneingang über die unterschiedlichen Produktionsstufen bis hin zum Warenausgang Digitalisierungsprozesse beschleunigen und gleichzeitig die Effizienz steigern lassen. Live-Daten können so aus der Produktion bzw. einer Maschine melden, wenn ein Auftrag abgearbeitet ist. Die Information über Gutmengen und Ausschuss werden zudem direkt an das führende ERP-System übermittelt und weiterverarbeitet.

Membrain GmbH
www.membrain-it.com

IoT-Gateways für die Vernetzung von Maschinen und Prozessen

Janz Tec hat sein Embedded-PC-Portfolio erweitert und die IoT-Gateway-Serie EmIOT auf den Markt gebracht. Sie ergänzt die EmPC-Produktlinie um speziell für die Vernetzung von Maschinen und Prozessen konzipierte Systeme als Grundlage für IIoT-Anwendungen. Alle IoT-Gateways sind optional auch mit maßgeschneiderten Industrial Security Features aus dem Security Eco System Toolkit verfügbar. Als erste Produkte der IoT-Gateway-Serie stellt das Unternehmen den EmIOT-A/iMX6 und EmIOT-X vor, denen bald beginnend mit dem EmIOT-Edge auch kleinerformatige Systeme nachfolgen. Die Systeme bieten als Edge Gateways alternativ verschiedene kabellose Schnittstellen an. So sind gängige Mobilfunktechnologien wie GPRS, UMTS und LTE verfügbar. LPWAN-Technologien, wie LTE NB-IoT for Industrial IoT solutions, sind ebenso möglich wie WLAN-Anbindungen für interne Netzwerkanwendungen. Die Edge Gateways zeichnen sich zudem dadurch aus, dass sie die Aufgaben mehrerer Geräte bündeln. Sie können über verschiedene Feldbusse kommunizieren und Daten bidirektional austauschen. Weiterhin ermöglichen zusätzliche Schnittstellen die Datenerfassung von externen Sensoren für die Überwachung einer Anlage. Die skalierbar designte Hardware-Plattform der Serie basiert auf den bisherigen Embedded-PC-Serien des Unternehmens. Damit bietet sie umfangreiche Anpassungsmöglichkeiten an spezielle Anforderungen bezüglich Performance, Umgebungsbedingungen oder benötigten Mengenschaffeln.



EmIOT-A/iMX6 und EmIOT-X sind die ersten Modelle aus der neuen IoT-Gateway-Serie von Janz Tec.

Janz Tec AG
www.janztec.com



Halle 7
Stand 591

Die Zukunft von CANopen FD

„Add-on für CANopen“

Mit der Einführung von CAN FD wurde das klassische CAN-Protokoll hinsichtlich einer höheren Übertragungsrates und mehr Nutzdaten pro Nachricht verbessert. Ende September gab die Nutzerorganisation CAN in Automation (CiA) die Spezifikation CiA1301 heraus. Sie behandelt die CANopen-FD-Anwendungsschicht und das CANopen-FD-Kommunikationsprofil. Uwe Koppe (Technischer Direktor, CiA), Christian Schlegel (Business Direktor, CiA) und Reiner Zitzmann (CiA-Geschäftsführer) haben mit dem INDUSTRIAL COMMUNICATION JOURNAL über die nächsten Schritte bei CAN gesprochen.

icj CAN FD ist international standardisiert und der CiA stellt einige erste Empfehlungen für CAN-FD-Geräteentwicklung und -Systemdesign bereit. Was brauchen CAN-FD-Anwender im industriellen Umfeld darüber hinaus?

Koppe: Aus meiner Sicht sollte eine Richtlinie entwickelt werden, die eine Kombination der Bitraten von Arbitrierungs- und Datenphase, zusammen mit Topologie-Beschränkungen wie der maximalen Leitungslänge, empfiehlt. So könnten Anwender eine Erweiterung für bereits vorhandene Netzwerke abschätzen. Außerdem hätten sie eine Vorgabe für die nächste Generation ihrer Maschinensteuerungen.

Schlegel: Beim klassischen CAN müssen die Anwender die physikalischen Parameter des Kabels nicht sonderlich berücksichtigen. Fast jedes Kabel ist eigentlich gut genug. Mit CAN FD und seiner höheren Übertragungsrates wird das Kabel aber ein wesentlicher Bestandteil. Es darf etwa keine Impedanz-Sprünge geben. Deshalb muss man unter anderem das Isolationsmaterial sorgfältig auswählen. Hier brauchen wir klare Spezifizierungen. Hierzu sollte die CiA mit den Kabelherstellern zusammenarbeiten, um spezielle Kabeltypen für CAN FD zu definieren.

Zitzmann: Aus der Spezifizierungssicht fehlen immer noch umfassende Implementierungsrichtlinien sowie Anwendungshinweise für die System- und Geräteentwicklung. Die Systementwickler würden außerdem eine detaillierte Kabelspezifikation begrüßen. Deswegen entwickelt die CiA Dokumente, um System- und Geräteentwicklern CAN FD in ihren Anwendungen zu ermöglichen. Passende CAN-FD-Hardware ist derzeit nur für die Entwickler verfügbar. Eine große Anzahl an Halbleiter- und Tool-Herstellern hat bereits CAN-FD-Produkte vorgestellt. Die Verfügbarkeit von geeigneten Geräten und Netzwerkkomponenten ist eine Voraussetzung für Systementwickler, um CAN FD in ihren zukünftigen Anwendungen in Betracht zu ziehen.

icj Die CANopen-FD-Spezifikation wurde Ende September CiA-intern herausgegeben. Was sind die größten Vorteile im Vergleich zum klassischen CANopen?

Koppe: Ich kann mir vorstellen, dass für die meisten Anwender die Geschwindigkeit und größere Nutzlast von CANopen FD im Fokus stehen. Ich glaube jedoch, dass die zusätzlichen Funktionen ebenso wichtig sind. Die allerwichtigste Änderung ist die Einführung des

USDO-Dienstes. Er ermöglicht neben Unicast- auch Multicast- und Broadcast-Kommunikation zwischen CANopen-Geräten. Es ist nun möglich mit einem Request Daten an alle CANopen-Geräte eines Netzwerks zu senden.

Schlegel: CANopen FD zieht vor allem einen Nutzen aus den vom CAN-FD-Protokoll und von der CAN-FD-Hardware zur Verfügung gestellten Möglichkeiten: erstens die Erweiterung der maximalen Länge einer Nachricht von 8 auf 64 Nutzdatenbytes, was sich auch in der überarbeiteten PDO-Spezifikation von CANopen FD widerspiegelt, und zweitens der Erhöhung der maximalen Datenrate von 1 auf derzeit 5Mbit/s während der Übertragung von Nutzlastdaten. Nebenbei konnte die Restfehlerwahrscheinlichkeit von CAN FD im Vergleich zum klassischen CAN sogar gesenkt werden. Eine weitere Verbesserung ist die Einführung von einem neuen SDO-Dienst sowie dem zugehörigen Protokoll Universal Service Data Object, kurz USDO. Es verwendet eine effizientere Segmentierung von langen Daten und bietet außerdem Funktionen wie Routing von Daten in andere CAN-FD-Netzwerksegmente.

Zitzmann: CANopen FD kann als Add-on für klassisches CANopen betrachtet werden. Es wahrt alle Vorteile des etablierten CANopen und behält somit alle seine Eigenschaften, wie die übersichtliche Gerätearchitektur, hohe Flexibilität in der Entwicklung und die Möglichkeit robuster Hardware-Plattformen mit sehr geringem Stromverbrauch. Der durch die CAN-FD-Hardware bereitgestellte Funktionsumfang ermöglicht es CANopen FD, auch zukünftig den Anforderungen an eingebettete Netzwerke gewachsen zu sein. Verlängerte PDOs ermöglichen einen schnellen Transport von Prozessdaten bis zu einer Länge von 64Byte. Auf der einen Seite erleichtert das die hohe Nachfrage an Daten zu bedienen, die z. B. in IIoT-Anwendungen besteht. Auf der anderen Seite profitieren auch Anwendungen in denen die Themen funktionale Sicherheit und Security eine Rolle spielen, von dem durch CAN FD bereitgestelltem, längerem Nutzdatenfeld. In einem PDO ist jetzt ausreichend Platz, um neben den Prozessdaten z. B. auch eine Signatur zur Identifikation der korrekten Datenquelle, zu übertragen. In vielen Anwendungen ist das Netzwerk nicht statisch, sondern wird vom Endanwender durch das Hinzufügen oder das Entfernen von Geräten modifiziert. Das in CANopen FD neu eingeführte USDO trägt dieser Entwicklung Rechnung.

Was sind die nächsten Schritte, um CANopen FD in verschiedenen Anwendungsgebieten erfolgreich zu machen?

Koppe: Eine gute Marketing-Kampagne mit Workshops und Schulungen für CiA-Mitglieder.

Schlegel: Es ist sehr wichtig, dass die Halbleiterhersteller CAN FD-fähige Mikrocontroller für industrielle Anwendungen anbieten. Es gibt zwar bereits Mikrocontroller mit CAN-FD-Schnitt-



„ Wenn die richtigen Mikrocontroller zur Verfügung stehen, wird sich der Erfolg von CANopen FD von alleine ergeben.

Christian Schlegel, Business Direktor der CiA

Bild: CAN in Automation (CiA) GmbH

stellen; allerdings sind diese eher auf komplexere Anwendungen und Steuergeräte in Autos ausgelegt. Das bedeutet, diese Mikrocontroller haben einige Schnittstellen und Funktionen, die in Geräten für industrielle Anwendungen gar nicht benötigt werden und somit sehr teuer sind. Am Besten wäre es, wenn die bereits vorhandenen Mikrocontroller, um CAN FD erweitert werden würden. Im Grunde ist es wie das Henne/Ei-Problem: Wer war zuerst da? Wenn die richtigen Mikrocontroller zur Verfügung stehen, wird sich der Erfolg von CANopen FD von alleine ergeben.

Zitzmann: Wir müssen die CANopen-Spezifikationen an CANopen FD anpassen. Dies sollte unter der Maßgabe erfolgen, so viele CANopen-Aspekte wie möglich stabil zu halten, aber sie wo notwendig und vorteilhaft anzupassen. Das ist eine Menge Arbeit. Die dringendsten Dokumente sind die XML-basierte Gerätebeschreibung, sowie der Konformitätstestplan. Aber auch eine Anpassung der Spezifikationen für CANopen-Zusatzfunktionen, Layer-Setting-Dienste und Remote-Zugriff auf CANopen-Geräte steht im Fokus. Um die verlängerten PDOs effizient nutzen zu können, benötigen CANopen-FD-Anwender aktualisierte Geräte- und Anwendungsprofile. Diese müssen nun überarbeitet werden.

Werden CANopen-FD-Netzwerke in Konkurrenz zu Ethernet-basierten Lösungen stehen?

Koppe: Der Hardware-Preis für eine Ethernet-basierte Lösung ist etwa drei- bis viermal höher als für CAN FD. Außerdem sollte man auch den höheren Speicherplatzbedarf und Stromverbrauch für Ethernet-basierte Lösungen bedenken. Andererseits hat Ethernet einen höheren Datendurchsatz. Es ist also keine Konkurrenzfrage: Beide Netzwerk-Konzepte werden je nach Anwendungsanforderungen in friedlicher Koexistenz nebeneinander eingesetzt werden.

Schlegel: Sicher wird es einige Märkte und Anwendungen geben, in denen beide Technologien konkurrieren. In große Fertigungsanlagen wo komplexe Maschinen über Fließbänder vollautomatisch Produkte herstellen, ist Ethernet mit seiner hohen Busbandbreite klar im Vorteil. Aber schon bei kleineren Anlagen kann CANopen FD durchaus genügen. CANopen FD ist auch überall dort im Vorteil, wo es um Robustheit und Zuverlässigkeit geht. Die CAN-FD-Hardware, ursprünglich für den Einsatz im Automobil entwickelt, ist nicht nur preisgünstiger als Ethernet, sondern auch für Outdoor-Anwendungen und Batterie-Anwendungen optimiert. Ethernet braucht in der Regel drei- bis fünfmal mehr Energie als CANopen FD. Außerdem benötigt CANopen FD keine aktiven Netzwerkkomponenten wie Router oder Hubs.

Zitzmann: Für jede Anwendung gibt es immer die Frage, welche Art des Kommunikationssystems den Anforderungen entspricht. Einerseits gibt es technische Kriterien wie Robustheit, unterstützte Topologien, Stromverbrauch, Hochlaufzeiten, Nachrichtengeschwindigkeit, Latenzzeiten oder Zykluszeit. Daneben gibt es Kriterien wie Verfügbarkeit von Geräten, unterschiedliche Bezugsquellen und Kosten. Nach einer Analyse aller relevanten Kri-

„ CANopen FD schließt die Lücke im Datendurchsatz zwischen den klassischen Feldbussystemen und Backbone-Netzwerken, die auf Ethernet basieren.

Reiner Zitzmann, CiA-Geschäftsführer



Bild: CAN in Automation (CiA) GmbH

terien für die gewünschte Anwendung, wird in Zukunft CANopen FD ein attraktiver Kandidat für eingebettete und tiefeingebettete Kommunikationslösungen sein. Ich erwarte, dass sich CANopen FD und Industrial Ethernet ergänzen werden. CANopen FD schließt die Lücke im Datendurchsatz zwischen den klassischen, so genannten Feldbussystemen und den Backbone-Netzwerken, die sehr oft auf Ethernet basieren.

Denken Sie, dass es notwendig ist, CANopen FD zu einem Teil des Internet der Dinge zu machen? Gibt es derzeit irgendwelche Tätigkeiten der CiA in dieser Richtung?

Koppe: Um Daten von CAN FD ins Internet zu bekommen, braucht man ein Gateway, welches Kenntnisse über das zugrundeliegende Netzwerk hat, einschließlich des Objektverzeichnisses der CANopen-FD-Geräte. Folglich müssen wir IoT-Methoden definieren, um auf diese Daten zuzugreifen.

Schlegel: Im Rahmen der Industriekontrolle und in Nicht-Automobilanwendungen sehe ich zwei Hauptanwendungsfälle im Zusammenhang mit CANopen bzw. CANopen FD und dem Internet der Dinge: Datenaustausch zwischen der IT- und der OT-Welt

mittels Gateway oder Edge-Controller sowie das Einsammeln von zusätzlichen Diagnose- und Betriebsdaten von den einzelnen Geräten im Netzwerk. Grundsätzlich existieren zwei Protokolle, die stark mit diesen Anwendungen verbunden sind: OPC UA und MQTT. Beide Protokolle sind TCP/IP-basiert und können deswegen nicht direkt mit CANopen benutzt werden. Um eine Verbindung zwischen CANopen FD und dem IoT zu schaffen, ist jedenfalls eine Spezifikation erforderlich, welche definiert wie OPC UA oder MQTT zu CANopen FD abgebildet sind.

Zitzmann: Der erzeugte Mehrwert durch web-basierte Anwendungen steigt: Predictive Maintenance, Condition Monitoring oder die Individualisierung eines Produktes sind nur einige Beispiele. Obwohl eingebettete Systeme wie CANopen nicht im Fokus dieser großen Datenanwendungen sind, stellen sie die Datenbank für die großen Datenanwendungen zur Verfügung. Um den Zugang zu eingebetteten Geräten aus dem Gesichtspunkt einer webbasierten Anwendung zu erleichtern, sind ein standardisierter Arbeitsablauf und der Gebrauch von standardisierten Datenformaten sehr vorteilhaft. CANopen unterstützt das bereits durch seine standardisierte CANopen-Gerätarchitektur und die standardisierten Anwendungsdaten, die in den einzelnen Geräten- und den Anwendungsprofilen angegeben sind. Allgemein ist CANopen FD bereits gut vorbereitet, um CANopen-Netze zu einem Teil des IIoT zu machen.

Wie ist Ihre Ansicht über die Zukunft von CAN-basierten Lösungen in industriellen Anwendungen?

Koppe: Der CAN- und CAN-FD-Markt werden in Zukunft wachsen, weil der Bus eine zuverlässige und robuste Kommunikation zu geringen Kosten anbietet. Außerdem ist es ziemlich einfach, funktionale Sicherheit gemäß EN50325-5 hinzuzufügen. Und schließlich erlaubt die vergrößerte Nutzlast sichere Kommunikation.

Schlegel: Auch in Zukunft werden wir weiterhin CAN-basierte Netzwerke in vielen Bereichen sehen. Basierend auf den bereits erwähnten Fähigkeiten von CAN FD/CANopen FD, gibt es mehrere Märkte und Anwendungen wie Medizintechnik, erneuerbare Energie, Transport, Automaten und kleine Maschinen, eingebettete Steuerungssysteme in Gebäuden, Roboter oder Nutzfahrzeuge. Da in vielen dieser Bereiche serielle Schnittstellen auf mannigfaltige Weise verwendet werden, würde CAN beträchtliche Verbesserungen zu solchen Systemen bringen. Deshalb können wir erwarten, dass sich der Einsatz von CAN noch verbreitern wird.

Zitzmann: Die Automobilindustrie führt im Moment CAN FD ein und plant langfristig, klassisches CAN durch CAN FD zu ersetzen. Auf Grund der von der Automobilindustrie benötigten, hohen Stückzahl an CAN-Komponenten ist davon auszugehen, dass eine ähnlich große Zahl an Varianten von Mikrokontrollern mit CAN FD, von vielen Halbleiterherstellern, angeboten werden wird, wie wir es vom heutigen CAN kennen. CAN-FD-fähige Mikrokontroller können das CAN-Protokoll sowohl im klassischen Format als auch im FD-Format kommunizieren. Auch wenn sie im Moment nur das klassische CAN verwenden, werden sie irgendwann erkennen, dass sie ihre Anforderungen



„CAN- und CAN-FD-Markt werden in Zukunft wachsen, weil der Bus eine zuverlässige und robuste Kommunikation zu geringen Kosten anbietet.“
 Uwe Koppe, Technischer Direktor der CiA

an eingebettete Vernetzung besser erfüllen können, wenn sie die bereits vorhandene CAN-FD-Funktionalität nutzen. CANopen FD wird in diesem Fall in vielen Märkten sicher ein interessanter Kandidat sein, da es nicht nur die CAN-FD-Funktionalität nutzbar macht, sondern CANopen um viele interessante Eigenschaften erweitert.

Firma: CAN in Automation (CiA) GmbH
www.can-cia.org

- Anzeige -

Immer alles im Blick

... ganz ohne Verrenkungen.




sps ipc drives
 Nürnberg
 28.-30.11.2017
 Halle 9, Stand 231

Optimal auf Ihren Schaltschrank zugeschnitten

- 3 industrielle Protokolle werden unterstützt
- 2 Installationsoptionen: Hutschienen- und Rackmontage für verschiedene Schaltschrank-Typen
- 1-seitiges Konfigurations-Dashboard

Moxa Lösungen – intelligent, einfach, sicher.

www.moxa.com

MOXA
 Reliable Networks ▲ Sincere Service

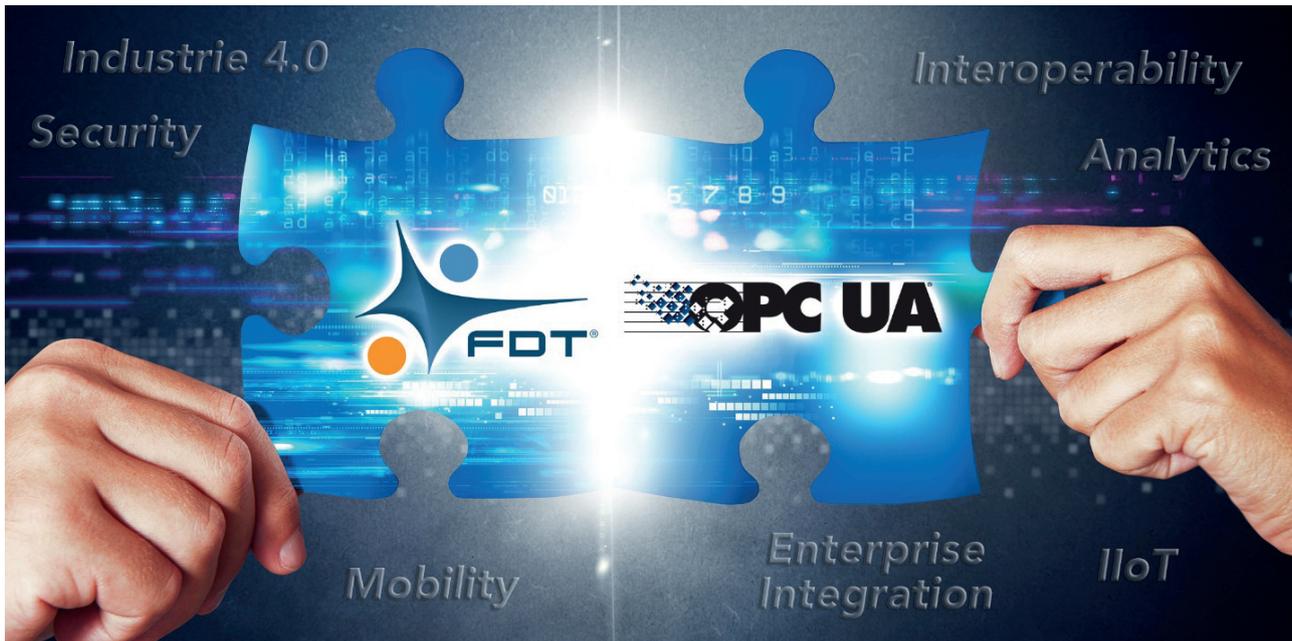


Bild: FDT Group

Vernetzung von IT- und OT-Ebene

Einheitlicher Ansatz

Das Zeitalter der digitalen Transformation nimmt in der Industrie immer konkretere Formen an, u.a. durch die native Integration des OPC-UA-Standards von FDT. Deren Zusammenspiel ermöglicht Informationsmodellierung und fortlaufende Verbesserungen für die Sensor-to-Cloud-Kommunikation und unternehmensweite Vernetzung. Die folgende Artikelserie beschreibt, wie die gemeinsamen Entwicklungen einen einheitlichen Ansatz für die Unternehmensintegration bestärken und die Mobilität von Arbeitnehmern im heutigen, komplexen Industriebetrieb erweitern.

Während der erste Teil des Beitrags die technologische Konvergenz von heute sowie aktuelle Entwicklungen im Bereich der Spezifikationen aufzeigt, widmet sich Teil 2 in Ausgabe 12 des SPS-MAGAZINS der Vereinfachung des Ökosystemaustausches und der Rolle von FDT. Für den erfolgreichen Wettbewerb in einer globalen, wettbewerbsorientierten, schnelllebigen Welt mit zunehmenden Kundenanforderungen müssen alle Arten von Technologie gezielt eingesetzt werden. Ohne einen effektiven Ansatz zur Unternehmensintegration verbleiben all diese Technologien jedoch in Silos und bringen dem Unternehmen keinen Nutzen. Das Industrial Internet of Things (IIoT) ist, gemeinsam mit Industrie 4.0, einer der wichtigsten Trends in der Automatisierung. Durch Verschmelzungen der Bereiche Datenverarbeitung und Kommunikation werden intelligente Geräte die Art der Interaktion zwischen Benutzern und Maschinen sowie die Verflechtung zwischen Maschinen komplett neu definieren.

Technologische Konvergenz von heute

Jedes Unternehmen hat Vorteile davon, sich mit der Integration von Systemen, Anwendungen und Daten zu befassen. Es gibt einen wesentlichen Bedarf an Interoperabilität zwischen Betriebsmitteln unterschiedlicher Anbieter und zwischen verschiedenen Plattformen in der industriellen Umgebung. Wichtigste Anforderungen an eine

aktuelle Automatisierungsarchitektur sind Sicherheit, Zuverlässigkeit und Datenintegration zwischen typischerweise grundverschiedenen Geräten und Anwendungen, die noch nie zuvor miteinander verbunden waren. Seit 2014 arbeiten die FDT Group und die OPC Foundation zusammen, um einen besseren Zugriff auf wichtige Informationen im gesamten Industrieunternehmen bereitzustellen. FDT wird als etablierter Integrationsstandard mit Hunderttausenden FDT/Frame-fähigen Steuerungs- und Asset-Management-Systemen und mehreren zehn Millionen FDT/DTM-fähigen Feldgeräten global eingesetzt. Die OPC Unified Architecture (UA) bietet hingegen eine Infrastruktur, mit der Unternehmensinformationen für beliebige andere Anwendungen und Plattformen bereitgestellt werden können. FDT unterstützt eine Vielfalt von Kommunikationsprotokollen, mittels denen intelligente Instrumente und übergeordnete Systeme verbunden sind, welche mit diesen Geräten interagieren. FDT etabliert eine offene, modulare und holistische Automatisierungsarchitektur, die sich an die wechselnden Anforderungen von Lieferanten und Endbenutzern anpasst. FDT beinhaltet eine Repräsentation der Anlagenhierarchie, die auf einer physischen Netzwerktopologie gepaart mit einer logischen Topologie basiert. Der Standard unterstützt alle wichtigen Kommunikationsprotokolle der Prozess-, Hybrid- und Werksautomatisierung und wird je nach Industrieanforderung auch künftige Kommunikationsprotokolle unterstützen. Durch diesen Ansatz können FDT-basierte Systeme auf transparente

Weise durch grundverschiedene Netzwerke tunneln, um Zugriff zu erhalten, und um mit jedem Endgerät zu kommunizieren.

Komplette Informationsmodellierung

OPC UA konzentriert sich auf die Bereitstellung einer kompletten Informationsmodellierung, die Industriepartnern erlaubt, Nutzen aus einer dienstorientierten Architektur zu ziehen. Diese Architektur ermöglicht, dass zuvor nicht verbundene Geräte und Anwendungen nahtlos zusammenarbeiten. OPC UA ermöglicht zum Beispiel die Verbindung von Client-mit Server-Anwendungen, ohne die Syntax und die Semantik der Daten zu verstehen, die in der Client-Anwendung erfasst werden. Bei diesem Ansatz geht es um die einfache Erkennung der Fähigkeiten des Servers und um die effiziente Nutzung seiner Dienste und Daten. Sowohl FDT als auch OPC sind offene, nicht-proprietäre und unabhängige Standards. Die Fähigkeit von FDT, sich nahtlos in eine Vielzahl von Kommunikationsnetzwerken zu integrieren oder durch sie durchzutunneln, um auf transparente Weise mit Endgeräten zu kommunizieren, veranschaulicht seine zentrale Stellung in einem intelligenten und verbundenen Unternehmen. Die Standardintegration der von FDT/DTM bereitgestellten Informationen in das OPC UA Informationsmodell ist essenziell für die Gerätediagnose, für die Konfiguration und für das Remote-Asset-Management sowie für die MES-Integration. Das FDT/OPC-UA-Informationsmodell verbessert das Management von Netzwerken und Geräten und unterstützt die Vernetzung im Unternehmen, indem es einen Datenzugriff gewährt, ohne eine protokollspezifische Verarbeitung zu erfordern, und eine breite Vielfalt von Geräten unterstützt. OPC UA sorgt für eine einheitliche Schnittstelle für viele verschiedene Client-Anwendungen, wohingegen FDT für eine Netzwerk-/Gerätekonfiguration und einen Zugriff auf Geräte sorgt. Der kombinierte Ansatz von beider Standards ermöglicht die Vereinheitlichung der Systemplanung, -konfiguration und -diagnose.

Aktuelle Entwicklungen bei der Spezifikation

Die Zusammenarbeit von FDT & OPC stellt eine einmalige Gelegenheit dar, um für die Anwendungen und Geräte, die von FDT unterstützt werden, die bestmöglichen Daten- und Informationsmodelle einzusetzen. Es wird ermöglicht, die Informationsmodellierung von OPC UA und entsprechende Dienste für eine vollständige Application-to-Device-Integration zu nutzen. Dies verdeutlicht die Device-to-Cloud-Datenverarbeitungsstrategie, welche die Konfiguration, die Kommunikation, den Laufzeit- und historischen Datenzugriff sowie die Dienste für Alarmierung und Ereignisbenachrichtigung für vorhandene und neue Geräte unterstützt. Im November 2016 haben die beiden

Nutzerorganisationen unter dem Namen FDT for OPC UA das Release der Partnerspezifikation für Informationsmodellierung angekündigt. Dies ist ein zentraler Baustein für die Standardintegration von Informationen, die von FDT/DTM im OPC-UA-Informationsmodell bereitgestellt werden – eine wichtige Fähigkeit für Gerätediagnose, Konfiguration und Remote-Asset-Management sowie die Integration in MES. Die Partnerspezifikation soll durch Hersteller von Automatisierungssystemen in FDT/Frame-Anwendungen implementiert werden. Diese Frame-Anwendungen sind in Entwicklungssystemen, Distributed Control Systems (DCSS), Asset-Management-Systemen und anderen Anwendungen eingebettet. Die Partnerspezifikation ermöglicht somit wahre Interoperabilität zwischen Anwendungen und Geräten für Konfiguration, Diagnose und Laufzeitbetrieb. Sie ermöglicht Geräten und Host-Anwendungen die mühelose Integration von Support in IT-Anwendungen, einschließlich Informationen, die in die Azure-Cloud von Microsoft eingehen. Endbenutzer können vollständige Protokollverfolgungs- und Nachverfolgungsinformationen für alle Aspekte des Informationsmanagements implementieren – von der Konfiguration bis zum Laufzeitbetrieb. Von der architektonischen Perspektive aus betrachtet, hat der FDT/Frame Zugriff auf alle Steuerungsnetzwerke in der Anlage sowie auf alle unterstützten Geräte, die mit diesen Netzen verbunden sind. Er erkennt außerdem die gesamte Topologie des Steuerungssystems. Daher erlaubt der OPC-UA-Server im FDT/Frame jeder Client-Anwendung, die Topologie der Steuerungsarchitektur zu durchsuchen, ein individuelles Gerät in einem beliebigen Netzwerk in der Topologie auszuwählen und wichtige Betriebsdaten über dieses Gerät abzurufen – z.B. seine Identität, seinen Zustand, seinen aktuellen Output-Wert und viele andere Informationen. Der FDT/Frame leitet den Datenverkehr transparent und automatisch zu allen erforderlichen Netzwerken weiter, sodass dass es für den OPC-UA-Client aussieht, als sei das Gerät direkt verbunden.

App für den Instandhalter

Jeder handelsübliche OPC-UA-Client mit den entsprechenden Sicherheitsberechtigungen kann auf den im FDT/Frame eingebetteten OPC-UA-Server zugreifen. Ein Beispiel dafür ist eine Android-App, die wie ein OPC-UA-Client agiert. Solch eine App ermöglicht es einem Wartungstechniker, den Betriebsstatus und den Zustand eines Assets durch die Abfrage des Remote-FDT/Frame festzustellen, während er oder sie in der Einrichtung unterwegs ist. Dem Wartungstechniker scheint es so, als sei das WLAN-Tablet direkt mit dem jeweiligen Asset verbunden. Der zweite Teil des Artikels geht auf die Vereinfachung des Ökosystemaustausches und die Rolle von FDT für globale Industriestandards ein. ■

Artikelserie FDT und OPC UA

Teil 1: Technologische Konvergenz und Spezifikationen (INDUSTRIAL COMMUNICATION JOURNAL 4/2017)

Teil 2: Datenaustausch und Rolle globaler Industriestandards (SPS-MAGAZIN 12/2017)

Autor: Glenn Schulz,
Managing Director,
FDT Group



Halle 2
Stand 439

Autor: Thomas Burke,
President and Executive Director,
OPC Foundation



Halle 7
Stand 572

Sercos SoftMaster Package als Open Source Software

Sercos für alle



Bild: Rovema GmbH

Die Schlauchbeutelmaschinen der BV-Reihe von Rovema konnten durch Einsatz des Sercos SoftMaster besser an Kundenanforderungen angepasst werden.

