

A *Computer &* **AUTOMATION**

Fachmedium der Automatisierungstechnik

IM FOKUS
**Smart
Factory**

Industrie 4.0
**Standards im
Praxistest**

Seite 18

TSN-Serie
**Open-Source-Chip
für Wireless-TSN**

Seite 28

ROBOTICS & AUTOMATION
**Zukunftsszenarien
für die Robotik**

Seite 37

Low-Power-Prozessoren ans Ethernet

SONDERHEFT **SAFETY & SECURITY**

ab Seite 47

DREIPHASIGER AC-SOFTSTARTER FÜR PUMPEN UND VENTILATOREN



Ausgestattet mit einem selbstlernenden Algorithmus, der Parameter automatisch anpasst, um Motoren optimal zu starten und zu stoppen.

Ständig weitere Automatisierungsoptionen.

digikey.de/automation

Telefon: (+49) 30 915 884 91



DIGI-KEY ELECTRONICS & AUTOMATION™
*Ihre Quelle für modernste elektronische Komponenten
und Automatisierungstechnik*



Wohlstand durch Robotik

Wenn sich im Jahr 2030 ein Großteil der Babyboomer-Generation in den Ruhestand verabschiedet, wird die Ressource ‚Arbeitskraft‘ knapp. Möchte Deutschland über das Jahr 2030 hinaus wettbewerbsfähig bleiben, führt kein Weg an der Robotik vorbei.

Dieses Problem mit der Ressource ‚Arbeitskraft‘ betrifft nicht nur Deutschland, sondern auch andere Länder. Und es betrifft nicht nur die produzierende Industrie, sondern auch den Pflege- und Dienstleistungssektor. Politiker weltweit haben das Problem erkannt und verschiedene Förderprogramme auf den Weg gebracht. Die ‚International Federation of Robotics‘ hatte bereits im Juni 2020 die internationalen Förderprogramme im Report ‚World Robotics R&D Programs‘ zusammengefasst; nun wurde dieser aktualisiert.

Viele Regierungen nutzten die Corona-Pandemie, um ihre Förderprogramme anzupassen – mit unterschiedlichen Schwerpunkten. Die Entwicklungsziele in Chinas Strategieplan ‚Made in China 2025‘ etwa setzen vor allem auf ein kontinuierliches Roboter-Wachstum im industriellen Einsatz. Auch sollen mindestens drei führende Unternehmen mit internationaler Wettbewerbsfähigkeit entstehen. Ein Sonderprogramm fördert die Entwicklung intelligenter Robotertechnologien, das die Innovationskette mit einbezieht.

Japan möchte Weltmarktführer bleiben und die Roboterichte in den eigenen Unternehmen weiter steigern. Hinzu kommt ein Aktionsplan für den Bereich Service-robotik in Landwirtschaft, Infrastruktur und Gesundheitswesen. Allein der Bereich Pflege & Medizin verfügt dabei über ein Budget von 997,3 Mio. Euro.

Deutschland hingegen fördert die Partnerschaft zwischen Forschung und Industrie, um gute Ideen schnell in innovative Produkte und Dienstleistungen umzusetzen. Bis 2025 sollen jährlich 3,5 % des BIP in Forschung und Entwicklung investiert werden. Außerdem wurde im Jahr 2020 im Rahmen der Mission ‚Technik für den Menschen‘ unter anderem das Programm ‚Miteinander durch Innovation‘ gestartet, das interaktive Technologien für Gesundheit und Lebensqualität fördert.

Die Ansätze sind unterschiedlich, doch alle zielen darauf ab, den Wohlstand für das eigene Land zu sichern. Japan und Deutschland setzen einen weiteren Fokus auf die Versorgung der Bevölkerung sowie auf die Lebensqualität der Menschen.

Welche Trends und Chancen sich darüber hinaus durch Robotik ergeben, erfahren Sie ab Seite 37 in unserem Spezial ‚Robotics & AUTOMATION‘.

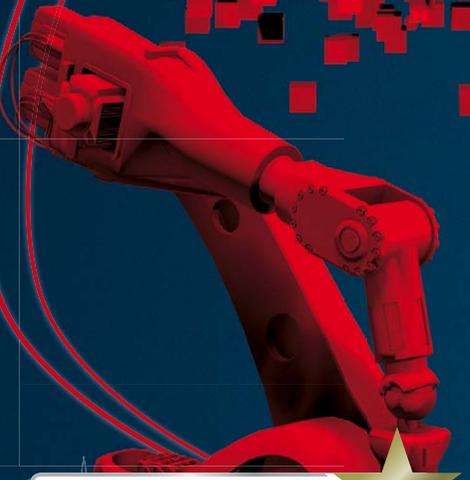
Andrea Gillhuber
Chefredakteurin

PS: Übrigens erwarten Sie auf <https://www.computer-automation.de/marktuebersicht/> drei neue, interaktive Marktübersichten zu den Themen Robotik, Safety und Security.



CODESYS

**EVERYTHING
UNDER CONTROL**



Computer &
AUTOMATION
**PRODUKTE
DES JAHRES**

2021

Steuern & Regeln

**Erhältlich im
CODESYS Store!**



**CODESYS
AUTOMATION SERVER**
Die Industrie-4.0-Plattform

Vereinfachen Sie Ihre Automatisierungsaufgaben. Nutzen Sie die Cloudplattform für einen komfortablen und sicheren Zugriff auf Ihre gesamte Steuerungslandschaft.
Egal, wo Sie gerade sind.

**CODESYS für
Maschinen- und
Anlagenbetreiber.**



Die Open-Source-Implementierung

Das Basissystem Industrie 4.0 im realen Einsatz

AKTUELL

- 6 News-Ticker**
Aktuelles aus der Branche
- 8 Autotuning für Industrienantriebe**
Automatisierte Regleroptimierung

TECHNOLOGIE

IM FOKUS: **Smart Factory**

- 15 Ein Meilenstein auf dem Weg der Umsetzung?**
Industrie 4.0 von der Theorie in die Praxis
- 18 Standards im Praxistest**
Die Verwaltungsschale an der Papiermaschine

- 21 Titel: Low-Power-Prozessoren ans Ethernet**
Die Feldgeräte-Anbindung an Single Pair Ethernet



- 25 Produkte**
- 28 Der Open-Source-Chip für drahtloses TSN**
TSN-Serie Teil 11: Die 5G- und WI-FI-Varianten
- 31 Design neu gedacht**
Vision-Sensoren schnell entwickeln und produzieren
- 33 Produkte**



Robotics & AUTOMATION

Wie Trends Robotikanwendungen beeinflussen

ROBOTICS & AUTOMATION

- 38 Roboter-Boom**
Welche Trends die Implementierung von Robotern befördern
- 41 Im Schwarm intelligenter**
Methoden und Anwendungsszenarien der Schwarmrobotik
- 44 Der Roboter als Edge-Gerät**
Den Mensch sichern und schützen
- 46 Produkte**
- 47 Sonderheft**
Safety & Security



47

Das Sonderheft **Safety & Security**

Funktionale Sicherheit und Industrial Security für vernetzte Fabrikanlagen

Bild: nipastock - shutterstock



Interaktive Marktübersichten online!

Beachten Sie die Marktübersichten zu den Themen Robotik, Safety und Security unter:

<https://www.computer-automation.de/marktuebersicht/>

RUBRIKEN

- 3 Editorial
- 9 Technik & Finanzen
- 12 IoT-Hotspot
- 58 Impressum / Inserenten
- 67 **Nachgehakt**
Marcus Eibach: 5G in der Halle 9 der Hannover Messe



Anschlusstechnik für Roboterapplikationen

PROFINET Anschlusstechnik für Robotik

Sensor-/Aktorleitungen

Maximale Biegewechsel & Torsion

Höchste Verfügbarkeit in dynamischen Anwendungen

Siemens und Schaeffler arbeiten zusammen



Bild: Siemens

Siemens Large Drives Applications (LDA) und Schaeffler arbeiten gemeinsam an einer intelligenten Zustandsdiagnose für Antriebssysteme. Dazu integriert Siemens den Analyseservice für die automatisierte Lagerdiagnose von Schaeffler in die eigene IIoT-Plattform ‚Sidrive IQ‘, die neben anderen Funktionen Antriebssysteme mit KI-basierten Analysen und digitalen Inhalten aufwertet. Die Analyse-Ergebnisse des Lagerzustands werden also in die Überwachung des Gesamt-Motorzustandes miteinbezogen. Dem Anwender steht am Ende eine automatisierte Wälzlagerdiagnose für Betriebs- und Wartungsentscheidungen zur Verfügung. Elektromotoren sind in vielen industriellen

Die 100-Millionen-Grenze geknackt

Trotz der Pandemie-bedingten Herausforderungen wurden die Produkte mit Profibus&Profinet International (PI) durch Anwender sehr gut angenommen. Die Gesamtzahl der in Anlagen installierten Profibus- und Profinet-Produkte hat mit 104 Mio. eine beeindruckende Schwelle überschritten. Profinet hat hierbei auf Jahressicht die bisher höchste Zahl von 7,3 Mio. in den Markt gebrachten Produkten erreicht. Die Gesamtzahl der installierten Profinet-Geräte stieg gegenüber dem Vorjahreswert um mehr als 22 % an und hat den Gesamtwert von 40 Mio. erreicht. Im Jahr 2020 wurden insgesamt 1,7 Mio. Profibus-Geräte in den Markt gebracht, von denen 0,8 Mio. in Anwendungen der Prozessindustrie gingen. Im Verlauf der letzten Jahre hat sich der Anteil der Profibus-Produkte, die in prozesstechnischen Anlagen verbaut wurden, kontinuierlich erhöht, und es wird erwartet, dass im Folgejahr die Mehrzahl der Profibus-Produkte für Anlagen der Prozessautomatisierung geliefert wird. In der Fertigungstechnik sind inzwischen circa viermal mehr Geräte mit Profinet- als mit Profibus-Schnittstelle ausgestattet.

Bei IO-Link wurde im Jahr 2020 mit 5 Mio. Geräten die bisher höchste Jahreszahl geliefert. IO-Link hat somit auch in schwierigen Zeiten eine Wachstumsrate von 31 % erreicht. Die Gesamt-

Lenze veräußert Geschäftsbereich ‚Mobile Drives‘

Die Entscheidung ist strategisch: Lenze möchte sich in Zukunft mehr auf das Kerngeschäft fokussieren und verkauft aufgrund dessen den Geschäftsbereich ‚Mobile Drives‘ des Schweizer Tochterunternehmens Lenze Schmidhauser. Dieser entwickelt und vertreibt Komponenten für die Elektrifizierung von Nebenaggregaten in Nutzfahrzeugen. Neuer Eigentümer des Bereichs mobiler Antriebstechnik ist Bucher Hydraulics, Hersteller für Hydrauliklösungen bei mobilen Arbeitsanwendungen. Der Vollzug der Transaktion erfolgt nach erfolgreicher Separierung des Geschäftsbereichs ‚Mobile Drives‘ von der Lenze-Gruppe. Bis dahin wird das Geschäft von Schmidhauser unverändert fortgeführt.

Christian Wendler, CEO von Lenze, zu den Hintergründen: „Wir freuen uns, dass wir uns mit der Veräußerung zusätzlichen Spielraum für weitere strategische Maßnahmen zur Stärkung des Kerngeschäftes geschaffen haben. Weiterhin freuen wir uns mit Bucher einen Käufer gefunden zu haben, der neben der Übernahme sämtlicher Mitarbeiter und dem Verbleib am Standort Romanshorn das Geschäft im Nutzfahrzeugbereich mit Engagement fortführen und weiterentwickeln wird.“

ag

Kernprozessen eine treibende Kraft und Wälzlager als zentrale mechanische Komponente erfahren alle im Motor auftretenden Belastungen und Beanspruchungen. Daher bietet die Wälzlagerdiagnose einen entscheidenden Indikator für den Gesamtzustand und die Zuverlässigkeit eines Motors. Mithilfe der intelligenten Zustandsdiagnose beider Unternehmen erhält der Betreiber spezifische Informationen, um zu entscheiden, ob das Antriebssystem in Betrieb bleiben kann oder ob ein Schaden unmittelbar bevorsteht und das Lager daher im nächsten Wartungsintervall oder aber sofort ausgetauscht werden muss.

ag

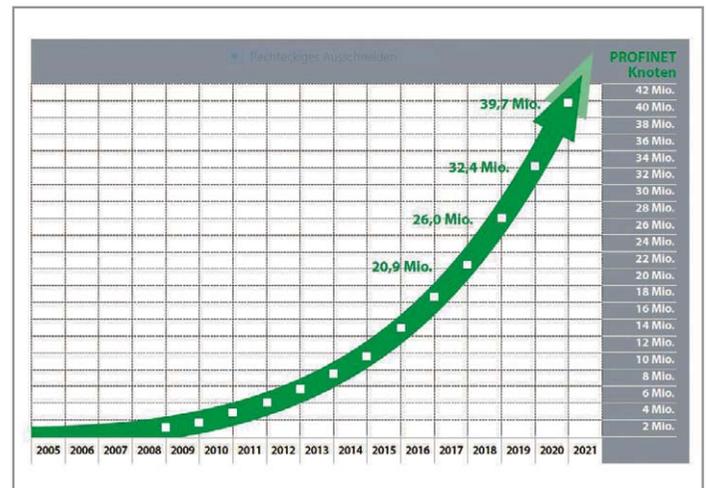


Bild: PI

Auch im Corona-Jahr 2020 konnte Profinet ein gutes Wachstum erzielen. Die installierte Basis hat nunmehr die 40-Millionen-Marke überschritten.

zahl der installierten IO-Link-Geräte beträgt jetzt mehr als 21 Mio. Bei Profisafe wurde mit den im Jahr 2020 installierten 2,6 Mio. Knoten der Wert vom Vorjahr knapp überschritten. Die Gesamtzahl der installierten Profisafe-Knoten liegt demnach bei mehr als 16 Mio.

hap

Eine erste Gaia-X-Lösung

Hewlett Packard Enterprise hat Lösungen angekündigt, die Unternehmen dabei helfen sollen, Gaia-X zu nutzen. Im Mittelpunkt stehen ein Framework, ein Marktplatz und Services. Das ‚HPE Solution Framework‘ für Gaia-X soll Unternehmen, Service Providern und öffentlichen Organisationen helfen, sich auf die Teilnahme an Gaia-X vorzubereiten. Es unterstützt praktisch alle Funktionen, die erforderlich sind, um Daten und Services in einer dezentralen, föderierten Umgebung sowohl bereitzustellen als auch zu nutzen. Als Ergebnis können Anwender ihre Fähigkeit zur Wertschöpfung aus Daten verbessern, riesige verteilte Datenpools anzapfen und ihre Souveränität über ihr datengetriebenes Geschäftsmodell stärken.

Das Framework basiert auf einer Referenzarchitektur, die sowohl Schlüsselkomponenten aus dem Software-Portfolio von HPE, Software von Drittanbietern und die Geschäftsplattform Cloud28+ nutzt. Cloud 28+ ist ein Marktplatz für die Monetari-

sierung von Daten und Diensten. Einzelne Lösungskomponenten des Frameworks und ganze Lösungsumgebungen sind als Service über ‚HPE GreenLake Cloud Services‘ verfügbar.

HPE hat außerdem den HPE Roadmap Service für Gaia-X angekündigt, der Kunden hilft, ihre Gaia-X-Bereitschaft zu bewerten und eine Roadmap zu entwickeln. Gaia-X tritt jetzt mit ersten Vorzeigeprojekten in die operative Phase ein, und die ersten Gaia-X-kompatiblen Lösungen werden voraussichtlich im Dezember 2021 zertifiziert werden. HPE ist seit der Gründung Mitglied der Non-Profit-Organisation Gaia-X AISBL und trägt zur Gaia-X-Architektur, den Standards und der Zertifizierung bei. Das HPE Solution Framework für Gaia-X und der HPE Roadmap Service für Gaia-X sind in Europa verfügbar. Einzelne Lösungskomponenten und ganze Lösungsumgebungen sind über HPE GreenLake Cloud Services verfügbar. Gaia-X-Schnittstellen und Konnektoren werden verfügbar gemacht, sobald die Gaia-X-Spezifikationen final sind. *hap*

Siemens kauft Supplyframe

Durch die Übernahme der Design-to-Source-Plattform Supplyframe baut Siemens die Strategie für digitale Marktplätze aus. Das lässt sich der Konzern 700 Mio. Euro kosten. Supplyframe ist ein sogenanntes DSI-Ökosystem (Design-to-Source Intelligence) mit weltweit mehr als 10 Mio. Ingenieuren und Einkäufern als Kunden. Es hilft Unternehmen bei Produktentwicklung, -beschaffung, -vermarktung und -verkauf von elektronischen Komponenten. Das Unternehmen wurde 2003 in Pasadena, Kalifornien, gegründet und erwartet für das Geschäftsjahr 2021 einen Umsatz von 70 Mio. Dollar mit den für das Software-Geschäft üblichen Gewinnspannen. Siemens erwartet durch die Übernahme einen erheblichen Mehrwert für Kunden: So soll der nahtlose Zugang zum Angebot von Siemens und das Marktplatz-Know-how von Supplyframe Kunden

dabei helfen, ihre Kosten zu reduzieren und Flexibilität und Geschwindigkeit zu erhöhen. Die Akquisition stärkt zudem das Portfolio von Siemens durch Software-as-a-Service (SaaS) – nicht nur im Bereich Electronic Design Automation (EDA) und Printed Circuit Boards (PCB), sondern auch anderen Geschäfts- und Technologiefeldern. Cedrik Neike, Mitglied des Siemens-Vorstands und CEO Digital Industries: „Supplyframe wird der Nukleus für die Beschleunigung unserer digitalen Marktplatz-Strategie. Das Ökosystem und das Marktplatz-Know-how von Supplyframe ergänzen unser Industrie-Software Portfolio perfekt.“

Der Vollzug der Transaktion steht unter dem Vorbehalt üblicher Bedingungen und wird für das letzte Quartal des Geschäftsjahres 2021 erwartet. *ag*



STEGOCONNECT

IO-Link

IIOT – 100% EASY!

Vereinigen Sie IO-Link Sensoren & Aktoren aller Hersteller in einer IIoT-Plattform!

STEGO CONNECT – alle IO-Link Devices:
vernetzen · monitoren · steuern

Industrie 4.0 ganz easy!
Jetzt informieren!

STEGO-CONNECT.COM/IIOT

Autotuning für Industrieantriebe



Die jüngsten Versionen der Servo-Drives i950 und i700 sind bereits auf das Autotuning vorbereitet. Dabei erfolgt die Regleroptimierung automatisiert.

Maschinen funktionieren nur dann optimal, wenn die eingesetzten Antriebe bei der Inbetriebnahme an den Antriebsstrang angepasst sind: Dafür müssen die Parameter der Software im Umrichter maschinenspezifisch eingestellt werden. Ein integriertes Autotuning verkürzt diesen Prozess.

Ob Roboter in der Montage helfen oder Regalbediengeräte (RBG) im automatisierten Lager fahren, alle Beispiele erfordern eine exakte Positionierung und damit höchste Präzision von der Antriebstechnik. Die Laufgeschwindigkeit muss genau eingehalten werden. Die bestmögliche Anpassung der Regelung an die Maschine ist die Voraussetzung.

Heute folgen viele Regelungstechnik-Experten der Theorie und nutzen physikalische Modelle, um Antriebe automatisch an die Eigenschaften der Maschine, also der Regelstrecke, anzupassen. Diese Modelle bilden das Verhalten der realen Maschine durch Berücksichtigen von Massen, Federn und Dämpfer vereinfacht nach. Würden Theorie und Realität übereinstimmen, dann wäre das Problem damit gelöst. Leider sind Abweichungen des Modells von der realen Maschine nicht zu vermeiden: Beispielsweise ist die Feder im Modell in Wahrheit eine Welle, und diese ist nicht masselos, sondern schwer, oder ein Getriebe hat Spiel und damit eine kraftabhängige Elastizität, die das Modell nicht exakt abbildet. Die Regelungsoptimierung kann

aber nur so gut sein, wie die Übereinstimmung der Maschine mit dem Modell. Außerdem ist für die Anpassung trotz der Abstrahierungen immer noch der Einsatz von Spezialisten notwendig, die zudem einen enormen Aufwand betreiben müssen.

In der Industrie ist es gängige Praxis, den Antrieb von Hand einzustellen: Dafür wird er an seine – hörbare – Stabilitätsgrenze gebracht, die verwendete Reglereinstellung wird mit einem Sicherheitsfaktor multipliziert. Gemäß der Veröffentlichung zur Schwingmethode von Ziegler und Nichols aus dem Jahr 1943 liegt der Faktor je nach Art des Regelkreises (P/PI/PD/PID) zwischen 0,45 und 0,6 – also grob bei der Hälfte. Dieses Verfahren ist einfach anzuwenden und beinhaltet keine Modellfehler. Der Nachteil: Der Mensch ist als Sensor nicht besonders genau, und auch hier wird ein Experte für die Einstellung benötigt.

Der Antrieb als Sensor

Lenze hat nun ein Autotuning entwickelt, der sich auf die Ziegler-Nichols-Methode stützt. Die jüngsten Versionen der Servo-Drives i950 und i700 sind bereits mit der

Autotuning-Funktion ausgestattet, bereits beim Anwender befindliche Geräte können per Firmware-Update nachgerüstet werden. Zusätzliche Messkomponenten sind nicht nötig, stattdessen wird der Antrieb zum Sensor: Während die Reglereinstellungen verändert werden, wertet die Steuerungslogik die Daten vom Positionsgeber und zum Stromfluss aus, um zu erkennen, wann die Stabilitätsgrenze erreicht wird. Anschließend werden die Einstellungen errechnet und in der Konfiguration des Antriebs hinterlegt.

Beim Autotuning setzt Lenze ausschließlich auf die Messung der physischen Regelstrecke. Statt Abstraktion und Näherungswerten gibt es eine exakte Messung in der realen Maschine. Fehler, die durch die Anwendung eines Modells entstehen, lassen sich so vermeiden, ebenso die Nachteile der manuellen Einstellung.

Aus der automatisierten Regleroptimierung mit dem Autotuner ergeben sich mehrere Vorteile: Die Einstellung der Regler ist reproduzierbar, sodass der Antrieb bei allen Anlagen gleich gut läuft. Insbesondere die Optimierung der Integralen-Anteile der Regler führt über eine Betrachtung der Schleppfehler zu signifikanten Verbesserungen, die über die Ziegler-Nichols-Methode hinausgeht. Außerdem ist das Autotuning sehr robust, da die Reglereinstellung einen ausreichenden Abstand zur Stabilitätsgrenze sicherstellt: es funktioniert auch bei Getrieben mit Spiel und bei veränderlichen Lasten.

Autotuning-Funktion zum Nachrüsten

Lenze hatte einige Anlagenbetreiber ausgewählt, bei denen die vorhandenen Maschinen mit der Autotuning-Funktion nachgerüstet wurden. Um bis zu 20 % höhere Taktzeiten konnten in Vor-Ort-Tests durch die Optimierung der Umrichterparametrierung erzielt werden. Bei zukünftigen Inbetriebnahmen reduziert sich der Zeitaufwand.

Umgesetzt wird die Autotuning-Funktion in den Tools Easy Starter und PLC-Designer. Beide bekamen zur Hannover Messe 2021 Digital Edition ein Update. *ag*

DR. JOHANNES KÜHN

ist Leiter R&D Motion Control bei Lenze.

Von Thomas Rappold

Programmiert auf Krypto

Schwache Rendite treibt private Anleger ebenso wie Unternehmen um. Alternativen sind gefragt. Kryptowährung ist die neue Asset-Klasse der Stunde. Welche Kryptowährungen gibt es, was zeichnet sie aus und welche Auswirkungen hat die Alternativwährung auf Industrie 4.0?

In Zeiten von Nullzinsen oder gar Strafzinsen sind Privat- wie Institutionelle Anleger auf der Suche nach Rendite. Auf dem Girokonto ist bekanntlich nichts mehr zu holen. Auch Unternehmer und Firmen werden inzwischen für hohe Bargeldbestände auf Bankkonten von ihren jeweiligen Instituten mit teils nicht unerheblichen Gebühren belastet. Gleichzeitig droht uns eine signifikante Inflationswelle. Rohstoffe wie Holz, Metalle und Baumaterialien wie Zement werden zu knappen Gütern und deren Preise gehen durch die Decke. Grund dafür sind die gigantischen

Konjunkturprogramme dies- und jenseits des Atlantiks, aber auch in Asien. Die synchrone Nachfragebelebung führt zur Verknappung der Güter und folglich zu starken Preisanstiegen. Auch Anleger müssen sich darauf einstellen und ihre Ersparnisse möglichst inflationssicher anlegen.