Seit Ende letzten Jahres steht ein Sercos SoftMaster als Open Source Package im Internet zum Download bereit. Während es im ersten Teil des Beitrags um die technischen Einzelheiten sowie Lizenz- und Geschäftsmodelle des Softwarepaketes ging, fokussiert dieser Teil konkrete Projekte und Erfahrungsberichte.

Die bisherigen Projekte der Anwender mit dem Sercos SoftMaster als Open Source Package sind in unterschiedlichen Stadien der Integration. Einige Beispiele sollen die Erfahrungen und die breite Anwendbarkeit illustrieren.

Werkzeugmaschinen

Die Open Source Software Machinekit hat sich als Ableger und Weiterentwicklung der Software LinuxCNC entwickelt. Damit

kann auch eine einfache Echtzeit-Kernel-Erweiterung zur Anwendung kommen. Dadurch ist Machinekit offen für viele Plattformen wie PC, embedded PC oder ARM Single Board Computer. Der Open Source Sercos SoftMaster eignet sich durch seine Unabhängigkeit vom Betriebssystem dafür in ein Linux-Echtzeitbetriebssystem auf der einen Seite und in eine vielseitig anwendbare Software wie Machinekit auf der anderen Seite integriert zu werden. Die Integration muss dabei an zwei Stellen erfolgen. Einmal an der Stelle an der das Echtzeitbetriebssystem den Zugriff auf

die Standard-Ethernet-Hardware abstrahiert und zum anderen auf der obersten Applikationsschicht. In der Open-Source-Community ist dieser Ansatz aufgegriffen worden und zeigt erste demonstrative Ansätze. Dr. Schiffler, einer der Entwickler, meint dazu: „Der Einsatz der Sercos-Lösung als praktikablem SoftMaster mit Standard-Ethernet-Hardware und PC bietet unzählige Möglichkeiten von einfachen Automatisierungsaufgaben über CNC-Achsen bis hin zu IoT-Anwendungen. Gerade letzteres ist durch den Sercos Bus möglich, da hier Standard-Ethernet- sowie Sercos-Telegramme über die gleiche Leitung geleitet werden. Die erste beispielhafte Implementierung in der Software Machinekit kann sicherlich einen Anstoß für weitere spannende Entwicklungen geben. Vielleicht sehen wir bald die CNC-Steuerung auf einem NanoPi.“

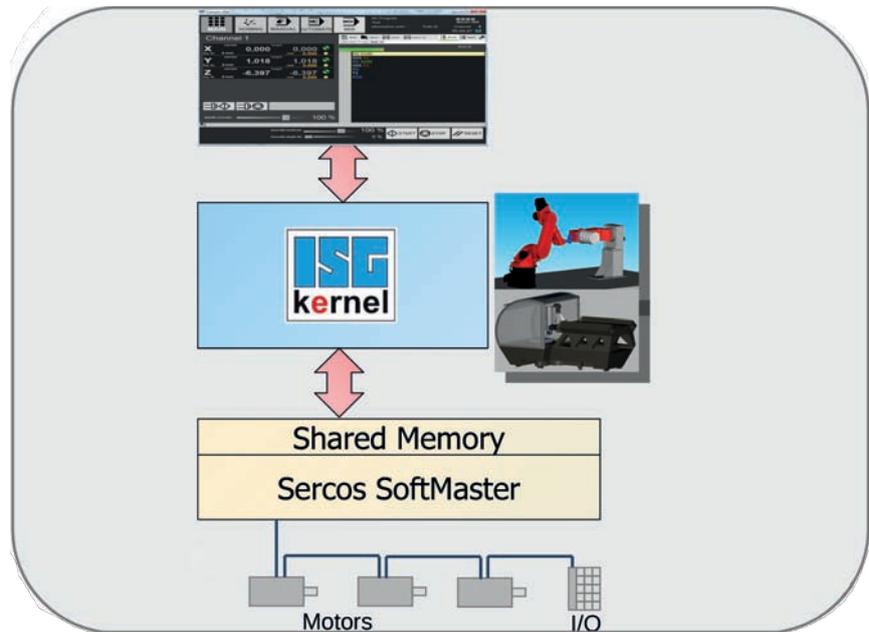


Bild: ISG Industrielle Steuerungstechnik GmbH

ISG-Kernel im Einsatz mit dem Sercos SoftMaster

Verpackungstechnik

Rovema liefert Verpackungslösungen und setzt dabei seit Einführung von Industrial Ethernet auf Sercos. Bereits 2015 hat Rovema die Integration des Sercos SoftMaster begonnen und steht nun an der Schwelle zur Produkteinführung. Siegfried Wacker, Leiter der Produktentwicklung, berichtet über Ziele und Erfahrungen: „Wir haben uns bewusst für Sercos als Systembus in unseren Anlagen entschieden, da dies Vorteile in Bezug auf Determinismus und Interoperabilität bedeutet. Speziell das hohe Niveau in Bezug auf funktionale Standardisierung erlaubt es, Geräte unterschiedlicher Hersteller wahlweise ohne Funktionseinbußen einzusetzen. Mit der Einbindung des Sercos SoftMaster verbinden wir eine weitere Reduktion von Hardware-Bauteilen und Kosten, die speziell im Einstiegssegment von großer Bedeutung sind, z.B. bei unserer Schlauchbeutelmaschine des Typs BVK.“ Auch ein US-amerikanisches Maschinenbauunternehmen, das seit vielen Jahrzehnten seine Produkte und Dienste im Bereich der Fleisch- und Fischverarbeitung anbietet, hat bereits begonnen den Open Source Sercos SoftMaster mit Unterstützung von Bosch Rexroth zu integrieren.

Werkzeugmaschinen & Robotik

Das Unternehmen ISG entwickelt und integriert NC- und Robotik-Steuerungslösungen als Softwarekomponente in Steuerungssysteme ihrer Kunden. Daneben bietet das Unternehmen ein Echtzeit-Simulationssystem ISG-virtuos an, das sowohl in Kundenlösungen integriert werden kann als auch als Hardware-in-the-Loop-System (HiL) für die virtuelle Inbetriebnahme geeignet ist. Im Rahmen der Evaluierung wurden mehrere Demonstrationssysteme unter Verwendung beider Produkte in Kooperation mit Tenasys, Phoenix Contact, dem Institut für Steuerungstechnik der Universität Stuttgart und Bosch Rexroth realisiert. Hannes Richter, Business Development Manager, berichtet über seine Erfahrungen: „Die Handhabung des Sercos SoftMaster zeichnet sich durch einfache Schnittstellen aus, die zu unserem SharedMemory-Kon-

zept passen. Wir beabsichtigen, die Lösung mit der Verfügbarkeit des freigegebenen Softwarepaketes als Option für unser Produkt ISG-Kernel aufzunehmen.“

Zusammenfassung

Die Voraussetzungen für eine Implementierung des SoftMaster in einem weiten Anwendungsfeld - vorsichtig geschätzt sind über 90 Prozent aller Feldbusanwendungen abgedeckt - sind durch die nachhaltige Verankerung als Open Source Projekt und in dem Lösungspaket Sercans XS von Bosch Rexroth sowie durch das Lizenzmodell nach MIT gegeben. Mit der Integration des Sercos SoftMaster in die Open Source CNC-Lösung Machinekit bzw. LinuxCNC steht eine kostenfreie Evaluationsplattform für die Bewegungssteuerung mit I/O-Hilfsfunktionen zur Verfügung. An Hand der Demonstrationssysteme, die mit ISG aufgebaut wurden und weiterer Evaluierungsprojekte lässt sich ableiten, dass innerhalb von vier bis acht Wochen eine Integration in jedes vorhandene Automatisierungssystem mit einer für diesen Zweck ausgelegten Feldbusschnittstelle möglich ist. Die in diesem Beitrag beschriebenen Randbedingungen zeigen, dass einer industriellen Anwendung unabhängig von Ort und Branche nichts im Wege steht. ■

Im ersten Teil des Beitrags, der in der Ausgabe 3/2017 des INDUSTRIAL COMMUNICATION JOURNALS erschienen ist, ging es um die technischen Einzelheiten sowie Lizenz- und Geschäftsmodelle des Softwarepaketes.

Autor: Friedrich Scheurer,
Produktmanager MotionLogic Control
und Sercos
Bosch Rexroth AG
www.boschrexroth.de



Halle 7
Stand 450

Direkt zur Marktübersicht [i-need.de](http://www.i-need.de)

www.i-need.de/?f9512

I/O-Systeme für Ethernet und Feldbusse ab IP65

Egal ob Steuerung, Umrichter, Sensor oder I/O-System – wenn es um den Einsatz im Feld geht, sind die Komponenten oft rauen Umgebungsfaktoren ausgesetzt: Dazu gehören neben Feuchtigkeit bzw. Nässe auch Staub und Schmutz, Späne, starke Vibrationen und Stöße sowie extreme Temperaturen.

Für elektronische Geräte, die auch unter erschwerten Umweltbedingungen sicher arbeiten, wurden die unterschiedlichen IP-Schutzarten (engl. International Protection Codes) eingeführt. Die beiden Ziffern des Codes charakterisieren den Schutz eines Gerätes vor Fremdkörpern (erste Ziffer) und Wasser bzw. Nässe (zweite Ziffer). Während ein Gerät in Schutzart IP20 also nur gegen Fremdkörper mit einem Durchmesser größer als 12,5mm geschützt ist und überhaupt nicht gegen Nässe, sind Komponenten in IP65 staub- und (strahl-) wasserdicht. So wie es bei einem direkten Einsatz an der Maschine oft gefordert ist. Die folgende Übersicht listet entsprechend geeignete I/O-Systeme auf. (mby) ■

Direkt zur Marktübersicht auf www.i-need.de/91



Anbieter	B&R Industrie-Elektronik GmbH	Balluff GmbH
Kennziffer	10991	11077
Ort	Bad Homburg	Neuhausen a.d.F.
Telefon	06172/ 4019-0	07158/ 173-291
Internet-Adresse	www.br-automation.com	www.balluff.de
Produktname	X67 System	BNI - PNT / EIP / ECT
Gehäuseschutzart IP xx	IP67	IP67
Maximale Anzahl E/A-Stationen im Gesamtsystem	253	IP Adressraum
Buskoppler-Typ bzw. Remote E/A	Feldbus-Koppler	Remote E/A
Max. dig. E/A pro Buskoppler bzw. Remote E/A	4048 / 4048	136 über IO-Link / 136 über IO-Link
Max. an. E/A pro Buskoppler bzw. Remote E/A	1012 / 1012	32 über IO-Link / 8 über IO-Link
Statusanzeige, Diagnoseinformationen	Status, Kurzschluss, Überlast	Status, Kurzschluss, Überlast, Drahtbruch
Programmierung eines Ethernet-Buskopplers/Feldbus-Controllers		Einbindung über Gerätebeschreibungsfeld in SPS Software
Programmspeichergröße		
Besonderheiten des Buskopplers		Integrierter Switch, Integrierter Web-Server, IO-Link V 1.1
Industrial Ethernet-Kommunikationsprotokolle	EtherNet/IP, Powerlink, Modbus-TCP	Profinet, Ethernet/IP, Ethercat
Weitere Industrial Ethernet Protokolle		
Feldbus-Kommunikationsprotokolle	CANopen, DeviceNet, Modbus, Profibus-DP	DeviceNet, Profibus-DP, CC-Link
Besonderheiten / Optionen bei den analogen Ausgängen	Signalzustand durch Leuchtdioden angezeigt, Diagnoseinformationen	Signalzustand durch LED angezeigt, Diagnoseinformationen
RS232, 20-mA, RS422/RS485	✓, ✓, ✓	
Wireless-Datenaustausch		
Safety-Bussystem	opensafety	



Anbieter	Molex Deutschland GmbH	Moog GmbH	Murrelektronik GmbH	Phoenix Contact Deutschland GmbH	Rockwell Automation GmbH
Kennziffer	10974	11012	10961	11049	11034
Ort	Walldorf	Böblingen	Oppenweiler	Blomberg	Düsseldorf
Telefon	06227/ 3091-0	07031/ 622-218	07191/ 47-0	05235/ 3-41713	0211/ 41553-0
Internet-Adresse	www.molex.com	www.moog.de	www.murrelektronik.com	www.phoenixcontact.com	www.rockwellautomation.de
Produktname	HarshIO	Moog Motion Controller	MVK Metall	Fieldline	Point I/O / ArmorPoint
Gehäuseschutzart IP xx	IP67	IP20 - IP67	IP67	IP65 / IP67	Point I/O: IP20, ArmorPoint: IP67
Maximale Anzahl E/A-Stationen im Gesamtsystem	abhängig vom Bussystem	> 100		netzwerkspezifisch	abhängig vom eing. Ethernet Scanner
Buskoppler-Typ bzw. Remote E/A	Ethernet-Buskoppler	program. Ethernet-Buskoppler (Controller)			Ethernet-Buskoppler
Max. dig. E/A pro Buskoppler bzw. Remote E/A	16 / 16	224 / 224	16 / 16	256 / 256	Max. 63 Module oder 504 Kanäle / ~ Max. 20 Module / Max. 20 Module
Max. an. E/A pro Buskoppler bzw. Remote E/A	/	16 / 4	4 / 4	64 / 64	Status: Einspeisung, Bus, Netzwerk, Modul, Netzwerk Aktivität
Statusanzeige, Diagnoseinformationen	Status, Überlast, Kurzschluss, Status	Status; Status, Drahtbruch	Status, Kurzschluss, Überlast, Drahtbruch	Netzwerkstatus, Busstatus, Status, Kurzschluss, Überlast	Über SPS: IEC 61131-3 Programmiersprachen KOP, FUP, ST und AS
Programmierung eines Ethernet-Buskopplers/Feldbus-Controllers		Codesys 2 und Codesys 3, alle IEC-61131 Programmiersprachen			Programm liegt in der SPS
Programmspeichergröße		32 MByte		kein integ. Programmspeicher (keine SPS)	DHCP Client oder Festadresse.
Besonderheiten des Buskopplers	Integrierter 3-port-switch, Watchdog, 4-Zeichen-Display für Diagnose & Set-up, UltraLock	Frei programmierbarer Mehrachs-Regler mit SPS-Funktionalität	integrierter Switch, Sync- und Freeze Modus	integrierter 3 Port-Switch auf dem Buskoppler, digitale E/As onBoard	Version mit integriertem Switch ist ebenfalls verfügbar
Industrial Ethernet-Kommunikationsprotokolle	Profinet, EtherNet/IP, Modbus-TCP	Ethercat	Profinet, EtherNet/IP	EtherNet/IP, Modbus-TCP, Profinet	EtherNet/IP
Weitere Industrial Ethernet Protokolle					
Feldbus-Kommunikationsprotokolle	CANopen, Profibus-DP, DeviceNet	CANopen; Ethernet; Profibus-DP; Ethercat; Profibus-DP, CANopen	Profibus-DP, CANopen, DeviceNet, Interbus	Interbus, Profibus-DP, DeviceNet, CANopen	ControlNet, DeviceNet, Profibus-DP
Besonderheiten / Optionen bei den analogen Ausgängen		Kabelbrückerkennung	Signalzustand d. LED, Diagnoseinform., kurzschluss- u. überlastfeste Sensorverso.	Signalausg. konfig., Status-, Diagnose-, Drahtbruch, Messbereichsüber- u. unters.	Signalzustand durch Leuchtdioden angezeigt, Kalibrierung erforderlich
RS232, 20-mA, RS422/RS485	Nein, Nein, Nein	✓, Nein, Nein	Nein, Nein, Nein	Nein, Nein, Nein	✓, Nein, Nein
Wireless-Datenaustausch				Bluetooth	über Partnerprodukte
Safety-Bussystem			Profinet / Profisafe		PointIO: (...).

					
Beckhoff Automation GmbH & Co. KG 11024 Verl 05246/ 963-0 www.beckhoff.de	Bosch Rexroth AG 11064 Lohr am Main 09352/ 181573 www.boschrexroth.de	Festo AG & Co. KG 11031 Esslingen 0711/ 347-2141 www.festo.de	Inter Control GmbH & Co. KG 22151 Nürnberg 0911/ 9522-855 www.intercontrol.de	Kendrion Kuhnke Automation GmbH 11072 Malente 04523/ 402-0 www.kuhnke.kendrion.com	Lumberg Automation - Belden D. GmbH 10988 Schalksmühle 02355/ 5044-000 www.lumberg-automation.com
Ethercat Box	IndraControl S67	CPX-Terminal, Ventilinsel mit CPX	digsy ICN-V	Ethercat I/O Modul in IP65	Lion-Link
IP67 (Kunststoff-, Edelstahl- o. Zinkgeh.)	IP67	IP65 / IP67	IP6K9K	IP65 / IP67	IP67
65.535		512	32	65536	30
Remote E/A	Feldbus-Koppler		Remote E/A	Remote E/A	Feldbus-Koppler
16 / 24	8 / 8	512 / 512	20 / 16	8 / 8	768 / 768
4 / 4	4 / 4	32 (busabhängig) / 18 (busabhängig)	4 / 8	8 / 8	48 / 48
Status, Kurzschluss, Drahtbruch, Kommunikationsfehler etc. unzutreffend	Diagnose LED, Fehlermel. an Steuerungs-, Status, Kurzschluss, Überlast, Drahtbruch	Status, Kurzschluss, Überlast, Drahtbruch, Kommunikationsfehler Codesys / IEC61131-3, KOP, AWL		Status	Status, Kurzschluss, Überlast, Drahtbruch
unzutreffend		32 MB			
E/A-Konfigurationseinstellung, Debug-Funktionalität, Zykluszeiteinstellung und -messung	On-Board E/As	Ethernet mit integr. Switch, speichert Konfigurationseinstellung, modulares Spannungsversorgungskonzept	8 PWM_Ausgänge		Buskoppler speichert E/A-Konfigurationseinstellung
Ethercat Gateway zu Profinet	Sercos III, Profinet, EtherNet/IP	Ethercat, EtherNet/IP, Modbus-TCP, Profinet		Ethercat	Profinet
nein	Profibus-DP	CANopen, DeviceNet, Interbus, Modbus, Profibus-DP	CANopen		Profibus-DP, DeviceNet, CANopen
Signalzustand durch LED, Diagnoseinformationen, V/I-parametrierbar	Diagnoseinformation: Kurzschluss, Drahtbruch	parametrierbar, LED für Signal/Diagnose, Anschlusstechnik M8/M12... (10 Optionen), ✓, Nein, Nein		Diagnoseinformation, Zustand über LED	Statusanzeige, Diagnoseanzeige, Diagnose: Kurzschluss Nein, Nein, Nein
✓, Nein, ✓ Nein Twinsafe	✓, Nein, ✓	Profisafe-fähig			

					
Schneider Electric GmbH 11033 Ratingen 01805/ 753575 www.schneiderelectric.de	Siemens AG 26483 Nürnberg / www.siemens.de/et200al	Sigmatek GmbH & Co KG 14641 Lamprechtshausen 0043/6274/ 4321-0 www.sigmathek-automation.com	Hans Turck GmbH & Co. KG 10970 Mülheim 0208/ 4952-0 www.turck.com	Weidmüller GmbH & Co. KG 10992 Detmold 05231/ 1428-259 www.weidmueller.de	wenglor sensoric GmbH 25218 Tettmang 07542/ 5399-718 www.wenglor.de
Advantys ETB	Simatic ET 200AL	P-Dias	BL67	SAI Aktiv Universal (IP 67 Remote E/A)	ZAI02PN02, ZAI02EN02, ZAI02CN02
IP67	IP67	IP67	IP67	IP67	IP67
unbegrenzt	unbegrenzt	65.280 dezentrale E/A-Modulgruppen	unbegrenzt	unbegrenzt	
Ethernet-Buskoppler	Remote E/A				
16 / 16	16 DI / 16 DO	80 / 160	288 / 288	16 / 8	16 / 16
/	4 AI / 4 AQ	- / -	126 / 126	4 / 2	/
Status, Kurzschluss	Kurzschluss; Status; Fehlende Versorgungsspannung	Link in, Link out, DC ok	Status, Kurzschluss, Überlast, Drahtbruch	Status, Kurzschluss, Überlast, Drahtbruch	Power-, Geräte-, Netzwerkstatus, Kurzschluss
			IEC 61131-3 Programmiersprachen KOP, FUP, AWL, ST und AS		
Integrierter 2port-Switch auf dem Buskoppler	Integration als modul. ET 200SP-Modul, Autom. Hochlauf mittels Topologieerkenn., Zuordnung zu unters. CPUs ü.Shared Dev.	nicht erforderlich	1 MB Busklemme speichert E/A-Konfigurationseinstellung	integrierter Switch bei Profinet Variante, speichert E/A-Konfigurationseinstellung, Zykluszeiteinstellung und -messung	Temperaturabschaltung, Gesamt-Stromüberwachung, Einzelpin-Stromüberwachung
EtherNet/IP, Modbus-TCP	Profinet	Varan-Bus	Profinet, EtherNet/IP, Modbus TCP TCP/IP, UDP/IP, FTP, HTTP	Modbus-TCP, EtherNet/IP, Profinet	Profinet, EtherNet/IP, Ethercat
	Profibus-DP	Varan-Bus	CANopen, DeviceNet, Profibus-DP		
Nein, Nein, Nein	Nein, Nein, Nein	Nein, Nein, Nein	Signalzustand durch LED, Diagnoseinfor. wie Kurzschluss oder Leitungsbruch ✓, Nein, ✓	Signalzustand durch LED, Diagnoseinfor. wie Kurzschluss oder Leitungsbruch Nein, Nein, Nein	

Alle Einträge basieren auf Angaben der jeweiligen Firmen.

Kommt Zeit, kommt TSN?

Das Time-Sensitive Networking großes Potenzial für industrielle Anwendungen mitbringt, wird mehrheitlich nicht angezweifelt. Wie stark TSN dabei die heutigen Kommunikationsprozesse und -standards beeinflussen wird, darüber sind sich die Experten nicht einig. Doch wie sieht es überhaupt auf der Zeitschiene aus? Wann werden sich erste TSN-OPC UA-Lösungen in der Branche etablieren und in welchen Anwendungsbereichen?

Pilotprojekte bereits in der Anwendung

In vielen Anwendungen basiert Kommunikation bereits heute auf OPC UA. Bisher war es jedoch nicht möglich, echtzeitrelevante Informationen zu übertragen. Diese Anwendungsfälle werden nun durch die Kombination von OPC UA und TSN erschlossen. Anwender profitieren von hundertprozentiger Interoperabilität und einer einheitlichen Kommunikationslösung – unabhängig von der Applikation. Die Kombination aus beiden Technologien ist in ersten Pilotprodukten in der Anwendung, die in Testbeds eingesetzt werden, und demonstriert eine durchgängige Kommunikation vom Sensor bis in die Cloud. Diese Kommunikation basiert auf offenen und herstellerunabhängigen

„ Wir erwarten 2018 erste Installationen basierend auf der Kombination von OPC UA und TSN.

Sebastian Sachse,
Technology Manager Open Automation bei B&R



Bild: B&R Industrial Automation GmbH

Standards und bildet so die Basis für moderne Innovationsprozesse. Anwender akzeptieren geschlossene Systeme nicht mehr, da diese Innovationen hemmen. Wir erwarten, dass bereits 2018 erste Installationen basierend auf der Kombination von OPC UA und TSN ausgerollt werden.

Es kommt auf den Anwendungsbereich an!

Wann TSN via OPC UA in der Branche wirklich ankommt? Nun, zunächst sollte mal die Spezifikation fertig werden. Das wird wohl Anfang 2018 der Fall sein. Und dann? Kommt auf den Anwendungsbereich an: Als Feldbusersatz in Maschinensteuerungen? Nie! Dafür ist OPC UA weder gedacht noch gemacht,

mit oder ohne Pub/Sub-Erweiterung und auch nicht mit TSN. Zur deterministischen Vernetzung von Steuerungen untereinander in komplett neuen Green-Field-Installationen? Sobald TSN-Switches mit handhabbaren Konfigurationswerkzeugen zu vertretbaren Kosten verfügbar sind – ich schätze, das wird mindestens noch zwei Jahre dauern. Nicht nur auf der Hardware-Seite (Chips), sondern gerade auch im Bereich der Konfiguration sind hier noch einige Hausaufgaben zu erledigen. Und noch ist nicht klar, ob sich wirklich herstellerunabhängige Konfigurationsmechanismen durchsetzen werden. Zu Steuerungsvernetzung in existierenden Fertigungsstätten (Brown Field)? Erst wenn die vorhandene Ethernet-Infrastruktur komplett mit TSN-Switches versehen ist, also die heute genutzten Geräte beim Kunden des Maschinenbauers ersetzt wurden.

„ TSN als Feldbusersatz in Maschinensteuerungen? Nie!

Martin Rostan, Geschäftsführer,
Ethercat Technology Group



Bild: Ethercat Technology Group

Arbeiten haben begonnen

Mit TSN zeichnet sich eine vielversprechende Technologie ab. Nicht nur für OPC UA, sondern auch für Profinet. Denn auch in der Zukunft werden die etablierten Feldbussysteme und Kommunikationsprotokolle eine wesentliche Rolle spielen. Vor allem zwischen Steuerungen und Feldgeräten, wie I/O-Systemen oder Antrieben. OPC UA dagegen wird vor allem zwischen Steuerungen unterschiedlicher Hersteller wichtig sowie für die vertikale Kommunikation zu überlagerten Systemen. Und das nicht erst mit TSN! Schon durch Client/Server- und Pub/Sub-Mechanismen, die derzeit in der OPC Foundation spezifiziert werden, kann eine leistungsfähige M2M-Kommunikation etabliert werden. Daher hat sich die Nutzerorganisation PI entschlossen, für Controller-Controller-Kommunikation auf OPC UA zu setzen. Die Feldebene wird aber weiterhin mit Profinet (künftig mit Profinet based on TSN) bedient werden. Da die Steuerungshersteller die OPC UA Technologie derzeit in ihre Controller integrieren, ist damit zu rechnen, dass vor allem der Maschinenbau und die Fertigungstechnik rasch

„ Automatisierungsanbieter müssen sich auf eine einheitliche Nutzung der vielen Standards von TSN einigen.

*Karsten Schneider,
Chairman, Profibus & Profinet International*

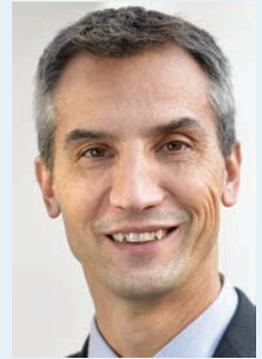


Bild: Profibus & Profinet International

OPC UA für die Szenarien oberhalb der Feldebene einsetzen werden. Parallel werden in der IEEE die Basisarbeiten zu TSN vorangetrieben. In Testbeds werden diese Mechanismen erprobt. Hier ist es aber essentiell, dass sich die Automatisierungsanbieter auf eine einheitliche Nutzung der vielen Standards von TSN einigen. Hier wird die IEC eine wesentliche Rolle spielen, um eine herstellerübergreifende Verwendung zu standardisieren. Die Arbeiten dazu haben bereits begonnen, jedoch müssen auch die Ergebnisse der Testbeds abgewartet werden, damit nicht nur ein interoperables, konvergentes Netzwerk entsteht, sondern auch eine gute Usability für die Anwender erreicht wird.

Grundlegender Substandard noch nicht verabschiedet

Erste Prototypen mit OPC UA und Ethernet TSN wurden bereits umgesetzt und beispielsweise in die Testbeds des IIC integriert. Allerdings wurde mit IEEE 802.1AS-rev ein grundlegender TSN-Substandard, der deutliche Verbesserungen bei der Zeitsynchronisation bringen soll, noch nicht endgültig verabschiedet. Und auch die OPC UA Spezifikationserweiterung für Pub/Sub ist zum aktuellen Zeitpunkt noch nicht abschließend freigegeben. Deswegen wird es noch ein wenig Zeit brauchen, bis eine breitere Auswahl an Produkten und Lösungen im Markt verfügbar ist und diese in realen Anwendungen eingesetzt wird. Es ist zu erwarten, dass sich TSN-OPC UA Lösungen zunächst in der Steuerungs- und Prozessleitebene etablieren werden, insbesondere dann, wenn Maschinen mit Steuerungen bzw. Maschinenperipherie unterschiedlicher Hersteller auf der Basis eines einheitlichen, unabhängigen

„ Es wird noch ein wenig Zeit brauchen, bis eine breitere Auswahl an Produkten verfügbar ist.

*Peter Lutz,
Managing Director, Sercos International e.V.*



Bild: Sercos International e.V.

Netzwerkconvergenz für das IIoT

Gegenwärtig existieren IT- und OT-Netze als getrennte Domains. Eine Kommunikation in beiden Richtungen ist begrenzt und bislang nur über dedizierte Gateways möglich. Die funktionale Zusammenführung dieser Netzwerke ist also ein Schlüsselfaktor zur Realisierung von cyberphysikalischen Systemen. An dieser Stelle kommt Time-Sensitive Networking, kurz TSN, ins Spiel. Doch wie lässt sich dessen Implementierung auf Elektronikseite abbilden?

Die aktuell gebräuchliche Architektur für Steueraufgaben in der Fertigungsautomation ist hierarchisch gegliedert. Auf der höchsten Ebene ermöglichen ERP-Applikationen ein integriertes Management und die Automation der geschäftlichen Kernprozesse. Darunter liegt die MES-Ebene, die den eigentlichen Fertigungsprozess steuert. SPS-Systeme führen die Automatisierungsaufgaben aus, unter Verwendung der dazu vorgesehenen industriellen Komponenten wie elektrische Antriebe, Sensoren oder I/Os, die die unterste Hierarchiestufe bilden: die Feldebene. Dieser Aufbau wird als Automationspyramide beschrieben. Sie verdeutlicht den beträchtlichen Aufwand an Bausteinen auf der unteren Ebene und in den High-Performance Computern an der Spitze.

Unterschiedliche Anforderungen

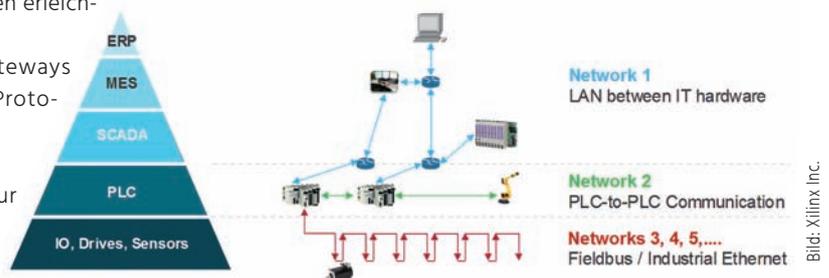
Die unterschiedlichen Schichten der Pyramide entsprechen den unterschiedlichen Anforderungen an die Netzwerke. Während die höheren Ebenen große Bandbreiten und flexible Topologien erfordern, sind die unteren Layer auf das deterministische Verhalten und den Transport der Samples in konstanten Intervallen mit geringer Variation der Paketverzögerung ausgerichtet. Dieses Problem bedingt den Einsatz mehrerer Netzwerke, die nebeneinander operieren. Ein konvergiertes Netzwerk hingegen kann etliche Herausforderungen der gegenwärtigen disparaten Netzarchitektur adressieren und beseitigen. Es ermöglicht:

- Mehr Transparenz: Auf alle Daten aller Hierarchien kann von jedem operativen Element der Fertigung ohne Umsetzungen zugegriffen werden.
- Weniger Netzwerkplanung: Flexiblere Topologien erleichtern mögliche Änderungen
- Weniger Verkabelungsaufwand, weniger Gateways zwischen Netzwerken mit unterschiedlichen Protokollen.
- Vereinfachung der Netzwerkverwaltung
- Höhere Bandbreite: Keine Eingrenzung auf nur eine Netzgeschwindigkeit.
- M2M-Optimierung: Interoperabilität von Maschinen durch gemeinsame Datenstruktur, wie OPC UA, über die gesamte Fertigung hinweg.

Diese Konvergenz soll sich mit TSN (Time-Sensitive Networking) erreichen lassen, also einer zeitsensitiven Vernetzung. Die Implementierung von TSN ermöglicht eine deterministische Kommunikation über Ethernet-Netze und bewahrt dabei die gewohnten Vorteile dieses Netzwerks in Bezug auf die Best-Effort-Kommunikation. TSN führt dazu unterschiedliche Klassen des Datenverkehrs ein, die sich einen Link teilen. Die TSN-Netzkonfiguration reserviert Ressourcen für Streams mit deterministischem Zeitverhalten. TSN ermöglicht somit die Implementierung eines gemeinsamen Netzes, das mehrere Kommunikationsstandards unterstützt.

Verbesserungen für Ethernet

Alles das bringt eine Reihe von Verbesserungen gegenüber dem Standard-Ethernet. Denn die Kommunikation via Standard-Ethernet berücksichtigt keine Laufzeitunterschiede. Sie verteilt die Daten über die gesamte Link-Bandbreite, und reiht die Pakete zur Übertragung nacheinander auf. Dagegen implementiert TSN ein zeitsensitives Verhalten (Time Awareness) des geplanten Datenverkehrs mit konfigurierten Offsets in zyklischen Intervallen. Es folgt einem Schema, das von einem Network Configuration Controller vorgegeben wird. Weitere TSN-Features umfassen die Filterung und Überwachung (Policing) von Streams, eine nahtlose Redundanz und die Unterstützung der zyklischen Datenübertragung, wobei auch der Vorrang für Pakete mit höherer Priorität berücksichtigt wird. TSN ist definiert als Satz von IEEE802.1-Standards, die die Implementierung spezifizieren. Derzeit sind vier dieser Standards bereits eingeführt, während die restlichen noch von



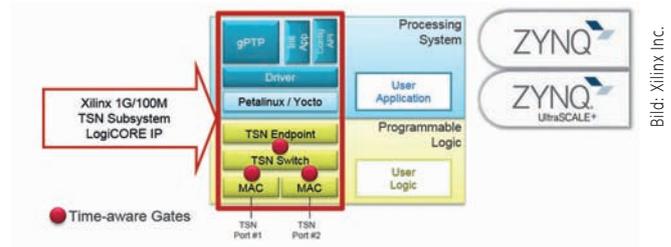
Automationspyramide mit typischer Netzwerk-Hierarchie.

der der zugehörigen Task and Working Group bearbeitet werden. Die neuen Standards werden per Ethernet (IEEE 802.3 Physical Layer) implementiert. Sie unterstützen die Star-, Chain-, Ring- und gemischte Topologie und sind nicht auf eine spezifische Datenrate beschränkt. Für industrielle Applikationen sind hauptsächlich Datenraten von 100Mbit und 1Gbit vorgesehen. Damit ermöglicht TSN die erstrebte Konvergenz von IT- und OT-Netzen. Diese Konvergenz soll die Kosten der Netzwerk-Implementierung sowie die Betriebskosten deutlich reduzieren.

TSN-Implementierung

Eine angemessene Implementierung von TSN erfordert eine Lösung, die geringe Latenz und deterministisches Verhalten an den TSN-Endpunkten und TSN-Brücken bereitstellt. Viele Applikationen lösen diese Herausforderung durch die Kombination eines Prozessors mit einem FPGA, die über einen Highspeed Link, etwa PCIe, verbunden sind. Diese Zwei-Chip-Lösung vergrößert jedoch nicht nur die benötigte Boardfläche, den Leistungsverbrauch, die Entwicklungszeit und die Kosten. Sie verhindert zudem die Entwicklung einer ganzheitlich integrierten Lösung. Und da das Design in zwei Bausteinen segmentiert ist, erhöht dieses Vorgehen auch die Komplexität der Verifizierung. Deshalb setzen die Anbieter von IIoT-Lösungen zunehmend auf Zynq-7000- und Zynq-UltraScale+MPSoC-Bausteine von Xilinx, um ihre Lösungen zu implementieren. Die genannten Bausteine vereinen und integrieren PS (Processing System) und PL (Programmable Logic) und ermöglichen auf diese Weise die Implementierung der Datenerfassung, der Steuerung und der Verarbeitung von Applikationen durch die effiziente Nutzung von PS und PL. Dies ist möglich durch die folgenden Eigenschaften:

1. Fähigkeit zum Anschluss und Steuern einer breiten Vielfalt von Sensoren, Aktuatoren, Motoren und anderen applikations-spezifischen Interfaces
2. Fähigkeit zur Implementierung komplexer Verarbeitungen an der Edge, wie Machine Learning, Sensor-Fusion, Bildbearbeitung und Echtzeitanalytik
3. Skalierbarkeit betreffend die Anzahl der Netzwerk-Interfaces



Die TSN-IP für Xilinx Zynq-7000 oder Zynq UltraScale+ MPSoC.

Bild: Xilinx Inc.

4. Sicherheit und die Fähigkeit, den Baustein und das System im Hinblick auf Information Assurance, Anti-Tampering, und Trust auszuliegen

Die Unterstützung des vielseitigen Any-to-Any Interfacing und die enge Kopplung von Prozessorsystem und programmierbarer Logik macht die Xilinx-Bausteine geeignet zur TSN-Implementierung im Rahmen einer Anwenderapplikation. Die 1G/100M-TSN-Subsystem-LogiCORE-IP von Xilinx umfasst die FPGA-Logik für MAC, TSN-Bridge und TSN-Endpoint. Die Auslegung mit dedizierten Logikressourcen stellt sicher, dass das Zeitverhalten strikt deterministisch ist. Die Software, die auf dem Prozessorsystem des SoC läuft, absolviert die Netzsynchonisierung, die Initialisierung und das Interfacing mit den Controllern zur Netzkonfiguration für die Stream-Reservierung. Diese Software ist für Petalinux ausgelegt und wird für Yocto-Builds verfügbar sein. Die LogiCORE-IP bietet außerdem einen optional integrierten zeitsensitiven L2 Switch, der die in vielen industriellen Applikationen erforderliche Linien- oder Baumtopologie erstellt, ohne einen weiteren Port für einen externen TSN-Switch zu belegen. Nahtlose Redundanz (P802.1CB) erfordert auch diesen zusätzlichen Port. Der Anwender kann die IP vor der Synthese frei konfigurieren, unabhängig davon, ob der Switch integriert werden soll oder nicht.

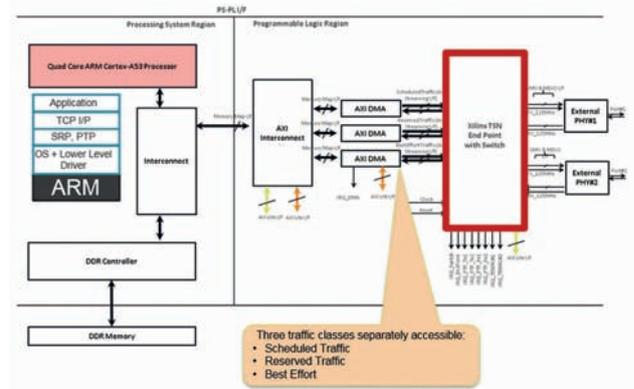
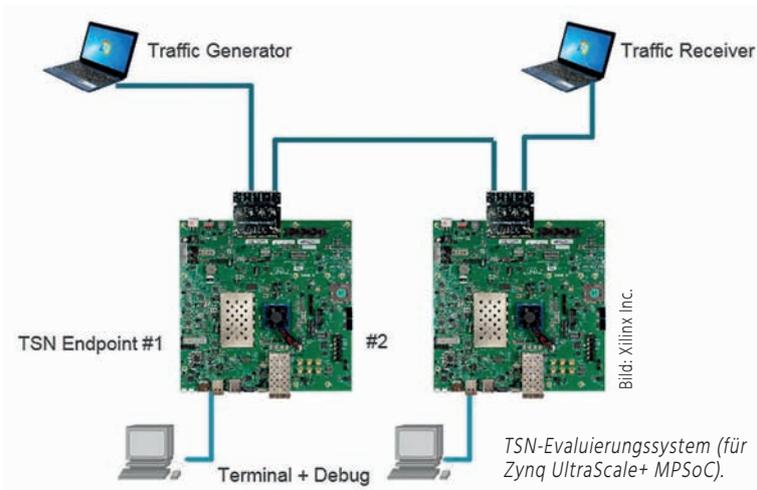
Ports für jede Verkehrsklasse

Nach der Instanzierung stellt der TSN-IP-Kern individuelle AXI-Streaming-Ports für jede Verkehrsklasse bereit. Dabei werden der reguläre Verkehr, der reservierte Verkehr, sowie Best-Effort-Verkehr unterstützt. Die AXI-Streaming-Ports verbinden mit einer Infrastruktur, die mit der Xilinx Vivado Design Suite eingebracht wird. AXI Lite dient zum Konfigurieren der TSN-Blöcke. Für Evaluierungszwecke bietet das Unternehmen eine einfach einsetzbare Implementierung mit separatem Direct Memory Access für jede Verkehrsklasse. Dieses Evaluierungssystem lässt sich so wie es ist zum Testen der Interoperation der Komponenten einsetzen, außerdem in der Kombination mit Equipment von Drittanbietern oder mit Protokoll-Analysern. Flexibel wie sie ist, bietet die programmierbare Logik auch die Möglichkeit zur Aktualisierung des IP-Kerns in dem Maße, wie sich die TSN-Standards und die marktsegmentspezifischen Konformanztests weiterentwickeln. Bausteine mit fester Hardwareimplementierung hingegen, wie Kunden-ASICs und ASSPs, bieten nicht die Option für funktionale Änderungen im weiteren Verlauf der TSN-Evolution. Um den TSN-IP-Kern in Aktion zu demonstrieren, hat Xilinx eine Demoapplikation für das ZCU102- und das ZC702-Entwicklungsboard entwickelt. Sie enthalten Bausteine der Zynq-UltraScale+MPSoC- und der Zynq-7000-Familien. Werden zwei dieser Boards verbunden, kann man Netzwerkdaten senden und empfangen. Damit lassen sich die TSN-Netzwerk-Fähigkeiten validieren. Als weitere Unter-

Bild: Xilinx Inc.

Standard / IEEE Draft	Title	User's Advantage
IEEE 802.1AS (evolving to P802.1ASrev)	Network Time Synchronization	All nodes share the same time
IEEE 802.1Qbv	Scheduled Traffic	Scheduled Ethernet frames never collide
IEEE 802.1Qci	Filtering & Policing	Removes babblers from the network (Security)
P802.1CB	Seamless Redundancy	Zero Loss switch-over
P802.1Qcc	Stream Reservation	Path provisioning according to IEEE
IEEE 802.1Qbu and IEEE 802.3br	Frame Pre-emption	Maximum bandwidth without compromising real-time behavior

Die IEEE TSN Standards.



TSN-Implementierung für Evaluierungszwecke (Zynq UltraScale+ MPSoC).

Bild: Xilinx Inc.

stützung des Einsatzes von TSN und entsprechenden Anwendungen ist Xilinx ein Mitglied des TSN-Testbed im IIC. Dieses Engagement Partizipation ermöglicht eine Durchführung von Interoperabilitätstests zwischen Anbietern, und außerdem das Testen von High-Performance- und latenzkritischen Applikationen. Diese Tests können auf einem von zwei permanenten Testbeds ausgeführt werden, entweder in den USA oder in Europa. ■

Autor: Adam Taylor,
Embedded Systems Consultant,
Xilinx GmbH
www.xilinx.com

Autor: Michael Zapke,
Product Marketing Manager Industrial,
Xilinx GmbH
www.xilinx.com



Halle 6
Stand 266

Industrial-Ethernet-Komponenten

Mit der Diskussion um Time-Sensitive Networking erfährt das industrielle Ethernet aktuell viel Aufmerksamkeit. Soviel steht fest: Auch in der Zukunft, in Zeiten von Industrie 4.0 und dem IIoT bleibt Ethernet als Basis für die Kommunikation in der Fertigung gesetzt.

Was die Anzahl der jährlich verbauten Knoten angeht, zieht Industrial Ethernet mittlerweile an den klassischen Feldbussen vorbei. Dafür spricht nicht die höhere Performance der jeweiligen Derivate, sondern auch speziell entwickelte Profile und dadurch steigende Funktionalität. Die Maschinenbauer nutzen bei neuen Baureihen also gerne die speziellen Eigenschaften und Vorteile der entsprechenden Standards wie Profinet, Ethercat, Powerlink, Sercos III, CC-Link IE oder Ethernet/IP. Die folgende Übersicht bietet einen spannenden Auszug aus dem Spektrum der verfügbaren und neu vorgestellten Produkte und Lösungen. (mby) ■

- Anzeige -



Industrial IT

ads-tec GmbH
72622 Nürtingen | Tel: +49 7022 2522-200
sales@ads-tec.de
www.ads-tec.de



Big-LinX® IoT-Service-Plattform

Die sichere Basis für Industrie 4.0

Sichere Kommunikation im Internet der Dinge. Weltweite Vernetzung von Maschinen und Anlagen über die ADS-TEC IoT-Service-Plattform. Als Endpunkt der Anlage dient die ADS-TEC Firewall der IRF2000 Serie – mit maximaler Sicherheit dank Smartcard Security.

Basis für die Fernwartung und noch viel mehr:

- Device Management
- Data Monitoring
- Predictive Maintenance
- Data Storage
- Remote-Bedienung

Erfahren Sie mehr unter
www.ads-tec.de



BECKHOFF

Beckhoff Automation GmbH & Co. KG
33415 Verl | Tel.: +49 5246 963-0
info@beckhoff.de
www.beckhoff.de

Durchgängig
Highspeed-Ethernet.



- Ethernet bis in die Klemme – vollständige Durchgängigkeit
- Ethernet-Prozessinterface, skalierbar von 1 Bit bis 64 kByte
- Ethernet-Lösung für die Feldebene
- exaktes Timing und synchronisierbar

HMS

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

Anybus



Gateways

Protokollumsetzer

Busmodule

Chip-/Brick-Lösungen

Industrial Ethernet
Produkte und Dienstleistungen

Anybus CompactCom: Flexible Feldbus-/Ethernet-Netzwerkanschlüsse für Ihre Geräte, als Modul-, Brick- oder Chip-Lösung.

Anybus X-gateways: 250 Varianten für die Verbindung unterschiedlicher Feldbusse sowie die Kopplung von Feldbus- und Industrial-Ethernet.

Anybus Communicator: Protokollkonverter für die einfache Feldbus- und Industrial-Ethernet-Anbindung Ihrer Geräte via serieller Schnittstelle

Dienstleistungen: Hard-/Softwareentwicklung und OEM-Varianten

MPL
High-Tech • Made in Switzerland

MPL AG Elektronikunternehmen
CH-5405 Dättwil | Tel.: +41 56 483 34 34
info@mpl.ch
www.mpl.ch

Rugged Industrial Ethernet
Firewall, Router, Switch, Embedded Computers



100% in der Schweiz entworfen und hergestellt

Highlights

- 10 Jahre Verfügbarkeit
- Mehr als 20 Jahre reparierbar
- Openframe bis IP67-Gehäuse
- OEM / kundenspez. Lösungen

Features

- managed & unmanaged Switch
- Media Converter
- Firewall / Router
- -40°C to +85°C

red lion

Red Lion Controls
80687 München | Tel.: +49 89 5795 9521
europe@redlion.net
www.redlion.net/de

Uptime. Anywhere

Ihr Gleis zur High-Speed Vernetzung

Industrielle IP67 Managed Gigabit Ethernet Switches mit PoE+

Red Lion's vielseitige gemanagten Switches NT24k-16M12 bieten 16 all-Gigabit Kupfer M12 X-Code Anschlüsse in einem staub- und wasserresistenten Gehäuse zertifiziert nach IP67. Der NT24k-16M12 Ethernet Switch ist für einen zuverlässigen Betrieb in Bahn- und industriellen Applikationen designed, wo Schock, Vibrationen und andere extreme Bedingungen vorherrschen. PoE ist konfigurierbar über alle 16 Anschlüsse, die Bypass Relais Ports ermöglichen eine zuverlässige Datenübertragung bei Energieausfall, ideal für Anwendungen in Bahn- und anspruchsvollen Industrieapplikationen.



sps ipc drives
Halle 8 - 327

Besuchen Sie www.redlion.net/NT24k für weitere Details

- Anzeige -



Nexans Deutschland GmbH
41238 Mönchengladbach | Tel.: +49 2166 27 2220
sales.ans@nexans.com
www.nexans.de/ans

Sichere und verlustfreie Redundanz mittels HSR/PRP



iGigaSwitch 1606 HSR SFP-6VI

- Hochverfügbare Redundanz gemäß IEC 62439-3
- Full Gigabit HSR/PRP Ports
- Live Fibre Monitoring
- IEC 61850 Data Modeling/Server/MMS/GOOSE
- KEMA/DNV-GL Level A Zertifikat
- Real-Time Betriebssystem
- Robust und kompakt, -40...+85°C, IEC 61850-3
- 240Watt Power over Ethernet
- 2x HSR/PRP und 4x Vario SFP Ports
- 10x 10/100/1000 Mbit/s RJ45 Ports
- 24/48/60V DC Versorgung
- 5 Jahre Gewährleistung



Weitere Informationen

www.nexans.de/ans



Made in Germany



Siemens AG
Process Industries and Drives
Prozess Automation
www.siemens.de/xc-200



SPS IPC Drives 2017
28. - 30. November
Halle 11
siemens.de/sps17

Switch in die Zukunft!

SCALANCE XC-200

Die managed Industrial Ethernet Switches SCALANCE XC-200 sind gigabitfähig, unterstützen VLAN und Redundanzmechanismen und können dank ihrer diversen Zertifizierungen in unterschiedlichsten Anwendungen eingesetzt werden, z. B. für Bahn, Tunnel, Automotive, Maschinenbau oder in explosionsgefährdeten Bereichen.

siemens.de/xc-200



Nexans Deutschland GmbH
41238 Mönchengladbach | Tel.: +49 2166 27 2220
sales.ans@nexans.com
www.nexans.de/ans

Robuste Industrial Ethernet Switches mit hoher PoE Leistung und Redundanz



iGigaSwitch 1002 SFP-2VI

- bis zu 8x Vario SFP Ports, 100/1000 Mbit/s
- bis zu 8x 10/100/1000 Mbit/s RJ45 Ports
- 240Watt Power over Ethernet, 8xPoE+
- Live Fibre Monitoring
- Kompaktes und lüfterloses Design
- Robust und kompakt, -40...+85°C, IEC 61850-3
- Redundanz, MRP/RSTP/MSTP/LACP
- IEC 61850 Data Modeling/Server/MMS/GOOSE
- Programmierbare I/O Schnittstellen, 2xIN/2xOUT
- 24/48/60V DC Versorgung
- 5 Jahre Gewährleistung



Weitere Informationen

www.nexans.de/ans



Made in Germany



Wachendorff Prozesstechnik
65366 Geisenheim | Tel.: +49 6722 9965-966
eea@wachendorff.de
www.wachendorff-prozesstechnik.de

Managed Switches für eine sichere Kommunikation



Gigabit Ethernet Power over Ethernet PoE/PoE+

- Managed, Full Gigabit, Layer 2
- VLANs, IEEE 802.1x (RADIUS)
- Ring-Redundanz <30 ms
- Extrem zuverlässig: MTBF 2.000.000+ h

www.wachendorff-prozesstechnik.de/eswitchm



Mit IP67-Schutz und PoE+ in industriellen Anwendungen

Der kann viel ab!



Immer mehr industrielle Geräte nutzen Power over Ethernet – kurz PoE. Auch die neuen Switch-Modelle von Red Lion sind darauf ausgelegt. Zudem bieten die Geräte Bypass-Relais und volle Gigabit-Leistung.

Die neuen Geräte eignen sich für industrielle Anwendungen, in denen es regelmäßig zu Erschütterungen, Vibrationen und extremen Temperaturen kommt.

Die N-Tron-Reihe der industriellen Ethernet-Switches von Red Lion hat Zuwachs bekommen. Die neuen PoE- und non-PoE-Modelle sind für Anwendungen konzipiert, bei denen es auf Gigabit-Leistung, erweiterte Managementfunktionen und Benutzerfreundlichkeit ankommt.

Zuverlässig und robust

Die Zuverlässigkeit der Geräte erhöht die Verfügbarkeit im Netzwerk, vermeidet Produktionsverluste und schließt Sicherheitsrisiken aus. M12-Kabelverbindungen gewährleisten Kontinuität bei den Anwendungen, in denen Bewegungen oder Vibrationen auftreten. Die Switches sind für den Betrieb in rauen Umgebungen ausgelegt. Sie verfügen mit IP67 Schutz über ein robustes, staubdichtes und wasserbeständiges Gehäuse mit sechzehn 10/100/1000Base-T(X)-M12X-kodierten Ports, und bieten dadurch ein zuverlässiges und sicheres Kommunikationsnetzwerk für Geräte in rauen Umgebungen. Sie eignen sich für industrielle Anwendungen, in denen es regelmäßig zu Erschütterungen, Vibrationen und extremen Temperaturen kommt. Zwei Bypass-Relais sorgen dafür, dass der Datenfluss selbst

bei Stromausfällen nicht unterbrochen wird. Die neuen Modelle sind mit M12-Kupferports, Plug&Play-Betrieb, Bypass-Relais Portoptionen, robuster Fernüberwachung, N-Ring und N-Link Ring-Technik sowie N-View Geräteüberwachung und Firmware-Management-Technologie ausgestattet.

Details

- NT24k-16M12: Der industrielle gemanagte GigaBit-Ethernet-Switch liefert 10 bis 49VDC redundante Spannungseingänge und ermöglicht eine Betriebstemperatur von -40 bis 85°C. Dieses Modell ist mit zwei Bypass-Relais-Portpaaren ausgestattet.
- NT24k-16M12-POE: Der industrielle gemanagte Gbit-Switch mit PoE+ verfügt über einen IEEE802.3af/at PoE-Ausgang, 240W PoE-Leistungsbudget, konfigurierbar über alle 16 Ports, bis zu 30W pro Port, 22 bis 49VDC redundante Spannungseingänge bei einer Betriebstemperatur zwischen -40 und 80°C. Das Gerät ist mit zwei Bypass-Relais-Portpaaren ausgestattet.

Die neuen NT24k-16M12-Switches sind gemäß CE, UL Class 1 Div 2 sowie für Bahnanwendungen zugelassen. Red Lions Portfolio an industriellen Vernetzungsprodukten bietet eine Vielzahl an Optionen, die Betriebsabläufe verbessern und dabei auf die Anforderungen der Industrie zugeschnitten sind. ■



Firma: **Red Lion Controls**
www.redlion.net



Halle 8
Stand 327

Direkt zur Marktübersicht i-need.de

www.i-need.de/?Produkt=12347



Die CAN-Busleitung Unitronic Bus Heat 6722 ist speziell für Aufbauten von Nutzfahrzeugen ausgelegt, kann aber durch ihr Brandverhalten auch in Innenräumen von Fahrzeugen verlegt werden.

Kabeltechnik für Nutzfahrzeuge

Brandsichere Brummis

Der CAN-Bus hat sich für die Kommunikation in Fahrzeugen fest etabliert. Doch gerade in Nutzfahrzeugen wird die Informationstechnik immer ausgefeilter und intelligenter. Für die schnelle und sichere Datenübertragung müssen Leitungen deshalb entsprechend robust, brandsicher und vielseitig sein.

Für Nutzfahrzeuge gab es bisher keine spezialisierten Leitungen. Vielmehr wurden für Nutzfahrzeuge und deren Aufbauten Standard-CAN-Bus-Leitungen verwendet. Der CAN-Bus ist seit mehr als 30 Jahren Kommunikationsstandard in der Automobilbranche. Er kann bis zu 100 Steuergeräte vernetzen. Das serielle Bussystem gilt auch heute noch als das zentrale Nervensystem zur Übertragung von Daten der Fahrzeugelektronik. Mit der Zunahme der Informationstechnik in Fahrzeugen sind auch die Mengen an CAN-Datenleitungen enorm gestiegen. In einem Mittelklassewagen stecken meist schon mehrere tausend Meter Datenleitungen, in Erntemaschinen, Müllwagen oder Feuerwehrfahrzeugen sind es noch erheblich mehr. Die Anforderungen an Leitungen, die unter freiem Himmel und in Nutzfahrzeugen ihren Dienst tun, sind meist viel höher als die, für die Standardleitungen ausgelegt sind. Um teure Ausfälle zu vermeiden, sollten sie viel robuster und flexibler sein.

Datenleitung nach CAN-Standard

Lapp hat eine neue Datenleitung speziell für Nutzfahrzeuge vorgestellt, die entsprechend robust, brandsicher und vielseitig einsetzbar ist, die Unitronic Bus Heat 6722. Sie trotzt Öl, Benzin, Diesel, Schmierstoffen, UV-Licht sowie Wind und Wetter und ist außerdem nach ISO6722 Klasse B temperaturbeständig von -40 bis +105°C. Des Weiteren wurde die CAN-Busleitung nach ECE-R 118.0 zertifiziert – eine wichtige Norm, die das Brandverhalten von Innenraummaterialien regelt. Sie dient dem Schutz von Personen im Brandfall, etwa von LKW-Fahrern oder auch von Fahrgästen in Omnibussen. Die Norm schreibt vor, dass das

Mantelmaterial halogenfrei sein muss. PVC-Kabel sind dafür nicht geeignet. Bei einem Feuer verbrennen PVC-Kabel zwar langsam, aber unter starker Rauchentwicklung, und mit dem Rauch gasen sie Halogene aus, darunter Chlor. Kommt Chlorgas mit Wasser in Verbindung – durch Löscharbeiten, oder wenn der Rauch in die Atemwege gerät – entsteht Chlorwasserstoff (Salzsäure), außerdem entstehen Säuren wie Fluorwasserstoff (Flusssäure) und Bromwasserstoff sowie das giftige Dioxin. Die Säuren verätzen die Atemwege und können schlimmstenfalls zum Tod führen, ebenso sind erhebliche Sachschäden möglich. Aus diesem Grund werden in sicherheitsrelevanten Bereichen meist Kabel mit PUR-Mantel eingesetzt. PUR ist halogenfrei. Ein normaler PUR-Mantel reicht heute allerdings nicht mehr aus, denn die Norm wurde 2015 verschärft und schreibt insbesondere strenge Flammtests vor: Dabei wird eine Flamme an die Mitte eines 50cm langen Kabelstücks gehalten und nach 15 bis 30s wieder entfernt. Der Brand am Kabelmantel muss innerhalb von 70s von selbst verlöschen, und die Flamme darf sich nicht weiter als zwanzig Zentimeter in jede Richtung ausbreiten. Ein normales PUR-Kabel würde diesen Flammtest nicht bestehen. Es würde zwar keine Halogene ausgasen, allerdings würde sich das Feuer wie an einer Zündschnur ausbreiten und könnte im Bus oder im Nutzfahrzeug weitere Kabel und die Inneneinrichtung in Brand stecken.

Brandschutz mit Spezial-PUR

Die Ingenieure von Lapp haben deshalb den PUR-Mantel entsprechend verbessert und einen Mantel aus Spezialpolyurethan ent-

wickelt. Die Herausforderung bestand darin, das Brandverhalten von PUR auf das Niveau von PVC zu heben. Die neue Rezeptur enthält einige Additive, die keinerlei Gesundheitsgefahr darstellen, auch wenn sie bei einem Brand in die Luft gelangen sollten. Und sie enthalten keine Halogene. Das hört sich einfach an, in der Praxis war die Entwicklung allerdings extrem aufwändig. Zwei Jahre lang haben die Ingenieure an der geeigneten Rezeptur getüftelt, ein weiteres Jahr dauerte es, bis die Zertifizierung bei einem der beiden in Deutschland zuständigen Prüflabore durch war.

Weniger Gewicht und Platz

Neben dem Mantel aus Spezial-PUR zeichnet sich die neue Leitung von Lapp durch ihren geringen Durchmesser aus, denn in Nutzfahrzeugen ist der Platz für Leitungen meist begrenzt. Deshalb ist die neue CAN-Bus-Leitung als Sternvierer aufgebaut: bei einem Kabel mit vier Adern werden jeweils die zwei gegenüberliegenden Adern miteinander verseilt und die Paare dann ebenfalls verseilt (Twisted Pair). Der Außendurchmesser eines Sternvierer-Kabels beträgt nur das 2,4-fache des Durchmessers der vier einzelnen Adern im Inneren. Damit ist das Sternvierer-Kabel um rund 30 Prozent dünner als ein herkömmlich aufgebautes Kabel. Das spart Platz und Gewicht

und erlaubt enge Biegeradien. Die CAN-Busleitung gibt es in vier Varianten mit Aderquerschnitten von 0,25 bis 0,75mm². Damit kann sie unterschiedliche Zahlen von Teilnehmern sowie verschiedene Segmentlängen abdecken.