Krypto-Anlagen schlagen alle anderen Anlagen

Ein Blick auf die Wertentwicklung der letzten zehn Jahre zeigt folgendes Bild: Anlagen in Rentenpapieren konnten im Schnitt um 0,9 % pro Jahr zulegen, die Reallöhne

wuchsen im selben Zeitraum in gleicher Höhe. Gold, die Fluchtwährung bei Inflation schlechthin, konnte immerhin um 2,4 % pro Jahr an Wert gewinnen. Deutschlands liebstes Kind, die Anlage in Immobilien, weist ein Zuwachs von 6 % pro Jahr aus. Noch besser entwickelte sich der DAX mit einem jährlichen Anstieg von durchschnittlich 6,5 %. Doch über allem steht die Kryptowährung Bitcoin mit einer jährlichen realen Rendite von 156,8 %. Kryptowährungen scheinen aktuell das Nonplusultra zu sein und wie aus dem Nichts werden innerhalb kürzester Zeit märchenhafte

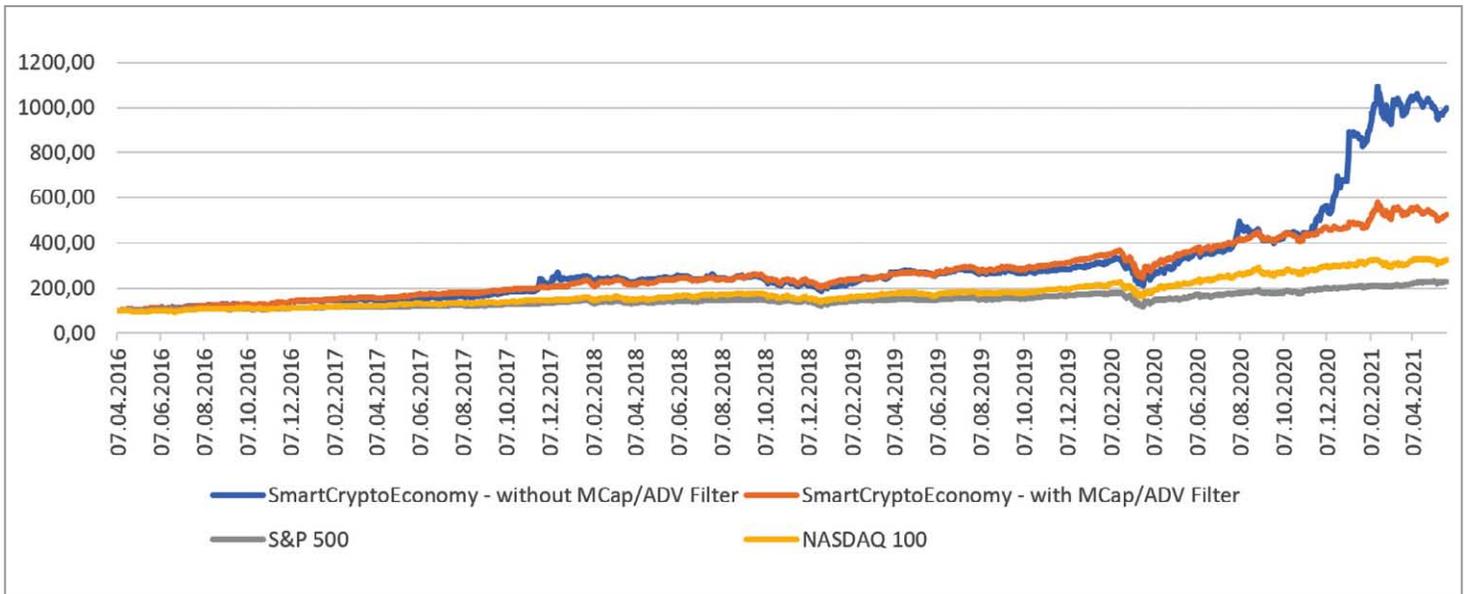


Der einfache Weg ins Industrial IoT from data to value

Der Weg ins Industrial IoT muss nicht kompliziert sein. Egal, ob bspw. ein Zugang zu wertvollen Daten benötigt wird oder neue, datenbezogene Services generiert werden sollen, Weidmüller bietet Komponenten und Lösungen und ermöglicht so den einfachen Zugang ins Industrial IoT.

Mit dem umfassenden, zukunftsorientierten und aufeinander abgestimmten IoT-fähigen Portfolio gelingt der Weg ins Industrial IoT - „from data to value“. Egal ob Greenfield oder Brownfield bietet Weidmüller Lösungen für die Datenerfassung, die Datenvorverarbeitung, die Datenkommunikation und die Datenanalyse.

www.weidmueller.de/iiot



Mit dem neuen Smart Crypto Index (ISIN: DE000VQ8SSC7) von Vontobel können Anleger nun weltweit erstmals über ein Indexzertifikat in die 20 wichtigsten Aktien des Krypto-Sektors sowie die fünf bedeutendsten Kryptowährungen investieren. Dabei deckt der Index die gesamte Wertschöpfungskette mit Unternehmen aus den Sektoren der Miner, Chip Designer, Börsen, eCommerce-, Bezahl- und Blockchain-Plattformen, Investment-, Retail-Banken, Broker sowie Asset Manager und Verwahrstellen ab.

Gewinne erzielt. Immer wieder gibt es solche ‚Boom&Bust‘-Zyklen, bei denen Anlageklassen von euphorischen Anlegern in die Höhe getrieben werden. Erinnert sei an die größte aller Blasen, die Tulpenmanie in den Niederlanden. Sie führte im Jahre 1637 zum ersten und größten Absturz an einer Börse in der Weltgeschichte. Die



Thomas Rappold ist Experte für Technologieinvestments, FinTech-Unternehmer und internationaler Bestsellerautor.

Eine-Million-Dollar-Frage lautet nun erneut: Ist diesmal alles anders?

Krypto - Eine neue Asset-Klasse?

Die renommierte Investmentbank Goldman Sachs überschrieb kürzlich eine Studie zum Thema Kryptowährungen mit dieser Frage und brachte es damit auf den Punkt. Bitcoin, Ether, Litecoin, XRP, die Fantasy-Währung Dogecoin und weitere Hunderte von Währungen bringen es zusammen auf eine Marktkapitalisierung von rund 2 Billionen Dollar. Eine Stange Geld, mit der man auch ein Unternehmen wie Apple – immerhin der gewinnträchtigste Tech-Konzern überhaupt – kaufen könnte. Allein Bitcoin bringt es auf einen Gesamtwert von über eine Billion Dollar. Die Fans von Bitcoin sehen darin eine der wenigen einheitlichen Wertaufbewahrungsmittel der Welt (engl. ‚Store of Value‘). Es ist inzwischen der am weitesten verbreitete Vermögenswert in der Geschichte außerhalb des Dollars und des Euros; 140 Millionen Menschen besitzen Bitcoins. Im Gegensatz zu Gold ist Bitcoin leicht zu lagern und zu transportieren. Wertaufbewahrungen sind soziale Konstrukte: Sie haben einen Wert, weil wir glauben, dass sie einen haben. Bitcoin und andere Kryptowährungen sind das ‚Digitale Gold‘ der Generation Z und Y. Nicht ohne Grund betonte der CEO der Consors-

bank, einer der größten deutschen Direktbroker, dass jeder dritte Kunde der Bank am Krypto-Handel Interesse bekundet habe. In unserer modernen, globalisierten Gesellschaft, in der ein erheblicher Teil der sozialen Interaktion und des Handels online stattfindet – vor allem bei jüngeren Menschen –, muss es auch digital sein.

Bitcoin ist daher ein plausibles alternatives Wertaufbewahrungsmedium zu Gold und aufgrund seiner breiteren gesellschaftlichen Akzeptanz mit ähnlicher Struktur im Moment der beste Kandidat unter den Kryptowährungen. Nourel Roubini, Wirtschaftsprofessor an der New York Stern School of Business, Bestsellerautor und in der Fachwelt auch als ‚Dr. Doom‘ bekannt, sieht dies ganz anders. Seiner Meinung nach ist es falsch, Kryptos als Währungen zu bezeichnen: „Denn Währungen müssen vier Eigenschaften haben: Sie müssen eine Rechnungseinheit, ein Zahlungsmittel, ein stabiles Wertaufbewahrungsmittel und ein einziges Zahlungsmittel sein. Bitcoin und die meisten anderen Kryptowährungen haben keine dieser Eigenschaften“, so der renommierte Ökonom. Auch handle es sich nicht um Vermögenswerte. Diese zeichneten sich entweder durch einen Cashflow (Dividenden bei Unternehmen oder Zinskupons bei Anleihen) aus oder durch einen Nutzen wie dies bei Rohstoffen

Bilder: Thomas Rappold

wie Öl und Kupfer der Fall sei. Immerhin ist auch Gold ein wichtiger Rohstoff für die Elektronik- und Schmuckindustrie.

Kryptowährungen als strategische digitale Infrastruktur

Die drei stärksten Bewegungen im Krypto-Ökosystem, nämlich Zahlungen, dezentralisierte Finanzen (DeFi) und die Verpackung von Werten in sogenannte Tokens (NFT), werden größtenteils auf Ethereum aufgebaut. Dabei handelt es sich um eine Art programmierbare Währung, die auf der Ethereum-Blockchain aufbaut und mittels der Softwareentwickler digitale Anwendungen in Form sogenannter ‚Smart Contracts‘ schreiben können. Die Blockchain-Technologie verbunden mit dazu

„ Kryptowährungen und Blockchain sind zentrale Bausteine einer kommerziellen digitalen Infrastruktur. “

THOMAS RAPPOLD

programmierbaren Währungen hat das Potenzial, das globale Finanzwesen aber auch den industriellen Sektor nachhaltig zu verändern und zu disruptieren. Der Verkauf digitaler Kunst ist erst der Anfang.

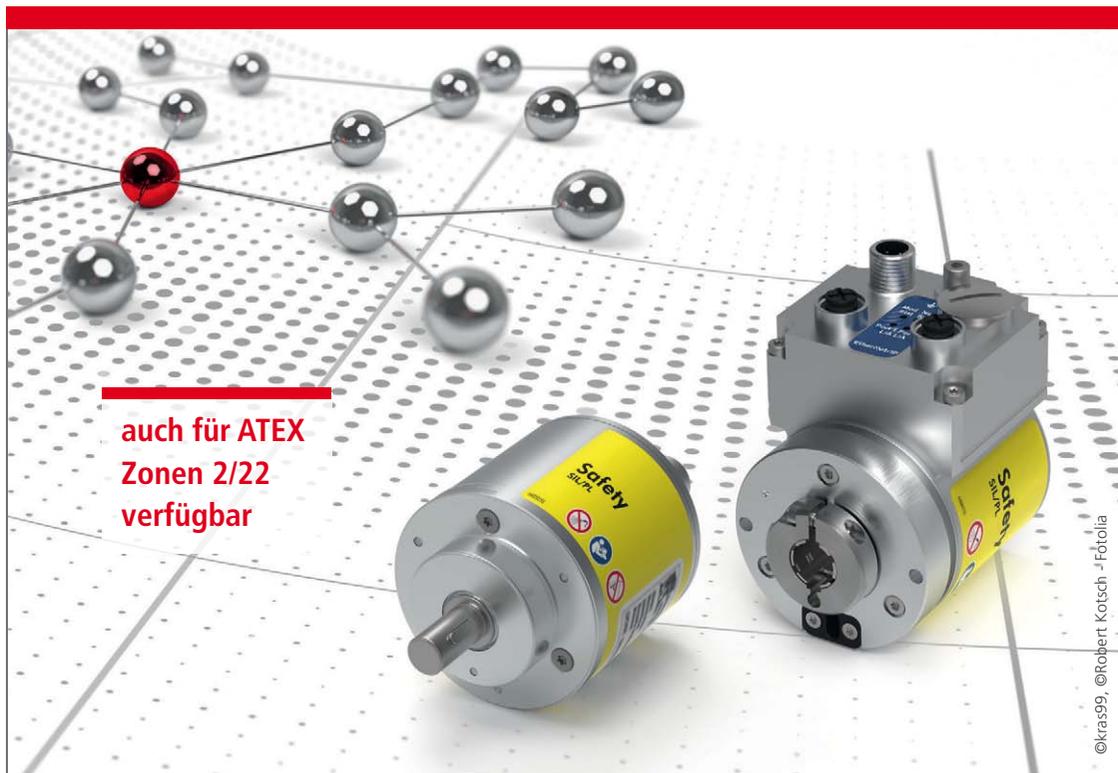
Kontext Industrie 4.0

Nachdem Deutschland die erste Halbzeit der Digitalisierung verloren hat, muss es nun seine Stärken im Bereich industrieller Software ausspielen. Dabei bedarf es eines Schulterschlusses der Paradebranchen Automobil und Maschinenbau, die beide vor großen Transformationsprozessen im Bereich der Digitalisierung stehen und durch ihre gegenseitigen Wirtschaftsbeziehungen stark voneinander abhängen. Deutschland hat bei den Themen Blockchain und Kryptowährungen eine exzellente Ausgangsposition: Die Bundesregierung hat die Bedeutung der Blockchain

erkannt und einen konkreten Fahrplan mit dem Ziel verabschiedet, die Chancen der Blockchain-Technologie zu nutzen und ihre Potenziale für die digitale Transformation zu mobilisieren.

Zudem steht die deutsche Industrie beim Einsatz von 5G an vorderster Front, bietet der neue Mobilfunkstandard doch mit seinen ultrakurzen Latenzzeiten erst-

malig eine echtzeitfähige M2M-Kommunikation, die sich in Kombination mit der Blockchain- und Kryptotechnologie hervorragend für die Etablierung neuer Geschäftsmodelle eignet. Wie die Digitalwirtschaft kann auch der Maschinenbau mittels Kryptowährung neue Erlösmodelle in Richtung flexibler Abonnement- und Pay-Per-Use-Modelle einsetzen. ag



auch für ATEX Zonen 2/22 verfügbar

Einschalten - absolute Position - SIL 3 Kat 4 Kleinster Absolutgeber für SIL 3-Anwendungen

TR-Electronic stellt funktional sicheren Drehgeber mit PROFIsafe und CIPsafety Ethernet/IP vor.

- SIL 3 / SIL 2 - PROFIsafe & CIPsafety Drehgeber im Industriestandard 58mm
- Redundanter Aufbau (KAT 4): zwei vollständig unabhängige Multiturndrehgeber in einem
- PROFINET Encoder-Profil (V4.2), IRT, MRP, Nachbarerkennung, Schnellstart, TCI, Reset Schalter, Preset on the fly
- PROFISafe Profil (V2.6.1), XP Protokoll, Shared device, dynamic IO configuration
- CIP Encoder Profil 0x22, ACD, DHCP, DLR, Preset on the fly
- CIP Safety 2.16, Hybrid Device



EtherNet/IP

TR electronic

www.tr-electronic.de

Ein Edge-App-Store der Industrie

Ende April stellte die OWL-Maschinenbau-Initiative den Industrial APP Marketplace vor: eine Online-Plattform für Docker-Container. Was steckt hinter dem Marketplace und welche Möglichkeiten bringt er den Anwendern?

Die Idee hinter der OWL-Plattform: Mit Hilfe der in der IT-Welt als De-facto-Standard etablierten Docker-Container-Technologie sollen sich Software-Anwendungen als ‚APPs‘ Anbieter-unabhängig auf verschiedensten Edge-Baugruppen – etwa Steuerungen oder Gateways – betreiben lassen. Damit wäre zukünftig der Hardware- und Software-Lieferant nicht mehr automatisch ein und derselbe. Das wiederum könnte in der industriellen Digitalisierung neue Geschäftsmodelle ermöglichen, allerdings

auch einige noch zu lösende Probleme aufwerfen.

Der Industrial APP Marketplace ist als verbindendes Element zwischen Maschinenbetreibern, Schaltschrankbauern und Entwicklern von industrietauglicher Software gedacht. Er orientiert sich funktional an App-Stores, wie wir sie für Smartphones kennen und nutzen. Es sollen aus Sicht der OWL-Maschinenbau-Initiative allerdings die speziellen Anforderungen und Bedingungen von Industrie-4.0-Anwendungen berücksichtigt werden.

Informationen statt Messwerte

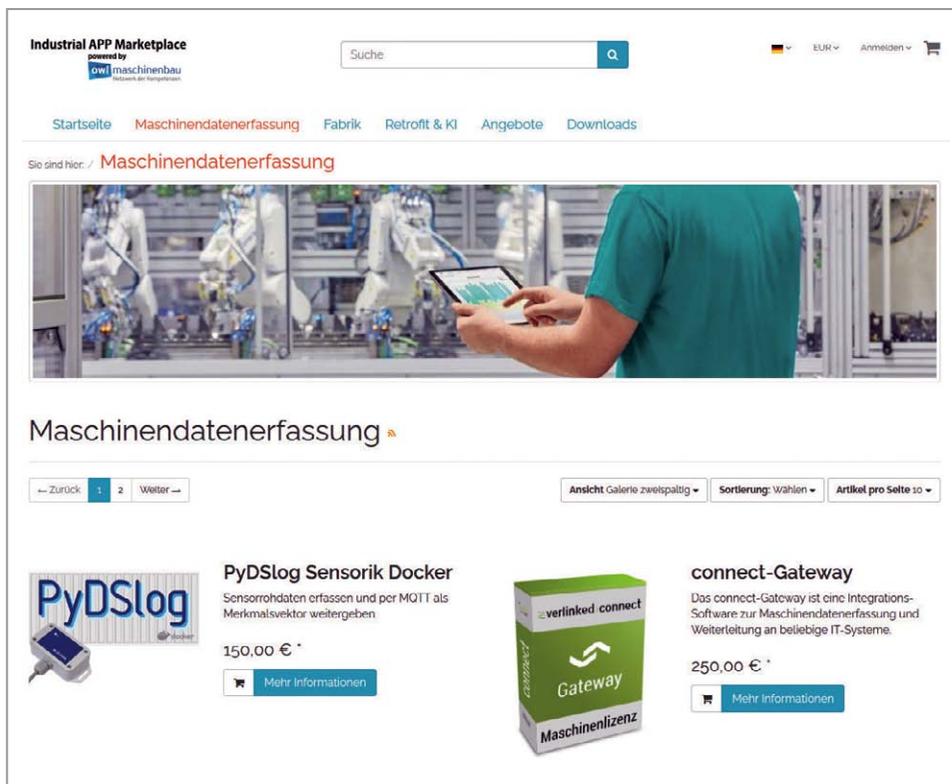
Docker-App-Stores für die Automatisierungstechnik, wie der Industrial APP Marketplace, schaffen für Anbieter und Anwender viele neue Möglichkeiten. Ein Beispiel aus der Sensorik: Bisher existiert in diesem Bereich ein sehr großes Produktangebot an hochentwickelten Industriensensoren, die aber lediglich relativ einfache Messwerte am Ausgang liefern. Dafür ist im Sensor selbst zwar eine sehr komplexe Technik notwendig, der Ausgangsmesswert ist für den Anwender jedoch nur ein einzelner Problemlösungsbaustein. Er benötigt darüber hinaus Softwarebausteine plus eine passende Laufzeitumgebung zur Messdatenverarbeitung, um die jeweilige Aufgabenstellung zu lösen. Die relevanten Softwarekomponenten müssen in der Regel individuell entwickelt werden. Dafür lassen sich sowohl Steuerungsbaugruppen mit IEC-61131-Programmierung als auch PCs plus Messdatensoftware (Matlab & Co.) einsetzen. Dadurch entstehen allerdings teilweise ein unerwünschter Vendor-Lock-in plus relativ hohe Zusatzkosten. Diese Situation lässt sich inzwischen über Docker-Container verbessern.

Mit Hilfe der Docker-Technologie und unabhängigen Marktplätzen sind standardisierte MSR-Sensorlösungen möglich, die aus den zwei Bausteinen ‚Sensor plus Docker-App‘ bestehen. Unabhängige Experten und Software-Anbieter könnten sich auf bestimmte Problemlösungen konzentrieren, die eingangsseitig zu verschiedenen Sensordatenbildern passen (etwa die Vibrations- oder Stromsensorik) und als Docker auf völlig unterschiedlichen Edge-Baugruppen verschiedener Hersteller einsatzfähig sind. Im Zusammenspiel mit KI-Funktionen, wie dem Machine Learning (ML), kann eine Docker-basierte App dann ausgangsseitig hochwertige Informationen zur Verfügung stellen, aus denen sich beispielsweise bei einer Predictive-Maintenance-Anwendung direkt der nächste Wartungstermin ableiten lässt.

Nur ein Docker reicht nicht

Qualitativ hochwertige Sensordaten plus maschinelles Lernen ermöglichen völlig neue Einblicke in die Zusammenhänge des Maschinen- und Anlagenbetriebs. Die dafür erforderliche Sensorik gibt es von unzähligen Anbietern. Die notwendigen ML-Algorithmen in Form von künstlichen

Bilder: SSV



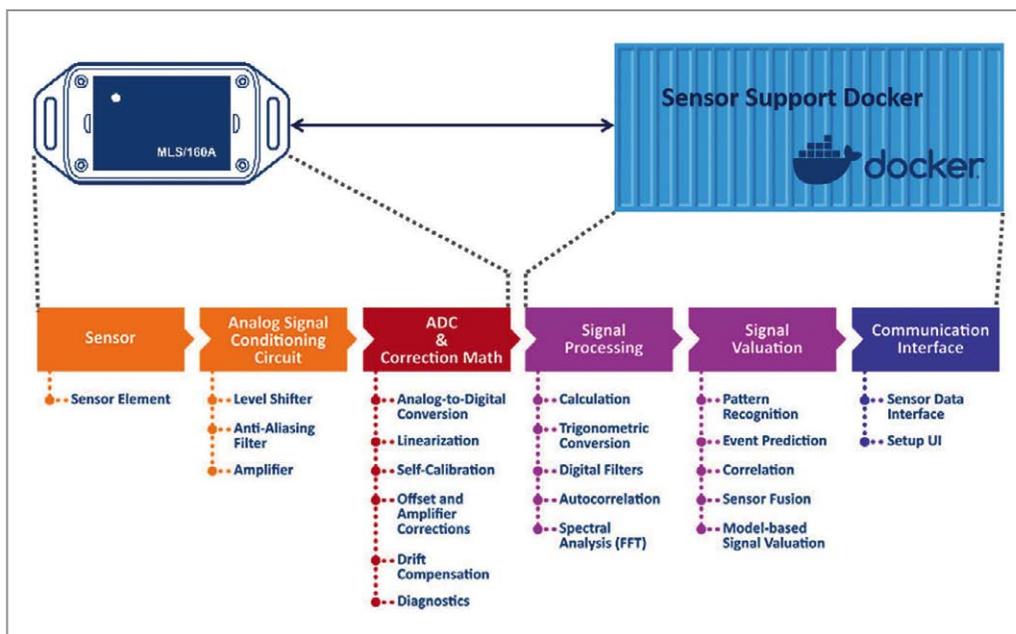
Der Industrial APP Marketplace wird als Webshop realisiert. Anbieter und Kunden benötigen jeweils ein eigenes Konto, um per Browser auf den Shop zugreifen zu können. Die einzelnen Produkte sind in Funktionsgruppen untergliedert und ausführlich beschrieben. Jedes einzelne Angebot steht als Docker zur Verfügung und kann im Rahmen eines Einkaufsvorgangs aus dem Webshop auf den eigenen PC geladen und von dort aus etwa direkt auf ein Edge-Gateway oder eine Docker-fähige Steuerung übertragen werden.

Ultra-kompakte Industrie-PCs: Multicore-Rechenleistung in IP 20 und IP 65/67



www.beckhoff.de/c6015
www.beckhoff.de/c7015

Mit Maßen von nur 82 x 82 x 40 mm und einzigartiger Montageflexibilität kann der Ultra-Kompakt-Industrie-PC C6015 auch kleinste Bauräume optimal ausnutzen. Die besonders robuste Variante C7015 dagegen bringt zusätzlich die Multicore-Rechenleistung direkt an die Maschine und erschließt so weitere Einsatzfelder. Die integrierte Intel-Atom®-CPU mit bis zu 4 Kernen erlaubt simultanes Automatisieren, Visualisieren und Kommunizieren auch in anspruchsvollen industriellen IP-65/67-Anwendungen. Neben klassischen Steuerungsaufgaben eignen sich beide Ultra-Kompakt-IPCs besonders gut für den Einsatz als Gateway zur Vernetzung von Maschinen und Anlagenteilen – dank hoher Rechenleistung auch mit aufwendiger Vorverarbeitung großer Datenmengen. Dank des integrierten EtherCAT-P-Anschlusses beim C7015 sind zusätzlich flexible I/O-Erweiterungen möglich.