Brandschutz in Bussen

Ein besonders brandsicheres Kabel mit Spezial-PUR hat Lapp auch für Omnibusse entwickelt. Es erfüllt die neue EU-Norm und darf im Fahrgastraum von Omnibussen verlegt werden. Gleichzeitig überträgt die Etherline Heat 6722 hohe Datenraten je Variante nach Cat5e, Cat6_A und Cat7. Die Leitung enthält acht flexible verzinnte Kupferleiter der Klasse AWG24 mit Querschnitten zwischen 0,18 und 0,20mm². Das erlaubt Power over Ethernet, das Übertragen kleiner elektrischer Leistungen zum Betrieb von kleinen Geräten wie Sensoren oder Überwachungskameras. ■

Autor: Jürgen Greger,
Produktmanager Automation,
U.I. Lapp GmbH
www.lappkabel.de



Halle 2
Stand 310

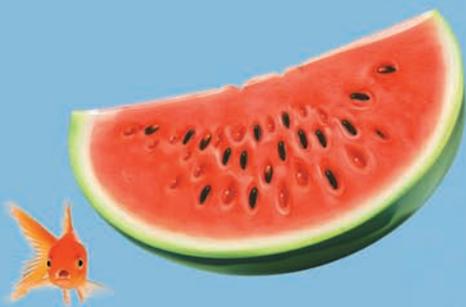
Direkt zur Marktübersicht i-need.de

www.i-need.de/?f10655

- Anzeige -

DTOS - DESIGN TO ORDER SERVICES

HMI - IPC - Embedded Systeme nach Maß



Das Standard Produkt entspricht nicht ganz ihren Anforderungen?



Dann lassen Sie sich Ihr IT-Produkt anpassen!



InoNet der kompetente DTOS-Partner von Advantech

Gerne können Sie uns auch auf der Homepage www.inonet.com oder www.advantech.eu besuchen. Sie benötigen eine Eintrittskarte zur SPS IPC Drives? Dann schreiben Sie uns unter: sales@inonet.com

Erfahren Sie mehr darüber und besuchen Sie uns auf der SPS IPC Drives  in Halle 7 am Stand 180 von

ADVANTECH

Enabling an Intelligent Planet



Technologieübergreifende Vernetzung von Werkzeugmaschinen

Automation ohne Grenzen

Wie können Maschinenbauer die Overall Equipment Effectiveness (OEE) steigern und gezielt Datenanalysen für Entwicklung, Vertrieb und Service nutzen? Fragen wie diese beantwortet ein neuer Industrie 4.0-Showcase, der unter anderem zwei Messemaschinen und eine Produktivanlage des weltweit tätigen Rundtaktmaschinenherstellers Pfiffner vernetzt.

Der Demonstrator zeigt dabei auch, dass die durchgängige Vernetzung keine technologischen Grenzen kennt. Denn mit dem Showcase vernetzt Bosch Rexroth nicht nur elektrische Komponenten, sondern auch Hydraulik und Lineartechnik. Die maßgebliche Software für zustandsbasierte Überwachung und Wartung bilden der neue Data Analytics Server (DAS) und das IoT Gateway. Eine sichere Verbindung zur Bosch IoT Cloud gestattet ein standortübergreifendes Performance Monitoring.

Vernetze Rundtaktmaschinen

Eine Live-Demonstration von Status, Zustands- und Leistungsüberwachung der Maschine konnten Besucher der Fachmesse Emo erleben. Die drei vernetzten RT und PT Rundtaktmaschinen des OEM-Partners sind für die Massenfertigung ausgelegt und werden vom hochperformanten und individuell skalierbaren CNC-System IndraMotion MTX advanced gesteuert. Der auf einem gängigen Industrie-PC installierte Data Analytics Server sammelt in Echtzeit aufschlussreiche Daten wie Betriebsmodus, Zykluszeit, Stückzähler oder Motortemperatur. Zur Kommunikation mit den Maschinen und den übergeordneten IT-Systemen nutzt der Data Analytics Server das OPC-UA-Protokoll. Mit dem IoT Gateway, das Sensor- und Maschinendaten sammelt, lassen sich insbesondere Bestandsanlagen ohne Eingriff in die Automa-

tisierungsinfrastruktur transparent machen. Neben dem DAS unterstützt das IoT Gateway auf der Auswertungsebene auch zahlreiche Cloud-Services.

Übermittlung von Echtzeitdaten

In einem Maschinenmodul von Pfiffner mit der Steuerung IndraMotion MTX advanced liefert ferner der via Sercos angebundene IndraDrive-Spindeltrieb Echtzeitdaten an den Data Analytics Server, ebenso das mittels Profinet angesteuerte Kompaktaggregat CytroPac. Erfasst werden hierbei Drehzahl und Druck sowie Ölstand, -temperatur und Filterzustand. Auf Basis aller gesammelten Daten berechnet, analysiert und visualisiert der DAS im Rahmen des Demonstrators den Zustand und die Nutzung der Maschinen. Die lokal gespeicherten Daten stehen dem Maschinenhersteller bei Bedarf ferndiagnostisch zur Weiterentwicklung und gezielten Fehlersuche zur Verfügung, insbesondere um die mit dem Endanwender vertraglich zugesicherte Produktivität sicherzustellen.

Sichere Anbindung an die Cloud

Für das standortübergreifende Performance Monitoring streamt der DAS vorverarbeitete Daten über eine sichere Verbindung in die Bosch IoT Cloud - zur anschließenden Auswertung durch den Production Performance Manager von Bosch Software Innovations. Auch darüber hinaus werden zahlreiche Daten übermittelt und verarbeitet. Stellvertretend für den Bereich Lineartechnik sind dies etwa Positions- und Beschleunigungsdaten aus dem integrierten Messsystem IMS-A. So lassen sich beispielsweise qualitätsrelevante Kollisionen aufdecken. ■

Firma: Bosch Rexroth AG
www.boschrexroth.de



Halle 7
Stand 450

Direkt zur Marktübersicht i-need.de

www.i-need.de/?Produkt=2472

TSN bereits im Nacken – Profinet noch vor der Brust

Switch mit Zukunft



Der Profinet Switch PROmesh P9 überwacht permanent Netzlast, Telegramme und sogar Ableitströme und dokumentiert sie für eine schnelle Fehlersuche.

Bild: Indu-Sol GmbH

Der technologische Wandel stellt neue Herausforderungen an die Datenkommunikation: Geringe Übertragungszeiten, hohe Verfügbarkeit, Echtzeit, Zuverlässigkeit und letztlich eine offene Plattform. Die derzeit eingesetzten, Ethernet-basierenden Übertragungsprotokolle kommen der Erfüllung dieser Ansprüche durchaus schon sehr nahe, haben aber in Bezug auf Bandbreite und Latenzzeiten noch erheblichen Nachholbedarf. Eine Lösung für die Forderung nach einer herstellerunabhängigen Kommunikationsplattform scheint erst mit Time-Sensitive Networking (TSN) in Sicht. Dann ist zu erwarten: Je intelligenter das Netz selbst, desto mehr verlieren klassische Steuerungen ihre zentrale Rolle.

Leistungsfähige Infrastrukturkomponenten wie Switches übernehmen nicht mehr nur die Verteilung, sondern auch Aufgaben der Datenspeicherung, -steuerung und -überwachung und werden somit zur zentralen Komponente im Netzwerk. Der Profinet-Switch PROmesh P9 von Indu-Sol ist ein erster Baustein dafür. Er ist darauf ausgelegt, den gesteigerten Performance-Anforderungen der Automatisierungsbranche Rechnung zu tragen und überwacht die EMV-Belastung des Netzwerks.

Überwachung von Ableitströmen

Highlight des Profinet-Switches ist eine permanente Überwachung von Ableitströmen. In der komplexen Automatisierungstechnik sind nicht selten überhöhte Schirmströme die Ursache für Unregelmäßigkeiten im Datenverkehr, welche bis hin zu zerstörten Geräten führen können. Eine punktuelle Bewertung mit Hilfe einer handelsüblichen Strommesszange greift hier zu kurz, da die beschriebenen Effekte mitunter nur zu bestimmten Zeitpunkten auftreten. Hier braucht es eine kontinuierliche Messung

über das gesamte Frequenzspektrum (20kHz). Es erfolgt hierbei nicht nur die Erfassung des Mittelwertes (RMS-Messung), sondern auch das Feststellen der Spitzenwerte (Peaks).

Bedürfnisse der Instandhaltung

Das Webinterface des Switches ist speziell auf die Instandhaltungsbedürfnisse der Automatisierungstechnik abgestimmt. Hier wurde besonderer Wert auf die einfache grafische Darstellung der Portstatistiken, Fehlerspeicher und ein integriertes Alarmmanagement gelegt. Die bekannten Ampelfarben geben Hinweise zum Netzwerkzustand und sind gleichzeitig Hinweis zum Handeln. Auf der SPS IPC Drives 2017 wird der Switch erstmals der Öffentlichkeit vorgestellt. ■

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



Halle 2
Stand 641

Direkt zur Marktübersicht **i-need.de**

www.i-need.de/?f15249

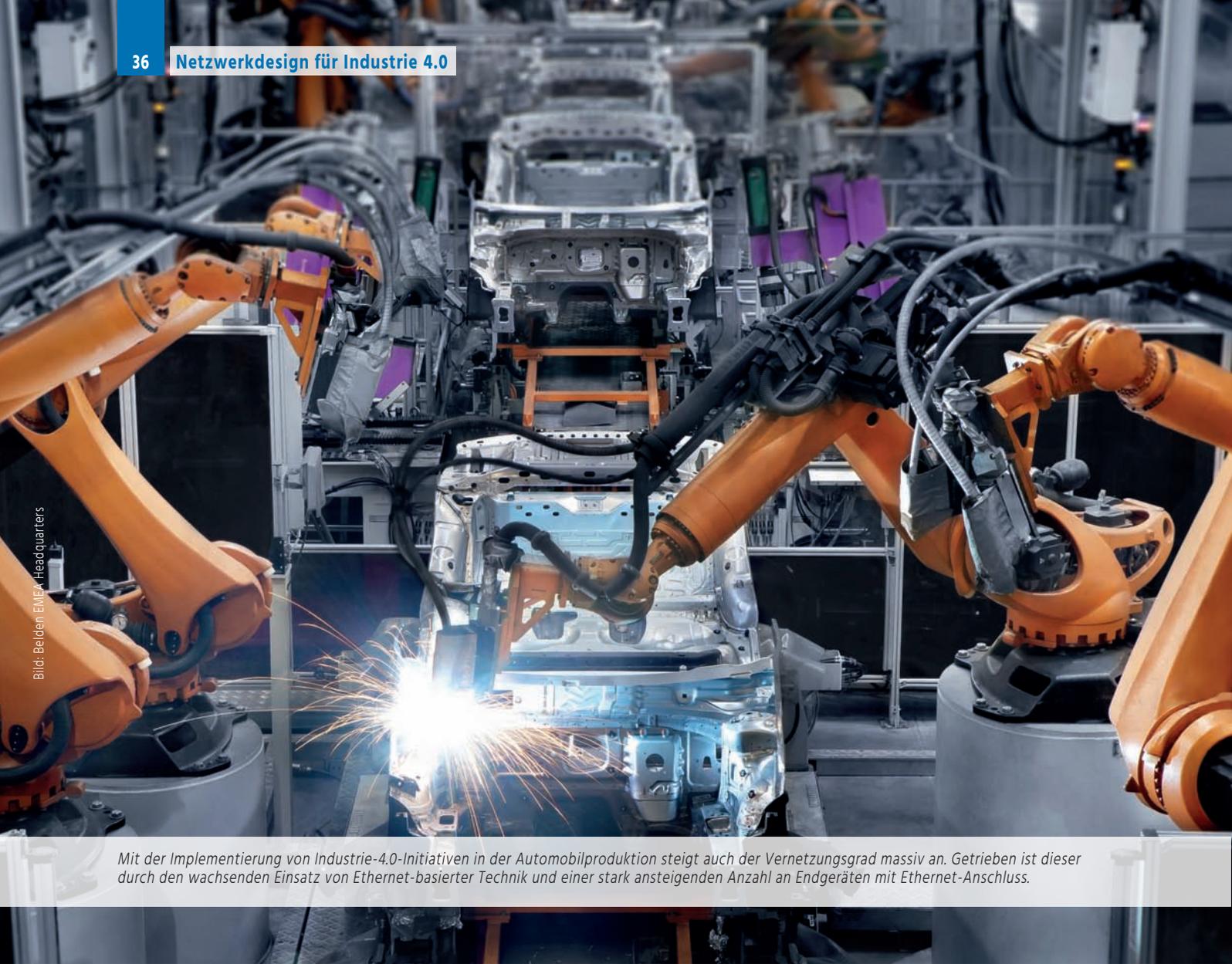


Bild: Beiden, EMEA-Headquarters

Mit der Implementierung von Industrie-4.0-Initiativen in der Automobilproduktion steigt auch der Vernetzungsgrad massiv an. Getrieben ist dieser durch den wachsenden Einsatz von Ethernet-basierter Technik und einer stark ansteigenden Anzahl an Endgeräten mit Ethernet-Anschluss.

Kommunikation für Produktionszellen aufbauen

Drei sind keiner zuviel

Die Integration aller Komponenten in einer Netzwerkstruktur ist notwendig, denn diese bilden das Fundament für die Digitalisierung von Produktionsprozessen. Die Segmentierung der Produktionsnetze in die drei wesentlichen Bereiche, Kern (Core) über die Verteilungsschicht (Distribution) bis hin zur Zugriffsebene (Access), wird auch zukünftig Bestand haben. Doch zukünftig kann man verstärkt von einem Netzwerkdesign zugunsten einer komplett gerouteten Topologie ausgehen.

Die zentralen Anforderungen und Hauptmerkmale für ein zukunftsfähiges Netzwerk im Kontext der Aktionsfelder von Industrie 4.0 über die drei Ebenen können wie folgt erläutert werden.

Backbone-Kommunikation für Anbindung nach oben

Um diese zunehmende Komplexität zu bewältigen, werden modernste Netzwerke in logische Segmente unterteilt, die jeweils

auf spezifische Produktionsprozesse mit einer überschaubaren Teilnehmerzahl ausgerichtet sind.

- **Bandbreitenreserven des übergeordneten Produktionsnetzwerks:** Bereits heute wird eine Vielzahl von Daten über das Kommunikationsnetzwerk verteilt, beispielsweise Arbeitsaufträge an Maschinen, Software-Updates sowie Video-Daten von Vision Systemen und vieles mehr. Der Datendurchsatz ist auf dieser Ebene sehr hoch und wird weiter rasant zunehmen.

Die Verbindung zwischen den Switches auf der Core Ebene ist zunehmend auf 10Gbit/s und mehr ausgelegt. Die Anbindung an die nächst untere Distribution-Ebene kann mit dem neuen 2,5Gbit/s-Standard nach IEEE802.3bz realisiert werden und ermöglicht höhere Datenübertragungsraten über Cat5e- und Cat6-Kabel auf 100m ohne Neuinvestitionen in die bestehende Verkabelungsinfrastruktur zu tätigen. Einer der Treiber für diese Zwischenstufe beim drahtgebundenen Ethernet ist die zunehmende Anbindung von Wireless, die inzwischen über 1Gbit/s und zukünftig mehr übertragen, woraus sich ein Bandbreitenengpass in dem Netzwerksegment ergibt.

- **Hochverfügbarkeit und Redundanz:** Die Erhöhung der Netzverfügbarkeit ist maßgeblich, so dass Störungen einzelner Netzwerkkomponenten keine Ausfallzeiten verursachen. Dies kann durch Redundanzmechanismen wie MRP (Media Redundancy Protocol) und DLR (Device Level Ring), die gewisse Umschaltzeiten einhalten, bis hin zu garantierten Zeiten von null Millisekunde via PRP (Parallel Redundancy Protocol) oder HSR (High availability Seamless Redundancy) erreicht werden. Weitere Protokolle wie das Virtual Router Redundancy Protocol (VRRP) erlauben eine redundante Anbindung von dem Produktionsrouter an das übergeordnete Unternehmensnetzwerk. In den Automobilwerken ist die Größe der Netzwerke ein bestimmender Faktor, der weiter stark wachsen wird. Hier ist der Einsatz von IT Standards wie das dynamische Routing-Protokoll OSPF (Open-Shortest-Path-First) von Vorteil, insbesondere in der schnelleren Konvergenz und der besseren Skalierbarkeit. Weitere IT Standards wie MPLS (Multiprotocol Label Switching) bieten eine Bandbreitenreservierung für die unterschiedlichen Dienste an. Der TSN Standard mit seiner Hochverfügbarkeit wird ebenfalls in der Produktion zukünftig zunehmend eingesetzt werden.
- **Echtzeit-Kommunikation:** Die Echtzeit-Kommunikation vom Feld bis in das Backbone ist eine Anforderung, um SPS-Geräte in der lokalen Cloud zukünftig anzubinden. Time-Sensitive Networking (TSN) ist vollständig kompatibel mit den heutigen Ethernet-Netzwerken. Es ermöglicht eine Übertragung von Daten mit harten Echtzeitanforderungen und Hintergrunddaten, ohne dass es zu wechselseitigen Störungen kommt. Die Unterstützung des Standards zeigt sich unter anderem an dem Beitritt von Rockwell Automation in die Time-Sensitive Networking Task Group (IEEE802.1) und vielen weiteren bedeutenden Automatisierungsunternehmen.

Netzwerkanbindung von Produktionszellen

Der Netzwerkzugang bietet einen Übergabepunkt, der jede Produktionszelle mit der Kommunikation mehrerer Maschinen in der Feldebene verbindet. Die Distributionsebene steht vor erheblichen technologischen Veränderungen, die sich aus den künftigen Anforderungen aus den Aktionsfeldern von Industrie 4.0 und der Virtualisierung von Anwendungssteuerungen ergeben.

- **Steigende Bandbreitenanforderungen:** Die Bandbreitenanforderungen nehmen auch in der Distributionsebene erheblich zu, getrieben von den zuvor ausgeführten Treibern.

- **Flexible Segmentierung und Schutz des Produktionszellen-netzwerks:** Die Anbindung der Produktionszellen bedingt durch die hohe Anzahl an Maschinen eine Segmentierung aus mehreren Gründen. Zum einen können durch eine Segmentierung die Auswirkungen von Netzwerkfehlern und Ausfällen sowie von Cyber-Angriffen lokal begrenzt werden. Zum anderen ermöglicht eine prozessorientierte Segmentierung mit einer überschaubaren Anzahl an Automatisierungsteilnehmern die Flexibilität der Anlagen durch einfaches Einbinden weiterer Komponenten zu erhöhen. Die Segmentierung erfolgt im Layer 2 durch VLANs in Kombination Layer 3 (Routing) Verfahren für die IP Kommunikationen. Durch die wachsende Zahl von IP-Geräten hat zum einen die Größe der einzelnen VLANs und zum anderen auch die Anzahl der VLANs zugenommen. Dies kann zu Broadcast-Stürmen oder anderen Flooding-Problemen führen. Im Gegensatz dazu reduziert das Routing zur Zugriffsschicht die Größe der Fehlerauswirkungen drastisch, nutzt alle Verbindungen und bietet eine anpassbare, dynamische Netzwerkumgebung. Der Einsatz von Stateful Firewalls erhöht die Netzwerksicherheit in einer durchgängigen Routing-Netzarchitektur, kombiniert mit Zugangsbeschränkungen über Access-Control-Listen (ACLs) in den Switches bereits auf der Ebene der Produktionszelle. Insbesondere das Zonenkonzept der IEC62443 findet eine starke Akzeptanz im Automobilumfeld. Neben dem Ansatz zentraler Firewalls wird der genannte dezentrale Ansatz nahe der Produktionszelle zunehmend an Bedeutung erlangen. Eine zusätzliche Kombination mit proaktiven industriellen Security-Überwachungslösungen, die Anomalien im Datenverkehr aufdecken, sorgt für eine weitere Erhöhung der Sicherheit im Feld.

Access: Kommunikation in der Feldebene

Das Netzwerk in der Feldebene zwischen und innerhalb von Maschinen ermöglicht es, Endgeräte innerhalb einer Produktionszelle miteinander zu verbinden. Die Kommunikation auf dieser Ebene wird sich voraussichtlich deutlich verändern, wenn die Standards des Industrial Internet of Things (IIoT) umgesetzt werden.

- **Deterministische Echtzeit-Kommunikation:** Bedingt durch den zunehmenden Einsatz von Profinet und Ethernet/IP-Netzwerken zur Steuerung und Vernetzung von Maschinen ergibt sich der Bedarf an Echtzeitkommunikation. Darüber hinaus ist mit einem Paradigmenwechsel der Anbindung von Feldgeräten in der Maschine hin zu virtuellen Steuerungen zu rechnen. Voraussetzung hierfür ist der Einsatz von Echtzeit-Switches, die auf neue offene Standardisierungsverfahren wie TSN beruhen und auf dem vorhandenen Ethernet-Kommunikationsprotokoll aufbauen.
- **Integration der Anlagen mit der gleichen IP Adresse:** Durch die zunehmende Verbreitung von Ethernet in den Maschinen besitzen Endgeräte wie I/O-Devices in jede Maschine eine eigene IP-Adresse. Zur Integration dieser Anlagen über den Netzwerkzugang in das übergeordnete Distributionsnetz können daraus IP-Adressen Engpässe entstehen. Durch den Einsatz der NAT-Funktionalität in den Layer-3 Switches oder rou-

tingfähige Firewalls kann eine individuelle Anpassung der IP-Adresse vermieden werden, da NAT diese automatisch übersetzt. Daraus ergibt sich der Vorteil, dass die Netze identisch aufgebaut werden können und somit für Automatisierungstechniker einfacher zu bedienen sind.

- **Beständig gegen Vibration, Schock, Schweißfunken, Chemikalien oder Temperatur:** In den Produktionszellen der Gewerke Powertrain und Body Shop sind die Anforderungen an die Komponenten im Feld besonders hoch. Im Body Shop erfolgt die Reinigung der Roboter zum Teil mit Trockeneis. Zusätzlich beanspruchen Schweißfunken und somit kurzfristig auftretende hohe Temperaturen bis 700 Grad die Leitungen und elektronischen Bauteile nahe dem Roboter. Im Powertrain Bereich spielt die Öl- und Chemikalienbeständigkeit sowie Vibrations- und Schockfestigkeit eine erhebliche Rolle. Getrieben durch den Trend zur Reduzierung der Automatisierungskosten rücken Bauteile wie Switches und IO Module näher an die Maschine und es erfolgt eine Eliminierung des Schaltschranks. Zunehmend kommen daher Komponenten in IP56 und höher sowie mit M12-Anschlusstechnik zum Einsatz.
- **Unterbrechungsfreie Kommunikation von Wireless LAN:** Der Anteil an selbstfahrenden Flurförderfahrzeugen und Warehouse Shuttles ist zunehmend ein zentraler Bestandteil zur Materialversorgung in den Automobil-Produktionsstätten und wird ein wesentlicher Baustein in der Industrie 4.0 Initiativen

werden. Die mobilen Einheiten erlauben einen losgelösten Materialfluss weg von dem Fließbandprinzip hin zu flexiblen Produktionsinseln. Eine hochverfügbare Wireless LAN Verbindung, die eine große räumliche Abdeckung sowie garantiertes unterbrechungsfreies Roaming ermöglicht, sind essentiell, um die Anforderungen zu erfüllen. Wireless LAN wird in weiteren Applikationen in den Produktionszellen Einzug finden bis hin zur drahtlosen Anbindung von Robotern, die Safety-Anforderungen erfüllen müssen. Interessante zukunftsweisende Lösungsansätze bieten sich mit WLAN in Verbindung mit PRP an. Weitere Einsatzbereiche wie Condition Monitoring zur Übertragung von Videosignalen und zur Zustandsüberwachung von Pressen sind zu nennen. Die Wireless-Anbindung von Akkuschaubern im Bereich Montage ist ein weiteres Feld von neuen Anwendungen. In Summe wird mit einem Anstieg auf deutlich über 10.000 Wireless-Schnittstellen in einem einzigen Produktionswerk in den nächsten Jahren gerechnet. Hierdurch ergeben sich weitere Anforderungen hinsichtlich Skalierbarkeit und Bandbreite für die eingesetzte Wireless-Technik. ■

Firma: **Belden EMEA Headquarters**
www.belden.com



Halle 10
Stand 121

Direkt zur Marktübersicht **i-need.de**

www.i-need.de/?f35692

Industrial Ethernet

Keine Bauchschmerzen

Für die industrielle Kommunikation sind Ethernet-basierte Netzwerke wie Profinet heute die erste Wahl. Das liegt nicht nur an den deutlich höheren Übertragungsraten im Vergleich zu seriellen Feldbussen, sondern auch an der wesentlich größeren Flexibilität.



Bild: IVG Göhringer

*Hans-Ludwig Göhringer
ist Geschäftsführer
der Firma IVG Göhringer.*

Verschiedene Protokolle laufen parallel und die Topologie lässt sich nahezu beliebig erweitern. Diese Vielfalt führt jedoch zu einer höheren Komplexität, die sich bei der Abnahme und bei der Fehlersuche in der laufenden Anlage bemerkbar macht. Eine sachgerechte Erdung der Anlage und eine saubere Schirmauflage sind das A und O. EMV-Störeinflüsse – beispielsweise ausgelöst durch Starkstrom, Frequenzumrichter oder geschaltete Induktivitäten

– lassen sich im Vergleich zu seriellen Feldbussen messtechnisch wesentlich schwerer erfassen, da die Frequenz von Nutz- und Störsignal bei Ethernet eng beieinander liegen. Zudem ist bei den Punkt-zu-Punkt-verkabelten Ethernet-Netzen nicht einfach ein Diagnosegerät an einer beliebigen Stelle des Netzwerks einklinkbar. Bei Anlagen, die zum Einbau einer Messstelle nicht abgeschaltet werden können, sollte bereits bei der Konzeption der Netzwerke sogenannte Test-Access-Points (TAPs) als Messstelle vorgesehen werden. Allerdings ist hier Vorsicht geboten, da einige TAPs am Markt Kurzschlüsse verursachen. Wichtig sind Messstellen mit echter galvanischer Trennung ohne Rückwirkung auf das Netzwerk. Andernfalls baut man eine zusätzliche Fehlerquelle ein, was bei der Suche von Störungen im Netzwerk eher hinderlich ist. ■

INDUSTRIAL
COMMUNICATION
JOURNAL

ETHERNET



WIRELESS



SECURITY



CC-Link *IE* ermöglicht Industrie 4.0 mit offenem Gigabit Ethernet

CC-Link IE und Industrie 4.0

Integriertes Industrienetzwerk
für das Internet of Things

Seite 41

CC-Link IE Field Basic

Erweiterung der CC-Link-IE-
Kompatibilität auf 100MBit-Ethernet

Seite 46

Partnerschaften und Netzwerk

Zusammenarbeit mit anderen
Organisationen ist zentrale Aufgabe der CLPA

Seite 49

Die Weiterentwicklung von CC-Link IE:

Integriertes Industrienetzwerk für die Industrie 4.0



Bild: CLPA Europe

Moderne Konzepte wie e-F@ctory und Industrie 4.0 in der IT-gesteuerten Produktion erfahren derzeit große Aufmerksamkeit. Gemeinsamer Grundgedanke dieser Technologien ist die Integration und Optimierung der IT auf Management-, Produktions- und Maschinenebene. Dafür sind Fertigungsnetzwerke mit hoher Datenrate und hoher Konnektivität notwendig. Die Nutzung der CC-Link-Familie liegt also nahe.

Die in der Fertigungsindustrie eingesetzten IT-Systeme lassen sich grob in drei Ebenen einteilen: Management, Produktion und Maschinen. Traditionell befinden sich die Managementsysteme in der Zentrale und die Produktions- und Maschinensysteme an den Fertigungsstandorten. Dem Globalisierungstrend entsprechend sind die Fertigungsstandorte häufig in aller Welt verteilt, dasselbe gilt für die entsprechenden Produktions- und Maschinensysteme. Hierbei wurden für die jeweiligen Regionen unterschiedliche Systeme entwickelt. Außerdem ist im Interesse der lokalen organisatorischen Optimierung bisweilen sogar die Managementebene regional aufgebaut. Hier ist die globale Integration von cloudbasierten Fertigungs-IT-Systemen auf dem Vormarsch.

Fertigungs-IT-Systeme der Zukunft

Cloudanbindung, Big Data und künstliche Intelligenz gehören zu den Megatrends in der Produktions-IT. Die Fertigungsindustrie kann auf der Basis von Informationen viele Verbesserungen und Kostensenkungen erzielen, um im Wettbewerb besser bestehen zu können. Sie können Instandhaltungsprozesse verbessern, Ausfallzeiten reduzieren, die Qualitätsstabilität erhöhen und auch Produktionsabläufe in Koordination mit der Lieferkette optimieren. Damit diese neuen Anwendungen genutzt werden können, sind auf der Maschinenebene Hochgeschwindigkeitsnetzwerke mit entsprechender Kapazität notwendig, um große Mengen an Daten zu verarbeiten. Außerdem geht der Trend in der Fertigung von der Massenproduktion zur kundenindividuellen Massenproduktion und tendiert zur Einzelfertigung vielfältiger Modellvari-

anten. Kostengünstige Einzelfertigung ist daher ein zentrales Ziel von Industrie 4.0. Sie stellt bestimmte Anforderungen an die Produktionstechnologie und auch an die herkömmlichen Technologien. Eine Herausforderung ist das Netzwerk auf der Maschinenebene. Diese Anforderungen lassen sich vereinfacht so zusammenfassen:

- Einfache Integration in die Produktionsebene unter Berücksichtigung von Echtzeitanforderungen
- Garantierte kontinuierliche Produktion UND Sicherheit (Safety) von Personen und Anlagen
- Integration und nahtlose Anbindung verschiedener Netzwerktypen, einschließlich Sensornetzwerke
- Hohe Geschwindigkeiten und Kapazitäten als Voraussetzung für die Nutzung neuer Anwendungen
- Einfache Netzwerkkonfiguration

Was die Systemintegration mittels der Cloud angeht, so verlangt das Netzwerk auf der Produktionsebene eine einfache und sichere vertikale Integration in das Managementsystem. Bei der Vereinfachung der vertikalen Integration spielt OPC UA eine immer größere Rolle. Zudem bietet das Protokoll eine Datensicherheitsfunktion (Security). Das Netzwerk auf Maschinenebene muss sich einfach an das Produktionssystem anbinden lassen. Die Echtzeitfähigkeit steht hier im Vordergrund. Auch unterscheiden sich die Security-Anforderungen von denjenigen der höheren Ebenen. Die Maschinenebene verlangt kontinuierliche Produktivität, auch im Falle eines unvorhergesehenen Ereignisses. Neben der Datensicherheit spielt hier auch die Sicherheit von Personen und Anlagen eine Rolle (Safety). Da zudem die Maschinenebene

unterschiedliche Netzwerke umfasst (z.B. Sensornetzwerke), ist eine nahtlose Einbindung der verschiedenen Netzwerkebenen wichtig.



Bild: CLPA Europe

Echtzeit-Performance und Integrationskomfort

Das SLMP (Seamless Message Protocol) ermöglicht die Verbindung zwischen einem überlagerten System und Feldgeräten unabhängig von den Unterschieden der Feld-Protokolle.

Aufgrund der Geschwindigkeitsleistung und der erweiterbaren Echtzeit-Performance findet CC-Link IE Control verstärkt Anwendung in der Flachbildschirmproduktion und im Automobilbau. CC-Link IE drückt Echtzeit-Performance mithilfe des 'Link-Scan-Time'-Index aus. Die untere Abbildung zeigt die Link Scan Time für eine Anordnung von 32 Stationen mit gleicher Speicherzuweisung über CC-Link IE Control. Neben der zyklischen Kommunikation in Echtzeit bietet CC-Link IE transiente Kommunikation für Rezeptweitergabe, Qualitätsdatenerfassung usw. Außerdem kann die hohe Bandbreite von 1Gbps für zyklische und transiente Kommunikation aufgeteilt werden. Auf diese Weise werden Störungen der zyklischen Kommunikationsperiode durch transiente Kommunikation vermieden.

Safety und Security mit CC-Link IE

Die Datensicherheit auf der Produktionsebene wird bei der Verwendung von CC-Link IE durch die Nutzung des OPC-UA-Standards realisiert. Im Hinblick auf die Zukunft und von Markttrends müssen die Koordination für ISASecure, EDSA-Zertifizierung usw. noch diskutiert werden. Für das Thema Sicherheit im Sinne von Safety wurde CC-Link IE Safety definiert, um Sicherheitskommunikation bei Verwendung von CC-Link IE zu realisieren. Das heißt, beim Anhalten eines Prozesses durch eine Sicherheitsfunktion werden abhängige Prozesse synchron gestoppt, sodass der Neustart nach der Fehlerbehebung beschleunigt wird.

Integration und Anbindung verschiedener Netzwerke

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

Komfortable Netzwerkkonfiguration mit CC-Link IE

CC-Link IE verwendet Ethernet als unterste Kommunikationsebene und Token Passing Methode für die Kommunikationssteuerung auf höherer Ebene. Hierbei werden die Datenübertragungsrechte (Tokens) im Netzwerk auf einer festgelegten Route von Station zu Station weitergegeben. Nur diejenigen Stationen mit Datenübertragungsrechten können Daten übertragen. Derzeit werden Tokens auf einer statisch festgelegten Route weitergegeben, aber es ist auch technisch möglich, diese Route dynamisch mit beliebigen Intervallen zu ändern. In der Zukunft wird dies Routen-Switching in Abhängigkeit von dem zu fertigenden Produkt ermöglichen. Das ist genau das, was Industrie 4.0 ausmacht. Simultane Fehlersuche ist bei der Netzwerkkonfiguration ebenfalls wichtig. Bei Störungen im Netzwerk muss die betreffende Stelle schnell zu finden sein. CC-Link IE bietet verschiedene Werkzeuge zur schnellen Auffindung von Fehlern: beispielsweise ein Managementwerkzeug für Netzwerkereignis Historie, ein Netzwerkd Diagnosewerkzeug usw.

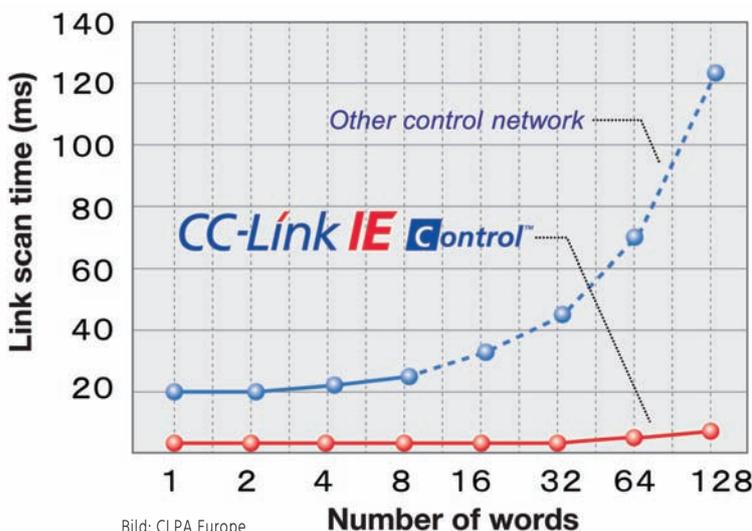


Bild: CLPA Europe

Im Vergleich zu anderen Controller-Netzwerken werden beeindruckende Geschwindigkeiten erreicht und man sieht, dass die Leistung selbst bei einem größeren Datenaustausch im Netzwerk (Gesamtanzahl an Link Points) nicht an Geschwindigkeit verliert.

Zusammenfassung

CC-Link ist nicht nur sehr schnell, sondern bietet darüber hinaus noch eine ganze Reihe anderer Faktoren, die es als integriertes Industrienetzwerk empfiehlt. Die zentralen Anforderungen, die die Industrie 4.0 oder e-F@ctory an die Kommunikation stellen, treffen hier sehr gut mit den Fähigkeiten von CC-Link aufeinander. (kbn) ■

Firma: CLPA Europe
eu.cc-link.org

Gigabit Ethernet überzeugt Analysten und Entscheider

Anlässlich ihres 15-jährigen Bestehens trat die CC-Link Partner Association (CLPA) als Corporate Sponsor des ARC Industry Forum Europe 2017 im spanischen Sitges auf. Das Forum ist Teil einer von der ARC veranstalteten und weltweit erfolgreichen Konferenzreihe, die Jahr für Jahr eine große Anzahl an Teilnehmern aus den Führungskreisen der wichtigsten europäischen Fertigungsunternehmen anzieht.

CC-Link IE und die Feldbus-Version CC-Link sind in Asien der offene Industriestandard für Automatisierungsnetzwerke und gewinnen auch weltweit immer mehr an Boden. Möglichst ungehinderte Kommunikation zwischen Geräten ist einer der wesentlichen Aspekte der Industrie 4.0, was die CLPA zum Anlass nahm, um einen Workshop zum Thema anzubieten. Kernpunkt war hierbei die einzigartige Gigabit Ethernet Performance von CC-Link IE als Entscheidungskriterium bei der strategischen Weichenstellung von Unternehmen für die Industrie 4.0. Im Rahmen der Veranstaltung fand eine Podiumsdiskussion unter der Leitung von Analytikern der ARC statt. Weitere Teilnehmer waren Vertreter führender Industrieunternehmen wie Hilscher, Mitsubishi Electric und der OPC Foundation. Die anschließende Präsentation veranschaulichte wie der führende Automobilhersteller Suzuki CC-Link IE für komplexe Aufgaben, wie z.B. in der Prozesssteuerung und

David Humphrey ist Analyst bei ARC Europe. Er verfügt über mehr als 25 Jahre Erfahrung in der industriellen Automatisierung. In seiner Bewertung von CC-Link IE hebt er die Bedeutung der schnellen Kommunikation in der modernen Fertigungswelt hervor.



Bild: ARC Advisory Group Europe

Entwicklungen wie Industrie 4.0 und das Industrial Internet of Things (IIoT) stellen neuartige Anforderungen an die betriebliche IT-Infrastruktur und Automatisierungsarchitekturen. Einerseits erschließen sich Maschinenbauern und Endanwendern noch nie dagewesene Möglichkeiten, wertvolle Prozessdaten zu erfassen und auszuwerten – andererseits stoßen sie dabei nicht selten auch an die Grenze ihrer Netzwerkbandbreite. Industrielle Ethernet-Technik wird in der Regel nicht so schnell aktualisiert wie Büronetzwerke, die meisten gehen über eine Geschwindigkeit von 100Mbit pro Sekunde (Mbps) noch nicht hinaus. Ein Netzwerk sticht jedoch mit einer Ultra-Highspeed-Kommunikation von 1Gps Bandbreite sowohl für den synchronen, deterministischen Datentransfer als auch für asynchrone Nachrichtenübertragung hervor: CC-Link IE. Dies bedeutet, dass neben maschinenbezogenen Funktionen wie etwa E/A-Steuerung oder Koordination von Servoachsen noch genügend Bandbreite für die Übertragung großer Datenvolumen von modernen IIoT-fähigen Maschinen übrig bleibt. ■



Bild: CLPA Europe

„Mit der konkurrenzlosen Gigabit-Bandbreite ist CC-Link IE prädestiniert für entsprechend leistungsfähige offene Netzwerke mit ausreichender Kapazität für Anwendungen der Industrie 4.0“, sagte John Browett, General Manager der CLPA, auf dem ARC Industry Forum Europe 2017.

-überwachung für die gesamte Fertigungslinie oder beim Schweißen, einsetzt. Im Ausstellungsbereich des Forums konnten Teilnehmer am Stand der CLPA Einzelgespräche mit Experten des Unternehmens führen und dabei die besonderen Eigenschaften von CC-Link IE und dessen Lösungsmöglichkeiten für konkrete Aufgabenstellungen in der Fertigung kennenlernen. Darüber hinaus kamen in einer Multimediapräsentation zahlreiche CLPA-Partner zu Wort und demonstrierten die breite Unterstützung, die CC-Link IE inzwischen in der Industrie hat. Die Präsentation können Sie auf dem YouTube-Kanal der CLPA unter <https://www.youtube.com/user/CLPAEurope> finden. John Browett, General Manager der CLPA Europe, sagte im Anschluss an die Veranstaltung: „Die Schaffung der technischen Voraussetzungen für die Industrie 4.0 ist eine der größten Herausforderungen, die die europäische Fertigungsindustrie derzeit zu überwinden hat. Mit der konkurrenzlosen Gigabit-Bandbreite ist CC-Link IE prädestiniert für entsprechend leistungsfähige offene Netzwerke mit ausreichender Kapazität für diese Anwendungen. Sehr gerne haben wir die Chance genutzt, Entscheidungsträger in der Industrie zu informieren und in Gesprächen auf hohem Niveau die durch unsere Technologie möglichen Lösungen zu diskutieren.“ ■ (kbn)

Firma: CLPA Europe
eu.cc-link.org

Neuheiten rund um CC-Link IE

Laufend bringen Automatisierungsanbieter Neuheiten für CC-Link IE auf den Markt. Die folgende kleine Auswahl greift exemplarisch einige Beispiele auf.

CC-Link IE Field-Systeme einfach vernetzen

Mit den neuen Varianten 2100 und 2300 der Produktfamilie FL Switch 2000 erweitert Phoenix Contact sein Angebot an Managed Switches für Automatisierungsaufgaben. Die Geräte eignen sich insbesondere für den Aufbau robuster und ausfallsicherer CC-Link IE Field-Netzwerke im Maschinen- und Anlagenbau. Erstmals umfasst das



Bild: Phoenix Contact GmbH & Co. KG

Neue Managed Switches von Phoenix Contact für CC-Link IE

Portfolio damit auch Managed Switches, die von der CLPA für den Einsatz in CC-Link IE Field-Systemen zertifiziert sind. Aufgrund der Gigabit-Kommunikation auf allen Ports lassen sich bis zu acht Komponenten in Echtzeit miteinander verbinden. Je nach Bedarf kann es sich dabei um flexible Netzwerkstrukturen mit einer Linien-, Stern- oder Ringtopologie handeln. Verschiedene Funktionen zur Konfiguration und Diagnose der Switches – beispielsweise über das Web-based Management, eine SD-Karte, SNMP (Simple Network Management Protocol) oder ein Command-Line-Interface (CLI) – stellen dem Nutzer bedienerfreundliche Möglichkeiten für die einfache und schnelle Inbetriebnahme und Wartung zur Verfügung.

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

Weidmüller-Produkte für CC-Link-IE

Weidmüller hat seine IE-Line-Produktpalette, basierend auf den RJ45-Anschluss mit Steadytec-Technologie sowie den M12 X-Type und den RJ45 gewinkelt, für CC-Link IE Field-Netzwerke zugelassen. Die Zulassung eröffnet exportorientierten Unternehmen einen Zugang zu asiatischen Märkten. Als einer der ersten Hersteller hat Weidmüller mit dieser Produktpalette auch die Zulassung von CC-Link Partner Association (CLPA) erlangt. Alle Weidmüller-Produkte mit RJ45-Anschluss in Steadytec-Technologie sowie der M12 X-Type-Stecker und der RJ45 gewinkelt lassen sich somit uneingeschränkt in CC-Link IE Field-Netzwerken einsetzen. In umfangreichen Tests und Prüfungen hat die CC-Link Partner Association (CLPA) die hochwertigen und zuverlässigen Produkte von Weidmüller getestet und für einen Einsatz in CC-Link-Anwendungen freigegeben. Alle Verkabelungskomponenten für CC-Link

zeichnen sich durch eine einfache Handhabung im Feld aus. So sind beispielsweise die Steckverbinder für die Kupferverkabelung durchgängig feldkonfektionierbar. Die verkürzten Installationszeiten, vermeidet Fehler und erleichtert die Wartung. Die Steadytec-Technologie überzeugt durch eine hochwertige Kontakttechnologie mit mehr als garantierten 750 Steckzyklen. Sie ist unempfindlich gegen Vibration, Schock und mechanischer Belastung. Mit einer Datenrate von bis zu 10Gbit/s unterstützen die Produkte den schnellen Austausch von großen Datenmengen in CC-Link-IE Field-Netzwerken.



Bild: Weidmüller GmbH & Co. KG

Weidmüller hat seine IE-Line-Produktpalette, basierend auf dem RJ45-Anschluss mit Steadytec-Technologie sowie den M12 X-Type und den RJ45 gewinkelt, für CC-Link IE Field-Netzwerke zugelassen.

Weidmüller GmbH & Co. KG
www.weidmueller.de

Basic Remote-I/O-Module von Mitsubishi Electric

Um Ethernet-Technologie bei kleineren Applikationen anwendbar zu machen, hat Mitsubishi Electric bei seinem Remote-I/O-Portfolio CC-Link IE Field Basic eingeführt. Sie sind nützlich, wenn eine Installation nahe am Feldgerät nötig ist und eine schnelle Steuerung nicht erforderlich ist. Die Remote-I/Os unterstützen CC-Link-IE-Field-Network-Basic-Diagnosefunktionen, wodurch Fehler im Netzwerk und I/O-Errors mithilfe von Engineering-Tools überprüft werden können. Außerdem können Netzwerkparameter durch ein einfaches Switch Interface festgelegt werden. Die CC-Link IE Field Basic Remote-I/Os sind in zahlreichen Konfigurationen erhältlich:

- DC Eingang, NZ2MFB1-32D, 32 Punkte, 24VDC, positiv/negativ gemeinsam, Schraubklemmleiste, 1-Wire
- AC Eingang, NZ2MFB2-16A, 16 Punkte, 100...120VAC, 50/60Hz, Schraubklemmleiste, 2-Wire
- Transistorausgang, NZ2MFB1-32T, 32 Punkte, 12/24VDC(0,5A), Senkungsart, Schraubklemmleiste, 1-Wire
- Transistorausgang, NZ2MFB1-32TE1, 32 Punkte, 12/24VDC(0,1A),



Bild: Mitsubishi Electric Europe B.V.

- Quellentyp, Schraubklemmleiste, 1-Wire
- Kontaktausgang, NZ2MFB2-16R, 16 Punkte, 24VDC/240VAC(2A), Schraubklemmleiste, 2-Wire
- I/O kombiniert, NZ2MFB1-32DT, Eingang 16 Punkte, 24VDC, Reak-

Die CC-Link IE Field Basic Remote-I/Os sind in zahlreichen Konfigurationen erhältlich.

- tionszeit 0...70ms, positiver gemeinsamer Ausgang 16 Punkte, 24VDC(0,5A), Senkungsart, Schraubklemmleiste, 1-Wire
- I/O kombiniert, NZ2MFB1-32DTE1, Eingang 16 Punkte, 24VDC, Reaktionszeit 0...70ms, negativer gemeinsamer Ausgang 16 Punkte, 24VDC(0,1A), Quellentyp, Schraubklemmleiste, 1-Wire

Mitsubishi Electric Europe B.V.
de3a.mitsubishielectric.com

Feldgeräte für das 1Gbit-Zeitalter

CC-Link IE Kommunikations-SoC mit Gigabit PHY

Im industriellen IoT-Zeitalter (Internet of Things) setzt die Industrie auf erhöhte Konnektivität sowie auf autonome und interaktive Maschinen. Industrie 4.0 führt zu einem exponentiellen Anstieg der Anzahl von Sensor-Knoten innerhalb einer Fabrik, was wiederum mehr Bandbreite der Netzwerke erfordert. Ein derartig zunehmender Datenverkehr bahnt den Weg für einen Umstieg auf industrielle Gigabit-Netzwerke.

Das industrielle Ethernet-Kommunikations-SoC (System on Chip) R-IN32M4-CL2 von Renesas Electronics eignet sich für die zunehmenden Produktivitätsanforderungen von Netzwerken und Fabriken im Kontext der Industrie 4.0. Dieses SoC ist ein weiteres Mitglied der bewährten R-IN32M3-Plattform-Familie und enthält die etablierte R-IN Multiprotokoll-Kommunikations-Engine mit Hardwarebeschleunigern, um die Leistung des Echtzeit-Betriebssystems (RTOS) sowie die Verarbeitung von Ethernet-Datenpaketen zu verbessern. Das neue R-IN32M4-CL2 wurde mit einem neuen, bei 100MHz Taktfrequenz arbeitenden ARM-Cortex-M4-Prozessor mit Fließkomma-Kern sowie mit einer Single-Precision FPU (Floating Point Unit) erweitert. Es eignet sich damit besonders für hohe Anforderungen in Prozess-Controllern, Gateways und I/O-Controllern.

Zweikanal-Gigabit-Ethernet mit integriertem PHY

R-IN32M4-CL2 bietet Gigabit-Ethernet-Konnektivität mit zwei integrierten Gigabit Ethernet PHYs, um die Komplexität bei der Entwicklung der typisch für eine Gigabit-Kommunikation erforderlichen Anlogschaltungen zu vermindern. Durch die vereinfachten HF-Analogschaltungsdesigns in PHY-Peripherieschaltungen lassen sich Entwicklungszeiten und -risiken verringern sowie der Platzbedarf der Gesamtschaltung und die Stücklistenkosten senken.

Multiprotokoll-Unterstützung

CC-Link IE zählt zu den führenden industriellen Ethernet-Protokollen für High-Speed-Feldnetzwerke mit höchster Kapazität, die eine Gigabit-Kommunikation sowie eine gemischte Übertragung von Anlagensteuerungs- und Management-Daten ermöglichen. Diese Technologie bietet die erforderliche Leistung für eine große Anzahl an Sensoren und Aktoren, wie sie in einem Industrie-4.0-Netzwerk zu erwarten sind. Das R-IN32M4-CL2 enthält einen in Hardware implementierten CC-Link IE Field-Slave-Controller.

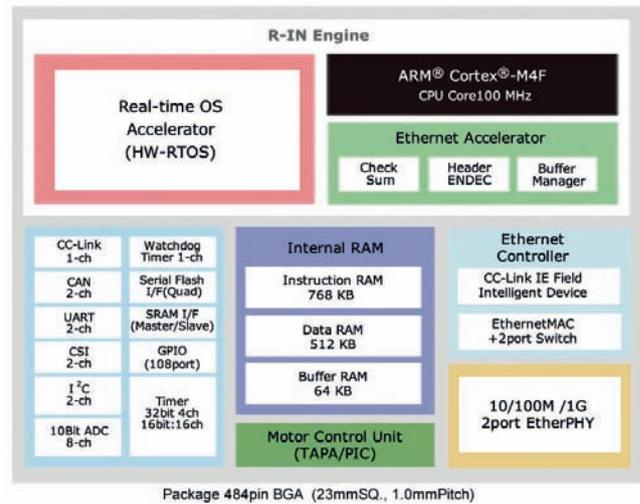


Bild: CLPA-Europe

Durch den explosionsartigen Anstieg von Sensorknoten ist zu erwarten, dass viele unterschiedliche Daten aus zahlreichen Netzwerkteilnehmern zu erfassen und zu übertragen sind: Von Prozessdaten wie Temperatur, Druck und Durchfluss bis hin zu komplexen digitalen Datensätzen intelligenter I/Os und Sensoren.

Breites Angebot an Peripherieschaltungen

Das R-IN32M4-CL2 enthält eine Fließkomma-Recheneinheit (FPU – Floating Point Unit) im CPU-Kern, einen 8-Kanal 10Bit-A/D-Wandler, einen 16-Kanal-16Bit-Timer sowie weitere Funktionen. Ein von der Firma Tessera gebautes Evaluierungs-Board mit dem neuen SoC hat bereits erfolgreich die CLPA-Zertifizierung durchlaufen. Dank der Multiprotokoll-Fähigkeit des R-IN32M4-CL2 ist das Board zu zahlreichen Protokollen kompatibel und ermöglicht eine Evaluierung diverser Schnittstellen wie u.a. CSI, I2C und UART (USB). (kbn) ■

Firma: Renesas Electronics Europe GmbH
www.renesas.com

Erweiterung der CC-Link-IE-Kompatibilität auf 100MBit-Ethernet

CC-Link IE Field Basic

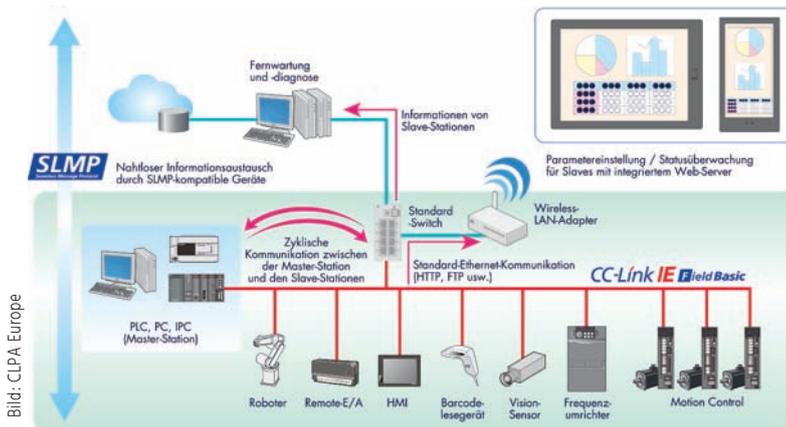


Bild: CLPA Europe

CC-Link IE Field Basic ist das neue Mitglied in der Familie der offenen Netzwerktechnologie CC-Link IE. Es erleichtert Geräteanbietern die Implementierung der CC-Link-IE-Kompatibilität für jedes beliebige Produkt mit einem 100MBit-Ethernet-Port. CC-Link IE Field Basic kann ganz einfach softwaremäßig in die Geräte oder Master-Steuerungen implementiert werden, Änderungen an der Hardware sind nicht notwendig. Entwicklungsdauer und Entwicklungskosten werden somit signifikant reduziert.

CC-Link IE Field Network Basic (IEFB) ermöglicht es Geräteherstellern, CC-Link-IE-Kompatibilität jedem Produkt mit einem 100Mbit-Ethernet-Port hinzuzufügen.

CC-Link IE war das erste und ist immer noch das einzige offene industrielle Ethernet-Protokoll mit Gigabit-Geschwindigkeit und hoher Bandbreite für datenkritische Echtzeit-Anwendungen. Als solches ist es das bevorzugte Protokoll für Unternehmen, die ihre Produktivität optimieren und Abläufe zukunftssicher gestalten wollen und gleichzeitig für die steigende Datenübertragung in Produktionsumgebungen der Industrie 4.0 vorbereitet sein möchten. Die Vorteile der Gigabit-Leistung greifen aber auch bei Produkten und Applikationen niedrigerer Ebenen. Aus diesem Grund hat die CLPA den CC-Link IE Field Basic entwickelt, der sich in jedes bestehende 100MBit-Gerät implementieren lässt. Darüber hinaus lässt sich der CC-Link IE Field Basic nahtlos mit bestehender Ethernet-Technologie verbinden (einschließlich Switches, Kabel, Stecker und drahtloser Systeme), weil es kompatibel mit TCP/IP & UDP/IP ist. Die Master-Steuerung des Netzwerkes ist dabei ebenfalls softwarebasiert. So kann jeder Industrie-PC oder jede andere Steuerung mit Ethernet ohne viel Aufwand zum Steuern eines CC-Link IE Field Basic-Netzwerkes verwendet werden. Besondere Interface-Karten, Treiberentwicklung oder andere Zusatzarbeiten sind dafür nicht erforderlich.

Produktentwicklung

Grundsätzlich ist jedes Produkt mit einem 100MBit-Ethernet-Port für die CC-Link-IE-Field-Basic-Funktionalität geeignet. Die CLPA bietet einen C-Sprache-basierenden Beispiel-Code in Verbindung mit Entwicklungsrichtlinien an, der verdeutlicht, wie die Implementierung ausgeführt werden sollte. Da der Code auch Winsock (Windows API Socket) verwendet, ist die Übertragung in andere Umgebungen unkompliziert. Um die für die Konfiguration eines Netzwerkes erforderlichen Dateien erstellen zu können, steht ein

Entwicklungs-Tool CSP+ (Geräteprofil) zur Verfügung. Außerdem ist ein halbautomatisches Tool für die Konformitätsprüfung verfügbar, um alle Funktionen eines Geräts für einen korrekten Betrieb zu testen.

Die Vorteile

Der CC-Link IE Field Basic bietet jetzt allen Geräteherstellern, die sich für die Unterstützung des CC-Link IE interessieren, die Möglichkeit zur Entwicklung von Produkten für dieses Netzwerk auf Basis ihrer 100MBit-Geräte, einfach durch Softwareentwicklung. So kann jetzt ein noch umfangreicheres Angebot von Geräten entwickelt werden, um Maschinenbauern und Endanwendern eine immer weiter zunehmende Wahlfreiheit und Anwendungsflexibilität bieten zu können. Auch erlaubt es die Entwicklung eines unterschiedlichen Portfolios an Produkten – im Gigabit-Bereich für Hochleistungsapplikationen, und im 100MBit-Bereich für Applikationen mit weniger hohen Anforderungen.

Industrielle Unterstützung

Die CLPA hat bereits zahlreiche führende Gerätehersteller in der Industrie für die Unterstützung des CC-Link IE Field Basic gewonnen. Zur Zeit ziehen Balluff, CKD, Hilscher, IDEC, Mitsubishi Electric, Molex, Phoenix Contact, Renesas Electronics und andere die Entwicklung von entsprechenden Produkten in Betracht. Wir gehen davon aus, dass in naher Zukunft weitere Interessenten folgen werden. (kbn) ■

Firma: CLPA Europe
eu.cc-link.org



YouTube Channel für schnelles Industrial Ethernet

CC-Link IE und CC-Link in Wort und Bild

Bewegtbilder sind beliebt bei Alt und Jung und aus der Kommunikation von Unternehmen und Organisationen nicht mehr weg zu denken. Die CLPA hat dies bereits vor vielen Jahren erkannt und im Jahr 2011 seinen eigenen Kanal auf YouTube etabliert. In fast 100 Videos zeigt die Herstellervereinigung Technologien, Aktivitäten und alles, was Anwender und Hersteller über CC-Link IE und CC-Link wissen sollten.

Will man sich heute schnell mal über eine Sache informieren, ist YouTube häufig eine erste Anlaufstelle. Deshalb ist die CLPA bereits seit 2011 mit seinem eigenen YouTube-Kanal online. Der Fokus liegt auf den Aktivitäten der Organisation und den Technologien rund um CC-Link IE und CC-Link und einem schnellen, industriellen Ethernet.

Umfang und Länge der Videos

Mit heute fast 100 Videos hat sich dort eine ganze Menge an Wissen angesammelt, das sowohl für Hersteller als auch für Anwender von Interesse ist. So erfahren Zuschauer vorwiegend in deutscher und/oder englischer Sprache Neuheiten über Produkte, Aktivitäten der Organisation und deren Hersteller sowie tiefere Einblicke in Form von virtuellen Seminaren, die sich auch von der Länge deutlich unterscheiden. Die durchschnittliche Länge der Videos liegt bei informativen 2-4 Minuten, die virtuellen Seminare



Bild: CLPA Europe/www.youtube.com

bei knapp 15-20 Minuten. Unser Tipp: Am einfachsten ist der Zugriff über die Playlists des Kanals. Dieser kombiniert die Videos nach nützlichen Kategorien, beispielsweise deutschsprachige Videos, englischsprachige Videos, CC-Link und CC-Link IE in Aktion oder virtuelle Seminare.

Mehr Wissen: Virtuelle Seminare

Als Einstieg in die CC-Link-Technologie eignen sich besonders die virtuellen Seminare, die die CLPA auf ihrem YouTube-Channel anbietet. Hier referieren Experten von Mitsubishi Electric, Weidmüller, Molex, Renesas, HMS und Hilscher über CC-Link-Themen aus ihren Fachgebieten. So erfährt man dort beispielsweise von Thierry Bieber, Business Development Manager bei Molex, wie

man CC-Link IE Safety in Produkte integriert. Simon Seereiner, Leiter Produktmanagement Industrial Ethernet und Sensor Actor Interface bei Weidmüller, erläutert, wie die Zusammenarbeit mit der CLPA und die Nutzung von CC-Link IE



Bild: CLPA Europe/www.youtube.com

Field Weidmüllers Erfolg in Asien ermöglicht. In einem Video von dem Unternehmen Renesas veranschaulicht Andreas Schwoppe von Renesas Electronics, Echtzeit-Kommunikations- und Applikationsmöglichkeiten und erklärt, wie der R-IN32M3-Chip von Renesas Echtzeit-Performance im Applikationsteil eines CC-Link IE Field Netzwerkes ermöglicht. Armin Pühringer, Business Development Manager bei Hilscher, erklärt wie Hilscher die CC-Link-Technologie nutzt und warum es für die Aktivitäten im asiatischen Markt unerlässlich ist. Einen Überblick über Anybus-Produkte, die CC-Link-Technologien unterstützen, gibt es im Video von Thomas Welsch, Technical Sales bei HMS Industrial Networks. Und Gerrit Buchholz, Team Leader Industrial Products Development bei Mitsubishi Electric, erläutert in einem virtuellen Seminar, wie Lösungen von Mitsubishi Electric CC-Link IE Field Produktentwicklungen unterstützen.

Aktivitäten der CLPA

Die Aktivitäten der CLPA, also des Partnernetzwerkes der CC-Link-Technologie, findet man vor allem unter dem Punkt CC-Link und CC-Link IE in Aktion. Beispielsweise wird hier über die Zusammenarbeit mit der Profinet-Organisation PI oder mit der OPC Foundation berichtet. Ebenso finden sich hier Berichte über das Zertifizierungsprogramm oder über die Profinet-Koppler von CC-Link IE.

Fazit

Wer mehr über CC-Link IE, CC-Link oder die CLPA erfahren will, sollte unbedingt einen Blick auf den YouTube Channel der Organisation werfen.

(kbn) ■

Das Netzwerk für die Industrie 4.0

Wir erleben derzeit die vierte industrielle Revolution (I4.0). Die Vorteile von I4.0 umfassen eine schnellere Produktion zu geringeren Kosten bei effizienterer Nutzung von Ressourcen, einer höheren Qualität und besserer Rückverfolgbarkeit von Produkten und Komponenten. Ethernet ist der Backbone dieser Entwicklung.

Das Tempo und das Ausmaß der Entwicklung – und die großen Chancen, die damit verbunden sind – werden dafür sorgen, dass Industrie 4.0 innerhalb weniger Jahre weite Verbreitung in der Fertigungsindustrie finden wird. Bei der Weiterentwicklung von kommerziellen und privaten Anwendungen ethernet-basierter Technologien war die Bandbreite der entscheidende Faktor für ein fortschrittlicheres und leistungsfähigeres Angebot. I4.0 wird in ähnlicher Weise bandbreitenabhängig sein. So wie Fernsehen über das Internet noch vor zehn Jahren utopisch erschien, wird auch die Fertigung in Zukunft auf Dienste angewiesen sein, die heute noch nicht einmal erdacht sind. Die Hauptvoraussetzung für diese Fortschritte ist und bleibt die entsprechende Bandbreite und derzeit kann CC-Link IE hierfür die beste Lösung liefern. Daneben bietet das System jedoch eine ganze Reihe zusätzlicher Vorteile.