Mit Hilfe der Docker-Technologie sind innovative MSR-Sensordatenlösungen möglich, die aus zwei aufeinander abgestimmten Bausteinen bestehen. Die sechs Funktionseinheiten eines intelligenten Sensorsystems sind dabei auf das eigentliche Sensorelement und den Docker verteilt. Anwendungsspezifische Softwarebausteine, wie Sensorfusionen, Sensordatenvorverarbeitung oder eine Datenauswertung per Machine Learning, sind innerhalb des Dockers realisiert. Updates und Weiterentwicklungen stehen als DevOps zur Verfügung.

neuronalen Netzwerken (Deep Learning) sind auch seit fast einem Jahrzehnt Stand der Technik – allerdings überwiegend in der IT- und weniger in der Automatisierungs- beziehungsweise MSR-Welt. Durch das Internet der Dinge entstanden vor einigen Jahren sogenannte Cloud-zentrierte Hub-and-Spoke-Systeme, also beispielsweise Sensor-to-Cloud-Lösungen mit zentraler Sensordatenverarbeitung. Über die beständig zunehmende Leistungsfähigkeit der Smartphone-Hardware und -Software lassen sich Deep-Learning-Anwendungen inzwischen auch mobil ohne Cloudverbindung nutzen. Über entsprechende Apps kann ein Smartphone eine ML-Inferenz – eine Schlussfolgerung einer Datenanalyse mit Hilfe eines Regelwerks – lokal ausführen, beispielsweise um Objekte in den Bilddaten des Kamerasensor zu erkennen. Eine solche Sensor-plus-App-Kombination ist durch Docker-App-Stores zukünftig auch in der Automatisierungstechnik möglich.

Allerdings verdeutlichen solche Anwendungen auch, dass nur ein Docker für den Edge-Einsatz nicht ausreichen wird. Da Deep Learning dem Supervised Machine Learning zuzuordnen ist, ist auch eine Machine-Learning-Pipeline für die Modell-erzeugung vonnöten, um ein geeignetes ML-Modell für den Inferenzbetrieb zu erzeugen. Diese Funktionsbausteine lassen sich zwar ebenfalls als Docker realisieren, sind dann aber für den Einsatz in der

Cloud beziehungsweise On-Premises auf IT-Systemen mit entsprechender Leistungsfähigkeit vorzusehen.

Die Sicherheitsaspekte

Docker, die aus öffentlichen App-Stores im Internet geladen und auf Edge-Gateways installiert werden, schaffen allerdings auch neue IT-Sicherheitsprobleme, für die möglichst vor der App-Store-Markteinführung Lösungen zur Verfügung stehen sollten.

Da der Faktor Mensch bei allen Security-Problemen in der Operational Technology eine sehr große Rolle spielt, sollte sich der App-Store-Betreiber darum kümmern, dass nur Angebote in den Store kommen, die eine dem Stand der Technik entsprechende IT-Sicherheit aufweisen. OT-Fachleute sind in erster Linie dafür verantwortlich, Maschinen am Laufen zu halten. Sie müssen die erforderliche Verfügbarkeit und Zuverlässigkeit garantieren. Das ist eine komplexe Aufgabe. Ein ausgeprägtes IT-Sicherheitsbewusstsein ist dafür nicht erforderlich. Aus diesem Grund müssen industrielle App-Stores von Haus aus entsprechende Sicherheitsrichtlinien zur Verfügung stellen und deren Einhaltung von den jeweiligen Anbietern einfordern.

Der Testbetrieb läuft

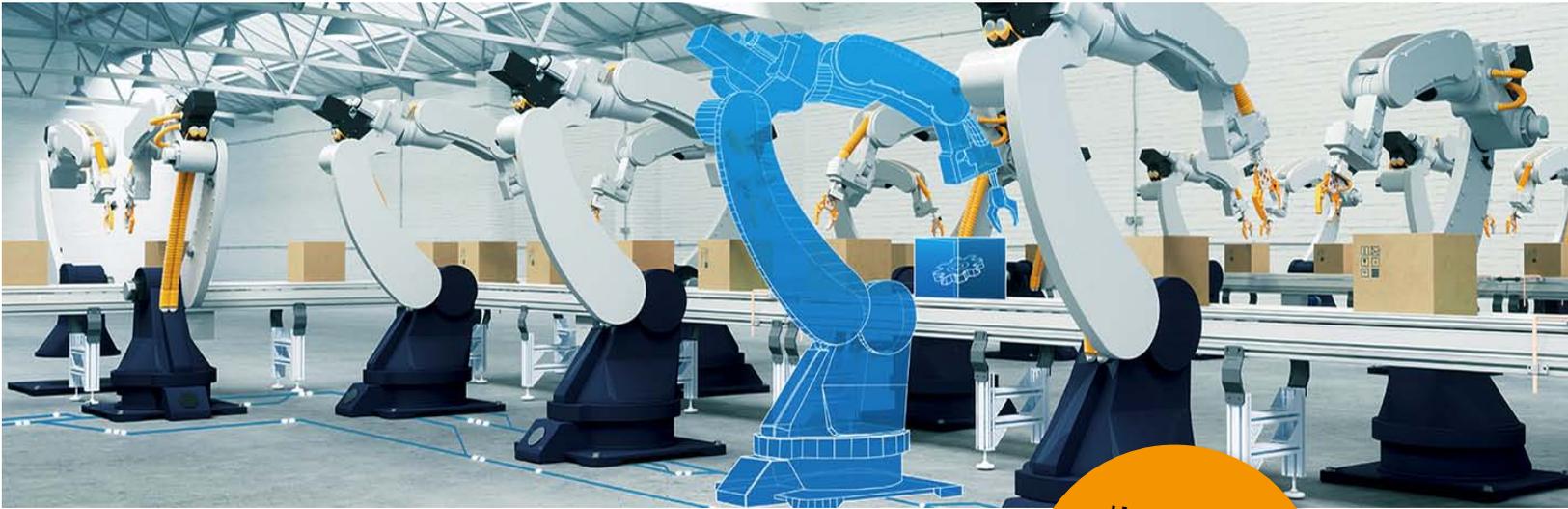
Die webbasierte Online-Plattform des Industrial APP Marketplace läuft seit einigen Monaten im Testbetrieb. Verschiedene Unternehmen und Organisationen aus

dem Umfeld der OWL-Maschinenbau-Initiative haben erste Docker-Apps entwickelt und testen den Einsatz auf unterschiedlicher Edge-Hardware. Auch der Docker-Verbundbetrieb, also das Zusammenspiel mehrerer Docker von unterschiedlichen Anbietern in einer einzigen Anwendung, wird zurzeit erprobt (ein Beispiel der Unternehmen Knowtion, PerFact, Phoenix Contact und SSV Software Systems aus dem Bereich des Condition Monitoring lesen Sie in Computer&AUTOMATION 2021, Heft 5, Seite 16f.). In Bezug auf den möglichst einfachen Einsatz für KI- beziehungsweise ML-Anwendungen sowie hinsichtlich der IT-Security ist jedoch noch etwas Entwicklungsarbeit erforderlich. Einfache Bedienbarkeit, echte Anbieter-unabhängigkeit und eine dem Stand der Technik entsprechende Cybersecurity sind anspruchsvolle Ziele. Ein möglichst schneller Markteintritt ist heute allerdings ebenfalls sehr wichtig. Hoffentlich finden die Verantwortlichen hinter dem Industrial APP Marketplace hier die richtige Balance.

hap



KLAUS-DIETER WALTER
ist Mitglied der Geschäftsführung bei SSV Software Systems.



IM FOKUS
Smart
Factory

Ein Meilenstein auf dem Weg der Umsetzung?

Die Umsetzung der Vision einer Industrie 4.0 läuft noch schleppend an! Der 1.0 Release der Open-Source-Referenzimplementierung Eclipse BaSys soll der Transformation ab sofort Flügel verleihen – ein Anwendungsbericht.

zung der relevanten Konzepte und Standardisierung als Software-Lösungen hat bei den Firmeninhaberinnen und -inhabern zusätzlich die Sorge geschürt, mit dem Beginn der Transformation ein großes Risiko einzugehen.

Die Angst war sicherlich in Teilen berechtigt; seit Mitte März 2021 ist jedoch ein Produkt auf dem Markt, das den digitalen Wandel beflügeln und deutlich sicherer machen könnte. Die Rede ist vom 1.0 Release der Eclipse BaSys Middleware. Zugegeben – der Name klingt abstrakt und lässt sich keineswegs in nur einem Satz erklären. Eines sei an dieser Stelle jedoch schon vorweggenommen: Der Release markiert einen bedeutenden Meilenstein in der Umsetzbarkeit von Industrie 4.0 und könnte die digitale Transformation ab sofort in die Breite tragen. Die Sachlage nun aber Schritt für Schritt:

Was ist die Middleware BaSys 4?
Mitte 2016 war es so weit: Das Bundesministerium für Bildung und Forschung hat gemeinsam mit 14 weiteren Partnern aus Wirtschaft und Forschung das Projekt ‚Basissystem Industrie 4.0‘ (kurz: BaSys 4.0) ins Leben gerufen. Die Konsortialleitung hat seitdem das Fraunhofer-Institut für Experimentelles Software Engineering

Zehn Jahre, nachdem deutsche IT-Fachleute erstmals den Begriff ‚Industrie 4.0‘ im Rahmen der Hannover Messe 2011 geprägt haben, wird die Bezeichnung inzwischen zwar weltweit mit der Bundesrepublik in Verbindung gebracht. Von der digitalen Zielgeraden ist Deutschland allerdings noch weit entfernt. Laut dem aktuellen ‚Digitalisierungsindex Mittelstand 2020/21‘ kommen die hiesigen Industrieunternehmen derzeit nur auf 62 von 100 möglichen Punkten hinsichtlich ihres Digitalisierungsgrades.

Berücksichtigt man zudem die Tatsache, dass Industrie 4.0 weit über die bloße digitale Transformation von Produktionsprozessen hinausgeht, würde das Ergebnis sicherlich noch erschreckender ausfallen. Irrtümlicherweise wird die vierte industrielle Revolution nämlich häufig mit dem Sammeln von Daten gleichgesetzt. Dabei geht es beim Wandel vielmehr darum, eine durchgängige Vernetzung aller Maschinen zu erzielen. Nur, wenn alle Maschinen

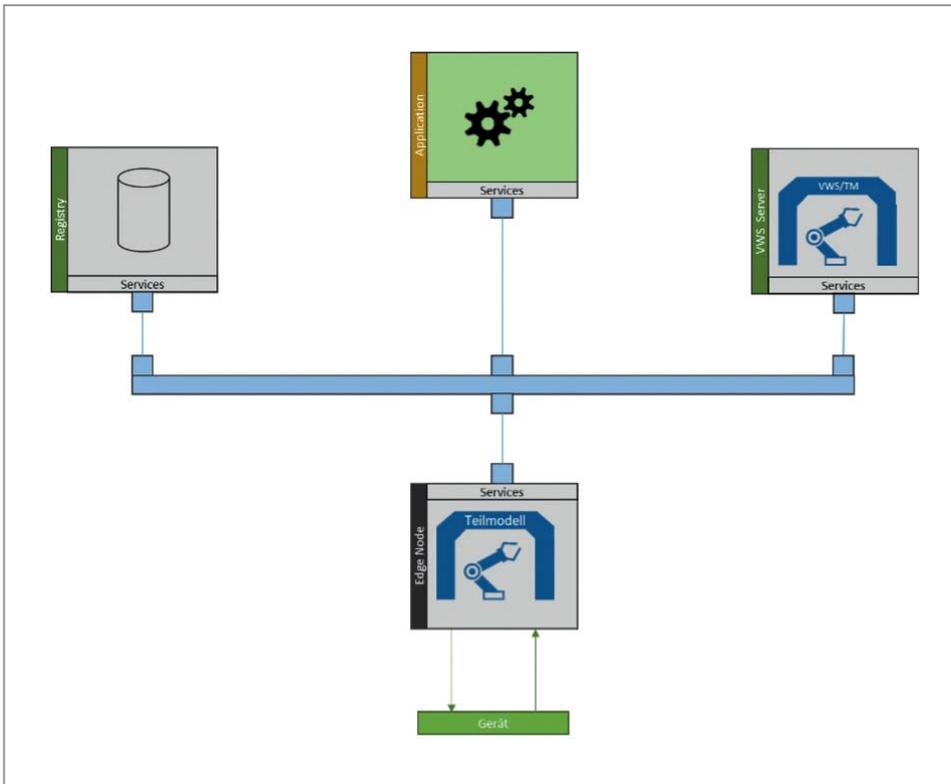
systemübergreifend miteinander kommunizieren können, ist eine entsprechend flexible – und somit wandelbare – Produktion überhaupt möglich. Zunächst stellt sich jedoch die Frage: Woran liegt es, dass wir in puncto industrieller Transformation derzeit maximal von 3.5 sprechen können? Vom angestrebten Status 4.0 sind wir noch weit entfernt.

Das Damoklesschwert für KMU
Die Gründe dafür sind vielseitig: Über vielen insbesondere kleinen und mittleren Unternehmen schwebt die Digitalisierung wie ein Damoklesschwert – es ist klar, dass der digitale Wandel unausweichlich ist. Wie er jedoch praktisch und möglichst effizient angegangen werden kann, scheint vielen Industriellen noch immer ein großes Rätsel zu sein.

Zudem erschweren die oftmals mangelnden finanziellen und personellen Ressourcen den Fortschritt zusätzlich. Und: Insbesondere die bislang fehlende Umset-

Bild: XiStock/onurdongel/Fraunhofer IES

Bild: Fraunhofer IESE



Übersicht über die Komponenten der BaSys 4 Middleware.

IESE in Kaiserslautern inne. Ziel des Forschungsprogramms war es, ein Technologiesystem für Produktionsanlagen zu entwickeln, das die effiziente Wandelbarkeit eines Herstellungsprozesses als zentrale Herausforderung der vierteln industriellen Revolution realisiert.

Der Plan wurde inzwischen in die Tat umgesetzt: Mit der ‚BaSys 4‘-Middleware hat das Konsortium eine Referenzarchitektur entwickelt, die die Umstellung der Unternehmen auf eine wandelbare Produktion breitenwirksam ermöglicht. Dafür ist es zunächst notwendig, die Datenmodelle und Protokolle so aufzubereiten, dass sie interoperabel sind – also miteinander ‚kommunizieren‘ können. Damit dies möglich wird, enthält die Middleware eine Sammlung wohldefinierter Building-Blocks, die zu einer zentralen oder dezentralen beziehungsweise verteilten Systemarchitektur verknüpft und miteinander integriert werden können. Kurzum: Der Aufbau der Middleware gleicht also einem Baukasten-Prinzip. Jedes Unternehmen kann dabei selbst auswählen, welche Komponenten es jeweils für seine Anwendungsfälle benötigt und diese dann individuell zum Einsatz bringen.

Angenommen eine Firma steht bei der Transformation noch gänzlich am Anfang, so muss beispielsweise zuerst der Shopfloor mit dem Officefloor verknüpft werden. Mit Hilfe des im Rahmen des Forschungsprojekts entwickelten Virtual Automation Bus (VAB) wurde eben dafür ein Konzept entwickelt, das eine netzwerk- und protokollübergreifende Peer-to-Peer-Kommunikation zwischen den Produktionsmaschinen und der IT Wirklichkeit werden lässt.

Liegen auf diese Weise sämtliche Daten einer Maschine digital vor, geht es anschließend darum, diese in eine gemeinsame Form ‚zu gießen‘. Denn: Eine einheitliche Sprache ist die Grundvoraussetzung, um die Produktionsanlagen vernetzen zu können.

Wie gelingt die Losgröße-1-Fertigung?

Für den Sprach-Transfer aller Daten sieht BaSys 4 das Prinzip der Verwaltungsschalen vor. Hierbei handelt es sich um standardisierte Digitale Zwillinge, die entsprechend einer einheitlichen Struktur aufgebaut sind. Jede Verwaltungsschale enthält Teilmodelle, die sowohl den Zustand eines realen Assets virtuell abbilden als auch bei Bedarf Live-Daten über

diese zur Verfügung stellen. Der Clou dabei: Die Verwaltungsschalen können nicht nur an andere Unternehmen weitergegeben werden; der Standard ist vor allem offen und jederzeit einsehbar.

Plant ein Unternehmen nun, eine effiziente Losgröße-1-Fertigung zu realisieren, hält BaSys 4 das Konzept der Führungskomponenten bereit. Jedes Gerät erhält dadurch eine einheitliche Dienstschnittstelle – und zwar indem die Ausführung von Produktionsprozessen von Produktionsdiensten getrennt wird. Zudem wird jede Fähigkeit einer Maschine ausreichend exakt beschrieben, sodass eine Fertigungsanlage möglichst einfach und effizient auf die Herstellung einer Sonderanfertigung umgestellt werden kann.

Damit die BaSys 4 Middleware möglichst vielen Unternehmen die digitale Umstellung erleichtern kann, steht die Referenzimplementierung Eclipse BaSys den Firmen Open Source zur Verfügung – und das gänzlich ohne Lizenzkosten. Software-Entwickler können den zur Verfügung gestellten Code in Form einbindbarer Bibliotheken direkt anwenden und sparen so wertvolle Zeit, die sie ansonsten selbst zur Code-Entwicklung und zum Beispiel zur Umsetzung des Verwaltungsschalenstandards und dessen Schnittstellen benötigen würden. Selbst Anwendern ohne Programmierkenntnisse ist es mittels der Off-the-Shelf-Komponenten somit möglich, direkt durchzustarten. Ebenso verringert es durch die vielen Beispiele die Einarbeitungszeit in die Thematik der Verwaltungsschale immens.

Was ändert sich mit dem 1.0 Release?

Beim 1.0 Release handelt es sich um ein Versprechen: Die Middleware macht es ab sofort möglich, die im Rahmen der vom Bundeswirtschaftsministerium 2013 gegründeten ‚Plattform Industrie 4.0‘ entwickelten Standards und Konzepte flächendeckend und standardkonform umzusetzen.

Als ein Teil der Plattform hat sich hierbei die Arbeitsgruppe ‚Referenzarchitekturen, Standards und Normung‘ in den vergangenen Jahren eingehend mit der Entwicklung offener und einheitlicher Standards für die Industrie 4.0 beschäftigt. Diese sollen sowohl einen fairen Wettbewerb sichern als auch die Investitionsrisiken für Unternehmen senken. Die Standards schließen sämtliche Bereiche einer vernetzten Produktion

mit ein: Hardware und Software, Anwender- und Anbieterbranchen sowie Produktdesign bis Produktrecycling.

Dank des 1.0 Release sind ab sofort nun auch sämtliche Schnittstellen der Eclipse BaSyx Middleware stabil und die Kompatibilität zu zukünftigen Updates gegeben. Dadurch haben die Unternehmen die Garantie, auch zukünftige Features und Updates ohne Änderungen an bestehendem Code integrieren zu können.

Wo kommt die Middleware zum Einsatz?

Eine Veranschaulichung, welche Vorteile der Einsatz der Middleware in der praktischen Anwendung bietet, liefert die Robert Bosch GmbH. Das Unternehmen war von Beginn an an der Entwicklung der Middleware beteiligt. Aktuell wird der 1.0 Release nun an vielen Stellen in der Produktentwicklung erprobt: von der Geräte- und Anlagenautomation über Plattformapplikationen bis hin zur Anwendung von Cloud-Szenarien.

Ein konkreteres Beispiel liefert etwa der Nexo-Funk-Akkuschrauber aus der industriellen Schraubtechnik von Bosch. Bereits die nächste Generation des Schraubers wird über eine Verwaltungsschale verfügen, die mittels BaSyx entstand. Das heißt: Durch die Modularität und die vielfältigen Deployment-Möglichkeiten der BaSyx Building Blocks kann eine Verwaltungsschale sogar auf einer (Kleinst-)Steuerung bereitgestellt werden, die direkt in der Schrauber-Hardware integriert ist.

Für die Zukunft erhofft sich Bosch eine breite Anwendung der BaSyx Middleware

in unterschiedlichsten Szenarien. Gerade beim Thema Vernetzung der Produktion sieht das Unternehmen großes Potenzial für die Anwendung der Middleware.

So etwa im Customer Experience Center am neuen Standort Ulm, wo die Middleware eingesetzt wird. Sämtliche Geräte, Maschinen und Anlagen verfügen dabei über eine Verwaltungsschale, die mittels BaSyx erstellt wurde. Diese integrieren sich

in einer zentralen Registry und ermöglichen dabei eine Vielzahl unterschiedlicher Anwendungsfälle, die als Applikationen darauf aufsetzen. Eine Anwendung ist die Ablaufsteuerung der Anlage mittels eines Business Process Modells (BPMN) und einer Workflow Execution Engine. Dieses System an Modellen und Applikationen für die Ablaufsteuerung bezeichnet Bosch als Orchestrierungslösung. *hap*

Bild: Fraunhofer IESE



FRANK SCHNICKE

ist Expert 'Industrie 4.0 System Architectures' am Fraunhofer-Institut für Experimentelles Software Engineering IESE in Kaiserslautern. Außerdem koordiniert er die Implementierung von Eclipse BaSyx am IESE.

Bild: Bosch

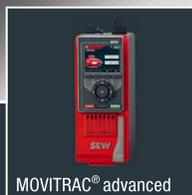
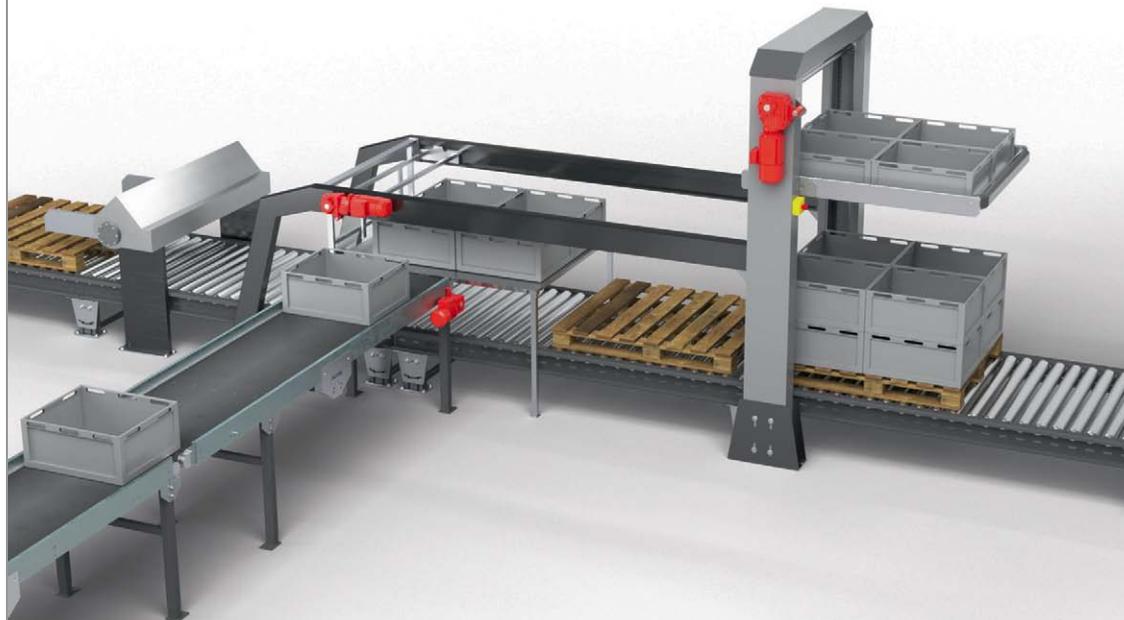


CONSTANTIN ZIESCHE

ist Projektleiter für Produktentwicklung bei der Robert Bosch GmbH und Hauptentwickler des .NET Stacks der Middleware Eclipse BaSyx.

SEW-EURODRIVE—Driving the world

**MOVITRAC® advanced:
Standard neu definiert!**



Zeit sparen und Flexibilität gewinnen – mit dem kompakten Standard-Umrichter für den flexiblen Einsatz in drehzahlgeregelten sowie dynamischen Förder- und Bewegungsapplikationen.

Vorteile

- flexible Anbindung an alle gängigen Kommunikationssysteme
- mehr Möglichkeiten durch integrierte, skalierbare funktionale Sicherheit
- ein Umrichter für Asynchron- und Synchronmotoren ohne und mit Geber
- innovative Einkabeltechnik mit standardisierter Anschlusstechnik
- intelligente Auto-Inbetriebnahme in wenigen Sekunden ohne Engineering-Tool

Nur eine von vielen Lösungen aus dem Automatisierungsbaukasten MOVI-C® – begegnen Sie der einzigartigen Beratungs- und Servicekultur eines globalen Technik- und Branchenexperten.



www.sew-eurodrive.de/movitrac-advanced





Bild: PTS/ stock.adobe

Standards im Praxistest

Individuell angepasste Industrie 4.0-Lösungen – auch in konservativen Branchen ist dies umsetzbar. Ifak und PTS belegen dies mit einem Beispiel in der Papierindustrie.