Kompatibilität

Eine weitere Frage der potenziellen Anwender des Protokolls ist die Kompatibilität mit dem TCP/IP-(UDP/IP)-Verkehr. Während Netzwerke in der Praxis aus Sicherheits- und Leistungsgründen segmentiert werden, müssen sie trotzdem manchmal anderen Datenverkehr als die Steuerkommunikation unterstützen. CC-Link IE ermöglicht dies durch Verkapselung von TCP/IP-(UDP/IP)-Paketen, die mittels 'Tunneling' im CC-Link-IE-Netzwerk übertragen werden. Außerdem bietet CC-Link IE Field Basic Kompatibilität zu anderen Ethernet-Technologien auf der Grundlage von TCP/IP und UDP/IP. Über das Seamless Message Protocol (SLMP) ermöglicht CC-Link IE außerdem die Einbindung von Geräten, die noch nicht 1-Gigabit-fähig sind. SLMP bietet die Option, das Netzwerkprotokoll ohne Hardwareentwicklung in ethernetfähige Geräte einzubetten. Das SLMP-kompatible Gerät kann über einen Adapter für asynchrone Punkt-zu-Punkt-Verbindungen mit einem CC-Link-IE-Gigabit-Netzwerk kommunizieren. CC-Link IE Field Basic ermöglicht den Aufbau eines Netzwerks aus 100Mbit-Ethernet, um eine Kommunikation über zyklische (synchrone) Übertragungen zu ermöglichen. Wie bei SLMP ist hierfür Softwareentwicklung ausreichend.

Weitere technische Vorteile

CC-Link-IE-Netzwerke ermöglichen diejenige Topologie, die sich für die konkrete Anwendung am besten eignet und bieten damit die größte Flexibilität. Diese Topologien sind gemischt aus Stern und Linie sowie Ring. Innerhalb eines Netzwerks können bis zu 120 Stationen über 100m Cat5E-Kabel mit einander verbunden

Diesem Beitrag liegt ein Whitepaper der CLPA zugrunde, das sehr ausführlich die Herausforderungen sowie mögliche Lösungen der Industrie 4.0 erörtert. In dieser stark gekürzten Fassung gehen wir auf die besonderen Fähigkeiten von CC-Link IE ein und erläutern, warum das System für I4.0-Anwendungen besonders geeignet ist. Das vollständige Whitepaper ist per Download bei der CLPA erhältlich.



www.sps-magazin.de/?22738

Bild: OisenMetrix Marketing/CLPA Europe

werden. Darüber hinaus können bis zu 239 Netzwerke miteinander verbunden werden, um einen Datenaustausch in enormem Umfang zu ermöglichen, der jeder Anwendung gerecht wird.

Breites Spektrum an Produkten

Derzeit hat CC-Link weltweit annähernd 20.000.000 installierte Geräte, mehr als 1.700 zertifizierte, CC-Link-kompatible Produkte von fast 300 Herstellern und über 3.000 Partnerunternehmen in aller Welt. Unabhängigen Marktforschungen zufolge gehört CC-Link IE zu den weltweit am schnellsten wachsenden ethernet-basierten, offenen Netzwerktechnologien. Die jährliche Wachstumsrate liegt derzeit im zweistelligen Bereich, wobei die Anzahl der weltweit insgesamt installierten Geräte im März 2017 annähernd 20 Mio. erreichte (gegenüber 17 Mio. im März 2016, 14,7 Mio. im März 2015 und 12,6 Mio. im März 2014).

Internationale Normen

Industrie 4.0 ist ein globaler Trend, weltweit verbreitete Standards waren daher noch nie so wichtig wie heute. Die CC-Link-Netzwerktechnologie wurde von zahlreichen internationalen und nationalen Organisationen, einschließlich der IEC und der ISO zertifiziert, ebenso wie von vielen nationalen Regierungen, so von China, Japan, Südkorea und Taiwan. Durch Vereinbarungen wie zuletzt mit OPC und PI sorgt die CLPA dafür, dass CC-Link durch die Verbreitung gemeinsamer Standards auch in Zukunft wegweisend sein wird, was die anbieterübergreifende Kompatibilität angeht.

Fazit

Die Produktionsweisen der Industrie 4.0 sind dabei sich zu etablieren. Daraus ergeben sich hohe Anforderungen an die Kommunikation in der Fertigung. Mit hohen Datenraten und vielen weiteren Vorteilen bietet sich CC-Link IE für alle Bereiche der industriellen Kommunikation an. (kbn) ■

Firma: CLPA Europe
eu.cc-link.org

Partnerschaften und Netzwerk

Offenheit ist heute gefragt, wenn es um den Aufbau von Fertigungsnetzwerken geht. Die Zusammenarbeit mit anderen Organisationen ist für CLPA daher eine zentrale Aufgabe.

CLPA gründet Arbeitsgruppe für Industrial Ethernet Security

Die CLPA hat eine Arbeitsgruppe zur Sicherheit von industriellem Ethernet eingerichtet. Diese soll einen Leitfaden für Anwender erstellen, die mit der offenen Gigabit-Ethernet-Technologie CC-Link IE sichere Netzwerke aufbauen möchten. Das Dokument soll Strategien für Anwender aufzeigen, die mit dem Seamless Message Protocol (SLMP) und CC-Link IE Field Basic der CLPA arbeiten möchten, bei denen sowohl die zyklische als auch die transiente Kommunikation als allgemeine IP-Kommunikation übertragen wird. Die Konvergenz von IT und OT (Operational Technology) infolge der weit verbreiteten Einführung von Ethernet- und Internet-Technik in der Fertigung hat in den vergangenen Jahren Sicherheitsbedenken in den Fokus gerückt, vor allem nach einer Reihe spektakulärer Cyberangriffe.

Zusammenarbeit von OPC Foundation und CLPA



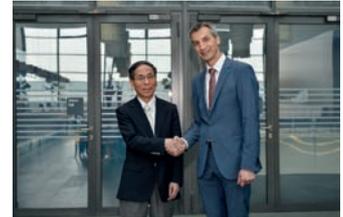
Thomas J. Burke, Geschäftsführer der OPC Foundation, und Naomi Nakamura, Global Director bei CLPA

Auf der Hannover Messe unterzeichneten Thomas J. Burke, Präsident und Geschäftsführer der OPC Foundation, und Naomi Nakamura, Global Director der CC-Link Partner Association, ein Memorandum of Understanding, in dem sich beide Orga-

nisationen auf eine enge Zusammenarbeit bei der Entwicklung dieser Schnittstellen einigten. Burke sagte: „Die Zusammenarbeit zwischen der OPC Foundation und der CLPA stellt eine Komplettlösung für CC-Link-Netzwerke und -Geräte in der Cloud dar. Endbenutzer, die sich für die zuverlässigen CC-Link-Netzwerke entschieden haben, können sich auch in andere disparate Systeme integrieren, um einen vollständigen Daten- und Informationsaustausch zu erreichen.“ Nakamura erläuterte: „CLPA ist führend bei der Bereitstellung von Lösungen, die Anwendern helfen, ihre Industrie-4.0-Anforderungen zu erreichen. So bietet der CC-Link IE mit unserem einzigartigen Gigabit-Ethernet bereits die größte Bandbreite für diese Anwendungen. Durch die Zusammenarbeit mit der OPC Foundation wollen wir nun einen Schritt weiter gehen. Unser Ziel ist es, durch die Unterstützung von Edge-Computing die Datenbeschaffung von Maschinen einfacher zu gestalten. Durch die Erweiterung unserer CSP-Technologie in Kombination mit OPC UA werden Maschinen so behandelt, als wären sie nur ein einziges Gerät. So können Informationen innerhalb und außerhalb des Unternehmens einfach ausgetauscht werden.“

Protokolltransparenz zwischen CC-Link IE und Profinet

Die CLPA und PI bieten Anwendern und Maschinenbauern jetzt vollständige Kompatibilität von CC-Link IE und Profinet. Unternehmen kaufen ihre Produktionsmaschinen heutzutage auf dem Weltmarkt ein. Deshalb sollen mit der neuen Spezifikation Szenarien überwunden werden,



Fumihiko Kimura, Chairman der CLPA, und Karsten Schneider, Vorstandsvorsitzender von PI

Bild: CLPA Europe

in denen eine neue Maschine nicht in der Lage ist, an einem anderen Standort mit einer fremden Protokollarchitektur zu kommunizieren. Die nahtlose Integration steigert die Transparenz zwischen Maschinen und Netzwerken und sorgt für bessere Konnektivität. Erreicht wird dies durch die Funktionen eines 'Kopplers', der den unkomplizierten Informationsaustausch zwischen den Protokollen ermöglicht. Die Spezifikation dieses Kopplers wurde auf der SPS IPC Drives 2016 gezeigt.

Koppler für CC-Link IE und Profinet

Hilscher war von Anfang an bei der Entstehung der oben erwähnten Koppler-Spezifikation zwischen CC-Link IE und Profinet dabei und stellte zur selben Zeit bereits einen entsprechenden Hardwareprototypen vor. Einen serienreifen Koppler namens NT 151-CCIE-RE wird es nun Mitte 2018 geben. Seit der Ankündigung implementiert Hilscher die Softwaredetails in den Koppler, der mit vier Ethernet-Ports eine transparente und effiziente Kommunikation zwischen den beiden Protokollen realisiert. Er verbindet Anlagenteile die von unterschiedlicher Art und Herkunft sind. Asiatische Hersteller von Anlagen oder Teilanlagen mit CC-Link IE vernetzten Maschinen ermöglicht der Koppler die transparente Abbildung der Anlagenschlüssel-daten in übergeordnete Profinet-Netzwerke, um die Anlagen rückwirkungsfrei auch in den Profinet dominierenden europäischen Markt liefern und dort einsetzen zu können. Gleiches gilt natürlich umgekehrt auch für europäische Hersteller, die ihre Profinet-Anlagen in den asiatischen Markt liefern wollen, wo CC-Link IE als das dominierende Protokoll erwartet wird. Im weiteren Verlauf des Jahres 2018 plant Hilscher Ausbaustufen des Kopplers, der mit Hilschers Multiprotokoll-chip netX ausgestattet ist. Er beherrscht neben Profinet auch die Protokolle EtherNet/IP, Ethercat und Powerlink. Bei gleichbleibender Hardware werden diese Konvertierungen dann als ladbare Softwarepakete zusätzlich angeboten.

(kbn) ■

Firma: CLPA Europe
eu.cc-link.org

Das einzige **OFFENE GIGABIT-ETHERNET.** Bereit für Industrie 4.0.



MIT UNTERSTÜTZUNG VON



CC-link IE ist aktuell die einzige verfügbare, offene Gigabit-Ethernet-Lösung. Bewährt im weltweiten Einsatz bei anspruchsvollen Anwendungen in der Unterhaltungselektronik bis hin zur Automobilindustrie, ist es ideal dazu geeignet, den Herausforderungen von Industrie 4.0 zu begegnen. Was bietet das Gigabit-Netzwerk?

- Unübertroffene Bandbreite für Applikationen im Kontext von Industrie 4.0
- Maximale Leistungsfähigkeit bei der Integration von Steuerung, Safety und Motion
- Unterstützt 100-MBit-Geräte

Kontaktieren Sie uns jetzt, um zu erfahren, wie CC-Link IE Ihre Anforderungen erfüllen kann.

partners@eu.cc-link.org | eu.cc-link.org



SPS/IPC/Drives 2017
Halle 2, Stand 2-431

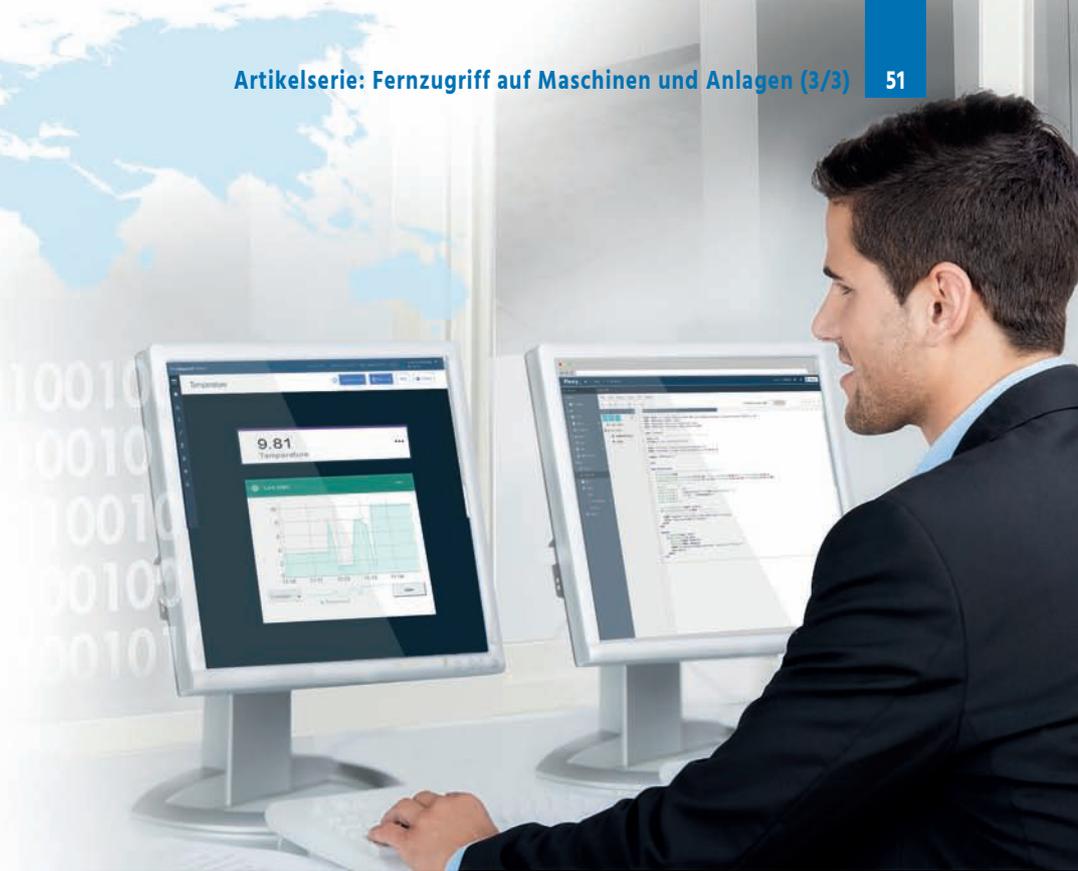
sps ipc drives

CC-Link
CC-Link IE

Bild: HMS Industrial Networks AB



Die Datenfernlösung von Ewon kombiniert den Fernzugriff mit Daten-diensten über das Ewon Flexy, IloT-Router und Datengateway zugleich.



Fernüberwachung mithilfe von IloT- Routern und Datengateways

Fernerfassung von Daten mit Java und Basic

Im zweiten Artikel dieser Serie wurde gezeigt, wie Daten von Maschinen und Anlagen, die sich an mehreren Standorten befinden, gesammelt werden und wie die Daten auf einem zentralen Server aggregiert und mithilfe einer Monitoringsoftware eines beliebigen Anbieters analysiert werden. Automatisierungs- und Softwareentwickler können nun mit Datenfernlösungen, die die Basic- und Java-Programmierung unterstützen, ihren eigenen Code schreiben, um IloT-Router an die jeweiligen Anforderungen anzupassen.

Das eWon Flexy unterstützt die Basic- und Java-Programmierung. Benutzer können so ihren eigenen Code schreiben, um den IloT-Router an ihre Anforderungen anzupassen. Die Syntax der Basic-Programmstruktur des Gerätes kommt der des Standard-Basic sehr nahe, bietet aber spezifische Zusatzfunktionen. Damit lassen sich z.B. folgende Funktionen ausführen:

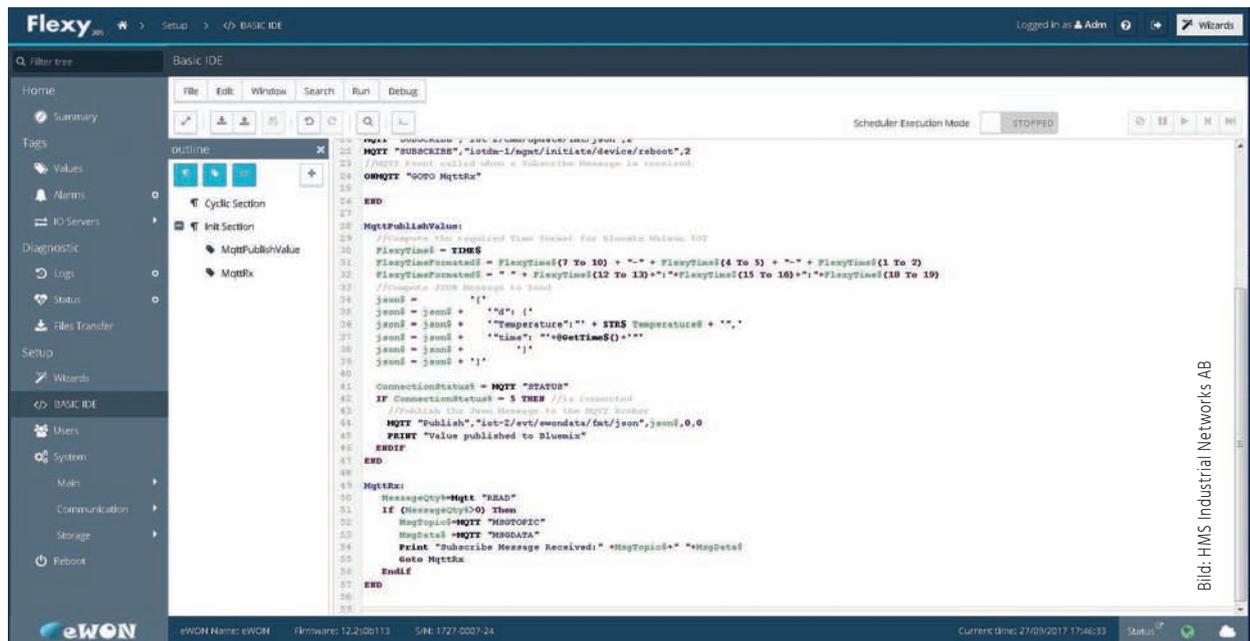
- Internet-Verbindung via WAN als Fallback für die Standard-Mobilfunkverbindung, falls diese temporär nicht zur Verfügung steht
- E-Mails senden, SMS senden/empfangen
- Historische Daten als CSV-Datei auf eine externe Speicherkarte exportieren
- Prüfen, ob die Alarmbenachrichtigung ordnungsgemäß gesendet wird
- Komplexere Alarmbedingungen erstellen
- Benutzerdefinierte Textdateien erstellen/ändern/löschen

- Ein eigenes Client-Protokoll (seriell oder IP) entwickeln, um Daten von nicht standardisierten Feldgeräten zu erfassen
- Daten über HTTP(S) und MQTT (ThingWorx, AWS, BlueMix, Azure), FTP oder per E-Mail senden.

Das Flexy verfügt zudem über eine integrierte Webentwicklungsumgebung, in der Benutzer ihr eigenes Basic-Programm erstellen können. Über diese Schnittstelle ist es z.B. möglich, Abschnitte innerhalb des Codes zu verwalten, einen Code zu importieren/exportieren, Syntax-Highlighting zu verwenden, eine Suche im Code durchzuführen, Codes schrittweise zu debuggen oder sich Fehler/Befehle direkt in der Konsole anzeigen zu lassen bzw. direkt von dort zu ausdrucken.

Programmierung mit Java

Das Gerät unterstützt ebenfalls die Java-Programmierung, die von IT-Entwicklern für komplexere Anwendungen bevorzugt wird, wie z.B.:



Das Ewon Flexy verfügt über eine integrierte Webentwicklungsumgebung, in der die Benutzer ein eigenes Basic-Programm erstellen können.

- Große Anwendungen/OEM-Anwendungen
- Erstellen eines eigenen Publishing-Protokolls (Flexy als Server)
- Programmieren eines I/O-Servers

Die Java-Programmierung bietet darüber hinaus die gleichen Möglichkeiten wie die Basic-Programmierung. Das Ewon Java Toolkit (ETK) basiert auf der J2SE-Technologie (JAVA Standard Edition). Gemeinsam mit ETK API bietet J2SE ein umfangreiches Framework mit zahlreichen Möglichkeiten für die Entwicklung von Anwendungen. Im Folgenden werden drei praktische Beispiele aufgeführt. Das erste Beispiel ist ein Fallback-Mechanismus, um die Netzwerkverbindung für den Fall zu gewährleisten, dass die Ethernet-WAN-Verbindung ausfällt. Das zweite Beispiel zeigt, wie Daten mit HTTP(S) über das Internet an die IoT-Plattform ThingWorx von PTC gesendet werden. Das dritte Beispiel beschreibt, wie mit MQTT Informationen mit der IoT-Plattform Bluemix von IBM ausgetauscht werden.

Beispiel 1: Änderung des Empfängers von Alarmbenachrichtigungen in Abhängigkeit von der Tageszeit

Beim Monitoring könnte es interessant sein, den Empfänger der Alarmbenachrichtigung in Abhängigkeit von der Tageszeit zu ändern. In diesem Beispiel wird die E-Mail-Alarmbenachrichtigung 'Tank1level', die mitteilt, wenn Tank1 voll ist, zwischen 8 und 16 Uhr an Ingenieur 1 gesendet. Außerhalb dieser Tageszeiten wird die E-Mail-Benachrichtigung an Ingenieur 2 gesendet. Die OnAlarm-Funktion wird hier genutzt, um jeweils nach der Änderung des spezifischen Alarmstatus einen bestimmten Skriptabschnitt auszuführen. Dann wird unverzüglich nach der Änderung des Alarmstatus von 'Tank1level' der Skriptabschnitt 'Send_Notification' ausgeführt. Die erste Skriptzeile ist dabei eine Bedingung, die prüft,

ob der Alarm aktiviert ist (IF AlarmStatus% = 2). Das heißt, dass keine Benachrichtigung gesendet wird, wenn der Alarmstatus von aktiviert auf deaktiviert wechselt. Danach werden die Zeitdaten vom Flexy abgerufen und in einer lokalen Variablen (Temp_Time\$ = Time\$) gespeichert. Da diese Variable auch das Datum, die Minuten und die Sekunden (z.B. 11.10.2017 15:02:53) beinhaltet, werden die Stunden durch Angabe der Position in der Zeichenfolge (Val Temp_Time\$(12 To 13)) extrahiert. Somit ist es einfach, die Bedingung zu erstellen: „Wenn die Uhrzeit (Stunden) einen Wert zwischen 8 und 16 hat, (Then) E-Mail-Benachrichtigung (SendMail) an Ingenieur 1 senden. Andernfalls (Else) die Benachrichtigung an den anderen Ingenieur (Engineer2) senden.“ Abschließend wird die Printfunktion genutzt, um eine Nachricht in der Konsole anzuzeigen und die Programmausführung zu debuggen.

Beispiel 2: Senden von Daten über HTTP(S) (ThingWorx)

Das Flexy kann Daten über HTTP(S) senden. Das lässt sich nutzen, um Daten zwischen dem Gerät und IoT-Plattformen von Drittanbietern wie AWS (Amazon), BlueMix (IBM), Azure (Microsoft) oder ThingWorx (PTC) zu übertragen. ThingWorx ist eine der bekanntesten IoT-Plattformen in den USA. Diese Plattform erfasst alle Arten von Daten und ermöglicht die Nutzung erweiterter Funktionen wie 'erweiterte Realität' (englisch: augmented reality, kurz AR) und Algorithmen für maschinelles Lernen. Im Script wird bei Änderung eines Tag-Werts (OnChange 'TagName') der Wert durch Aufrufen der Funktion 'UpdateThingWorxProperty' an ThingWorx gesendet. Der Thingworx 'AppKey' sowie der 'TagName' des Tags, der die Funktion aufgerufen hat, werden direkt in den Funktionsparametern angegeben. Nach dem Aufruf der Funktion werden einige weitere Parameter benötigt, wie die Thingworx-Projekt-URL, die HTTP(S)-Methode (\$Method\$ = 'Put')



for a greener tomorrow

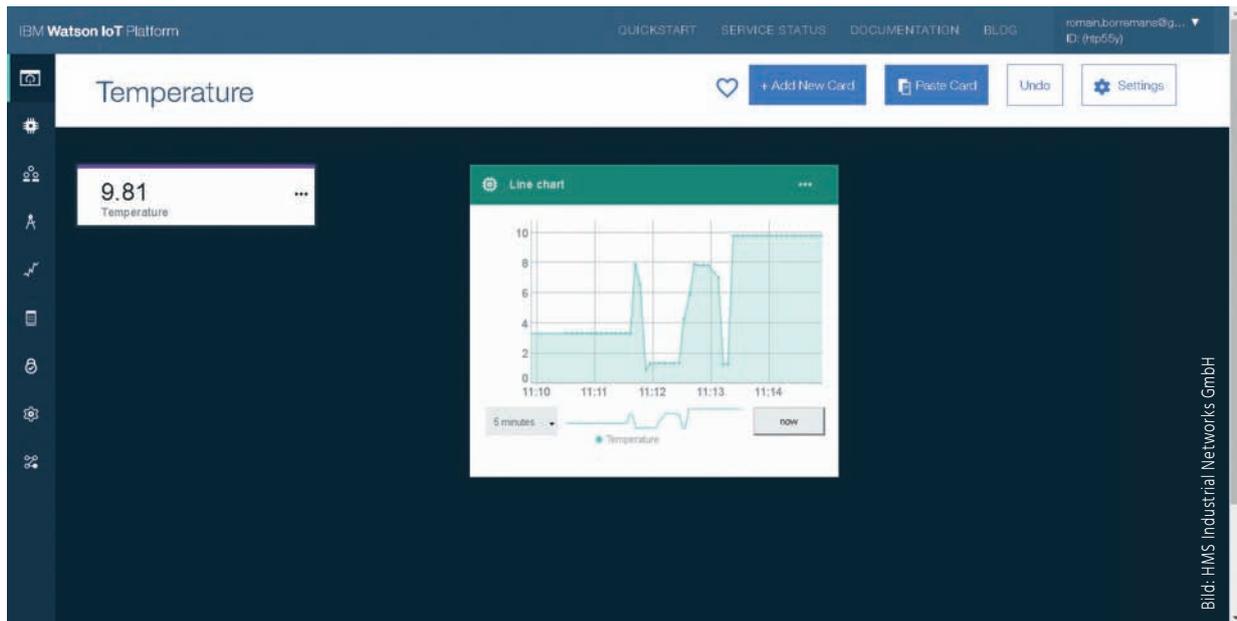
Das Ganze im Blick – mit e-F@ctory und unserem Partner-Netzwerk



Gemeinsam mit Ihnen gehen wir die Herausforderung Industrie 4.0 an und begleiten Sie als verlässlicher Partner bei der digitalen Transformation Ihres Unternehmens. Als Mitglied der e-F@ctory Alliance, unserem global aufgestellten Partnernetzwerk, beraten wir Sie ganzheitlich auf Grundlage Ihrer spezifischen Anforderungen. Denn unser Netzwerk ist spezialisiert auf maßgeschneiderte Hard- sowie Softwarelösungen innerhalb der Fabrikautomation. Mit der nahtlosen Integration von Anlagenbetrieben und Steuerungssystemen sorgen wir so für ein Höchstmaß an Transparenz und Produktivität. Damit Sie auch weiterhin den Blick aufs Ganze nicht verlieren.

e-F@ctory

Detaillierte Infos: de3a.mitsubishielectric.com/fa/de/solutions/efactory



Tag-Werte wie 'Temperatur' lassen sich auf der IoT-Plattform von IBM mithilfe von MQTT und einem Basic-Skript publizieren.

und der entsprechende Tag-Wert ($\$tagvalue = GETIO \$tagname\$$). Sobald diese Daten korrekt in Variablen gespeichert sind, können die JSON-Datei (zu sendende Daten) und der HTTP-Header (Inhaltstyp und ThingWorx AppKey) zusammen mit der ThingWorx-URL und der HTTP-Methode mit der Funktion `RequestHTTPX` verkettet werden.

Beispiel 3: Tag-Werte über MQTT auf der IoT-Plattform Bluemix veröffentlichen

Das Ewon Flexy unterstützt ebenfalls das Message-Queue-Telemetry-Transport (MQTT)-Protokoll. MQTT wurde entwickelt, um die Übertragung kleiner Datenmengen zu vereinfachen, die sich auf einer großen Anzahl an Servern und Clientgeräten befinden, die durch geringe Bandbreiten, hohe Latenzzeiten oder unzuverlässige Netzwerke eingeschränkt sind, und eignet sich somit für dynamische Kommunikationsumgebungen. Der Hauptzweck ist dabei die Fernüberwachung. Die Vorteile der Nutzung des MQTT-Protokolls mit Ewon Flexy bestehen in der Möglichkeit, Operationen ohne Datenverlust ab einem beliebigen Haltepunkt wieder aufzunehmen. Darüber hinaus lassen sich Daten bei Netzwerkunterbrechungen puffern, bis die Netzwerkkommunikation wieder aufgenommen wird und ein Client die Daten liest. Um Tag-Werte (hier 'Temperatur') auf der IoT-Plattform Bluemix von IBM mithilfe von MQTT und einem Basic-Skript zu publizieren, stellen Anwender zunächst die benötigten Parameter über 'MQTT SetParam' ein und stellen eine Verbindung zum MQTT-Broker (MQTT 'Connect') her. Timer 1 des Flexy ist dann so eingestellt, dass alle 5s die Funktion 'MqttPublishValue' (TSet 1,5; OnTimer 1, 'Goto MqttPublishValue') ausgeführt wird. Es ist erforderlich, in die `MqttPublishValue`-Funktion ein kurzes Skript zu integrieren, um die Struktur der Flexy-Zeitwerte (Time\$) an die der IoT-Plattform anzupassen. Sobald das erledigt ist, kann die JSON-Mitteilung ermittelt und über MQTT (MQTT 'Publish') auf der Plattform veröffentlicht werden. Schließlich wird nach der Überprüfung des Verbindungsstatus (If `ConnectionStatus% = 5`) der Printbefehl genutzt, um durch An-

zeige der Zeichenfolge 'Value published to Bluemix' auf der Konsole zu bestätigen, dass das Skript ordnungsgemäß ausgeführt wurde. Ein wichtiger Hinweis: Obwohl im Beispiel zur Vereinfachung und Erleichterung des Verständnisses kein verschlüsseltes MQTT verwendet wird, wird dringend empfohlen das ebenfalls unterstützte MQTT TLS zu benutzen.

Fazit

Diese Beispiele haben gezeigt, wie einfach es für Entwickler ist, die Funktion des IIoT-Routers und Daten-Gateways an die eigenen Anforderungen anzupassen. Viele weitere Beispiele von Basic- oder Java-Programmen, die von der Ewon-Entwickler-Community erstellt wurden, finden sich auf <https://developer.ewon.biz> bzw. auf dem Ewon-Techforum <https://techforum.ewon.biz/>. Die Website developer.ewon.biz wurde speziell für Entwickler erstellt und bietet umfassende Informationen über die im Ewon Flexy verwendeten Technologien sowie über die Talk2M-Plattform. ■

Artikelserie: Fernzugriff auf Maschinen und Anlagen

ICJ 2/2017: Schritt für Schritt zur Remote-Access-Lösung
 ICJ 3/2017: Plug&Play-Lösung für die Datenfernerfassung
 ICJ 4/2017: Fernüberwachung für Automatisierungs- und Software-Entwickler

Autor: Romain Borremans,
 eWon Business Unit,
 HMS Industrial Networks SA
www.hms-networks.de



Halle 2
 Stand 419

Autor: Simon Detollenaere,
 eWon Business Unit,
 HMS Industrial Networks SA
www.hms-networks.de



Halle 10
 Stand 420

Direkt zur Marktübersicht i-need.de

www.i-need.de/?Produkt=16795

Auf dem Weg zum Cloud-Historian

Wenn Grenzen verwischen

Bild: © Bruce Rolff/shutterstock.com

Ein Vorteil des Cloud-Modells ist, dass es Rechenressourcen aus den Anlagen und Rechenzentren der Kunden zu einem Cloud-Anbieter verlagert und dadurch Infrastrukturanforderungen reduziert.

Im Zeitalter der vernetzten Technologien rückt das Thema Cloud in den Mittelpunkt vieler Gespräche. Was zunächst nicht ebenso spannend klingt, aber dennoch ein wichtiges Element im IIoT-Puzzle ist, ist der Prozessdaten-Historian. In der Diskussion um das IIoT kann man es sich nicht erlauben, ihn nicht mit einzubeziehen, da er eine wichtige Rolle auf dem Weg zum Erfolg spielt.

Um zu verstehen, welche Auswirkungen die Cloud auf Historian-Systeme hat, ist es wichtig, die Hauptgründe hinter der Cloud-Einführung zu verstehen. Mit der Verbreitung von intelligenten Geräten wird mehr Speicherkapazität benötigt, und die Cloud als Lösung liegt daher nahe. Cloud-Technologien sind besser skalierbar und in der Lage, große und komplexe Datensätze durch Big Data (einem Schlüsselement des IIoT) besser zu nutzen. Tatsächlich geht aus einer jüngsten Befragung unter 200 Führungskräften der verarbeitenden Industrie hervor, dass zwei von drei Unternehmen bereits in Datenanalytik investieren und die Mehrzahl der Unternehmen plant, diese Investitionen zu erhöhen. Und obwohl viele Unternehmen gezwungen sind, Budgets zu kürzen, nehmen Investitionen in die Cloud zu. Der Grund hierfür ist deutlich erkennbar: Flexibilität und Skalierbarkeit sind wesentlich höher, Betriebskosten sind aufgrund von Skaleneffekten mit der Cloud geringer. Bestehende Systeme können zur Abdeckung von Kundenanforderungen kurzfristig erweitert werden, im Gegensatz zur einer kompletten Neuinstallation von Systemen.

- Anzeige -





Leitstand 2 Go.

Mit der neuen App ControlRoom von Schmalz installieren, parametrieren und steuern Sie Ihre Vakuum-Anlage einfach per Smartphone. Die Vollversion ist noch bis Ende 2017 kostenlos im Google Play Store erhältlich.

WWW.SCHMALZ.COM/CONTROLROOM
 T: +49 7443 2403-201



J. Schmalz GmbH · Johannes-Schmalz-Str. 1 · 72293 Glatten · schmalz@schmalz.com



Mit der Weiterentwicklung des IIoT werden die Grenzen zwischen Prozess- und Unternehmens-Historian verwischen, wenn nicht sogar vollständig verschwinden.

Vorteile der Cloud

Einer der offensichtlichen Vorteile ist, dass ein Cloud-Modell Rechenressourcen aus den Anlagen und Rechenzentren der Kunden zu einem Cloud-Anbieter verlagert und dadurch Infrastrukturanforderungen reduziert. Der Cloud-Anbieter kann dabei größere Skaleneffekte nutzen und dadurch attraktive Preise anbieten. Der tatsächliche Wert der Cloud liegt jedoch in der Fähigkeit, eine bessere Lösung für die Verwaltung und Nutzung historischer Daten zu bieten. Heutzutage konzentrieren sich Unternehmen darauf, mehr Daten zu erfassen und verfügbar zu machen, jedoch sind aktuelle Historian-Systeme in ihrer Skalierbarkeit oft eingeschränkt. Mit der Cloud können jetzt zwei bis dreimal mehr Tags bei sehr viel höheren Frequenzen erfasst werden, als dies mit Anlagen mit traditionellen Methoden der Prozessdatenerfassung in Minuten-Intervallen möglich war. Cloud-Technologien unterstützen eine erheblich bessere Skalierbarkeit als aktuelle Historian-Architekturen, welche von einzelnen Servern abhängen. Dies gilt sowohl im Hinblick auf den Datendurchsatz als auch in Bezug auf die Speicherkapazität. Cloud-Technologien verwenden darüber hinaus Clustering und Lastverteilung sowie neue Speichermöglichkeiten, um praktisch unbegrenzte Skalierbarkeit sicherzustellen. Mit den Möglichkeiten zur Skalierung werden auch Strategien mit verteilten Standorten unterstützt. Heutzutage haben einzelne Standorte innerhalb eines Unternehmens zu meist ihr eigenes Historian-System, was eine standortübergreifende Analyse und Fehlerbehebung (z. B. durch Unternehmenskompetenzzentren) schwierig macht. Mit der Cloud ist es möglich, Daten von allen Standorten in einer gemeinsamen Umgebung zu integrieren und auf Unternehmensebene allen Beteiligten in gleichem Umfang zugänglich zu machen. Außerdem zeichnet sich die Cloud-Technologie durch Unterstützung von Big-Data-Analytik aus. Technologien wie Hadoop, R, Python usw. unterstützen komplexe Prozessdatenanalysen in Kombination mit anderen Datentypen, um zu Erkenntnissen zu gelangen, die mit bestehenden Archivierungstools nicht gewonnen werden können. Die Industrie nutzt unterschiedliche Konzepte, um Prozessdaten in Cloudbasierte Lösungen zu übertragen. Der vorherrschende Ansatz dabei ist, entweder den Prozessdatenhistorian zu virtualisieren oder die Prozessdaten in einem sogenannten Data Lake zu integrieren.

Virtualisierung in der Cloud

Der logische Schritt zur Verringerung von standortbezogener Hardwareinfrastruktur ist, Server in der Cloud zu virtualisieren. Die meisten Prozessdaten-Historian unterstützen - wie die Cloud selbst auch - Virtualisierung durch VMware, Microsoft Hyper-V usw. zur vereinfachten und flexibleren Serververwaltung. Hersteller haben bereits mit der Virtualisierung von Serverkomponenten in der Cloud begonnen, wozu auch ihre Prozessdaten-Historian-Systeme gehören. Dieser Ansatz wird auch von Anbietern von Historian-Systemen als erster Schritt hin zu Cloud-Applikationen angeboten. An die Stelle von Kunden, die ihre Server selbst virtualisieren, treten vorkonfigurierte Cloud-Technologien, die von Herstellern angeboten werden. Dieser Ansatz bietet eine bessere Skalierbarkeit, da virtuelle Images im Vergleich zu physischen Computern eine einfachere Skalierung und eine bessere Nutzung der gemeinsamen Serverfarmressourcen erlauben. Die Skalierbarkeit ist jedoch weiterhin aufgrund der traditionellen Architektur des Historian limitiert. Durch diese Einschränkung kann trotz Cloud-Virtualisierung keine neue Cloud-Technologie genutzt werden und eine Skalierung in vollem Umfang und ohne Unterbrechung des Betriebes, wie mit aktuellen Cloud-Technologien heutzutage machbar, ist ebenfalls nicht möglich. Letztendlich bietet dieser Ansatz lediglich einen Historian in der Cloud anstatt in der Serverfarm des Kunden. Damit sind keine neuen Technologien oder neuen Funktionsmerkmale verbunden. Einer der wesentlichen Gründe für diesen Ansatz liegt in der Reduzierung der Hardware-Infrastruktur und der Betriebskosten.

Der Data-Lake-Ansatz

Viele Anwender und Hersteller beschäftigen sich mit Big-Data-Technologien, um eine höhere Wertschöpfung aus Prozessdaten zu erzielen. Ob es sich dabei um Hadoop, Data-Lake-Technologien, spaltenorientierte Datenbanken oder um andere Konzepte handelt: das Ziel besteht grundsätzlich darin, große Mengen von Prozessdaten zur Unterstützung von Analysen in diese Systeme zu übertragen. Meist findet noch ein Bewertungsprozess seitens der Anwender und Hersteller statt, was die Fähigkeit von Daten und Tools als Unterstützung bei Vorhersageanalysen oder anderer wertschöpfender Ergebnisse betrifft. Teilweise werden Datenbanken befüllt, ohne dass die weitere Vorgehensweise bekannt ist. Ein Beispiel ist, dass Rohdaten allein nicht ausreichen. Trotz der

Beteuerungen mancher Hersteller ist es unrealistisch „die Tools auf die Daten loszulassen“, um aussagekräftige Ergebnisse zu erhalten. Prozessdaten sind kaum strukturiert, was ein Zusammenführen und einen Vergleich von Daten schwierig macht. Ein hilfreicher Schritt wäre die Einordnung der Daten nach einem Asset-Modell, um die Prozesswerte in Kontext zu setzen und einen einfachen Vergleich mit ähnlichen Assets, wie z.B. Kompressoren und Wärmetauschern, zu erlauben. Vielfach ist es erforderlich, diese Daten anderen Quellen wie z.B. Wartungsaufzeichnungen zuzuordnen und so Ausfälle zu identifizieren, oder die Daten mit anderen Zeiträumen, die von Interesse sind, in Beziehung zu setzen. Der Vorgang des Übertragens, Organisierens und Verarbeitens der Rohdaten – häufig als Data Wrangling bezeichnet – kann bis zu 80 Prozent des Aufwands eines Analyseprojekts ausmachen, welcher in der Regel vor einer aussagekräftigen Analyse stattfindet. Eine Lösung, die diese Wrangling-Problematik auf systematische Weise behandelt, ermöglicht eine schnellere Wertschöpfung für die vorliegende Analyseart. Ein weiteres Merkmal von typischen Big-Data-Tools ist, dass Zeitreihen nicht von anderen Datentypen unterschieden werden. Dies ist nicht von ausschlaggebender Bedeutung für Offline-Analysen, allerdings kann es mit diesen Tools – insbesondere bei Aggregationsanforderungen und Leistung – zu Problemen mit interaktiven Zeitreihen-Abfragen kommen, die typisch in der Prozessindustrie sind. Eine passende Lösung würde spezialisierte Zeitreihen zur Unterstützung von betrieblichen Erfordernissen enthalten (schnelle Abfragen, Tools zur Fehlerdiagnose oder Mustererkennung von Zeitreihen) und gleichzeitig Teil des Big-Data-Analyse-Frameworks sein.

Der Prozessdaten-Historian der nächsten Generation

Mit der Weiterentwicklung des IIoT werden die Grenzen zwischen Prozess- und Unternehmens-Historian schließlich verwischen, wenn nicht sogar vollständig verschwinden. Die Migration in die Cloud ist dabei einer der wichtigsten Gründe für diesen Wandel. Die folgenden vier Hauptaspekte muss der Cloud-Historian unterstützen:

- Traditionelle Zeitreihen-, Alarm- und Ereignisdaten usw.; Nutzung von traditionellen Tools zur Visualisierung und Analyse von Daten. Die Mehrzahl der Analysen sowie die

Ursachenerkennung bei Problemen kann durch eine Visualisierung von Zeitreihen und mit entsprechenden Anomalien der Prozessvariablen nach wie vor effizienter durchgeführt werden.

- Data Lake für große Datentyp-Analysen: Der Schlüsselfaktor für mittelständische bis große Unternehmen, wenn es um Cloud-Technologien geht. Alle Anlagen- und Standortdaten sollten in diese Umgebung übertragen werden, damit neue fortschrittliche Tools zum Erkennen schwer zu findender Zusammenhänge genutzt werden können.
- Weiter gefasste Datentypen: Alle relevanten Daten sind im Data Lake gespeichert. Auf diesen lassen sich Tools anwenden, ohne dass weitere Zugriffe notwendig werden – ein Plus in Bezug auf Einfachheit und auch Leistung. Abgesehen von Zeitreihendaten sollte der Data Lake folgendes umfassen: Alarmer und Ereignisse, Produktionsdaten, Transaktionsdaten, Anwendungsdaten, Geografische Standortdaten, komplexe Daten, Internetdaten wie Wetter, Preisgestaltung in Echtzeit usw.
- Enterprise-Asset-Kontextdaten: Im Umgang mit umfangreichen Datensätzen ist es sehr schwierig, wenn nicht unmöglich, genaue Analysen ohne Asset-Kontext durchzuführen. Tagnamen sind überwiegend nur Prozesstechnikern und -bedienern bekannt. Nachdem die Daten in die Cloud übertragen und im Unternehmen zur Verfügung gestellt worden sind, benötigen die Anwender zum Verständnis und zum Nachvollziehen entsprechender Zusammenhänge (entweder zwischen Anlagen- und Standortdaten oder zwischen ähnlichen Assets im Unternehmen) einen Datenkontext, der relevant und brauchbar ist.

Der Cloudbasierte Prozessdaten-Historian der nächsten Generation muss mehr sein als ein traditionelles Archivsystem, das in der Cloud virtualisiert bzw. für die Cloud entwickelt wurde. Es muss mehr sein als ein Data Lake unstrukturierter Daten. Der Cloud-Historian der Zukunft muss beides vereinen und noch mehr. Der Cloud-Historian der Zukunft muss die Datenplattform für alle Applikationen in der Cloud und für alle Applikationen vor Ort mit Cloud-Anbindung sein. ■

Autoren: Jan Pingel und Matthew Burd, Honeywell Process Solutions, Honeywell Building Solutions GmbH www.honeywell.com

Direkt zur Marktübersicht i-need.de www.i-need.de/?f5241

opcfoundation.org/resources/brochures/'. The second section is titled 'm2m' and features a thumbnail for 'Condensed Security Advises for OPC UA Applications' with an orange call-to-action box: 'Condensed Security Advises for OPC UA Applications – Whitepaper'. The third section features a thumbnail for 'OPC UA Security Analysis' with an orange call-to-action box: 'OPC UA is secure. Proved by experts. opcfoundation.org/security'. The fourth section is titled 'NEW' and features a thumbnail for 'Industrie 4.0 Communication Guideline' with an orange call-to-action box: 'VDMA-Guideline OPC UA ISBN 978-3-8163-0709-9'. At the bottom of the banner, the website 'www.opcfoundation.org' is displayed."/>



Bild: Phoenix Contact Deutschland GmbH

Die in Wildeshausen ansässige Firma Hermes Systeme unterstützt Anwender seit mehr als 30 Jahren bei der Umsetzung von Scada-Systemen.

Fernzugriff auf Scada-Netze über die Cloud

Entlastung im Wartungsfall

Eine zentrale Forderung jedes Betreibers ist die hohe Verfügbarkeit seiner Maschine oder Anlage. Die Firma Hermes Systeme setzt daher im Rahmen ihres Fernwartungskonzepts auf eine flexible und wirtschaftliche Cloudlösung. So lässt sich sicher auf die jeweilige Kundenapplikation zugreifen.

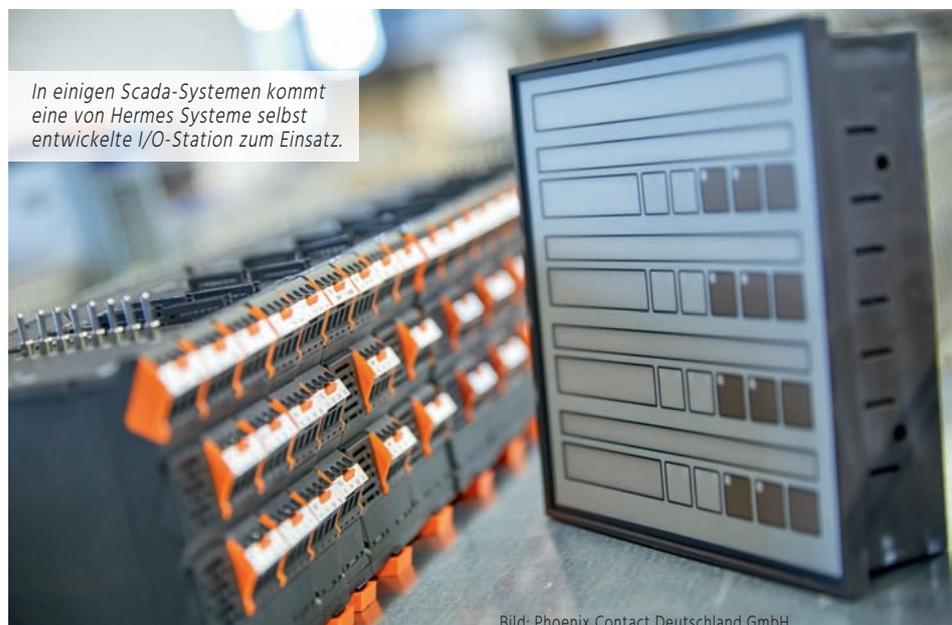
Die Firma Hermes Systeme entwickelt Lösungen für den Bereich MSR- und Automatisierungstechnik. Das Leistungsspektrum umfasst neben der Anlagenmodernisierung die Wartung und Reparatur der bestehenden Technik sowie Lieferung und Installation neuer Systeme. Dabei fokussiert sich Hermes Systeme auf die Industrie- und Gebäudeautomation sowie die Wasser-, Schwimmbad-, Kläranlagen-, Kälte-, Informations- und zentrale Leittechnik. Als Systemintegrator betreut das Unternehmen seit mehr als 30 Jahren industrielle und kommunale Anwender auch bei der Umsetzung von Scada-Systemen. Hier kommt eine von Hermes Systeme selbst konzipierte I/O-Station zum Einsatz. Zur Fernwartung werden Security Appliances von Phoenix Contact verwendet, die für die Servicetechniker einen sicheren Zugang zum jeweiligen Scada-Netz schaffen. „Anlagen ohne Fernwartungstechnik sind nicht mehr wettbewerbsfähig, da jeder Betreiber eine hohe Verfügbarkeit fordert“, erklärt Geschäftsführer Ingo Hermes. „Störungen müssen schnellstmöglich beseitigt werden.“

Kostenfreie Nutzung der Cloudlösung

Im Bereich der Fernwartung setzt Hermes Systeme auf die Technik von Phoenix Contact. Hier geht es vor allem um die schnelle Problembeseitigung, aber auch einen nachvollziehbaren Sicherheitsstandard, ohne den der Anlagenbetreiber die Fernwartung nicht akzeptiert. Die Nutzung der Phoenix-Contact-Cloud stellt deshalb eine gute Lösung für entsprechende Anwendungen dar und schont die Ressourcen. Denn die Verwendung der Cloud ist kostenfrei und die Verantwortung für die Bereitstellung der Cloudfunktionalitäten liegt bei Phoenix Contact. Durch den Einsatz einer Cloud-basierten Lösung entstehen folgende Vorteile auf Anwenderseite:

- keine Hardware-Kosten für die Fernwartungszentrale
- einfache Nutzung der Clouddienste via Webbrowser
- sowohl stationärer als auch mobiler Zugriff möglich
- gleichzeitiger Zugriff für mehrere Servicetechniker
- für die Sicherheit der Cloud ist Phoenix Contact verantwortlich
- weniger Kapitalbindung und Personalkosten
- hohe Verfügbarkeit
- Skalierung und Anpassung der Performance durch den Anbieter

Tritt der Servicefall ein, kann sich der Techniker sofort aus der Ferne über den Betriebszustand der Anlage informieren. Dazu wertet er per Knopfdruck umfangreiche Logfiles und andere historische Daten aus, die einen Hinweis auf die Fehlerursache geben. Die Aufzeichnungen aus der Sensorik der Anlage lassen auf Störungen schließen und zeigen gleichzeitig Verbesserungsmöglichkeiten auf. Scada-Systeme setzen sich meist aus einer oder mehreren Steuerungen sowie einer grafischen Benutzeroberfläche zu-



In einigen Scada-Systemen kommt eine von Hermes Systeme selbst entwickelte I/O-Station zum Einsatz.

Bild: Phoenix Contact Deutschland GmbH

Der FL mGuard RS2000 kombiniert die Anforderungen der IT mit einer robusten Hardware für die raue Industrieumgebung.

Bild: Phoenix Contact Deutschland GmbH

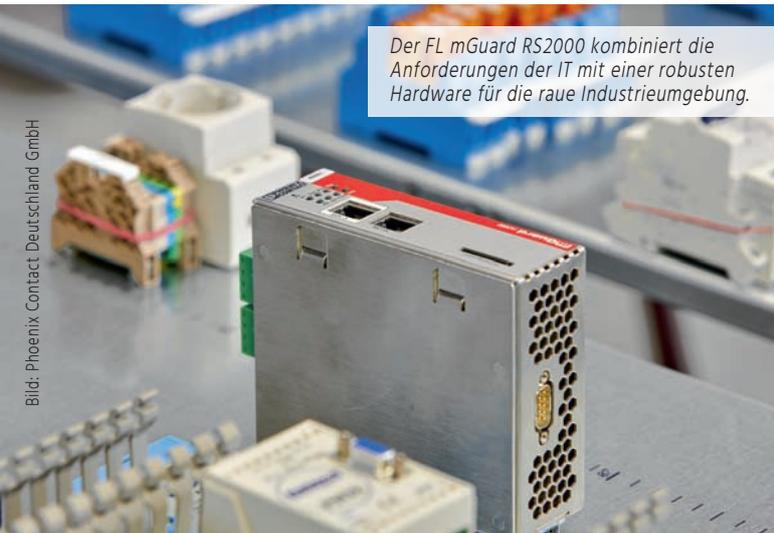


Bild: Phoenix Contact Deutschland GmbH



Die Mitarbeiter des Systemintegrators Hermes Systeme erstellen selbst komplexe Schaltschränke.

sammen. „Etwa 80 Prozent aller Probleme können wir durch den Fernzugriff abschließend beheben“, erläutert Christian Nölker, Elektroingenieur und Programmierer bei Hermes Systeme. „Zu diesem Zweck holen sich unsere Servicetechniker den Bedienerbildschirm der Anlage auf ihren Rechner und arbeiten dann gemeinsam mit dem Mitarbeiter vor Ort an der Fehlerbeseitigung.“

Einfache Verwaltung

„Um die richtige Fernwartungslösung auszuwählen, reicht ein Blick auf die technischen Parameter und Preise nicht aus“, betont Nölker. Bei einer mit der Zeit steigenden Anzahl an Anlagen kann der Aufwand für die Verwaltung der Online-Zugänge und die Konfiguration der entfernten Routerstationen schnell sehr groß werden. Darüber hinaus erschweren Themen wie die sichere Authentifizierung, das Managen kundenindividueller Zugangs- und Konfigurationsdaten sowie die unterschiedlichen Software-Umgebungen eines kontinuierlich gewachsenen Anlagenparks die Entscheidung. „Wir haben daher nach einem Anbieter gesucht, der eine Lösung für die einfache Verwaltung sowohl der Anlagen als auch der Servicemitarbeiter bietet“, erklärt Geschäftsführer Hermes. Vor diesem Hintergrund fiel die Entscheidung auf die Komplettlösung von Phoenix Contact, denn sie umfasst neben einem hohen IT-Security-Standard ebenfalls ein Management der Anlagen und Servicemitarbeiter. Die erforderliche Konfiguration der Endgeräte wird automatisch in der Cloud generiert und auf die Geräte geladen. Die Umsetzung sämtlicher Vorgänge wie VPN-Konfiguration, Routingeinstellungen oder die Zertifikatsverwaltung erfolgt mit der Cloud. „Die Cloud verwaltet als Portal die immer größer werdende Vielfalt verschiedener Wartungsumgebungen der Anlagen und stellt dem Servicemitarbeiter automatisch das richtige Umfeld zur Verfügung“, so Nölker. Mit jedem Servicezugriff wird eine temporäre virtuelle Maschine gestartet und anschließend wieder gelöscht. Sie ermöglicht auch den parallelen Betrieb unterschiedlicher Softwaregenerationen. Diese Art der Fernwartung hat sich für Hermes Systeme als effiziente Lösung erwiesen, die bei den Kunden des Unternehmens für eine höhere Anlagenverfügbarkeit sorgt.

Robuste Lösung für die Industrie

„Seinerzeit suchten wir nach einer Lösung, mit der wir uns über das Internet in das Scada-Netz der Anlage einwählen und es gleichzeitig vor unbefugten Zugriffen schützen können“, fährt Nölker fort. Idealerweise sollte diese Lösung auf eine industrielle Umgebung zugeschnitten sein. „Die meisten am Markt erhältlichen Sicherheitsanwendungen sind allerdings für Officeumgebungen entwickelt worden.“ Die Produktfamilie FL mGuard ist hingegen auf die Ansprüche des Industrieumfelds ausgelegt. Sie umfasst Sicherheitskomponenten mit integrierten Firewall-, Routing- und VPN-Funktionen für industrielle Netzwerke genauso wie eine robuste Hardware im Metallgehäuse. „Die von uns verwendete Variante FL mGuard RS2000 lässt sich auf der Tragschiene montieren und verfügt über eine 24VDC-Stromversorgung“, erklärt Nölker. „Je nach den vor Ort vorgefundenen Gegebenheiten nutzen wir entweder die RJ45-Version oder die Mobilfunk-Variante, um die Anlage mit der Cloud zu verbinden.“ Weil das Gerät als sicheres Gateway ein System vor nicht autorisierten Zugriffen absichert, kann das Scada-Netz direkt mit dem Internet verbunden werden und sich so an die Cloud ankoppeln. Die Servicetechniker setzen einen VPN-Softwareclient ein, mit dem sie ebenfalls eine Verbindung zur Cloud aufbauen. Dabei sorgt die VPN-Funktion dafür, dass nur Berechtigte mit entsprechenden Zugangsdaten die Kommunikation initiieren können. Ist die VPN-Verbindung eingerichtet, funktioniert sie zudem wie eine direkte Ankopplung an das lokale Netzwerk. Die Programmiersoftware der Steuerung erkennt die Securitygeräte somit und kann sie einfach anbinden. ■

Autor: Ingo Hilgenkamp,
Produktmarketing Network Technology,
Phoenix Contact Electronics GmbH
www.phoenixcontact.de



Halle 2
Stand 439

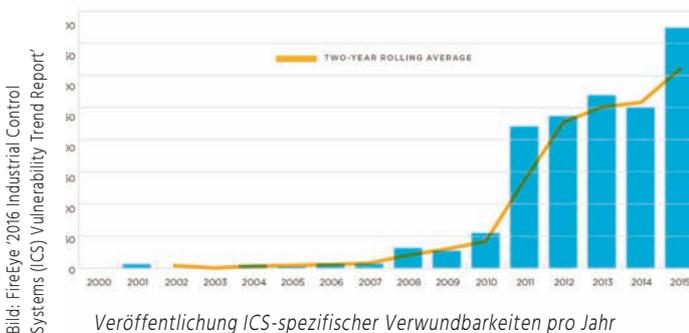
Direkt zur Marktübersicht i-need.de

www.i-need.de/?Produkt=21460

Egal ob Stromnetz, Wasserversorgung oder Produktionslinien: In den letzten Jahren ist ein enormer Anstieg von Cyberattacken auf industrielle Steuerungssysteme (engl. Industrial Control Systems, ICS) zu verzeichnen. Was sind die größten Einfallstore für Hacker und wie kann sich ein Unternehmen schützen?

Tipps zur Risikominimierung

Einfallstore schließen



Fehlende Authentifizierung bei ICS-Protokollen

Unternehmen nutzen in der Produktion ICS-Protokolle, die oft über keine Authentifizierungsmöglichkeit verfügen. Fehlt diese Funktion, ist es schwierig festzustellen, ob ankommende Daten aus einer vertrauenswürdigen Quelle stammen. Denn ohne Authentifizierung können von jedem Rechner Befehle gesendet werden, die in der Lage sind, die Produktion zu manipulieren. Fehlerhafte Produkte, Zerstörung von Werkzeugen und Maschinen sowie Verletzungen bei Mitarbeitern sind mögliche Folgen.

Tipps 1:

Um den genannten Manipulationsversuchen zuvorzukommen, sollten im Unternehmen alle Protokolle mit fehlender Authentifizierungsmöglichkeit identifiziert werden. Im Zuge dessen ist es sinnvoll, auch gleich den Schwere- und Verbreitungsgrad der Sicherheitslücken zu ermitteln. Als weitere sicherheitsfördernde Maß-

nahme empfiehlt sich, herauszufinden, ob die Anlagen Authentifizierungsoptionen unterstützen und diese gegebenenfalls zu implementieren. Im Anschluss sollten Tests durchgeführt werden, ob die Produktionsstätten mit zwischengeschalteten Authentifizierungsoptionen reibungslos laufen. Durch eine Firewall und/oder von Deep Packet Inspection (DPI) lassen sich nicht-authentifizierte Befehle blockieren.

Veraltete Hardware

Oft ist Hardware für Industrieanlagen jahrzehntelang im Einsatz. Diese veraltete Hardware bietet einen begrenzten Funktionsumfang sowie ungenügende Rechenleistung und Speicherkapazitäten, um moderne Cyberbedrohungen zu verhindern. Ein weiteres Sicherheitsrisiko stellt die End-of-Life-Phase von Geräten und Software dar. Hier unterstützen Hersteller beispielsweise Software nicht mehr mit Patches, was zu schwerwiegenden Sicherheitslücken führt.

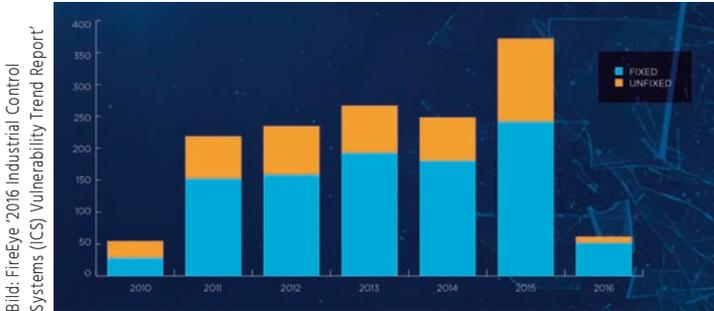
Tipps 2:

Regelmäßige Upgrades für ältere Geräte, die mit dem Netzwerk verbunden sind und wichtige Funktionen in der Prozesssteuerung inne haben, senken das Sicherheitsrisiko für einen Hackerangriff. Sinnvoll ist es auch, Firewall-Regeln aufzusetzen, um Netzwerkverbindungen zu veralteter Hardware und Software zu sichern.