Die Herstellung von Papier ist sehr kapitalintensiv. So belaufen sich die Kosten einer neuen Papiermaschine schnell auf 500 Mio. Euro. Neuinvestitionen sind in Europa aufgrund der wirtschaftlichen Lage im Papiersektor selten und der globale Markt unterliegt einem stetigen Preisdruck.

Damit steht die Branche vor der Herausforderung, dass eine Vielzahl von Bestandsmaschinen in das digitale Zeitalter transformiert werden müssen. Gleichzeitig ist der Prozess der Papierherstellung sehr komplex, sodass sich prozesstechnische Änderungen nur sehr vorsichtig vornehmen lassen, um einen gut laufenden Prozess nicht zu destabilisieren. Dies sind Gründe, warum die Branche in Bezug auf Veränderungen als sehr konservativ gilt. Trotzdem bietet die Digitalisierung auch in

der Papierindustrie Potenzial für revolutionäre Fortschritte. Durch die nahezu vollständige Automatisierung ist der Prozess mit einer Vielzahl an Aktoren und Sensoren ausgestattet, die qualitative Daten des Prozesses liefern. Dies bildet eine solide Basis für die Anwendung von neuen Analysemethoden, Industrie 4.0-Konzepten und dem Einsatz von KI-basierten Algorithmen zur selbstoptimierenden Produktion für die Transformation einer Papierfabrik hin zu einer Smart Factory. Die Vielzahl an möglichen Technologien und Standards stellt die Unternehmen oft vor die Herausforderung, die Interoperabilität der Bestandssysteme mit den zukünftigen Technologien bewerten zu müssen.

Die folgenden Ausführungen belegen an Beispielen, wie eine Industrie 4.0-Transform

mation schrittweise mit Bestandsmaschinen gelingen kann.

Schrittweise Anpassung

Bei der schrittweisen Integration von Industrie 4.0 in Maschinen sind die Sensoren, Aktoren und die Steuerung digital zu beschreiben. Diese real existierenden Gegenstände werden in der I4.0-Sicht als Assets bezeichnet. Zu jedem Asset existiert eine Verwaltungsschale, welche für die digitale Beschreibung und Kommunikation mit dem restlichen Industrie 4.0-System verantwortlich ist. Die Architektur der Bestandssysteme gilt es so zu entwickeln, dass über die Verwaltungsschale I4.0-konform kommuniziert werden kann. Die Migrationsschritte hin zu einer Industrie 4.0-Architektur umfasst folgende Schritte:

- Schrittweise Einführung IP-basierter Kommunikationsprotokolle
- Definition und Nutzung standardisierter Informationsmodelle
- Bereitstellung darüberhinausgehender Mehrwerte.

Entsprechend lässt sich die Architektur für die firmenübergreifende Nutzung der Daten wie folgt gestalten.

Generell existieren drei Elemente, welche jeweils durch eine Verwaltungsschale zu vernetzen sind:

1. Das Erfassen und Bereitstellen von Daten (*Bild: a* und *b*) erfolgt durch das Einbinden von Sensoren, von Engineering-Dokumenten, Dokumentationen, Produkt- und Planungsdaten oder einer Softwarequelle, welche Daten bereitstellt. Wichtig dabei ist, dass hier die Daten durch technische Maßnahmen nur in eine Richtung übertragen werden können. Dies schließt die Rückwirkung der Analyse-Plattform auf den Prozess aus. Das Ziel ist hier, Daten über einheitliche Schnittstellen in das System zu bringen. Damit ist nicht nur eine Vereinheitlichung hinsichtlich des Protokolls beziehungsweise der API verbunden,

sondern vielmehr die Definition einer einheitlichen Semantik über die Teilmodelle einer Industrie 4.0-Verwaltungsschale.

2. Die Anwendung von Algorithmen auf Daten (*Bild: c*) nutzt die bereitgestellten Daten als Basis für eine modellbasierte Analyse, für das Lernen von KI-Anwendungen oder zur Bewertung durch eine bereits trainierte KI-Anwendung. Die Semantik der Daten wird über die Teilmodelle der Verwaltungsschale definiert. Dabei gibt es neben Teilmodellen für zum Beispiel Temperatursensoren oder Stellventile auch Teilmodelle zur Realisierung der Interaktion zwischen Verwaltungsschalen. Damit sind verschiedene Arten der Interaktion definiert – vom simplen Abfragen von Werten bis hin zur Umsetzung einer Verhandlung (Smart-Contracts).

Es werden also sowohl herkömmliche Geschäftsmodelle als auch zukünftige IoT-Geschäftsmodelle unterstützt.

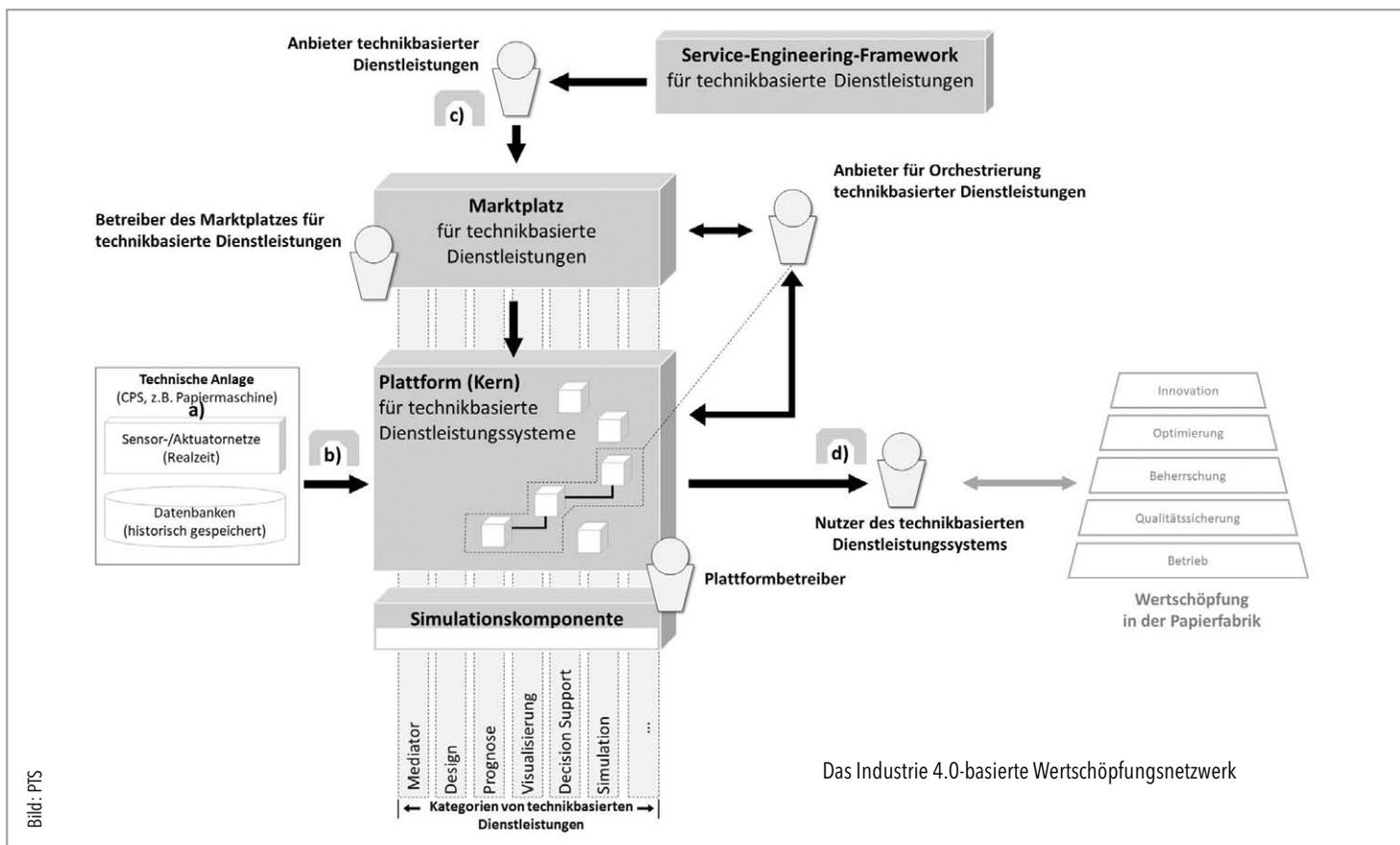
3. Zur Einbindung der Daten (*Bild: d*) welche durch die Analyse gewonnen wurden, gilt es zunächst zu entscheiden, ob aus Sicherheitsgründen nur ein lesender Zugriff auf den Prozess erfolgen soll, oder ob ein schreibender Zugriff erlaubt wird.

Mit einem lesenden Zugriff lassen sich diverse interessante Mehrwerte schaffen: Eine Qualitätskontrolle, eine Optimierung oder vorbereitende Simulationen. Die Umsetzung des schreibenden Zugriffs erlaubt die Realisierung von Regelkreisen; zum Beispiel die Nutzung der Daten als Input für einen modellprädiktiven Regler oder von Online-Optimierung durch ein neuronales Netz.

Die Architektur erlaubt es, die Daten firmenübergreifend im selben Netzwerk zu nutzen. So lässt sich etwa die Analyse-Hardware eines Herstellers in das System einbinden und die Daten für die Analyse-Software eines weiteren Herstellers zur Verfügung stellen. Dabei gilt es, den Datenaustausch möglichst Plug&Play-fähig zu gestalten.

Aufbau der Verwaltungsschale

Zu Beginn lassen sich in der Verwaltungsschale statische Informationen zum Asset, vergleichbar mit einer Bedienungsanleitung oder Typenschild, speichern. Die Lagerung von Produktinformationen in Aktenordnern kann somit ein Relikt der Vergangenheit werden. Ein Speichern und



Betrachten von Produktdatenblättern, CAD-Dateien oder weiteren Dokumenten ist mit geeigneter Software möglich. Die Plattform Industrie 4.0 empfiehlt die kostenfreie Open Source Software AASX-Explorer (Asset Administration Shell) zum Anlegen und Darstellen von Verwaltungsschalen.

Innerhalb eines Forschungsprojektes erfolgte die Ausstattung der Messgeräte der Papiertechnischen Stiftung mit einer solchen Verwaltungsschale, unter Nutzung des AASX-Explorers. Die Daten, die bis dahin als Tabelle in Excel vorlagen, wurden in eine XML-Darstellung transformiert und lassen sich nun über den AASX-Explorer übersichtlich betrachten. Mit der standardisierten XML-Darstellung sind die Informationen nicht mehr nur für den Menschen lesbar, sondern auch maschinenlesbar und zum Weiterverarbeiten geeignet.

Eine Möglichkeit der Verknüpfung der statischen Informationen des Sensors mit dynamischen Informationen – wie kontinuierlich erzeugten Messwerten – bietet OPC UA. Innerhalb des Projektes wurde zusätzlich eine Datenbanklösung entworfen, die Messwerte abspeichert und über eine OPC-UA-Schnittstelle verfügt. Eine solche Verwaltungsschale, welche dynamische Daten mit anderen Systemkomponenten austauschen kann, enthält die folgenden Komponenten A bis D.

A: Der Adapter an das Industrie 4.0-System ist spezifisch für das konkret eingesetzte Kommunikationsprotokoll umzusetzen und bindet die Verwaltungsschale an ein I4.0-Netzwerk an, welches auf dem gleichen Protokoll beruht. Aktuell ist keine spezifische Kommunikationstechnologie für Industrie 4.0 vorgeschrieben. Für die Umsetzung einer Verwaltungsschale empfiehlt es sich, den Adapter von der restlichen Logik der Verwaltungsschale zu separieren, um die weitere Entwicklung flexibel verfolgen zu können.

Sollen Verwaltungsschalen nicht nur ein reiner Datenlieferant sein (passiv), sondern von sich aus weitere Industrie 4.0-Komponenten anfragen (aktiv), müssen sowohl die Client- als auch die Serverrollen beziehungsweise Publisher-/Subscriberrollen implementiert werden.

B: Das Asset-Modell beinhaltet Asset-spezifische Analysefunktionen und Modell-

transformationen wie die Interaktion mit Kommunikationsprotokollen. Die Asset-Modelle stellen den Hauptbestandteil einer Verwaltungsschale dar. Dabei handelt es sich in der Regel um Software, welche die Schnittstelle zum Asset nutzt. Des Weiteren liegen hier zusätzliche Softwarekomponenten wie Datenbanken vor. Es liegt daher nahe, die Umsetzung einer Verwaltungsschale generell als Problem der Abbildung von Softwaremodellen auf die Industrie 4.0-Schnittstellen aufzufassen. Softwaremodelle entstehen durch Bibliotheken zum Zugriff auf die Kommunikationsprotokolle oder Datenstrukturen, welche Engineeringdaten beschreiben.

C: Die Schnittstelle zum Asset: Sie dient zur Kommunikation der Verwaltungsschale mit dem Asset. Je nach Asset kommt hierfür eine Kommunikationstechnologie wie beispielsweise OPC UA oder Profinet zum Einsatz. Wird das Asset durch Daten oder Software wie Simulationsmodelle gebildet, kommt hierfür die entsprechende Schnittstelle zur Anwendung.

D: Die Abbildung des Asset-Modells zum Industrie 4.0-Teilmodell: Diese dient der Anbindung der Asset-spezifischen Modelle an die standardisierten Teilmodelle einer Industrie 4.0-Verwaltungsschale, beispielsweise der Zustandsmaschinen zur Interaktion. Das Asset-Modell beschreibt den Zugriff auf das Asset und ist dabei eine Software-Komponente. In vielen Fällen lassen sich diese Software-Komponenten teilautomatisiert untersuchen (durch Reflexion oder eine Compiler-gestützte Analyse). Auf diesem Weg lässt sich die Abbildung der Asset-Modelle auf standardisierte Industrie 4.0-Modelle teilautomatisiert vornehmen. Die standardkonformen Teilmodelle lassen sich leicht aus der offiziellen Swagger-Schnittstellenbeschreibung für die gewünschte Plattform generieren. Mit der von den Autoren entwickelten Software können diese Teilmodelle anschließend automatisch an das Industrie 4.0-System über OPC UA, REST Services oder MQTT angebunden werden.

Die Datensicherheit

Die Verwaltungsschale muss den Anforderungen an die Datensicherheit der Industrie entsprechen. Eine Möglichkeit, dies umzusetzen, ist die Verwendung der Verwaltungsschale als Datei. Mit der Produktübergabe wird diese Datei mit übergeben

und liegt auf den Servern des Kunden. Dies hat den Vorteil, dass keine permanente Datenverbindung zwischen den Unternehmen existieren muss, welche eine potenzielle Gefahr darstellen kann. Der Nachteil besteht darin, dass die Verwaltungsschale auf die Informationen begrenzt ist, welche bei Produktverkauf übergeben wurden. Eine kontinuierliche Aktualisierung des Herstellers ist nicht möglich. Außerdem können keine Fehler entdeckt werden, die dem Kunden beim Umgang mit der Verwaltungsschale unterlaufen.

Die M2M-Connectivity

Weiterhin wurde im Projekt eine Möglichkeit untersucht, M2M-Connectivity über eine Cloud zu entwickeln. Am Use Case des Sensors bedeutet dies, dass beim Kunden eine Messung stattfindet, die Daten in eine Datenbank auf der Cloud eingespeist werden und von dort aus in die Systeme des Kunden eingelesen werden können. Für die Integration dieser Industrie 4.0-Anwendungen in das IT-Security-Konzept erfolgte eine Erweiterung der Firewall-Lösung um eine Demilitarisierte Zone (DMZ). In diesem Bereich können die Anwendungen laufen, welche über eine permanente externe Datenverbindung verfügen, ohne dass sie eine Gefahr für den Rest des Unternehmens darstellen.

Die Entwicklungen erfolgten im Rahmen des BMWi-geförderten Projekts INVITE4.0.

hap



RICHARD FANKHÄNEL
ist Projektmitarbeiter, Papiertechnische Stiftung, Heidenau.



BJÖRN ZIMMERMANN
ist Projektleiter, Papiertechnische Stiftung, Heidenau.



HOLGER ZIPPER
ist wissenschaftlicher Mitarbeiter im ifak e.V. Magdeburg.

Bild: PTS

Bild: PTS

Bild: ifak

Low-Power-Prozessoren ans Ethernet

Single Pair Ethernet hat in der Fabrik- und Prozessautomation eine große Zukunft vor sich. Aber was ist bei der Anbindungs-Entwicklung gerade der stromsparenden Feld- oder Edge-Geräten zu beachten?

Die Anwendungsfälle für Single-Pair-Ethernet 10BASE-T1L, darunter Ethernet-APL, werden im Prozess-, Fabrik- und Gebäudeautomatisierungsbereich immer zahlreicher, denn es müssen immer mehr Geräte an Ethernet-Netzwerke angebunden werden. Wenn mehr Geräte eine Netzwerk-Anbindung erhalten, lassen sich den übergeordneten Management-Systemen umfangreichere Datenbestände zur Verfügung stellen, was einerseits erhebliche Produktivitätssteigerungen gestattet und andererseits die Betriebskosten und den Energieverbrauch reduziert.

Für den Feld- beziehungsweise Edge-Bereich birgt Ethernet die Perspektive, dass sämtliche Sensoren und Aktoren an ein konvergiertes IT/OT-Netzwerk (Informationstechnologie und operative Technologie) angebunden werden können. Zur Umsetzung dieser Vision gilt es allerdings einige systemtechnische Herausforderungen zu überwinden, da einige der besagten Sensoren hinsichtlich der verfügbaren Leistung und ihres Platzbedarfs eingeschränkt sind. Für Sensor- und Aktor-Anwendungen gibt es ein wachsendes Angebot an Low-Power-

und Ultra-Low-Power-Mikrocontrollern mit großer interner Speicherkapazität. Die Mehrzahl dieser Prozessoren hat jedoch die Gemeinsamkeit, dass sie wegen des fehlenden integrierten Ethernet-MAC kein MII-, RMII- oder RGMII Media Independent (Ethernet) Interface unterstützen. Ein traditioneller PHY lässt sich an diese Prozessoren somit nicht anschließen.

Was spricht für einen 10BASE-T1L MAC-PHY?

Um immer mehr Low-Power-Bausteine mit einer für große Distanzen geeigneten Ethernet-Verbindung auszustatten, ist ein 10BASE-T1L MAC-PHY nötig. Dieser Baustein stellt die Ethernet-Anbindung des Prozessors per SPI her. Letzterer wird somit entlastet, weil kein integrierter MAC notwendig ist, denn die MAC-Funktionalität ist jetzt direkt in den 10BASE-T1L PHY integriert. Ein 10BASE-T1L MAC-PHY beschert Geräte-Entwicklern also mehr Flexibilität und Auswahl, da eine große Zahl von Ultra-Low-Power-Prozessoren in Frage kommt. Durch eine optimale Partitionierung der Applikation erlaubt ein 10BASE-T1L MAC-PHY die Realisierung

stromsparender Feldgeräte für eigensichere Zone-0-Anwendungen. Hier kommt das zum Zug, was in der Prozessindustrie als Ethernet-APL bezeichnet wird. In intelligenten Gebäude-Anwendungen erlaubt ein MAC-PHY die Anbindung einer größeren Zahl stromsparender Geräte an ein Ethernet-Netzwerk.

Erweiterte Paketfilterung

Die Integration der MAC-Funktionalität in einen 10BASE-T1L PHY stellt neue Features zur Verfügung, mit denen sich der Ethernet-Traffic im Netzwerk optimieren lässt. Ein 10BASE-T1L MAC-PHY mit erweiterter Paketfilterung reduziert ganz erheblich den durch die Abwicklung des Broadcast- und Multicast-Traffics entstehenden Aufwand. Entscheidend ist das Filtern nach der Ziel-MAC-Adresse. Anstatt nach nur einer MAC-Adresse zu filtern, unterstützt ein MAC-PHY das Filtern unter Verwendung von bis zu 16 Unicast- oder Multicast-MAC-Adressen. Des Weiteren ist eine Adressmaskierung für zwei MAC-Adressen möglich. Das Filtern nach der Geräte-Adresse sowie nach allgemein unterstützten

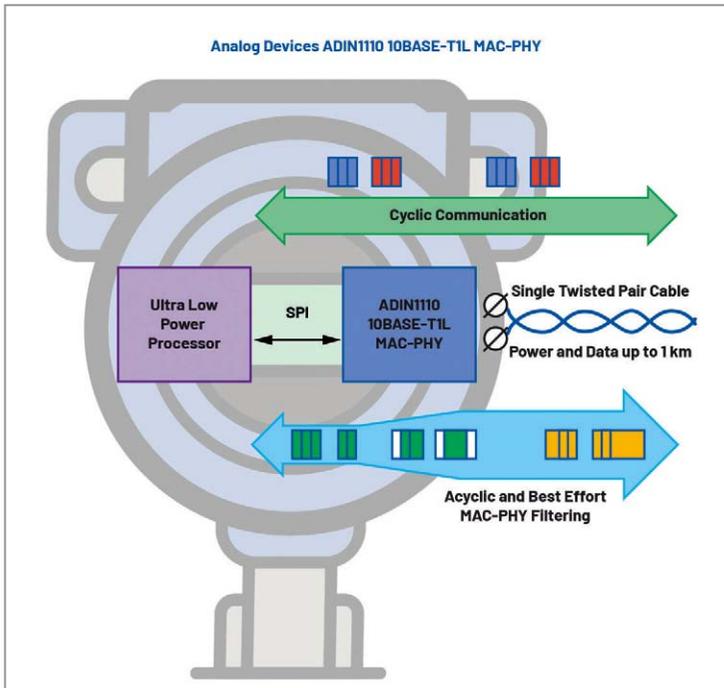


Bild 1. Ein 10BASE-T1L MAC-PHY bewirkt eine entscheidende Verringerung des Stromverbrauchs und der Komplexität von Geräten mit erweiterter Paketfilterung.

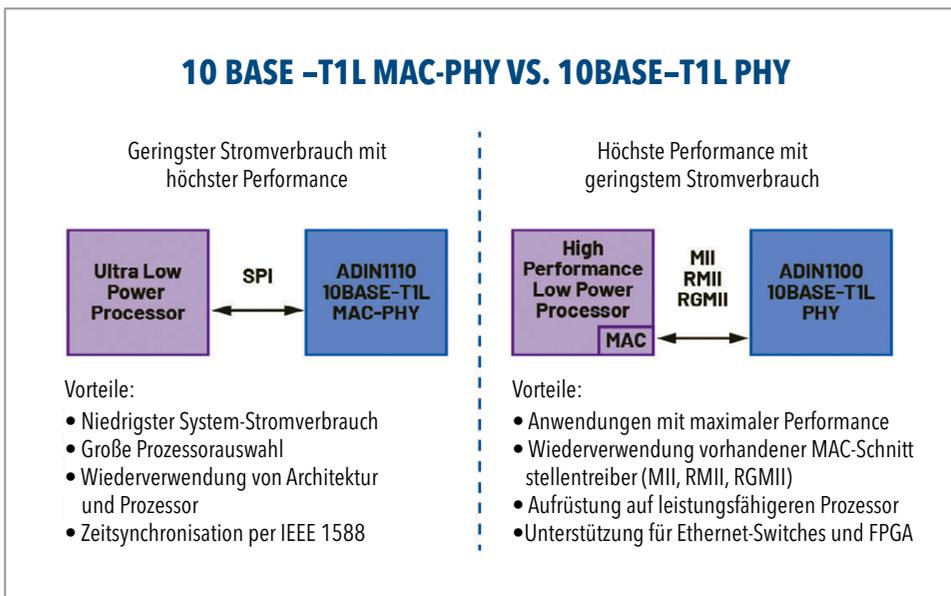


Bild 2. Vergleich der Vorteile eines MAC-PHY und eines PHY für die 10BASE-T1L-Anbindung.

Multicast-Adressen wie etwa LLDP (Link Layer Discovery Protocol) ergibt ein hohes Maß an Freiheit. Durch die Unterstützung eines zusätzlichen Pfads für höhere Prioritäten besteht die Möglichkeit, einige Nachrichten zu priorisieren, um auf diese Weise eine Verbesserung der Latenz und Betriebssicherheit zu erzielen. Die Priorität eines Frames lässt sich anhand der MAC-Filtertabelle identifizieren. Zum Beispiel können Broadcast-Nachrichten einer Warteschlange niedriger Priorität zugeführt werden, während Unicast-Nachrichten an die mit

höherer Priorität gehen. Auf diese Weise vermeidet man eine Überlastung des Empfängers durch einen Broadcast Storm oder eine kurzzeitige Traffic-Spitze. Diese Filterfunktionen des MAC-PHY ermöglichen die Realisierung von Geräten, die hinsichtlich der Netzwerklast robust sind. Der MAC sammelt außerdem Frame-Statistiken, um bei der Überwachung des Netzwerkverkehrs und der Verbindungsqualität zu helfen (siehe Bild 1).