Schwache Benutzerauthentifizierung

Benutzerauthentifizierungen stellen sicher, dass nur berechtigte Personen oder Personenkreise Zugriff auf Programme haben. Die

Authentifizierung erfolgt meist über die Eingabe eines Passwortes. Bei alten Steuerungssystemen sind Kennwörter oft einfach zu knacken, da sie hart codiert sind, in leicht zu entschlüsselnden Formaten



ICS-spezifische Verwundbarkeiten in Relation zur Verfügbarkeit von Patches zum Zeitpunkt des Bekanntwerdens der Schwachstelle

ten abgespeichert oder direkt im Klartext übermittelt werden. Hacker haben hier leichtes Spiel und können nach der Entschlüsselung der Passwörter die Produktionsprozesse beliebig manipulieren.

Tipp 3:

Um das Risiko zu senken, sollte in einem ersten Schritt der interne ICS-Gerätebestand mit der Liste der Geräte, die hart codierte Passwörter haben, abgeglichen werden. In einem weiteren Schritt gilt es, die Geräteprotokolle und den Netzwerkverkehr zu überwachen - so lassen sich passwortbezogene Sicherheitslücken aufspüren.

Unzureichende Integritätsprüfungen

Durch die Integritätsprüfung werden Herkunft und Vollständigkeit von Daten sowie Codes durch kryptografische Überprüfung verifiziert. Doch Industrieanlagen leiden häufig unter folgenden drei Schwachstellen:

- **Unzureichende Überprüfung der Softwaresignaturen:** Software-Signaturen geben an, ob eine Software von einer vertrauenswürdigen Quelle stammt. Durch eigene Zertifikate oder externe Zertifizierungsstellen garantieren Anbieter eine Prüfung der Quellen. Sind keine Signaturen vorhanden, haben Hacker die Möglichkeit, über mit Schadcode infizierter Software in die Systeme einzudringen.
- **Unzureichende Überprüfung der Firmwareintegrität:** Firmware wird in der Regel nicht so häufig geändert oder aktualisiert wie Software. Gelingt es einem Hacker durch ungenügende unternehmensseitige Überprüfung schadhafte Firmware hochzuladen, kann er den gesamten Funktionsbereich eines Gerätes übernehmen.
- **Unzureichende Überprüfung der Integrität der Steuerungslogik:** Unter Steuerungslogik versteht man ein Programm zur Prozesssteuerung, das von einem programmierbaren Controller, beispielsweise einer SPS ausgeführt wird. Ohne Integritätsüberprüfung der Steuerungslogik übernehmen jedoch SPS-Geräte jede aufgespielte Logik. Angreifer können, nachdem sie in das System gelangt sind, unter anderem Grenz- und/oder Sollwerte manipulieren und die Kontrolle über Werkzeuge, Maschinen und Anlagen übernehmen.

Tipp 4:

Damit Hacker hier kein einfaches Spiel haben, sollte das Betriebssystem so konfiguriert werden, dass nur signierte Codes ausgeführt werden können. Zudem ist es ratsam, Software und Updates jeweils in einer simulierten Umgebung zu testen, bevor sie in den Produktionsbetrieb übergehen.

Einfallstor Windows-Betriebssysteme

Viele Workstations für Produktentwicklung und für die industrielle Produktion laufen mit veralteten Versionen von Windows-Betriebssystemen - mit teilweise bekannten Schwachstellen. Hacker nutzen diese Sicherheitslücken, um Zugriff zu erhalten.

Tipp 5:

Dieses Einfallstor lässt sich durch die Einführung und Pflege einer Bestandsliste der verwendeten Betriebssysteme, die nicht gepatcht sind, beziehungsweise nicht mehr unterstützt werden, schließen. Zusätzlich müssen regelmäßig Upgrades installiert und/oder Patches während Wartungsarbeiten eingespielt werden. Außerdem sollte man auf ergänzende Lösungen setzen, um bekannte Schwachstellen zu schließen.

Die Krux mit Drittanbietern

ICS-Anwender sind selten über die Abhängigkeiten ihrer ICS-Software von Produkten von Drittanbietern im Bilde. Denn ICS-Anbieter wissen meist nicht im Detail, welche Komponenten sie von Drittanbietern verwenden. So können ICS-Anbieter ihre Kunden auch nur bedingt über Schwachstellen informieren. Findige Hacker kennen diese Abhängigkeiten und nutzen Softwaresicherheitslücken aus, von deren Existenz der Anwender nichts weiß.

Tipp 6:

Unternehmen sollten vom ICS-Anbieter eine Liste anfordern, die die enthaltene Software von Drittanbietern in den Produkten auflistet - so lassen sich erste Schwachstellen entdecken und beheben. Zusätzlich ist es ratsam, regelmäßig nationale und internationale Schwachstellendatenbanken auf Sicherheitslücken in der Software von Drittanbietern zu durchsuchen.

Aus Fehlern lernen und vorbereitet sein

Nur bekannte Schwachstellen lassen sich auch beheben - die Auflistung der größten Einfallstore für Hacker im ICS-Bereich basiert auf Erfahrungswerten und soll dabei helfen, dass Verantwortliche und Entscheider die Gefahrenlage besser erkennen und verstehen. ■

Autor: Mike Hart,
Vice President Central Europe,
FireEye, Inc.
www.fireeye.de

Verschlüsselung für Fertigungsnetze

Offen aber sicher

Bild: ©Kru/UA/istockphoto.com



Wichtiger Aspekt bei der Investitionsentscheidung ist die Fähigkeit, Komponenten auch nachträglich in die digitale Prozesskette einbinden zu können.

Industrie 4.0 verbindet zukünftig die funktionelle Sicherheit von Mensch, Maschine und Umwelt mit der IT. Parallel dazu verliert das bisherige Credo 'Sicherheit durch Abschottung' seine Berechtigung, denn eine regelmäßige Kommunikation mit Kunden, Lieferanten oder Partnern macht eine gewisse Offenheit unerlässlich. Im Rahmen dieses neuen Sicherheitsverständnisses gewinnt dementsprechend die Thematik Verschlüsselung zentrale Bedeutung. Dabei kann und muss dieses oft mit dem Ruf der Kompliziertheit versehene Feature kein Hexenwerk sein, sofern bestimmte Faktoren Beachtung finden.

Eine der zentralen Folgen der Digitalisierung – und damit der Vernetzung – ist die nachhaltige Veränderung der bestehenden Sicherheitsarchitektur. Denn diese ist eine Grundvoraussetzung dafür, die notwendigen Schritte zur Sicherung der Produktion und des Unternehmens zu erreichen. Betrachtet man heute Fabriknetze, so sind diese nur aus ganz bestimmten Gründen überhaupt mit dem Internet gekoppelt, etwa um Fernwartungslösungen oder Logistik Anwendungen zu ermöglichen. In Zukunft reichen diese Szenarien bei weitem nicht mehr aus – es werden deutlich mehr und komplexere Anwendungen ins Haus stehen. Eine vernetzte Betriebsintelligenz ist in der Lage, die verteilten operativen Daten zu verbinden und eine vereinheitlichte Sicht in Echtzeit zu liefern und schnellere Entscheidungen zu tref-

fen, Energieeffizienzmaßnahmen senken die Kosten in der Produktion, der Datenaustausch mit Partnern, Lieferanten oder Kunden zur Verbesserung oder Individualisierung der Produkte verändert die gesamte Prozesskette. Ohne eine in- und externe Vernetzung ist das jedoch überhaupt nicht möglich. Vor diesem Hintergrund wird schnell deutlich, dass die seit Jahren eingesetzten IT-Sicherheitsregeln wie Viren-Scan, Backup-Strategie, Zugriffsrechte oder Firewalls zur Verhinderung ungewollter Zugriffe bei weitem nicht mehr ausreichen können. Denn Offenheit in der Kommunikation der Netzwerke mit Kunden, Partnern oder Zulieferern ist wesentliche Basis einer vernetzten Wirtschaft. Die langjährig bewährte Regel 'Sicherheit durch Abschottung' ist damit obsolet geworden.

Schutz des Datenverkehrs

Offene Kommunikation erfordert dabei zuerst eine entsprechend ausgearbeitete bzw. überarbeitete IT-Sicherheit, denn der Schutz des exponentiell wachsenden Datenverkehrs sollte hohe Priorität genießen. Nur dann kann gewährleistet werden, dass Menschen und Unternehmen gegen Vorfälle wie Eingriffe in Maschinenbefehle, fremdgesteuerte Anlagen oder gar das Ausspähen von (Produktions-) Daten geschützt werden. Hilfreiches Instrument ist dafür aktuell – und auch mittel- bis langfristig – die Verschlüsselung. Sie leidet aber immer noch unter dem Ruf, kompliziert, rechenintensiv und anwenderunfreundlich zu sein. Allein das Handling von und mit privatem und öffentlichem Schlüssel, hält viele Anwender vom Einsatz der Verschlüsselung ab. Jedoch bietet gerade die exponentiell steigende Leistungsfähigkeit in der Digitalisierung die realistische Chance, Verschlüsselung einfach zu integrieren, so Datendiebstahl zu verhindern und unberechtigte Infrastrukturoder Prozessmanipulation zu unterbinden.

Durchgängige Digitalisierung

Dabei steht die Produktion vor einer besonderen Herausforderung, denn längst nicht alle Komponenten sind mit der erforderlichen Technologie für die durchgängige Digitalisierung ausgestattet. Daher sollte bei der Investitionsentscheidung für Komponenten deren Fähigkeit im Vordergrund stehen, bestehende Fertigungsnetzwerke auch nachträglich in eine digitale Prozesskette einbinden zu können. Dieser Retrofit-Ansatz bietet jedoch die Chance, mit der richtigen Investitionsentscheidung zügig die gesamte Produktion nachrüsten zu können. Idealerweise verfügen derartige Lösungen bereits auf Ebene der Microcontroller über ein Verschlüsselungs-Tool, sodass die Kommunikation zwischen Maschine und Gateway über die gängigen Übertragungswege Funk, Kabel oder via WLAN gesichert ablaufen kann. Hier sollte der bewährte Advanced Encryption Standard (AES mit 128 Bit) das Mittel der Wahl sein. Der Vorteil liegt auf der Hand: Verschlüsselte Sensordaten können weder von Dritten mitgelesen noch durch unbefugte Schaltbefehle gestört werden. Besitzt zudem jedes Gerät einen individuellen Schlüssel, dann ist selbst ein erfolgreicher, interner Angriff nicht in der Lage, das gesamte System zu korrumpieren. Die bereits erwähnten Vorbehalte gegenüber der Verschlüsselung und deren Handhabbarkeit lassen sich relativ einfach umgehen – die für die Verschlüsselung notwendigen Schlüssel sollten bereits bei der Produktion der Senso-

ren integriert werden. So kann deren Einrichtung entfallen, das Risiko einer Fehlbedienung tendiert gegen Null. Hochmoderne Lösungen gehen an dieser Stelle noch einen kleinen, aber entscheidenden Schritt weiter, der das Sicherheitsniveau nochmals steigern kann: Sie verwenden die vorinstallierten Schlüssel selbst nicht für die Verschlüsselung, sondern nutzen sie lediglich zur Generierung neuer Schlüssel in vorab definierten Abständen. Erhält ein Angreifer einmal einen Schlüssel, so ist dessen Gültigkeit zeitlich begrenzt und dieser begrenzte Zeitraum kann jeweils individuell festgelegt werden.

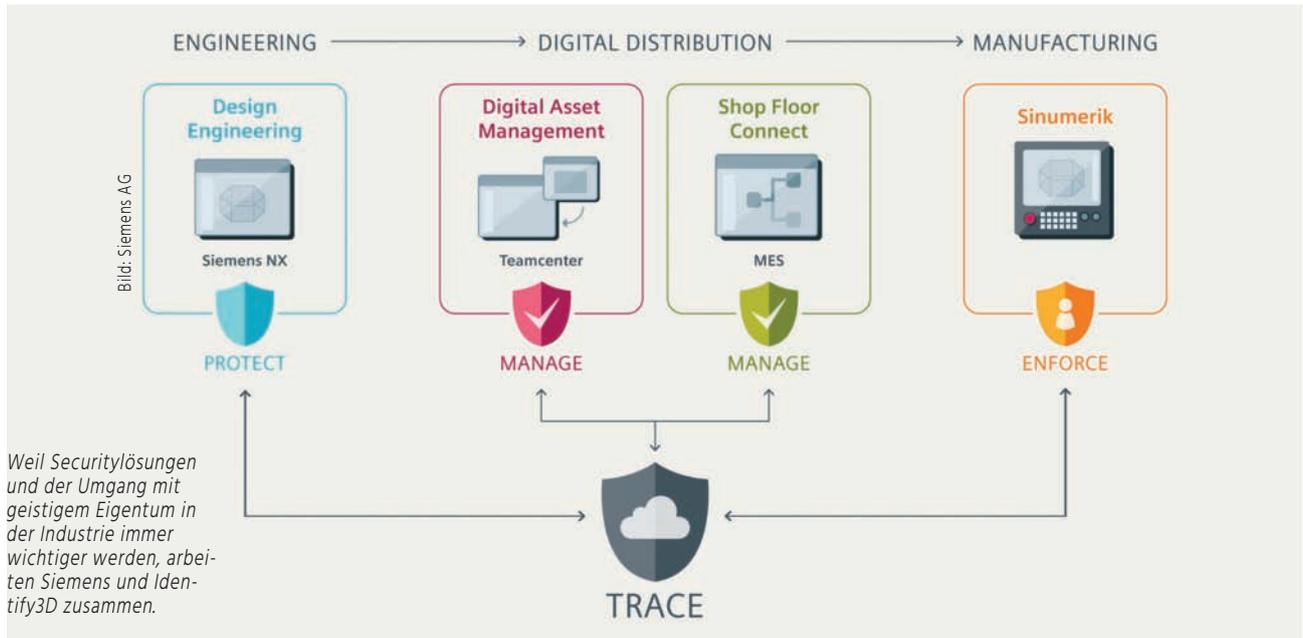
Zyklische Redundanzprüfung

Zur weiteren Absicherung bietet sich der sogenannte CRC-Check (Cyclic Redundancy Check) an, der die übertragenen Daten zyklisch auf ihre Redundanz überprüft. Sind Daten fehlerhaft oder wurden sie gar von Unbefugten erzeugt, werden sie direkt verworfen – der Sensor überträgt das entsprechende Datenpaket nochmals. Dieses Vorgehen steigert gepaart mit einem integrierten Zeitstempel nachhaltig das Sicherheitsniveau, denn so sind auch nachträgliche Angriffe, sogenannte Replay-Attacken, ausgeschlossen. Denn der Zeitstempel ist integraler Bestandteil der AES-Verschlüsselung. Dementsprechend können Angreifer einmal aufgezeichnete Daten nicht mit einem anderen Zeitstempel versehen und in das System einschleusen. Abgerundet wird eine professionelle Verschlüsselungslösung durch ein möglichst granulares, integriertes User-Management. Es gestattet extern Beteiligten wie Partnern, Lieferanten oder Kunden den temporären Zugriff auf für sie vorab definierte Datensätze. Die direkte, dauerhafte und komplette Offenheit der Produktionskette ist nicht erforderlich. Last but not least können auch Akteure sicher angesteuert werden, beinhaltet die gesicherte Kommunikation doch auch die Geheimhaltung der Aktorkommandos. Angreifer haben dadurch keine Gelegenheit, dieses mitzulesen, wiederzuerkennen oder zu verfälschen. Das Security-by-Design-Prinzip ermöglicht eine Sicherheitsarchitektur, die jedoch nicht technischen Begrenzungen unterliegt. Denn der Aufwand beim Versand der Daten ist so gering, dass Strom- und Datennetz alle Maßnahmen problemlos durchführen können. Produzierende Unternehmen sind also in der Lage, sowohl die Vertraulichkeit von Sensordaten, als auch die der Schaltbefehle an Akteure mit der Verschlüsselung ebenso zu wahren, wie die an- und abgehenden Daten von Partnern, Lieferanten und Kunden. Sie können daher sicher sein, Chancen und Möglichkeiten der Digitalisierung zu nutzen und Optimierungspotenziale beispielsweise durch niedrigere Fertigungskosten, eine höhere Produktivität oder eine klare Kalkulation der Maschinenauslastung zu heben. An Sicherheitsfragen und der Integrität und Vertraulichkeit der Produktion scheitern Projekte der Digitalisierung jedenfalls nicht – die bewährte Verschlüsselung stellt die notwendige Sicherheit bereit. ■

Checkliste Sicherheit

- IoT-Lösungen ohne Verschlüsselung setzen Produktion und Datenaustausch mit Partnern hohem Risiko aus
- Können auch ältere Maschinen eingebunden werden?
- Flexible Übertragungswege (Funk, LAN, WLAN) erleichtern die Anbindung der Maschinen!
- Welche Verschlüsselungstechnik wird eingesetzt? (Standard AES 128Bit)
- Zeitlich limitierte Schlüssel verbessern nochmals die Sicherheit.
- Prüfung der Daten auf Redundanz inklusive Zeitstempel vermeidet Fehler und nachträgliche Angriffe.

Autor: *Christian J. Pereira,*
Geschäftsführer,
Q-loud GmbH
www.q-loud.de



Datenverschlüsselung sichert digitale Wertschöpfungskette

Neue Schutzmöglichkeiten

Siemens bietet neue umfangreiche Möglichkeiten zum Schutz von Daten im Bereich der Digitalisierung, wenn Drittdienstleister in den Fertigungsprozess eingebunden werden. Dazu geht der Konzern mit Blick auf die Lizenzierung und Verschlüsselung mit Identify3D (ID3D) eine strategische Partnerschaft ein.

ID3D hat die Lösungen für Sicherheit und Nachverfolgbarkeit digitaler Fertigungsprozesse in das Sinumerik- und PLM-Portfolio von Siemens integriert. Die Datenverschlüsselung einschließlich Zeitstempel ist bereits in die 3D-CAM-Software NX integriert. Die Entschlüsselung erfolgt auf der Sinumerik 840D sl. Durch die Zusammenarbeit mit Identify3D will Siemens mit durchgängigen Sicherheitslösungen die Integrität sämtlicher Prozessdaten entlang der gesamten Wertschöpfungskette beim Betrieb der Werkzeugmaschine sichern. Mit der Integration der neuen Lösungen in das Siemens-Portfolio sollen Kunden in der Lage sein, ihr geistiges Eigentum zu schützen, ihre Produkte gemäß den individuell definierten Parametern fertigen zu lassen und die produzierten Teile vollumfänglich nachzuverfolgen.

Wiederholbarkeit in der Fertigung

Die neuen Möglichkeiten zum Schutz von Konstruktions- und Fertigungsdaten – und damit letztlich zum Schutz vor Diebstahl geistigen Eigentums – umfassen mehrere Elemente. Ein wesentliches Element ist die Wiederholbarkeit in der Fertigung. Innerhalb der Datenver- und entschlüsselung auf der CNC stellt ein Lizenzierungssystem sicher, dass ein Fertigungsteil exakt nach den technischen Spezifikationen produziert wird. Diese für die Entschlüsselung qualifizierten Komponenten und Einheiten sind genau definiert. Darüber hinaus kann der Programmentwickler die Anzahl der vom Drittanbieter gefertigten Teile beschränken, was einen effektiven Schutz vor Diebstahl geistigen Eigentums darstellt. Sowohl die Produktionsmaschine, auf der die Teile gefertigt werden, als auch das ein-

zusetzende Material können genau vorgegeben werden. Die von NX verschlüsselten Daten werden in ein Ordnersystem, zum Beispiel Teamcenter, hochgeladen und können von dort auf ShopFloorConnect, Siemens MES und ähnliche Lösungen übertragen werden.

Gemeinsam zur Sicherheit

„Securitylösungen und der Umgang mit geistigem Eigentum werden in den verschiedensten Industriezweigen immer wichtiger“, sagt Uwe Ruttkamp, Leiter Machine Tool Systems in der Business Unit Motion Control der Siemens-Division Digital Factory. „Identify3D bietet sichere Datenübertragung für den Schutz von digitalen Produktionsdesigns und Qualitätskontrolle. Das Unternehmen ist ein Experte auf dem Gebiet der Datenübertragung und bei Sicherheitslösungen, um den Schutz geistigen Eigentums und die Datenintegrität entlang der gesamten Wertschöpfungskette beim Betrieb der Werkzeugmaschine zu gewährleisten – vom Produktdesign bis hin zum fertigen Produkt.“ Stephan Thomas, Mitgründer von Identify3D, ergänzt: „Siemens ist sich der Bedeutung einer effizienten und zuverlässigen digitalen Wertschöpfungskette bewusst und setzt einen industriellen Standard für die digitale Fabrik. Als strategischer Partner von Siemens tragen wir dazu bei, einen sicheren und wiederholbaren digitalen Fertigungsprozess zu gewährleisten.“

Firma: **Siemens AG**
www.siemens.com



Halle 11
Stand 101

Direkt zur Marktübersicht i-need.de

www.i-need.de/?Produkt=2455

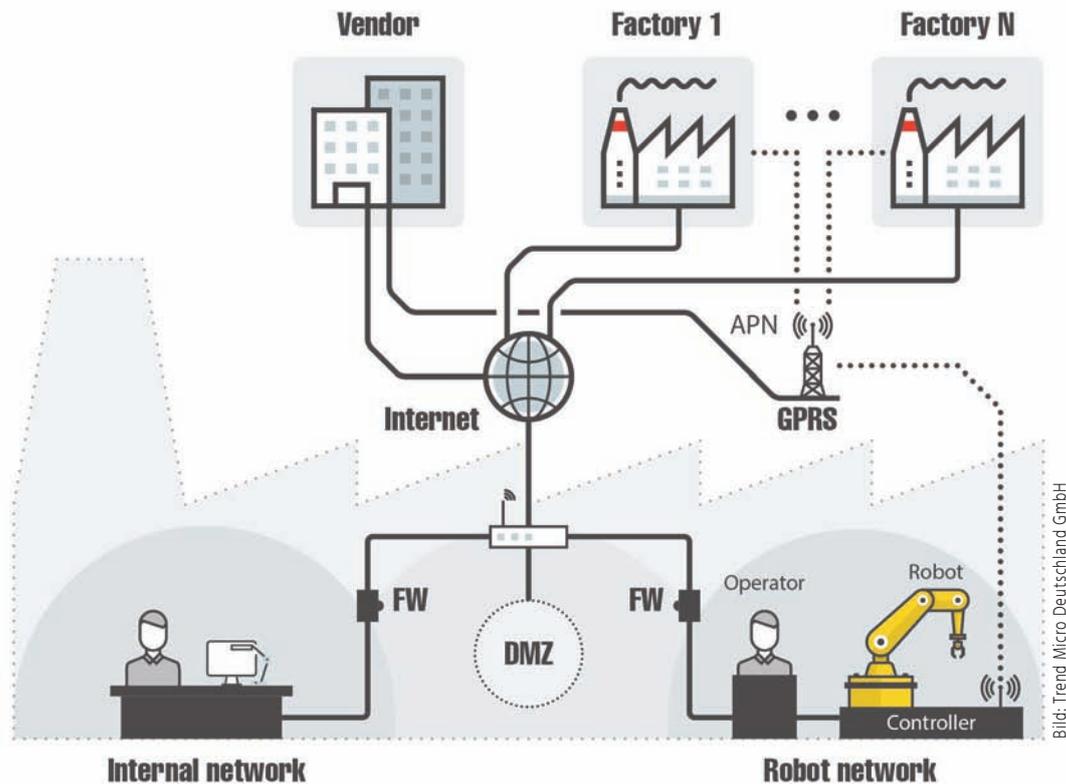


Bild: Trend Micro Deutschland GmbH

Ganzheitlich schützen

Rundumblick für die Sicherheit

Sobald Industrieanlagen mit dem Internet verbunden sind, können sie zum Einfallstor für Cyberangriffe werden. Um vernetzte Industrielösungen zu schützen und eine sichere Industrie 4.0 zu schaffen, bedarf es einer ganzheitlichen Anstrengung von Betreibern, Softwareentwicklern und Sicherheitsexperten.

Auch wenn kritische Systeme nicht mit dem Internet verbunden sind, können sie sich Malware über das interne Netz oder USB-Sticks einfangen. Zielgerichtete Angriffe nehmen meist ihren Anfang über die Office-IT oder auf Engineering Workstations. Eine Herausforderung ist dabei, die Netzwerkinfrastruktur und die Produktionsanlage sicher miteinander zu vernetzen. Es bedarf spezieller Lösungen, die die Produktionsanlagen absichern und Probleme bereinigen.

Industrierobotersysteme absichern

In der Karosseriefertigung sind 3D-Anwendungen mit dem Industrieroboter schon längst Stand der Technik und auch in anderen Industrien übernehmen Robotersysteme eine breite Palette von Aufgaben, wie das Verpacken in der Lebensmittelherstellung oder den Druckguss in der Metallindustrie. Im Zeitalter von Industrie 4.0 sind die Robotersysteme in automatisierten Produktionsanlagen zunehmend miteinander vernetzt. Mithilfe neuer APIs können Mitarbeiter die Roboter von Smartphoneapps aus kontrollieren und manche Industrieroboter sind direkt über das Internet erreichbar, um Monitoring oder Wartung durchzuführen. Mit der zunehmenden Vernetzung und externen Zugriffsmöglichkeiten gewinnt die Absicherung nach außen an Bedeutung. So sollten beispielsweise technische Dokumente nicht auf öffentlich zugänglichen Sites zur Verfü-

gung stehen und Zertifikate nicht über alle Produktinstanzen hinweg, üblicherweise selbst signiert, wiederverwendet werden. Weitere Schwachstellen sind nicht gepatchte und veraltete Software-Komponenten, schlechte Authentifizierungspraktiken, schwache Transportverschlüsselung oder unsichere Weboberflächen.

Schützen – entdecken – säubern

Um die sensiblen Systeme vor Cyberattacken zu schützen, bedarf es einer ganzheitlichen Anstrengung von Betreibern, Roboter- und Software-Entwicklern und Sicherheitsexperten. Dabei geht es um mehr als eine Verbesserung der Qualität von Embedded Software. Zullererst sollten Betreiber die Schwachstellen analysieren. Dann ist ein Sicherheitskonzept vonnöten, mit Prozessen und standardisierten Abläufen, die entsprechend installiert werden müssen. Zu einem ganzheitlichen Sicherheitskonzept gehört z.B. Security by Design (sichern ohne Installation von Software), um auf Gefährdungen von außen reagieren zu können. Manche Unternehmen haben bereits Cyber Security Operations Center eingerichtet, um auf Sicherheitsvorfälle schnell reagieren zu können. ■

Autor: Udo Schneider,
Security Evangelist,
Trend Micro Deutschland GmbH
www.trendmicro.de

Vorschau Industrial Communication Journal 2018

	Protokolle und Standards	Komponenten und Lösungen	Wireless und Remote	Sicherheit	Industrielle Kommunikation 4.0
Ausgabe I ET: 28.03.2018 RS: 28.02.2018	Profibus und Profinet AS-Interface	OPC UA als Backbone für Industrie 4.0 Kommunikationslösungen für die Antriebstechnik Serielle Adapter für Ethernet <i>mit Marktübersicht</i>	Industrielle Mobilfunk-Standards und -Lösungen	Redundante Kommunikation (PSP, HSR etc.) Plagiats- und Know-how-Schutz Sicher kommunizieren mit FSOE	Industrial IoT Cloud & M2M Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN
Ausgabe II ET: 15.05.2018 RS: 17.04.2018	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 Cloud & M2M Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN
Ausgabe III ET: 05.10.2018 RS: 07.09.2018	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 Cloud & M2M Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN
Ausgabe IV ET: 19.11.2018 RS: 22.10.2018	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 Cloud & M2M Big Data & Analyse Datendurchgängigkeit Security Ethernet TSN

ET: Erscheinungstermin, RS: Redaktionsschluss

Inserentenverzeichnis

ads-tec GmbH	28	Nexans Deutschland GmbH	30
Beckhoff Automation GmbH & Co. KG	11, 29	MKU Metrofunk Kabel-Union GmbH	67
CLPA Europe	39-50	Moxa Europe GmbH	17
Hans Turck GmbH & Co. KG	5	MPL AG	29
Helmholz GmbH & Co. KG	68	ODVA Inc	3
HMS Industrial Networks GmbH	29	OPC Foundation	57
IBHsoftec GmbH	13	PROFIBUS Nutzerorganisation	Titel
InoNet Computer GmbH	33	Red Lion Controls	29
J. Schmalz GmbH	55	Siemens AG	30
Mitsubishi Electric Europe B. V.	53	Wachendorff Prozesstechnik GmbH & Co. KG	30
Mitsubishi Electric Europe B. V.	53	WAGO Kontakttechnik GmbH & Co. KG	2

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-Scheiky (V.i.S.d.P.)

REDAKTION:
Kai Binder (Chefredakteur, kbn),
Mathis Bayerdörfer (Chefredakteur, mby),
Clara Luise Josuttis (clj),
Georg Hildebrand (ghl)

WEITERE MITARBEITER:
Inka Bach, Tamara Gerlach,
Anja Giesen, Frauke Itzerott,
Pascal Jenke, Victoria Kraft,
Kristine Meier, Melanie Novak,
Kristina Sirjanow, Marco Steber,
Florian Streitenberger, Natalie Weigel

ANZEIGEN:
Sina Debus, Heiko Hartmann,
Daniel Katzer, Markus Lehner,
Thomas Möller

ANZEIGENDISPOSITION:
Michaela Preiß
Tel. 06421/3086-0

Es gilt die Preisliste der Mediadaten 2017.

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

DRUCK:
Offset vierfarbig
L.N. Schaffrath GmbH & Co. KG
Marktweg 42 - 50, 47608 Geldern

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

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

ISSN 0935-0187
Vertriebskennzeichen G30449

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

© Copyright by
TeDo Verlag GmbH, Marburg.



Die DNA von Metrofunk

für Systemerhalt
hinter der Kulisse



Metrofunk Kabel-Union GmbH
D-12111 Berlin, Tel. 030 79 01 86 0
info@metrofunk.de – www.metrofunk.de





SICHERER IOT-MASCHINENFERNZUGRIFF

myREX24 V2 Portal – Erleben Sie wie einfach Fernwartung in Zukunft sein kann

Visualisierung der Anlagenwerte, Alarmierung bei Überschreitung von Grenzwerten, Protokollierung von Betriebsdaten und der Zugriff von jedem Ort der Welt auf Ihre Anlagen via WEB2go – Das alles bietet Ihnen das myREX24 V2 Portal. Dank der umfangreichen Monitoring und Alarmfunktionen wird Predictive Maintenance für jeden Anlagenhersteller und Maschinenbauer möglich.

- Speziell auf das Automatisierungsumfeld zugeschnitten
- Durchgängiges System für den Zugriff auf Steuerungen, Antriebe, Regler, etc.
- Frei konfigurierbare Dashboards zur individuellen Darstellung der Daten
- Auf Ihre eigene Server-Infrastruktur portierbar
- Praxiserprobtes durchdachtes Sicherheitskonzept