Der MAC im MAC-PHY unterstützt außerdem IEEE 1588 und damit auch die

Zeitsynchronisation gemäß 802.1AS, wie es in der Prozessautomatisierung erforderlich ist. Vom MAC-PHY unterstützt werden auch ein synchronisierter Zähler, das Time-stamping empfangener Nachrichten und die Timestamp-Erfassung für zu sendende Nachrichten. Dies verringert die Komplexität des Software-Designs entscheidend, da über den MAC-PHY hinaus kein Hardware-Support mehr erforderlich ist, um die Zeitsynchronisation zu implementieren. Der MAC kann ein auf den synchronisierten Zähler abgestimmtes Ausgangssignal generieren, was zur Synchronisation externer Abläufe auf der Anwendungs-Ebene genutzt werden kann. Das SPI-Interface unterstützt das Open Alliance 10BASE-T1x MAC-PHY Serial Interface. Das Open Alliance SPI ist ein neues, höchst effektives SPI-Protokoll, das eigens für die Verwendung mit einem MAC-PHY entwickelt wurde.

10BASE-T1L MAC-PHY oder 10BASE-T1L PHY?

Ein 10BASE-T1L PHY und ein 10BASE-T1L MAC-PHY bieten in unterschiedlichen Anwendungsfällen signifikante Vorzüge. Wenn es auf den Stromverbrauch ankommt, ermöglicht ein 10BASE-T1L MAC-PHY die Senkung der System-Leistungsaufnahme, da er eine flexiblere Auswahl des Host-Prozessors erlaubt, denn damit kommen auch Ultra-Low-Power-Prozessoren ohne integrierten MAC in Betracht. Soll die Ethernet-Anbindung an einem bestehenden Gerät nachgerüstet werden, bietet ein 10BASE-T1L MAC-PHY die Möglichkeit zur Wiederverwendung des vorhandenen Prozessors, indem die Ethernet-Anbindung über den SPI-Port realisiert wird. Der Umstieg auf einen leistungstärkeren Prozessor mit integriertem MAC ist dann nicht notwendig.

In Anwendungen mit hohen Performance-Ansprüchen ist das Feld- oder Edge-Gerät möglicherweise bereits mit einem sehr leistungsfähigen Prozessor mit eingebautem MAC bestückt. Hier ist mit einem 10BASE-T1L PHY mit MII-, RMII- und RGMII-MAC-Schnittstellen die schnelle Entwicklung einer 10BASE-T1L-Schnittstelle möglich. Dies geschieht durch Wiederverwendung der vorhandenen MAC-Schnittstellentreiber zum Nachrüsten der Ethernet-Konnektivität (Bild 2).

Für die Geräte-Entwickler bedeutet die Verfügbarkeit von 10BASE-T1L PHYs und 10BASE-T1L MAC-PHYs eine höhere Flexibilität, um die Anforderungen künftiger

Fertigungsanlagen mit Ethernet-Konnektivität zu erfüllen. Geräte mit niedrigstem Stromverbrauch und solche mit hoher Performance lassen sich in ein und demselben Ethernet-Netzwerk einrichten – unter Einhaltung der Leistungs-Obergrenzen für Anwendungen in Gefahrenbereichen. 10BASE-T1L Power Switches und 10BASE-T1L Field Switches verlangen nach der Verwendung robuster, stromsparender 10BASE-T1L PHYs um in Verbindung mit industriellen Ethernet Switches, eine Netzwerk-Topologie nach dem Trunk-and-Spur-Prinzip zu realisieren, das sowohl die Versorgungsspannung als auch die Daten über ein einziges Twisted-Pair-Kabel überträgt – auch hinein in Gefahrenbereiche.

Für die Anbindung von Feldgeräten werden sowohl 10BASE-T1L PHYs als auch 10BASE-T1L MAC-PHYs benötigt, damit ein breites Spektrum von Feldgeräten mit einer Ethernet-Anbindung ausgestattet werden kann. Feldgeräte mit höherem Stromverbrauch, wie etwa Durchflussmesser, dürften bereits mit einem Hochleistungs-Prozessor mit integriertem MAC sowie einem 10BASE-T1L PHY ausgestattet sein. Feldgeräte mit niedrigerem Stromverbrauch, zu denen beispielsweise Temperatursensoren gehören, sind dagegen mit einem Ultra-Low-Power-Prozessor ohne integrierten MAC bestückt und greifen für die Ethernet-Konnektivität daher auf einen 10BASE-T1L MAC-PHY zurück, der via SPI mit dem Prozessor verbunden wird (Bild 3).

Vergleich der wichtigsten Merkmale

Der ADIN1110, ein 10BASE-T1L MAC-PHY von ADI, ermöglicht die stromsparende Ethernet-Anbindung über ein SPI-

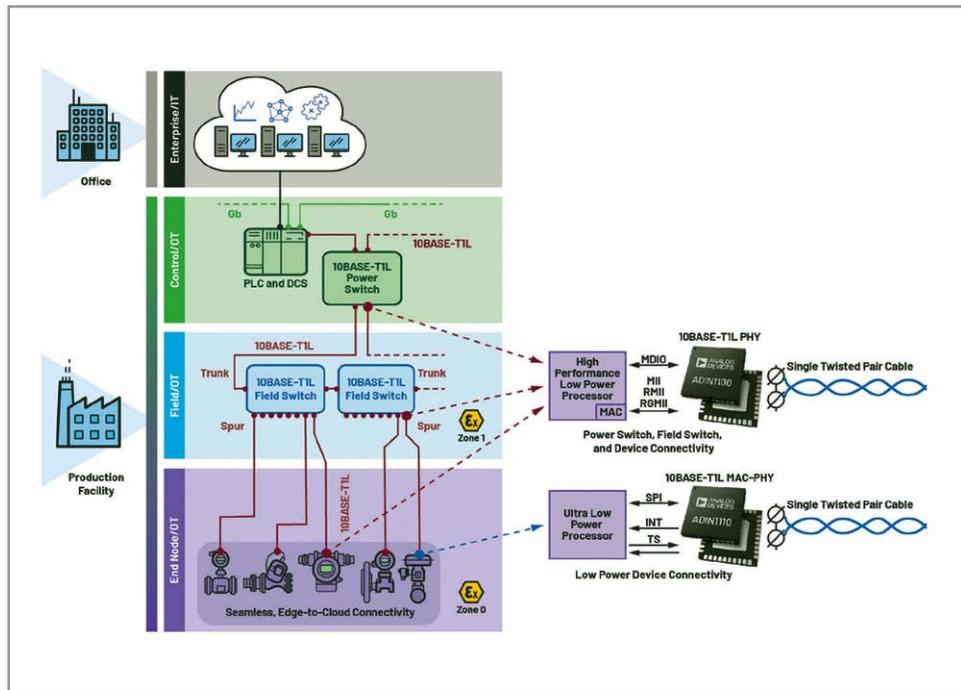


Bild 3. Netzwerk-Topologie nach dem Trunk-and-Spur-Prinzip für die Prozessautomatisierung, bestückt mit 10BASE-T1L MAC-PHY und 10BASE-T1L PHY.

Interface zum Host-Prozessor bei einer Leistungsaufnahme von nur 42 mW. Der Baustein unterstützt das Open Alliance 10BASE-T1x MAC-PHY Serial Interface für die Vollduplex-SPI-Kommunikation bei einer Taktfrequenz von 25 MHz.

Der ADIN1100, ein 10BASE-T1L PHY von ADI, dient dagegen der stromsparenden Ethernet-Anbindung über MII-, RMII- und RGMII-MAC-Interfaces an einen Hostprozessor mit nur 39 mW Leistungsaufnahme. Die unten stehende Tabelle enthält eine Gegenüberstellung des 10BASE-T1L PHY vom Typ ADIN1100 mit dem 10BASE-T1L MAC-PHY des Typs

ADIN1110. Beide Produkte basieren auf der zentralen Eignung von 10BASE-T1L für die vollduplex-fähige, gleichspannungsfreie Punkt-zu-Punkt-Kommunikation mit PAM-3-Modulation bei einer Symbolrate von 7,5 MBaud mit 4B3T-Codierung.

10BASE-T1L unterstützt dabei zwei Amplituden-Modi: 2,4 V_{ss} bei Kabellängen bis zu 1000m und 1,0 V_{ss} für kürzere Entfernungen. Mit dem 1.0 V_{ss}-Modus kann diese neue Physical Layer Technologie auch für Systeme in explosionsgefährdeten Bereichen eingesetzt werden, da damit die strengen Anforderungen an die Leistungsbegrenzung erfüllt werden können. hap

	ADIN1100 10BASE-T1L PHY	ADIN1110 10BASE-T1L MAC-PHY
Interface	MII, RMII, RGMII	SPI
Integrierter MAC	nein	ja
Unterstützung für eigensichere Systeme	ja	ja
Leistungsaufnahme	39 mW	42 mW
Auto-Negotiation-Fähigkeit	ja	ja
On-Chip FIFO	nein	20 kB in Empfangs- und 8 kB in Senderichtung
MAC-Filter (16 Einträge)	nein	ja
Traffic-Priorisierung	nein	ja
Unterstützung für Timestamp gemäß IEEE 1588	nein	ja
Temperaturbereich	-40 °C bis +105 °C	-40 °C bis +105 °C
Gehäuse	LFCSFP-40pin	LFCSFP-40pin

Der Vergleich zwischen PHY ADIN1100 und MAC-PHY ADIN1110.



MAURICE O'BRIEN

ist bei Analog Devices als Strategic Marketing Manager für industrielle Konnektivität tätig.



VOLKER E. GOLLER,

arbeitet als Systems Applications Engineer bei Analog Devices.

Carlo Gavazzi GmbH



Das NRG-System



- Bis zu 32 digitale Halbleiterrelais und -schütze an einem Steuergerät/Gateway
- Flexibel durch kompakten modularen Aufbau
- System mit Diagnosefunktion in Echtzeit
- Direkter Datenzugriff durch den Remote-Kundensupport
- Vorausschauende Unstandhaltung durch Früherkennung von Lastfehlern
- Echtzeitüberwachung des Energieverbrauchs



Pfnorstrasse • D-64293 Darmstadt
Tel.: +49 6151 8100-0
info@gavazzi.de
www.gavazzi.de



HMS Industrial Networks GmbH



Fernwartungslösungen
für die Industrie

Maschinendaten.
Überall. Jederzeit.

- Maschinendaten verschiedener Standorte sammeln
- Einfache Inbetriebnahme auch bei komplexen IT-Umgebungen
- Historische Daten für Analyse-Anwendungen
- Anzeigen & Überwachen von Maschinendaten in Echtzeit (Alarmer, HMI, etc.)
- Einfache Integration von Maschinendaten in führende IoT-Plattformen
- Profitieren Sie von einer erstklassigen Fernzugriffslösung

www.ewon.biz/de

Emmy-Noether-Str. 17 • D-76131 Karlsruhe
Tel.: +49 721 989777-000
info@hms-networks.de
www.hms-networks.de



Indu-Sol GmbH



Netzwerk-Monitoring
ohne zusätzliche Hardware

DER FITNESSTRACKER FÜR OT-NETZWERKE

- ✓ Zentrale Überwachung von ethernetbasierten Netzwerken
- ✓ Praxisorientierte Störquellen-Früherkennung
- ✓ Automatische Benachrichtigung bei Auffälligkeiten
- ✓ Visualisierung der Zustandsdaten Ihres Netzwerks



Blumenstraße 3 • D-04626 Schmölln
Tel.: +49 (0)34491 580-0
Fax: +49 (0) 34491 580-499
info@indu-sol.com • www.indu-sol.com

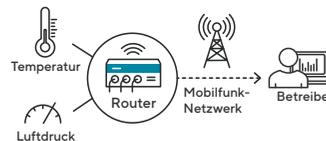


NetModule GmbH



NetModule verbindet!

Zustandsüberwachung und Fernwartung:
Sichere Vernetzung mit unseren Routern.



Tel.: +49 6196 779979-0
Fax: +49 6196 779979-99
info@netmodule.com
www.netmodule.com

NET MODULE
Robust Communication

Displays

PMOLEDs in vielen Varianten

Data Modul hat mit der Passivmatrix-OLED-Produktpalette von WiseChip kompakte PMOLEDs für den industriellen Anwendungsbereich im Portfolio. Zu den verfügbaren Ausführungen zählen unter anderem flexible PMOLEDs, die mit 0,3 mm extrem dünn sind und einen Biegeradius von bis zu 40 mm, einen uneingeschränkten Blickwinkel und eine schnelle Reaktionszeit von maximal 10 µs bieten. Ebenso im Angebot sind transparente PMOLEDs, die dank der Transmission von 50 % bei einer Wellenlänge von 550 nm trotz Durchsichtigkeit ein klares Bild bieten. Als Ergänzung sind Hyperfluoreszenz- und InCell-Touch-PMOLEDs hinzugekommen. Während sich die Hyperfluoreszenz-Displays durch eine 2,5-fach höhere Helligkeit auszeichnen, werden monochrome PMOLEDs in den Größen 0,96 Zoll und 1,71 Zoll auch mit integrierter InCell-Touch-Lösung angeboten.



www.data-modul.com

HMI

Produktfamilie erweitert

Garz & Fricke hat mit dem *Tanaro 7.0 BX PCT* die Produktfamilie an Human Machine Interfaces (HMIs) weiterentwickelt. Das HMI basiert auf dem ‚Tanaro‘-Board des Anbieters und ist mit der aktuellsten Prozessorgeneration (NXP i.MX 8M Mini ARM Cortex) ausgestattet. Die vollständig integrierte HMI-Lösung im Panel-Mount-Format lässt sich sowohl zur Interaktion des Nutzers in der eigentlichen Endanwendung als auch zur zentralen Steuerung nutzen. Dabei ist das 7 Zoll große Panel Mount HMI im robusten Design mit dem jüngstem SBC-Modell der Garz & Fricke Group bestückt. Das Display verfügt über eine hohe Auflösung mit 1024x600 Pixel und einen kapazitiven Touchscreen zur erweiterten Nutzerinteraktion. An Verbindungsmöglichkeiten stehen RS232, RS485, CAN, mehrere USBs sowie 1GB Ethernet und integriertes Wifi/BT zur Verfügung. Zudem bietet die integrierte Kameraschnittstelle MIPI-CSI die Möglichkeit, Kameralösungen zu integrieren. Konzipiert ist das General-Purpose-HMI für den Einsatz in rauen Umgebungen mit besonders hohen Beanspruchungen.



www.garz-fricke.com

Industrie-Tablets

Mit ‚Fully-Rugged‘-Schutzeigenschaften

Werock Technologies bringt mit der Serie *Rocktab Ultra U200* zwei industrielle Tablets mit sonnenlichtlesbaren Displays und leistungsstarken Prozessor-Optionen auf den Markt. Die robusten Tablets sind speziell auf den Einsatz unter härtesten Bedingungen ausgerichtet und bieten ‚Fully-Rugged‘-Schutzeigenschaften. Sie sind mit Intel-Prozessoren und bis zu 16 Gbyte RAM ausgestattet. Gute Bedienbarkeit bieten die im Freien lesbaren, mit 11,6 Zoll beziehungsweise 13,3 Zoll großen Displays mit einer Helligkeit von bis zu 1000 cd/m² und einem Blickwinkel von 89° aus allen

Seiten. Die Bedienung des robusten Touchscreens erfolgt mit Fingern, Arbeitshandschuhen oder dem mitgelieferten Touchstift. Auch eine Bedienung bei Regen oder verdrecktem Touchscreen ist möglich. Eine ‚Anti-Glare‘-Oberfläche sorgt für verminderte Reflektionen bei der Arbeit im Freien.



Der eingebaute 2x2 MU-MIMO WLAN-Adapter unterstützt den 802.11ax-Standard, ist Wi-Fi 6 zertifiziert und ermöglicht Datenraten bis 2,4 Gbps. Dank der integrierten ‚Intel My Wifi‘-Technologie agieren die Tablets bei Bedarf ebenfalls als eigener Accesspoint und stellen das WLAN-Netz für umliegende Maschinen bereit.

www.werocktools.com

HMI Komplettlösungen

- Spezialist für Eingabesysteme und kundenspezifische Lösungen
- kompetenter Partner für Komplettsysteme
- HMI Lösungen mit Touchscreens, Folientastaturen, kapazitiven Schaltelementen, Displays, Gehäusesystemen, Elektronik und Komponenten
- Service über den gesamten Produktlebenszyklus
- weltweite Präsenz mit Kompetenzzentren
- nach Medizinnorm ISO 13485 zertifiziert

info.de@schurter.com | +49 7642 6820
schurter.de/inputsystems

ELECTRONIC COMPONENTS

BRESSNER Technology GmbH

TOUCAN PRO

Lüfterloser 8th Gen. Panel PC mit
brilliantem Multi-Touch Display

21.5" (54,6cm)



- ◆ Intel® Core™ Whiskey Lake-U CPU
- ◆ Ultra-flaches 48mm Gehäuse
- ◆ IP65 Front mit Multi-Touch Display
- ◆ M.2 2280 SSD PCIe x4 Erweiterung

Industriestr. 51 • D-82194 Gröbenzell
Tel.: 08142/47284-0
Fax: 08142/47284-77
info@bressner.de



Christ Electronic Systems GmbH



Next Level HMI - Experience the Future

Brandneue Touch Panel Generation



Touch Panel mit besonders hoher Modularität und Skalierbarkeit. Konfigurieren Sie sich Ihr Standardpanel, ganz nach Ihren Anforderungen.

Highlights der neuen Touch Panel Generation:

- Displaydiagonalen von 7-24" (Full HD ab 13,3")
- Einsatz des neuesten Touch Controllers
- Performanceklassen von Monitor bis Panel PC
- Schnittstellenerweiterungen & Speicherupgrades
- Kompakte Technik im Rückdeckel
- Anbindung an unterschiedliche Feldbussysteme
- Leichte Reinigung dank abgeschrägten Kanten
- Image- und BIOS Anpassung (Windows & Linux)
- Schutz bis IP65

Verschiedene CPU Varianten:

- Intel® Celeron™ N3350 1.1 GHz
- Intel® Celeron™ 3965U 2.2 GHz
- Intel® Core™ i3-7100U 2.4 GHz
- Intel® Core™ i5-7300U 2.6 GHz
- Intel® Core™ i7-7600U 2.8 GHz

Dank der Trennung von **Front- und Rückeinheit**, kann das Display im Servicefall schnell ausgetauscht werden, ohne aufwendige Datenspeicherung.

Alle weiteren Informationen finden Sie hier:
www.christ-es.com/de/produkte/touch-panel

Alpenstrasse 34 • D-87700 Memmingen
Tel.: +49 8331-8371-0
Fax.: +49 8331-8371-99
info@christ-es.de • www.christ-es.com

Kontron

HMI SERIE FlatClient/FlatView

Widescreen- oder Standardformat:
Vielseitig und Industrietauglich



7.0" - 23.8"

- ▶ Displaygrößen von 7.0" bis 23.8" im Wide- und Standardformat
- ▶ Front: PCAP Touch, resistiver Touch oder Schutzglas
- ▶ Auflösung bis Ultra-HD
- ▶ Industrietauglich – robust, zuverlässig und wartungsfrei
- ▶ Varianten mit Edelstahlfront oder Schutzart IP 69K

Gutenbergstraße 2
D-85737 Ismaning
Tel.: +49 821 4086-0
info@kontron.com • www.kontron.com



spstiger UG (haftungsbeschränkt)



Die neue **Kinco IoT HMI-Serie** - jetzt auf **spstiger.de**
So kommen eure Anlagen und Maschinen günstig in die Cloud. Kommunikationstreiber zu über 100 SPS, Fernwartung und Fernsteuerung, HMI- und SPS-Fernupdate, MQTT und OPC UA.



www.spstiger.de
E-Mail: anfrage@spstiger.de
spstiger UG (haftungsbeschränkt) - Hans-Stoll-Str. 36 - 21035 Hamburg

Steuerungen

Bedienkomfort verbessert

Mit der *EDD*-Einheit hat NSK eine neue Steuerung für die Megatorque-Direktantriebe der PS/PN-Serie entwickelt. Zu ihren Merkmalen gehören ein verbesserter Bedienkomfort und ein höheres Sicherheitsniveau. Zentrale Elektronik-Komponenten wurden ebenfalls erneuert. Die Steuerung ist 1:1 kompatibel zum Vorgängermodell. Ein neues Steckerdesign ermöglicht eine verwechslungssichere Anschaltung der Steuerung. Zudem verhindert ein Verriegelungsmechanismus ein unbeabsichtigtes Abziehen der Verbindungselemente. Eine 100- bis 240-V(AC)-Einheit kommt als Netzteil für die Stromversorgung zum Einsatz. Standardmäßig verfügt die *EDD*-Antriebseinheit über einen Analogeingang zur Steuerung von Drehzahl und Drehmoment. Dabei steigt die maximale Eingangsfrequenz der Positionsabfrage von 1 MHz auf 2 MHz, was ein exakteres Positionieren des Direktantriebs in Hochgeschwindigkeits-Anwendungen ermöglicht. Neu ist daneben ein USB-Anschluss, über den die Steuerung an einen Computer angeschlossen und mit der ‚*EDD* Megaterm‘-Software parametrierbar werden kann.



www.nskeurope.de

Steuerungen

CNC-Daten in Industrial Edge-Anwendungen integriert

Softing erweitert die auf Docker-Technologie basierende ‚dataFeed edgeConnector‘-Produktfamilie: Der Container *edgeConnector 840D* unterstützt den einfachen Zugriff auf Daten aus ‚Sinumerik 840D‘-Steuerungen und stellt diese über OPC UA und MQTT auf Edge-Geräten oder virtuellen Umgebungen bereit. Damit wird eine flexible Einbindung lokaler OPC UA Clients und MQTT Broker in eine Cloud-Umgebung und das industrielle IoT möglich. Laut Anbieter ist das neue Softwaremodul die weltweit erste Container-Anwendung für den Zugriff auf ‚Sinumerik 840D Solution Line‘- und ‚Power Line‘-Steuerungen und unterstützt das Auslesen aller Prozessparameter und Antriebsdaten. Dazu ist kein Eingriff in die Konfiguration der Werkzeugmaschine notwendig. ‚dataFeed edgeConnector 840D‘ erlaubt die nahtlose Einbindung von bis zu fünf CNC-Steuerungen in eine Cloud-Umgebung wie Azure IoT Edge oder AWS IoT Greengrass. Damit lassen sich etwa Fertigungsqualität und -toleranzen überprüfen, Maschinendaten erfassen und in übergeordnete Managementsysteme integrieren oder Prozessparameter und andere Leistungsindikatoren visualisieren.

industrial.softing.com

Spectra GmbH & Co. KG



PROZESSE REMOTE STEUERN

SPS mit Virtual-HMI



spectra.de/virtualhmi

Einfacher und plattform-unabhängiger Remote-Zugriff auf Ihre SPS.

Mit einer für alle Betriebssysteme verfügbaren App die Bedienoberfläche ganz einfach auf Ihrem Smartphone, Tablet oder PC anzeigen.

Mahdenstraße 3 • D-72768 Reutlingen
Tel.: +49 (0) 7121-1432-10
Fax: +49 (0) 7121-1432-190
vertrieb@spectra.de • www.spectra.de



Wachendorff Prozesstechnik GmbH & Co.KG



„Future Interface“
Zukunftsweisend und ganzheitlich

CTIT Serie

- Die displaylosen HMI-Server bieten Ihnen über eine APP die Möglichkeit der Visualisierung auf Tablet, Smartphone, PC oder dem Display cMTiV6 in bis zu 10 Instanzen.
- Das All-in-One HMI (Display mit Server) bietet Ihnen die Vorteile eines Displays + die Möglichkeiten des HMI-Servers
- IIoT-Protokolle: OPC UA, MQTT und 300+ Kommunikationstreiber für SPSen, Frequenzumrichter etc.
- Integrierter Fernzugriffsservice **EasyAccess2.0**
- Integrierte Codesys 3.5 SPS

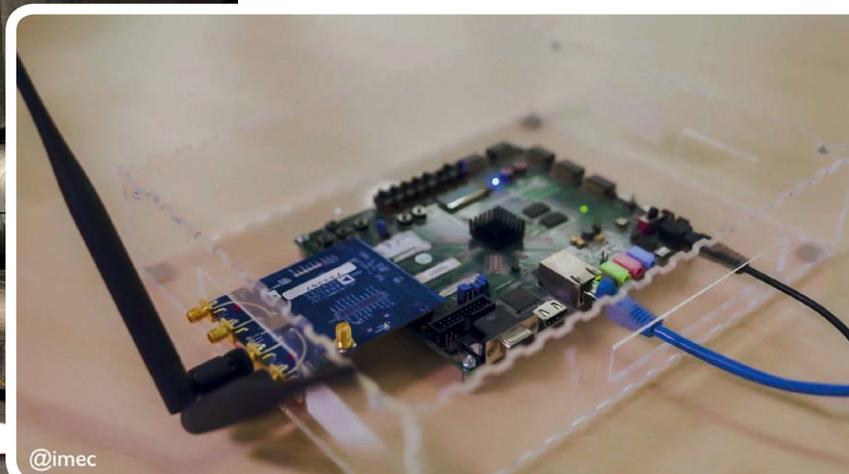
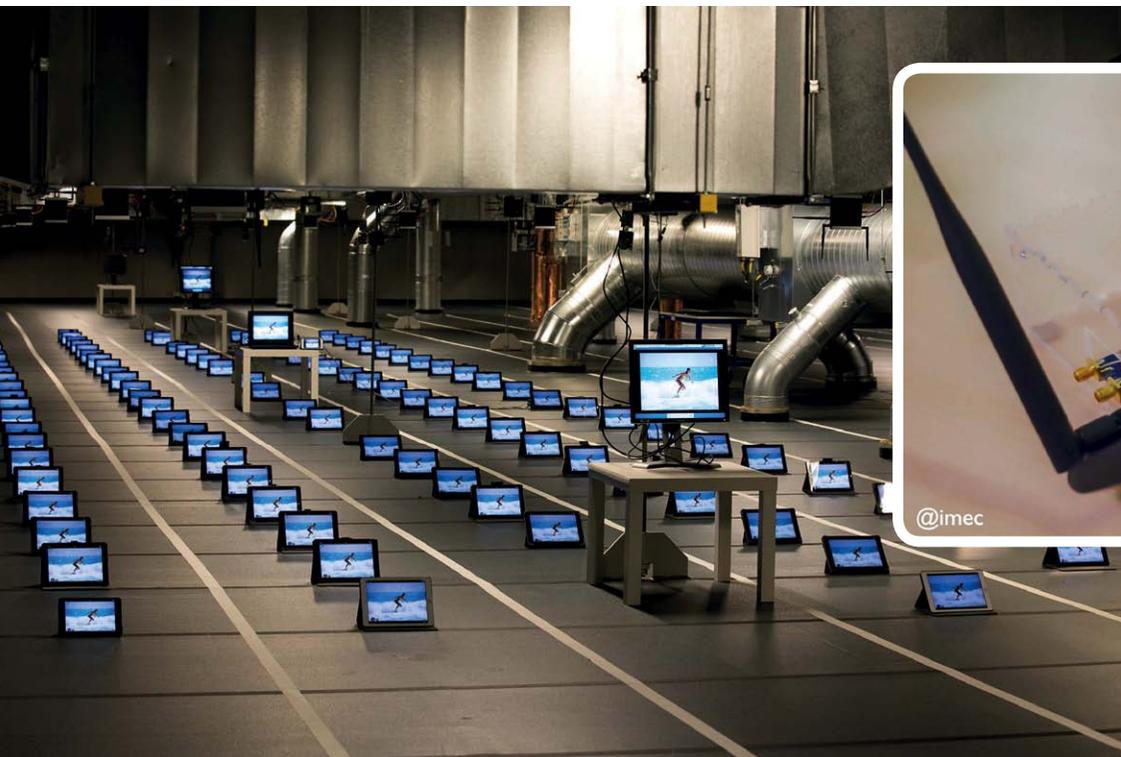
wachendorff-prozesstechnik.de/smart-hmi-iiot



Industriestrasse 7 • 65366 Geisenheim
Tel.: +49 67 22 99 65-544
Fax: +49 67 22 / 99 65-78
beratung@wachendorff.de • www.wachendorff-prozesstechnik.de



Der Open-Source-Chip für drahtloses TSN



Welche Optionen für ein drahtloses TSN gibt es? Ingrid Moerman und Jeroen Hoebeke, Experten der Universitäten Gent und Antwerpen, gehen auf die 5G- und Wi-Fi-Varianten ein und stellen einen Open-Source-Chip für Wireless-TSN vor.

Ingrid Moerman und Jeroen Hoebeke sind Experten für drahtlose Netzwerk-Technologie bei IDLab, einer imec-Forschungsgruppe an der Universität Gent, und der Universität Antwerpen. In diesem Artikel bewerten sie die verschiedenen Technologie-Optionen für die Einführung von drahtlosen TSN-Netzen. Sie gehen auch auf die Bedeutung einer exakten Zeitsynchronisation ein und zoomen dabei auf den kürzlich entwickelten Open-Source-Chip ‚Openwifi‘.

5G versus Wi-Fi

Ingrid Moerman: „Wenn es um die Einführung von drahtlosen TSNs geht, setzt die 5G-Community auf die kürzlich spezifizierte 5G-URLLC-Funktion – die ‚Ultra Reliable Low-Latency Communication‘. Mit der Einführung von 5G URLLC will die Community so nah wie möglich an die Leis-

tungsspezifikationen von Ethernet-basierten TSNs herankommen. Konkrete Ziele sind eine Signalverzögerung von nicht mehr als 1 Millisekunde, eine Zeitsynchronisationsgenauigkeit von nicht mehr als 1 Mikrosekunde und eine Zuverlässigkeit von 99,999 %. Damit hat 5G unbestreitbar einen großen Trumpf in der Hand.“

„Davon abgesehen hat Wi-Fi aber auch seine Vorteile“, so Moerman. „Zum einen lässt sich ein Wi-Fi-Netzwerk viel einfacher, schneller und kostengünstiger installieren als ein zellulares. Und zum anderen ist da der Faktor Kompatibilität: Ethernet – IEEE 802.3 – und Wi-Fi – IEEE 802.11 – gehören zur gleichen Familie von Standards. Das macht Wi-Fi zur naheliegendsten Technologieoption für Unternehmen, die ihr kabelgebundenes Ethernet-Netzwerk in eine drahtlose Alternative umwandeln wollen.“

„Auf der Funkebene sind 5G und Wi-Fi ziemlich ähnlich – sie können ungefähr die gleichen Bitraten verarbeiten. Der große Unterschied ist, dass 5G lizenziertes Spektrum nutzt, das exklusiv einem Telekommunikationsbetreiber zugewiesen ist. Wi-Fi hingegen arbeitet im freien Spektrum – und ist daher an strengere Höflichkeitsregeln gebunden“, sagt sie.

„Wenn ein Wi-Fi-Gerät das freie Spektrum nutzen möchte, muss es zunächst überprüfen, ob keine anderen Geräte dasselbe Funkband nutzen“, fügt Jeroen Hoebeke hinzu. „Das hat zur Folge, dass jedes Mal, wenn ein drahtloses Paket übertragen wird, eine – unvorhersehbare – kürzere oder längere Pause eingelegt werden muss. Und das kann die Latenzzeit erhöhen. Hier hat also 5G – das strenger reguliert ist – einen klaren Vorteil.“

„Aber das könnte sich ändern“, meint er. „Einige Länder erlauben bereits den Kauf von lokalem Spektrum für den Aufbau eines privaten 5G-Netzwerkes. Da das Funkspektrum aber technologieneutral ist, könnte man das gleiche Prinzip anwenden, um ein Wi-Fi-Netz aufzubauen, das nicht mehr an diese strengeren Höflichkeitsregeln gebunden wäre.“

Ingrid Moerman: „Aber letztendlich erwarten wir, dass 5G und Wi-Fi koexistieren werden. Auch wenn es um die Unterstützung zeitkritischer Netzwerke geht. Aufgrund ihrer größeren Reichweite wer-

den Mobilfunktechnologien wie 5G bei TSN-Einsätzen im Freien leicht im Vorteil sein, während Wi-Fi a priori für den Einsatz in Innenräumen geeignet ist. Aber letztlich hängt alles davon ab, dass die Technologien eine noch genauere Zeitsynchronisation unterstützen.“

Der Openwifi-Chip

Jeroen Hoebeke: „Wie bereits erwähnt, muss jedes Wi-Fi-basierte TSN seine Kommunikation in bestimmten Time Slots planen. Daher ist eine genaue Zeitsynchronisation zwischen den verschiedenen angeschlossenen Geräten von entscheidender Bedeutung, da jegliche Ungenauigkeiten bei der Synchronisation durch Puffer – die sogenannte Guard Time – aufgefangen werden müssen. Das wiederum geht auf Kosten der Effizienz. Schließlich will man nützliche Time Slots möglichst dicht beieinander einplanen und die Puffer, in denen keine Kommunikation möglich ist, minimieren.“

„Eine der Herausforderungen von Wi-Fi ist, dass es heute nur eine Zeitsynchronisationsgenauigkeit von einigen zehn Millisekunden zulässt; und das, obwohl ein typisches Wi-Fi-Paket nur etwa hundert Mikrosekunden lang ist. Wenn man zwischen jedem dieser kurzen Pakete einen Puffer von, sagen wir, 30 Millisekunden einfügen muss, ist das alles andere als effizient“, erklärt er.

Ingrid Moerman: „Aber jetzt gibt es Openwifi, unseren maßgeschneiderten Funkchip, mit dem wir die Hardware, in die die Zeitsynchronisationsfunktionen eingebettet sind, vollständig kontrollieren können. Und das ist einzigartig, denn wenn man mit kommerziellen Chips experimentiert, hat man normalerweise keinen Zugang zu dieser Art von Funktionalität.“

„Dank Openwifi konnten wir eine Weltneuheit erreichen – die Verbesserung der Zeitsynchronisationsgenauigkeit von Wi-Fi um den Faktor 10.000 im Vergleich zum Stand der Technik; bis hinunter auf den Wert von 1 µs. Das ist viel besser als die Ambitionen der internationalen Wi-Fi Alliance, die ein Ziel von 5,5 µs gesetzt hatte.“

Open-Source-Software zum Experimentieren

Ingrid Moerman: „Um die Forschung und die kommerzielle Einführung von drahtlosen TSNs zu beschleunigen, haben wir



„Wir haben uns entschieden, einige der grundlegenden Funktionalitäten von Openwifi als Open-Source-Software zur Verfügung zu stellen.“

INGRID MOERMAN

uns entschieden, einige der grundlegenden Funktionalitäten von Openwifi als Open-Source-Software zur Verfügung zu stellen. Das soll Anwendungsentwicklern und Chipherstellern aus der ganzen Welt die Möglichkeit geben, mit Openwifi zu experimentieren.“

Openwifi macht sich bereits gut auf Github – der größten Open-Source-Software-Entwicklungsplattform der Welt – wo es unter den Top 4 der meistgeschätzten FPGA-Beiträge rangiert und bereits über 200-mal heruntergeladen wurde.

Jeroen Hoebeke: „Es ist unsere Absicht, industriellen Partnern eine einzigartige Gelegenheit zu geben, ihre Anwendungen auf Openwifi zu testen und zu evaluieren, ob diese Anwendungen mit den zeitkritischen Wi-Fi-Lösungen von morgen kompatibel sind. Um ein Beispiel zu nennen: Televic, ein belgischer Anbieter von spezialisierten Kommunikationslösungen, hat bereits Interesse an Openwifi gezeigt, um eines seiner Low-Latency-Audio-Streaming-Systeme zu testen.“

„Wir ermöglichen diesen Unternehmen, eine Reihe von Wi-Fi-basierten TSN-Funktionen zu testen – unabhängig von herstel-

Konkurrenz oder Symbiose?

„Wird sich TSN oder 5G durchsetzen?“ ist eine häufig gestellte Frage. In Anbetracht der Art und Weise wie die Technologien präsentiert und vermarktet werden, wundert es kaum, dass viele einen Technologiekampf wittern. In diesen scheint nun auch noch deterministisches Wi-Fi eingestiegen zu sein. Doch gibt es diese Konkurrenz überhaupt?

Sicherlich gibt es insbesondere bei den Drahtlos-Technologien eine gewisse Überschneidung des potenziellen Marktes, dennoch sollten die Technologien aus Anwendersicht als komplementäre Bestandteile des konvergenten Netzwerks der Zukunft gesehen werden. Ein Blick auf die technologischen Details offenbart, dass insbesondere bei TSN nicht ‚entweder oder‘ gilt, sondern TSN stets ein integraler Teil der drahtlosen Echtzeitleösungen ist. Bei Wi-Fi ist dies aufgrund derselben Standard-Familie recht offensichtlich. Bei 5G lohnt sich ein genauer Blick hinter die Kulissen der ‚Ultra Reliable Low-Latency Communication‘, um zu erkennen, dass aus Endpunktsicht ein TSN-Netzwerk vorliegt.

Eine Betrachtung der Technologien für die industrielle Kommunikation hinsichtlich deterministischer Eigenschaften wie Synchronisationsgenauigkeit und Latenz, Umgebungsbedingungen, Komplexität, Flexibilität und Kosten legt nahe, dass wir mittelfristig eine ähnliche Aufteilung der Anwendungen sehen werden, wie es heute im IT-Umfeld der Fall ist.

Entscheidend für den Erfolg aller Technologien ist, dass diese gemeinsam als konvergentes Echtzeitnetz funktionieren und effizient durch den Anwender nutzbar sind. Während viele der offenen Punkte innerhalb der einzelnen Technologien bereits in einem sehr fortschrittlichen Stadium sind, stehen uns die großen Herausforderungen bei der Konvergenz in nächster Zeit bevor. Doch auch hier ist ein gewisser Optimismus angebracht: Selbst wenn auf den großen Bühnen bisher noch nicht allzu viel davon zu sehen ist, so erhält man bei einschlägigen Konferenzen wie der TSN/A Conference am 29. und 30. September 2021 sowie im Gespräch mit involvierten Firmen häufig schon Informationen über sehr vielversprechende Entwicklungen und Ergebnisse.

In dieser Ausgabe legen Ingrid Moerman und Jeroen Hoebeke von IDLab ihre Sicht auf drahtlose TSN-Netzwerke dar und stellen eine offene Chip-Lösung vor, welche der Forschung und Entwicklung gute Dienste erweisen könnte. Wie immer freuen wir uns über Rückmeldungen, Kommentare oder Anregungen zu unserer Serie.

Ihr Florian Frick und Meinrad Happacher

FOLLOW US



shutterstock.com - Alexander Supertlamp

Computer & AUTOMATION
Fachmedium der Automatisierungstechnik

computer-automation.de

TSN -Serie

lerspezifischen Implementierungen und Chipsätzen –, die bis dato ohnehin noch nicht kommerziell verfügbar sind. Das sollte ihnen einen erheblichen Wettbewerbsvorteil verschaffen“, sagt er.

„Darüber hinaus sind wir in der Lage, Wi-Fi-Pakete mit Echtzeit-Netzwerk- und End-to-End-Monitoring-Informationen anzureichern. So können wir – während die Pakete durch das Netzwerk laufen – feststellen, wie die Leistung eines bestimmten Wi-Fi-Netzwerks aussieht. Wir messen damit, was tatsächlich mit einem Wi-Fi-Paket passiert, ohne zusätzlichen Traffic durch das Netzwerk schicken zu müssen. Das macht es viel einfacher, herauszufinden, wo Probleme ihren Ursprung haben. Außerdem könnte man diesen Input für die Neukonfiguration des Netzwerks nutzen oder um zu überprüfen, ob die vereinbarte Dienstgüte eingehalten wird. Das ist eigentlich eine Technik, die schon seit einiger Zeit in Rechenzentren eingesetzt wird, aber wir sind die ersten, die diese Funktion in einem drahtlosen Netzwerk implementieren“, fasst Hoebeke zusammen.

Die ersten Schritte sind getan

Wann also werden Fabriken in der Lage sein, drahtlose TSNs einzusetzen? Da sind sich Ingrid Moerman und Jeroen Hoebeke völlig einig: Soweit ist es noch nicht.

Nähere Informationen

Openwifi ist eines der Ergebnisse aus dem ORCA-Projekt, das vom europäischen Horizon2020-Programm unterstützt wurde. Ein Openwifi-Evaluierungskit mit einem vollständigen TSN-Wi-Fi-Stack und dem notwendigen Support ist derzeit in der Entwicklung. Das Evaluierungskit wird die Schwelle für Unternehmen, die Vorteile von zeitkritischem Wi-Fi zu evaluieren, deutlich senken. Mehr Infos über Ingrid.Moerman@imec.be. Der Openwifi-Linux-Treiber und die Software können heruntergeladen werden von <https://github.com/open-sdr/Openwifi> (Linux mac80211 compatible full-stack IEEE802.11/Wi-Fi FPGA design based on SDR). Mittels der (Remote-)IDLab-Testinfrastruktur von imec, der Universität Antwerpen und der Universität Gent können alle möglichen Funktechnologien auf den Prüfstand gestellt werden – von Wi-Fi über 4G, 5G und sogar zukünftige 6G-Funkarchitekturen auf Basis von verteiltem Massive MIMO.



” Wir ermöglichen Unternehmen, eine Reihe von Wi-Fi-basierten TSN-Funktionen zu testen – unabhängig von herstellereinspezifischen Implementierungen und Chipsätzen. “

JEROEN HOEBEKE

„Wir werden in den nächsten Jahren nach und nach TSN-basierte Funktionen in drahtlosen Netzwerken sehen, aber das wird Schritt für Schritt geschehen. Zuerst müssen die kommerziellen Chips, die diese Funktionen unterstützen, entwickelt werden; erst dann können die Anwendungen folgen. In der Zwischenzeit wird es jedoch interessant sein, zu sehen, wie 5G und Wi-Fi den Bedarf an drahtlosen TSNs weiter angehen werden. Klar ist schon jetzt, dass beide einen klaren Mehrwert in der Unterstützung zeitkritischer Anwendungen sehen“, sagen sie. hap



Wim Van Daele ist im Imec Science Communication Team.

Design neu gedacht

Das Design von Bildeinzug und Bildverarbeitung für Vision-Sensoren ist aufwendig. Gleichzeitig werden Innovationszyklen immer kürzer und Sensoren für immer mehr und immer spezifischere Applikationen benötigt. Die Lösung sind Technologien, mit denen sich Vision-Sensoren schnell, kostengünstig und individuell entwickeln und produzieren lassen.

Vision-Sensoren kommen überall dort zum Einsatz, wo Personen, Gegenstände und Muster identifiziert und unterschieden werden müssen. Häufig lösen sie dabei komplexe Aufgaben und können mehrere Objektmerkmale erfassen – gleichzeitig und in höchster Verarbeitungsgeschwindigkeit. Besonders kosteneffizient sind Lösungen, die dafür keine externen Rechensysteme benötigen, sondern Bildfassung, Bildverarbeitung und Analyse in einem Embedded System kombinieren. Sie werden speziell auf die jeweiligen Aufgaben zugeschnitten und verzichten auf alle nicht notwendigen Komponenten. Dies spart Kosten für die Serienfertigung und sorgt für geringe Stromaufnahme, was wichtig ist

beim Einsatz als Edge-Device oder in mobilen Lösungen.

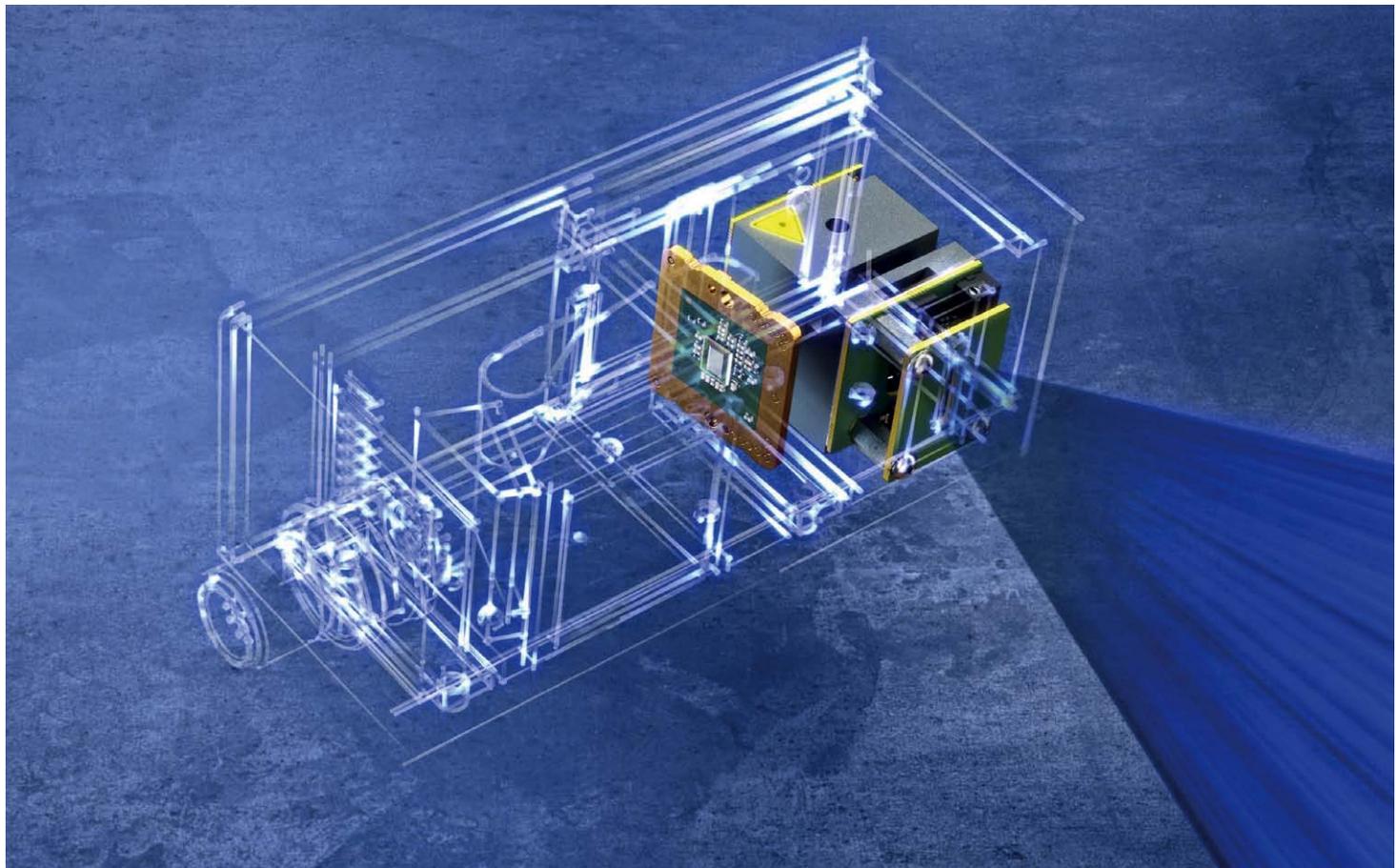
Die Entwicklungs-Historie

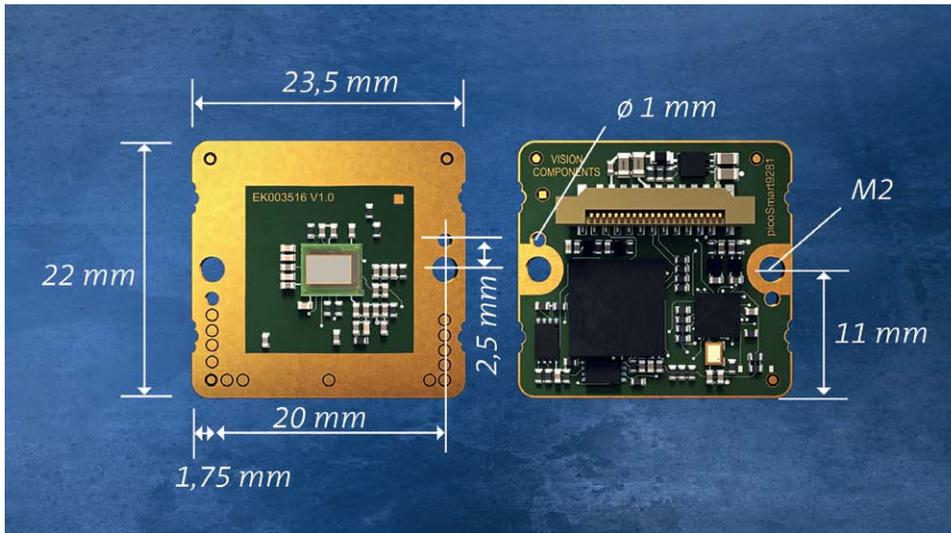
Als Basis für universell einsetzbare Vision-Sensoren hat Vision Components schon 1996 die erste industrietaugliche Smart Kamera (VC11) auf den Markt gebracht. Sie kombinierte erstmals Bildfassung und Verarbeitung der Signaldaten in einem Gerät. Dabei war die Kamera etwa gleich groß wie übliche Industriekameras, die jedoch lediglich Daten erfassen und sie zur Auswertung an ein externes PC-System übertragen.

Die nächste Ausbaustufe dieser Technologie waren echte Vision-Sensoren, die

zusätzlich zur Bilderfassung und -verarbeitung über Optik, Beleuchtung und ein gemäß IP65 geschütztes Industriegehäuse verfügten, wie etwa die ,VC M'-Familie von Vision Components. Hersteller von Vision-Sensoren implementierten ihre Software und konnten so mit kurzer Entwicklungszeit individuelle Produkte mit bewährter Optik und Elektronik in den Markt bringen.

Von dieser Technologie ausgehend haben OEM-Hersteller im Lauf der Zeit eigene Sensoren entwickelt – von der Integration der Elektronik von Vision Components als Grundlagenpaket bis hin zu kompletten Eigenentwicklungen. In den letzten Jahren wurden die intelligenten Sensoren immer kleiner, leistungsfähiger und besser an die





Mit seinen Abmessungen von 23,5 mm x 22 mm ist das OEM-Modul ‚VC picoSmart‘ das derzeit kleinste komplette Embedded-Vision-System weltweit.

jeweiligen Anwendungen angepasst. Maßgeblich getrieben war diese Entwicklung durch den Einsatz von ARM-Prozessoren mit frei programmierbaren Linux-Betriebssystemen. Sie ermöglichten eine unkomplizierte Entwicklung und stellten den Vision-Sensoren eine immer größere Rechenleistung zur Verfügung. Wenngleich hochmoderne Prozessoren mit Image-Processing-Units, Neural-Processing-Units und weiteren Recheneinheiten immer komplexere Bildverarbeitungsalgorithmen und den Einsatz von Künstlicher Intelligenz ermöglichen, ist das weitere Optimierungspotenzial in Bezug auf Miniaturisierung und Preis nahezu erreicht.

Am Prinzip der Entwicklung selbst hat sich gleichzeitig wenig verändert – die große Herausforderung bei der Entwicklung von Vision-Sensoren besteht nach wie vor darin, das System rund um den Bildeinzug und die Bildverarbeitung auszuwählen, aufeinander abzustimmen und umfassend zu testen, bevor die Integration in die Serienhardware und die Produktfertigung erfolgen können.

Komplettes System auf einer Platine

An dieser Stelle, dem Design von Vision-Sensoren, kommt ‚VC picoSmart‘ von Vision Components ins Spiel. Hierbei handelt es sich um ein 22 mm x 23,5 mm großes OEM-Modul, auf dem Bildsensor, Prozessoren, Speicher und ein Echtzeit-Betriebssystem bereits komplett fertig integriert sind. Die Komponenten dieses kompletten

Embedded-Vision-Systems sind haargenau aufeinander abgestimmt. So können OEM-Hersteller das Grundlagenpaket einfach in ihre Vision-Sensoren ein-designen und sparen Zeit und Kosten bei der Entwicklung. Zudem reduzieren die erprobten und getesteten Komponenten die Design-Risiken.

Auf der Platine, die etwas gleich groß ist wie herkömmliche Bildsensor-Module, sorgt ein monochromer 1-Megapixel-CMOS-Bildsensor mit Global Shutter für schnelle und kontrastreiche Bildaufnahmen. Die Prozesseinheit mit Speicher ist ebenfalls auf dem Board integriert und direkt an den Sensor gekoppelt. Hier findet die Verarbeitung der Daten statt. Ein FPGA übernimmt in erster Instanz den Großteil der Bildverarbeitung in Echtzeit. Für die Folgeaufgaben steht ein High-end-FPU-Prozessor als weitere Prozesseinheit zur Verfügung. Das Echtzeit-Betriebssystem ‚VCRT‘ wird auf diesem Rechenkern ausgeführt. Verglichen mit den ersten intelligenten Vision-Sensoren der ‚VC M‘-Familie ist die Rechenleistung um circa den Faktor 1000 höher.

Bildverarbeitung in Echtzeit

Eine Stärke des ‚VC picoSmart‘ ist die Bildverarbeitung in Echtzeit, mit der typische Anwendungen wie Objekterkennung, Lagekontrolle, das Lesen von Identifikationscodes und anderen Merkmalen sowie Überwachungen von Füllständen oder Bahnkanten direkt onboard erfolgen. Sen-

sorhersteller können direkt mit Fertigstellung von Funktionalität und Benutzerführung ihrer geplanten Applikationen beginnen. Dafür erhalten sie ein entsprechendes Development Kit für die Inbetriebnahme und den Entwicklungsstart. Für die Objekterkennung ist bereits eine Beispielanwendung mit Echtzeit-Auswertung im FPGA vorhanden. Mit ihr können über einen Tastendruck Muster eingelernt werden, die in den Folgebildern in Echtzeit erkannt und ausgegeben werden.

Als weitere Grundlagenauswertung entwickelt Vision Components eine Laserlinienextraktion. Zusammen mit dem OEM-Modul ist sie die Basis für unkomplizierte Designs und Entwicklungen kompakter Triangulationssensoren.

Die dritte Komponente des Baukastens für individuelle Laser-Profilsensoren ist ein entsprechendes Lasermodul. Es ist bereits auf die Bildaufnahme-Hardware des ‚VC picoSmart‘ abgestimmt und beinhaltet Technologien wie zum Beispiel die Ambient-Light-Suppression-Technologie (ALS). Damit ist der Triangulationssensor unempfindlich gegenüber Umgebungslicht von bis zu 100.000 Lux Helligkeit.

In drei Schritten zum OEM-Vision-Sensor

OEM-Hersteller erhalten mit der kompakten Platine ein komplettes und abgestimmtes Grundlagenpaket, das sie unkompliziert in ihr Gesamtdesign integrieren können. Vision Components übernimmt die Programmierung des FPGAs für die gewünschte Aufgabenstellung, sodass der Hersteller nur Optik, Beleuchtung, Gehäuse, Display, Stecker et cetera hinzufügen muss. Im Fall eines Triangulationssensors werden noch ein Scheimpflug-Block und das Lasermodul benötigt. Der Vision-Sensor kann dann endkundenfertig konfiguriert und unter eigenem Branding vertrieben werden. Für die Parametrierung und Anpassung der Bedienung steht eine SDK-Oberfläche zur Verfügung. *ik*



JAN-ERIK SCHMITT
ist Geschäftsführer von Vision Components in Ettlingen.

Radnabenmotoren

Einsatz in FTS, Industrierobotern und Intralogistik

Maccon lanciert den Radnabenmotor *XR15-05e* für Anwendungen mit Industrierobotern in der Intralogistik. Der Radnabenmotor ist ein Außenläufermotor und wurde als Direktantrieb ohne Getriebe konstruiert. Bei einem Außenläufermotor dreht sich der Rotor um den Stator, sodass er als Antriebsrad verwendet werden kann, indem eine gummibeschichtete Felge am Rotor angebracht wird. Merkmale des Radnabenmotors sind eine geringe axiale Länge (<50 mm) bei laut Anbieter hoher Leistungsdichte. Mit dem Motor lassen sich Nenndrehmomente von 8 Nm und eine Nenndrehzahl bis 480 U/min realisieren.

Ausgestattet ist der Radnabenmotor mit einem integrierten magnetischen Encoder zur präzisen Erfassung der Position beziehungsweise zur Drehzahlregelung. Der Motor wird mit 36 bis 60 V(DC) betrieben. Dichtungen zwischen dem drehenden Rotor und dem Anbauflansch beziehungsweise dem Stator verhindern den Eintritt von Schmutz und Feuchtigkeit. Durch den Einsatz eines Schrägkugellagers eignet sich der Motor zudem für die Aufnahme hoher radialer und axialer Belastungen.

www.maccon.de



Servoverstärker

100.000 Umdrehungen und mehr



Den Servoverstärker *Acosos P3* von B&R gibt es auch in einer speziellen Variante ohne Beschränkung der Ausgangsfrequenz. So werden in vielen Anwendungen Motordrehzahlen möglich, die 100.000 Umdrehungen in der Minute überschreiten. Diese Variante kann somit für Anwendungen im Werkzeugmaschinenbau, in der Stein- und Glasbearbeitung oder in der

Holzbearbeitung eingesetzt werden. Bei der Standardvariante des ‚Acosos P3‘ wird die elektrische Ausgangsfrequenz des Gerätes überwacht. Überschreitet die Ausgangsfrequenz den Grenzwert von 598 Hz für mehr als eine halbe Sekunde, wird die Bewegung gestoppt und ein Fehler ausgelöst. Bei der neuen Variante des Servoverstärkers wird die elektrische Ausgangsfrequenz des Gerätes nicht überwacht. Damit unterliegt es den Dual-Use-Exportbeschränkungen gemäß der Verordnung (EG) Nr. 428/2009 der Europäischen Gemeinschaft.

Die Servoverstärker sind für Spindelmotor-Operationen aller Art geeignet. Dabei können die Motoren im offenen Regelkreis und im vollständig geschlossenen Regelkreis mit einer Zykluszeit von 50 µs gesteuert werden.

www.br-automation.com

Servomotoren

TSN-kompatibel

Die TSN-kompatiblen Servoantriebe der Serie *Melservo MR-J5* von Mitsubishi Electric bieten ein Ansprechverhalten von 3,5 kHz und eine Mindestzykluszeit von 31,25 µs. Mit dem zugehörigen Motion-Modul ‚Melservo-J5‘ können Anwender zudem bis zu 256 Achsen synchronisieren. Bei der Inbetriebnahme generiert die Quick-Tuning-Funktion alle Parameter innerhalb von circa 0,3 s automatisch, die Maschine ist dann sofort nach der Freigabe des Servos betriebsbereit. Die Integration der ‚CC-Link IE TSN‘-Technologie (Time Sensitive Network) mit Übertragungsgeschwindigkeiten von 1 Gbit/s stellt die Synchronisation aller angeschlossenen Geräte sicher, einschließlich Sicherheitsgeräten, die wie klassische Steuerungsprodukte im selben Netzwerk angeschlossen werden können. Dabei erfolgt die Konfiguration aller Safety-Funktionen wie STO/SS1/SS2/SOS/SBC/SLS/SSM/SDI/SLI/SLT in der Software, dadurch sind die Geräte IEC-/EN-61800-5-2-konform für vereinfachte Sicherheitszertifizierung.

Andere Netzwerk-Protokolle wie Ethercat (CANopen over Ethercat, CiA 402) werden ebenfalls als Standard angeboten. Integriert sind zudem Funktionen zur vorausschauenden Wartung. Diese Funktionen werden durch die ‚Maisart AI‘-Technologie des Herstellers unterstützt. Sie ermöglicht es der Servoantriebsreihe, eine Verschleißerscheinung von mechanischen Maschinenkomponenten zu erkennen, lange bevor eine zyklusmäßige Wartung erforderlich ist.

de3a.mitsubishielectric.com



Schrittmotor-Controller

Vereinfachte Konfiguration

Zur Konfiguration und Diagnose der digitalen Schrittmotor-Controller aus den ‚DDS‘-Familien bringt LAM Technologies die Inbetriebnahme-Suite *OmniAutomation für Windows* auf den Markt. Sie ist kostenlos zum Download erhältlich und unterstützt die Geräteserien DDS1 (Takt-/Richtung, Drehzahl- und Drehmomentsteuerung), DDS6 (CANopen), DDS7xM (Modbus TCP), DDS7xE (Ethercat) und DDS7xP (Profinet IO). Die Verbindung vom PC zum Gerät erfolgt über das galvanisch getrennte Interface UPD30. Der Controller der Geräte kann über das UDP30 vom USB-Bus versorgt werden, sodass eine Parametrierung auch bei abgeschalteter Anlage möglich ist.



Als Distributor von LAM für den deutschsprachigen Raum hat mechapro die Übersetzung der bisher nur auf Englisch und Italienisch verfügbaren GUI von OmniAutomation übernommen. Die nun 3-sprachige Version steht ab sofort zum Download auf der Unternehmenswebseite bereit.

www.mechapro.de

Rotolineare Antriebe

Kompakte koaxiale Bauweise

Maccon lanciert den Aktuator *Z-Theta*, der für die einfache Integration in OEM-Systemen entwickelt wurde und lineare und rotatorische Punkt-zu-Punkt-Bewegungen in einem kompakten Gehäuse bietet. Der Aktuator zielt auf Anwendungen in Laborautomation, Halbleitertechnik sowie allgemeiner Automatisierung. Er basiert auf dem patentierten ‚ScrewRail‘ und wird durch die direkte Integration eines Rotationsmotors zum Antrieb der Theta-Bewegung ergänzt. Diese Konstruktion ist dann mit einem zweiten Schrittmotor gekoppelt, um die lineare Bewegung des Schlittens über eine Leitspindel zu steuern.

Sowohl für die Linear- als auch für die Rotationsachse sind optional Drehgeber erhältlich, die entweder eine Positionsbestätigung oder eine vollständige Schritt-Servo-Steuerung des Geräts ermöglichen. Hersteller der Aktuatoren ist die Firma Haydon-Kerk-Pittmann aus USA. Maccon ist Vertriebspartner für den deutschsprachigen Raum.



www.maccon.de

Winkelgetriebe

Alternative für Zahnstangenantriebe

Hypoidverzahnte Präzisions-Winkelgetriebe von Neugart verkürzen den Antriebsstrang und eignen sich daher für beengte Platzverhältnisse. Es gibt sie in drei Baureihen, die sich jeweils durch die Ausführung der Abtriebswelle unterscheiden: Die Reihe *WPLN* verfügt standardmäßig über eine glatte Abtriebswelle, die *WPSFN*-Modelle sind mit einer Flanschabtriebswelle ausgestattet, und die Baureihe *WGN* bietet eine ein- oder beidseitige Hohlwelle. Bei allen Baureihen ist die Drehrichtung von Antriebs- und Abtriebswelle gegensinnig.

Teil des Winkelgetriebe-Portfolios sind zwei Varianten mit werkseitig vormontiertem Ritzel: Für die Baureihe ‚*WPLN*‘ steht eine verzahnte Abtriebswelle mit vormontiertem Ritzel zur Verfügung, wobei eine Verzahnung gemäß DIN 5480 für die notwendige Verbindungssicherheit sorgt. Die Baureihe ‚*WPSFN*‘

umfasst eine Flanschabtriebswelle mit vormontiertem Ritzel, das – wie alle Modelle der Baureihe – mit einer Schnittstelle gemäß EN ISO 9409-1 ausgestattet ist. Dabei ist eine hohe Varianz an Baugrößen und Übersetzungen verfügbar.



www.neugart.com

Motoren

Portfolio erweitert

Siemens ergänzt das Einkabel-Servoantriebssystem ‚Sinamics S210‘ um neue Servomotoren. Speziell für die Pharma- und Lebensmittelindustrie gibt es den *Simotics S-1FS2*, eine Motorausführung im Edelstahlgehäuse, mit Schutzart IP67/IP69 sowie hochauflösenden 22-Bit-Absolut-Multiturngewernern. Die Servo-Planeten-Getriebemotoren *Simotics S-1FK2* (Bild) kommen zum Einsatz, wenn hohe Taktzahlen mit einer leichten und trägheitsarmen Getriebeausführung erreicht werden sollen oder wenn es um Trägheitsanpassung zum präzisen Bewegen schwerer Lasten geht. Die Motoren sind fertig montiert und als Einheit in diversen Getriebeübersetzungen und -baugrößen erhältlich. Dabei erfolgt die thermische Auslegung über den digitalen Zwilling im TIA Selection Tool.

Der *Simotics S-1F72* ist ein Servomotor, der eine Vielzahl unterschiedlicher Optionen für das Servoantriebssystem ‚Sinamics S210‘ bietet: Beispielsweise verbessern Geber mit einer Auflösung von bis zu 26 Bit die Systemgenauigkeit und durch Schutzart IP67 sowie verschiedene Motorlackierungen eignet sich die Lösung für den Einsatz in rauerer Umgebungen.



www.siemens.com

Schrittmotoren

Jetzt auch mit Profinet

Die Produktreihe der Schrittmotoren der AZ-Serie mit mechanischem Absolutwertsensor von Oriental Motor wurde durch Treiber mit Profinet ergänzt. Die Treiber sind wahlweise kompatibel zu den Feldbus-Systemen Profinet, Ethercat und Ethernet/IP. Über auf Ethernet basierende Feldbus-Systeme kann sowohl die Einstellung und Ausführung von Betriebsdaten sowie die Anpassung verschiedener Parameter als auch die Ausgabe von Alarminformationen und das Monitoring des Antriebs erwirkt werden. Alle Befehle und Statusmeldungen werden in Echtzeit übermittelt. So können die Bewegungen mehrerer synchron arbeitender Schrittmotoren präzise ausgeführt werden. Durch die Direktanbindung der Schrittmotoren mit netzwerkfähigem Treiber an die übergeordnete Steuerung ist nur ein einzelnes Datenkabel erforderlich.

Erhältlich sind zwei Treibervarianten für 24 und 48 V(DC) sowie für 230 V(AC).

Die Motoren sind in Flanschmaßen von 20 bis 90 mm verfügbar und erreichen in Kombination mit Getrieben Haltemomente bis 157 Nm.



www.orientalmotor.de

Hybridkabel

Verbunden auf Distanz

Stöber Antriebstechnik hat die *One Cable Solution (OCS)* in Zusammenarbeit mit dem Encoder-Hersteller Heidenhain weiterentwickelt und die nächste Generation auf den Markt gebracht. Mit dem Protokoll Heidenhain EnDat 3 kann das Hybridkabel Motoren und Antriebsregler bei einem Abstand bis 100 m verbinden. Anwender erhalten ein komplettes System aus Synchron-Servomotor, Kabel und passendem Antriebsregler. Endat 3 unterstützt den strukturellen Aufbau der Antriebsregler ‚SC6‘ und ‚SI6‘. Die beiden Antriebsregler besitzen denselben Transceiver-Chip wie der EnDat 3-Encoder. Zudem wurde die Firmware entsprechend angepasst. Die neue Ein-Kabel-Lösung ist für die Synchron-Servomotoren der Baureihen ‚EZ‘ und ‚EzS‘ ausgelegt, die mit allen Stöber-Getrieben im Direktanbau kombinierbar sind. Das System aus Motor, Kabel und Antriebsregler verfügt über ein elektronisches Typenschild, das eine automatische Systeminstallation ermöglicht. Jeder Motor sendet automatisch bei der Inbetriebnahme die eigenen elektronisch und mechanisch relevanten Daten per Plug-and-Play an die zugehörigen Antriebsregler.



www.stoeber.de

Datenschränke

Nach IP54 zertifiziert

Die dtm group erweitert ihr Lösungsportfolio um modulare Datenschränke für raue IT-Umgebungen: Die im Standard offenen Standverteiler *STV40/45n* und Server-racks *40/45HE* gibt es nun auch als geschlossene Systeme mit abgedichteten Seitenwänden, Türen, Böden, Deckenblechen und Sockeln. Nach IP54 zertifiziert bieten sie Schutz vor Staub und Spritzwasser. Die Serverracks sind mit integrierten Kabeltrassen ausgestattet und können mit Gaslöschanlagen sowie verschiedenen Klimalösungen wie etwa Seitenkühlern kombiniert werden. Stromaufnahme, Temperatur und ähnliche Parameter lassen sich optional mit dem herstellerunabhängigen Monitoring-system ‚EnviMonitor‘ überwachen. Damit eignen sich die Server-racks sowohl für den Industrie- und Office-Bereich als auch für Rechenzentren und kleinere Edge-Standorte. Die Bauteile der IP54-Erweiterung sind rückwärtskompatibel zum bestehenden System. Modular aufgebaut erlauben die Datenschränke eine Tiefenerweiterung von 270 bis 830 mm auf max. 1.430 mm.



www.dtm-group.de

Wellrohrsysteme

EMV-Sicherheit inklusive



Um einen sicheren EMV-Schutz in Umgebungen zu erreichen, in denen elektromagnetische Störstrahlungen auftreten, hat Pflitsch die *Uni ProTect EMV* entwickelt, die den EMV-Schutz am Fitting und im Wellrohr sicherstellt. So lassen sich auch ungeschirmte Kabel EMV-sicher upgraden. Das Wellrohr wird dazu mit einem innenliegenden Metallgeflecht versehen. Bei Fittings gibt es eine Version mit Konuskontaktierung, insbesondere für Anwendungen in der Robotik/Automation. Eine Version mit Federkontaktierung aus dem ‚Uni HF Dicht‘-Programm bietet EMV-Abschirmung auch bei größeren Kabeldurchmessern. Bei der Montage können Kabelschirm und Kabelmantel direkt weitergeführt werden, da der Kabelschirm an der Kontaktstelle nicht getrennt werden muss. Um mehrere Kabel EMV-sicher zu installieren, gibt es das ‚ProTect EMV‘-Fitting mit Mehrfachkontaktierung, wobei die verschiedenen Kabelschirme separat durch einzelne ‚TRI‘-Federn kontaktiert werden. Diese Lösung wird kundenspezifisch entsprechend der verwendeten Kabelquerschnitte gefertigt.

www.pflitsch.de

Steckverbinder

Anschlusstechnik für Profinet

Ein Standard namens ‚Typ R‘ definiert Anforderungen an Profinet-Leitungen, die in Roboterapplikationen eingesetzt werden. Escha bietet ein umfassendes Produktportfolio unter dem Namen ‚Profinet robotic‘ an, das optimale Schleppketteneigenschaften (5 Mio. Biegezyklen) mit sehr guten Torsionseigenschaften (5 Mio. Torsionszyklen) verbindet und damit exakt die Anforderungen des Industriestandards erfüllt. Die flexible Leitung mit der Bezeichnung ‚S5100‘ basiert auf einer zweipaarigen Datenleitung, die eine Fast-Ethernet-Übertragung nach Cat5e garantiert. Mit Anschlusstechnik aus der Reihe ‚Profinet robotic‘ lassen sich Datenübertragungsraten bis zu 100 Mbit/s bis an die Spitze eines Roboterarms bringen. Die ‚S5100‘-Leitung hält einer kombinierten Belastung aus horizontaler Bewegung und Torsion stand, sodass zum Beispiel Greifer mit intelligenten Sensoren oder Kameras zuverlässig angesteuert werden können. Aufgrund ihrer UL-Zulassung eignet sich die PUR-Leitung für den nordamerikanischen Markt. Die Produktfamilie besteht aus unterschiedlichen Steckverbindern in den Bauformen M8, M12 und RJ45.



escha.net

Gehäuse

Ex-e-Lösungsportfolio komplettiert



Mit der Serie *SR* positioniert sich Pepperl+Fuchs weiter als Anbieter für Ex-Equipment. Die in Edelstahl ausgeführte Gehäusebaureihe gesellt sich zu der in glasfaserverstärktem Kunststoff ausgelegten *GR*-Serie und komplettiert somit das Portfolio an Steuerungs- und Verteilungslösungen in Zündschutzart Ex e (erhöhte Sicherheit). Die *SR*-Serie umfasst über 30 Gehäusegrößen in Edelstahl. Zur Steigerung

der Kosteneffizienz sind die IP66/NEMA-4X-Gehäuse immer auf eine Grundaufbauform reduziert. Jegliches Zubehör, wie Flanschplatten, Scharniere, Drehriegel oder Deckel-Sicherheitsverschlüsse, wird nur nach entsprechender Kundenspezifikation durch Pepperl+Fuchs integriert.

Die Montage der für einen Temperaturbereich von -60 bis +120 °C zertifizierten Gehäuse am Einsatzort ist sowohl in vertikaler als auch horizontaler Ausrichtung möglich. Strategisch und technologisch fügt sich die Serie neben der *GR*-Serie ein, die eine Bandbreite von IP66/NEMA-4X-Gehäusen umfasst, die aus glasfaserverstärktem, antistatischem und besonders resistentem Polyester bestehen.

www.pepperl-fuchs.de

Zylinder

Mit Lebensdauerschmierung



Die elektromechanischen Zylinder *EMC* von Bosch Rexroth gibt es nun mit deutlich verlängerten Schmier-Intervallen. Viele Anwendungen profitieren laut Anbieter sogar von einer Lebensdauerschmierung, sodass die Zylinder in diesen Lösungen wartungsfrei sind. Die Zylinder mit der Option *„Lubricated For Life“* erreichen mit der werksseitigen

Grundschröpfung eine nominelle Lebensdauer von bis zu 15.000 km. Ob eine Lebensdauerschmierung innerhalb der geplanten Anwendung erreicht wird, finden Konstrukteure mithilfe des Auswahl- und Auslegungstools *„LinSelect“* heraus. Die elektromechanischen Zylinder verbinden eloxierte Aluminiumprofile in ISO-Standardmaßen mit einem integrierten Kugelgewindetrieb zu einer einbaufertigen Lösung. Dabei umfasst die *EMC*-Familie fein skaliert sieben Baugrößen. Die größte Variante *„EMC100-XC-2“* stellt Vorschubkräfte bis 56 kN zur Verfügung. Auf die verschiedenen Baugrößen abgestimmt, stellt der Anbieter ein breites Spektrum an Servomotoren und Antriebsreglern bereit. Ein optionaler Kraftsensor ermöglicht auch dezentrale Prozessregelungen ohne übergeordnete Steuerung.

www.boschrexroth.com

RFID-I/O-Module

Schnelle Interfaces für Ethercat

Turck erweitert mit der *TBEC*-Familie das Angebot an robusten und kompakten RFID-Lösungen um schnelle Interfaces für Ethercat-Netzwerke. Das *„TBEC“*-Modul im vollvergossenen Kunststoffgehäuse ist in Schutzart IP67/IP69K ausgeführt und im erweiterten Temperaturbereich von -40 bis +70 °C einsetzbar. Das Ethercat-RFID-Modul erlaubt den parallelen Betrieb von HF- und UHF-Schreib-Lese-Köpfen. Wie alle Ethernet-Multiprotokoll-Geräte von Turck unterstützt auch das *„TBEC“* den HF-Continuous-Busmodus, mittels dessen an jedem der vier RFID-Kanäle bis zu 32 busfähige HF-Schreib-Lese-Köpfe angeschlossen werden können. In Applikationen mit vielen Schreib- oder Lese-Positionen senkt dies Verdrahtungsaufwand, Kosten und Inbetriebnahmezeiten.



An den acht universellen DXP-I/Os lassen sich Sensoren, Lampen oder andere Aktuatoren anschließen. Alle Anschlüsse sind als 5-polige Steckverbindung in M12 ausgeführt, die Spannungsversorgung (L-codiert) erfolgt über die M12-Power-Technologie.

www.turck.com

Signalleuchten

Strahlen Licht über einen 360°-Bereich aus

Werma Signaltechnik bringt die LED-Drehspiegelleuchte 883 auf den Markt. Diese Signalleuchte ist mit einem energiesparenden und langlebigen LED-Leuchtmittel ausgestattet und strahlt Licht über einen Bereich von 360° aus. Typischerweise werden mit der Signalleuchte Warnhinweise im Außenbereich gegeben, wie beispielsweise an einem Tor oder einer Schranke. Dank der extrem hellen LED-Technologie im Inneren der Drehspiegelleuchte ist die Sichtbarkeit auch bei direkter Sonneneinstrahlung gewährleistet. Auch im Einsatz im Gebäudeinneren, im Bereich von großen Maschinen oder weitläufigen Anlagen, ist die Signalwirkung laut Anbieter sehr hoch und wird durch die entstehenden Reflexe an Wänden oder Flächen

noch verstärkt. Eine Statusänderung ist so auch dann erkenntlich, wenn man nicht direkt in die Signalleuchte blickt.



Der Anschluss der Leuchte erfolgt ohne Ausbau der Mechanikgruppe. Um Vandalismus oder versehentlicher Zerstörung vorzubeugen, kann ein robuster Drahtschutzkorb aus rostfreiem Stahl angebracht werden.

www.werma.com

A *Robotics &* **AUTOMATION**

**Roboter-
Boom**

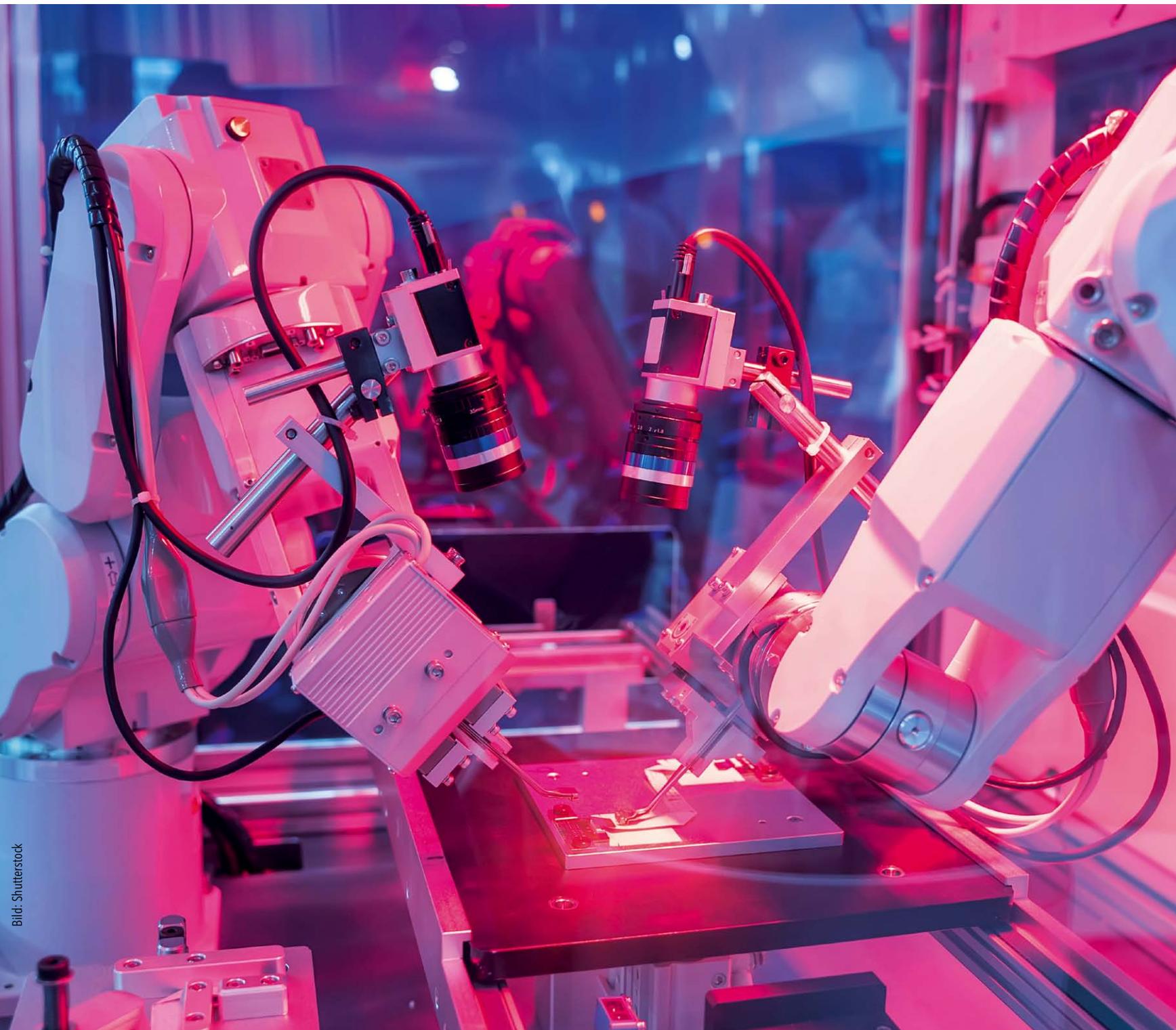
Seite 38

**Im Schwarm
intelligenter**

Seite 41

**Der Roboter als
Edge-Gerät**

Seite 44





Roboter-Boom

Auch in Deutschland ist mittelfristig mit einer verstärkten Implementierung von Robotern in Unternehmen zu rechnen. Welche Trends werden diese Entwicklung beschleunigen?
Eine Einschätzung der Investmentbanking Beratungsgesellschaft Cowen.

Der Robotics-Bereich ist ein milliardenschwerer Markt, der weiterhin sehr dynamisch wächst. Die Gründe dafür sind unterschiedlicher Art: Zum einen erschließt der technologische Fortschritt in puncto Sensorik sowie Software mit künstlicher Intelligenz neue Anwendungsbereiche für die Automatisierung. Zum anderen gibt es immer mehr Wachstumstreiber – beispielsweise die E-Commerce-Branche, die automatisierte Lösungen in der Logistik und in der Auftragsabwicklung dringend erforderlich machen. Doch auch die voranschreitende De-Globalisierung der Wertschöpfungsketten spielt dem Einsatz von Robotern hierzulande in die Karten. Noch vor einigen Jahren wurden Roboter ausschließlich in geschützten und abgesonderten Arbeitsbereichen eingesetzt. Dem ist künftig nicht mehr so: Roboter werden sich schon bald freier bewegen können und in ihrer jeweiligen Arbeitswelt nicht nur vernetzt, sondern auch vollständig integriert sein.

Neue Anwendungsfelder durch Innovationen

Roboter sind zunehmend in der Lage, auch sehr komplexe Aufgaben zu übernehmen. Sie können mittlerweile zudem mit Menschen Hand in Hand arbeiten und sind immer einfacher anzulernen. Wurden Roboter in der Vergangenheit mehrheitlich

in der Automobilbranche sowie in der Elektronikindustrie eingesetzt, kristallisieren sich heute ganz neue Branchen für deren Einsatz heraus: Eine davon ist die Logistik-Industrie, in der die Auftragsabwicklung vermehrt vollständig automatisiert abläuft. Angetrieben wird das Ganze unter anderem durch den E-Commerce-Sektor sowie das Gesundheitswesen. Letzteres setzt Roboter beispielsweise zunehmend in Operationssälen oder bei der Pflege von Patienten und Patientinnen ein.

Auch in der Agrarindustrie wird im Zuge von ‚Smart Farming‘ der Anbau- und Ernteprozess neu gedacht: Hier werden Roboter zum Beispiel eingesetzt, um Bodenmessungen vollautomatisch durchzuführen. Und beim Militär übernehmen die Maschinen mittlerweile gefährliche Aufgaben, wie das Entschärfen und Entsorgen von Sprengkörpern. Soviel zu einigen wenigen Beispielen für Anwendungsmöglichkeiten von Roboter-basierten Automatisierungslösungen.

Nachholbedarf in Industrienationen

Die meisten Industrienationen bemerken bereits heute, dass sie im Segment Robotik gegenüber den darin führenden Ländern aufholen müssen: Die Vorreiter Singapur und Südkorea weisen im Vergleich zu Industrienationen wie Deutschland, Japan, den

USA und China eine achtfach höhere Dichte von Industrierobotern in der Herstellerindustrie vor. Das ist eine um Faktor 8 höhere Anzahl installierter Roboter im Verhältnis zur Anzahl der Erwerbstätigen. Dies kann als eine Art Kompass für die Automatisierungspotenziale in den meisten Ländern dienen – allerdings ohne dass technologische Innovationen, demographische oder politische Einflüsse eingerechnet sind.

Eine Reihe an Trends beschleunigt den Robotics-Bereich zusätzlich in seiner Wachstumsdynamik.

Der E-Commerce

Was mit Büchern und weiteren handlichen Artikeln begann, erstreckt sich heute auf eine immer größere Zahl von Gütern: Roboter sind aus dem Bereich Logistik im E-Commerce beziehungsweise dem Online-Kauf von Artikeln nicht mehr wegzudenken. Sie ermöglichen es, die komplexe Artikelvielfalt in modernen Verteilzentren automatisiert abzubilden. Auftragsbezogen entnehmen Roboter die Waren selbstständig aus dem Lager und führen Kommissionierung, Verpackung sowie das Labeling bis zum Versand ebenfalls eigenständig durch.

De-Globalisierung von Wertschöpfungsketten

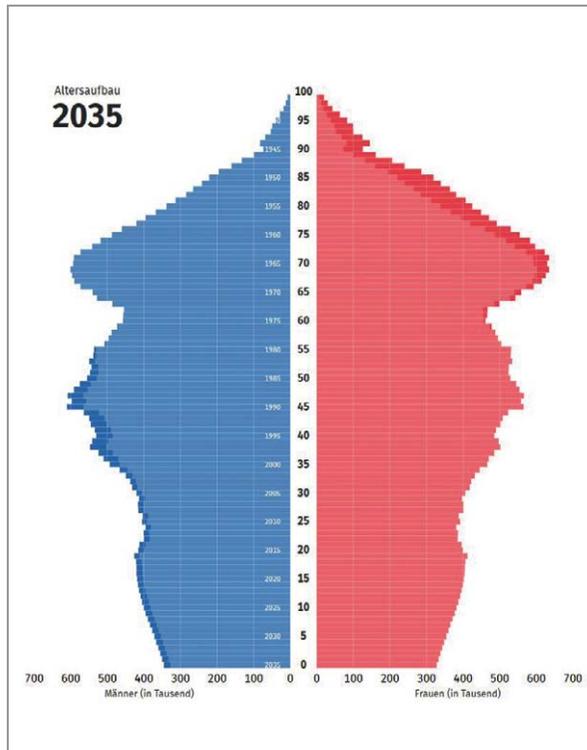
Aufgrund der zunehmenden De-Globalisierung werden Firmen sich künftig wieder verstärkt in heimischen Regionen ansiedeln, um Lieferketten resilienter zu machen. Einer der Anknüpfungspunkte ist die Versorgungssicherheit lebensnotwendiger Güter beispielsweise im medizinischen Bereich. Die lokale Versorgung mit solchen Gütern ist in turbulenten Zeiten etwa durch Pandemien häufig schwierig oder auch gar nicht zu realisieren. Firmen sollten deshalb verhindern, dass Lieferketten zusam-

menbrechen, indem sie diese verkürzen und stärker kontrollieren. Aus diesem Grund erscheint es sinnvoll, die industrielle Produktion nach der Pandemie wieder in den europäischen Raum zurückzuführen. Für Länder mit einem hohen Lohnniveau, wie Deutschland oder Dänemark, ist die Relokalisierung der Produktionsstätten aus asiatischen Schwellenländern aber nur dann sinnvoll, wenn die industriellen Prozesse hierzulande hochgradig automatisiert werden können. Denn nur so können Firmen wettbewerbsfähige Preise bieten und Abnehmer weiter binden. Die De-Globalisierung der Supply Chains wird mittel- bis langfristig europaweit zu einer weiteren Erhöhung des Automatisierungsgrades führen. Aber: Wird die Wertschöpfung aus Billiglohnländern zurückgeführt, gilt es, sich mit zwei Herausforderungen zu beschäftigen: Wie lassen sich die Herstellungskosten im Griff behalten? Und wie ist der zunehmende Mangel an Arbeitskräften aufzulösen? In beiden Fällen liegt die Lösung in der Automatisierung der Wertschöpfungskette.

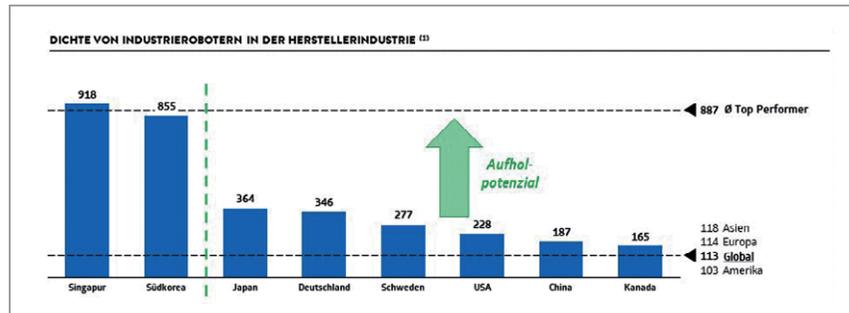
Die alternde Bevölkerung

Die Bevölkerung wird immer älter und weniger Nachwuchskräfte folgen, wodurch menschliche Arbeitskraft in der Industrie knapper wird. Der Bedarf jedoch steigt weiter an. Die Wertschöpfungsketten in relevante Industrien zurückzuführen, ist nicht nur aus diesem Grund dringend notwendig. Dies lässt sich allerdings nur noch durch weitere Automatisierung und somit mittels innovativer Roboter-Lösungen realisieren. Moderne Sensorik und mit künstlicher Intelligenz ausgestattete Roboter können bereits heute mit Menschen kommunizieren und zusammenarbeiten. Mobile Roboter erledigen so beispielsweise in der Pflege von Menschen einfache Aufgaben: Sie bringen den Pflege-

Bild: Statistisches Bundesamt



In Deutschland sinkt sowohl die Sterbe- als auch die Geburtenrate, wodurch die Bevölkerung gleichzeitig altert und leicht schrumpft.



Singapur und Südkorea weisen mit weitem Abstand die höchste Dichte an Industrierobotern im Verhältnis zur Einwohnerzahl auf. Für die meisten Länder gibt es ein erhebliches Aufholpotenzial – insbesondere auch für Deutschland.



Zwischen 2010 und 2019 hat sich der Umsatz der Top 20 Lieferanten für automatisiertes Materialhandling mehr als verdoppelt. Der Trend ist weiterhin ungebrochen steigend.



FORUM SAFETY & SECURITY

22. - 23. Juni 2021
virtuelles Event

PROGRAMM ONLINE!

**JETZT
ANMELDEN!**

Während des Forums werden die Einzelthemen Safety und Security sowie das Zusammenspiel beider Aspekte diskutiert und zwar einerseits anwendungsübergreifend, andererseits auch aus Sicht der Anwendungsbranchen Industrie und Automotive. Das Vortragsprogramm spannt den Bogen von den verfügbaren Hard- und Softwarekomponenten, Methoden und Tools, Hilfsmitteln und der Zertifizierung bis zum praktischen Einsatz sicherer Systeme.



21. Juni 2021
Einstiegsseminar Funktionale Sicherheit und Security in Embedded Systemen
Prof. Dr. Peter Fromm Hochschule Darmstadt



22. Juni 2021
Keynote: Ein absolutes Muss: Safety-Security-Interaktion und Crypto-Agilität
Hans Adlkofer, Senior Vice President Automotive System Group Infineon Technologies



23. Juni 2021
Keynote: Herausforderungen in der Funktionalen Sicherheit in Verbund mit der Künstlichen Intelligenz
Prof. Dr. Ossmane Krini, Duale Hochschule Baden-Württemberg Lörrach, Leiter des Instituts für Funktionale Sicherheit, Cyber Security und Künstliche Intelligenz

Silber Sponsor



Bronze Sponsor



powered by



Detaillierte Informationen zum Programm unter:
www.safety-security-forum.de

bedürftigen Getränke oder unterstützen in der Rehabilitation. Damit wird das Pflegepersonal entlastet und kann sich auf die wesentlichen, zwischenmenschlichen Aufgaben konzentrieren.

Software ersetzt Hardware

Bisher war es stets notwendig, höchste Präzision bei Komponenten oder Antrieben der Roboter an den Tag zu legen. Mittlerweile ersetzen Software-Lösungen dieses erforderliche Maß an Präzision und tragen damit letztendlich dazu bei, die dahinter stehenden Robotersysteme einfacher zu gestalten.

Haptische Sensorik

Roboter sind heutzutage vielfach weder gefährlich noch räumlich abgeschirmt – wie es noch vor Jahren mehr oder minder immer der Fall war. Innovationen in der Sensorik in Verbindung mit intelligenten Bilderkennungssystemen schaffen heute Maschinen, die sich in ihrer jeweiligen Umwelt gut zurechtfinden und mit den Menschen direkt interagieren können. Dabei bleibt allerdings die Feinmotorik der menschlichen Hand das Maß der Dinge, an das sich die Roboterwelt immer mehr annähert. Dies stellt stets die Basis für eine Mensch-Maschinen-Interaktion dar.

Einfache Inbetriebnahme

Roboter werden in Firmen immer mehr zur Automatisierung eingesetzt werden und damit den Trend hin zur De-Globalisierung unterstützen. Auch deshalb liegt ein Fokus darauf, leicht zu installierende autonome Systeme zu entwickeln. Die Gründe liegen auf der Hand: Die Roboter lassen sich den jeweiligen Anforderungen mit deutlich geringeren Ressourcen wie beispielsweise Kapital und Installationsaufwand anpassen. Für die Inbetriebnahme eines Roboters müssen künftig keine Spezialisten und Spezialistinnen mehr herangezogen werden. Sogenannte Teach-in-Software vereinfacht die ersten Schritte. Durch Vernetzung wird die Umwelt eingebunden und GPS-Lösungen sowie selbstlernende Algorithmen ermöglichen es, dass Roboter ihren Aufgaben rasch nachgehen können. So werden Roboter bald zum Standard zählen.

Robotik für immer mehr KMUs zugänglich

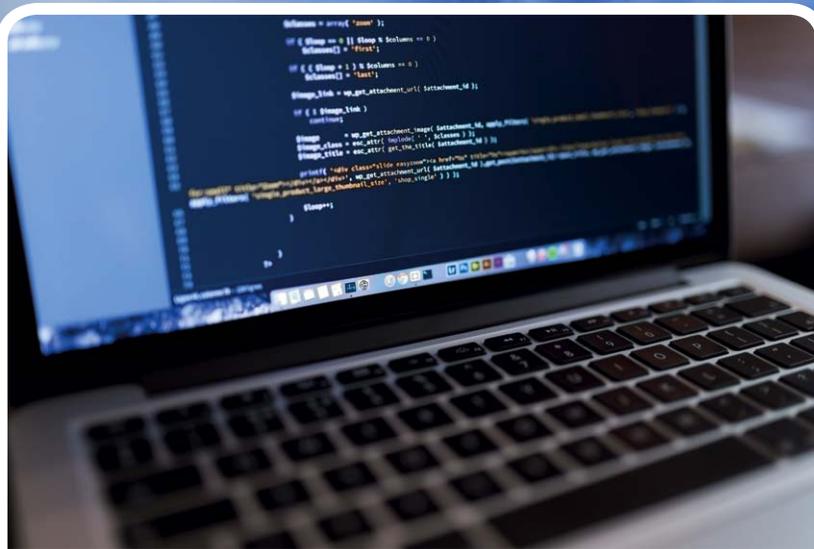
Roboter werden verstärkt in KMUs zur Automatisierung eingesetzt werden, die hierzulande einen Großteil der Wirtschaft ausmachen. Ein Fokus der Innovationen im Bereich Robotics liegt auf der Entwicklung von leicht zu installierenden und autonomen Systemen, die sich mit reduziertem Ressourceneinsatz den jeweiligen Anforderungen anpassen lassen. Dieser Trend führt zu einer weiteren Verbreitung von Robotik, indem sich die Maschinen auch für kleinere Unternehmen und weniger skalierte Tätigkeiten rechnen. Die Produktion in Billiglohnregionen könnte damit zunehmend überflüssig werden. ik



DANIEL KROLL
ist Director bei der
Investmentbanking
Beratungsgesellschaft
Cowen in Leipzig.

Im Schwarm intelligenter

Weshalb schwimmen Fische in Schwärmen, fliegen Vögel in Scharen oder Bienen im Schwarm? Weil sie gemeinsam intelligenter und effizienter sind. Dies gilt auch für die Schwarmrobotik – dezentralisierte, sich selbst organisierende Systeme, die sich aus einzelnen, einfach aufgebauten Agenten zusammensetzen.



- Lokale Interaktionen: Die Roboter zeigen ein kollektives Verhalten durch lokalen Informationsaustausch.

Überblick über bestehende Modelle

Im Laufe der Jahre wurden viele unterschiedliche Schwarmalgorithmen entwickelt. Die am häufigsten eingesetzten Modelle sind Artificial Bee Colony (ABC), Boids (Bird-oid object) und Ant Colony Optimization (ACO).

ABC – Artificial Bee Colony

ABC wurde 2005 entwickelt. Der Algorithmus ist vom Verhalten der Honigbiene bei der Suche nach Nahrungsquellen (Nektar) und dem anschließenden Informationsaustausch über diese Nahrungsquellen mit anderen Bienen im Bienenstock inspiriert. Der ABC-Algorithmus umfasst drei Phasen: die Employed Bee Phase, die Onlooker Bee Phase (Startphase) und die Scout Phase (Suchphase). Jede Arbeiterin (Employed Bee) wählt eine ihr bekannte Nahrungsquelle aus und bestimmt den nächstliegenden Ort. Dabei schätzt sie die dort vorhandene Nektarmenge ab und gibt die Information durch ihren Tanz im Bienenstock an die anderen Bienen weiter. Die Beobachterin (Onlooker Bee) beobachtet den Tanz der Arbeiterin, wählt auf der Grundlage dieser Information eine der Nahrungsquellen aus

Die Mitglieder eines Schwarms interagieren lokal miteinander und mit ihrer Umgebung. Diese Interaktionen führen zu einem adaptiven Suchverhalten und schließlich zur globalen Optimierung des Schwarms. Dieser von der Natur inspirierte Optimierungsansatz hat sich in den letzten Jahren rasant entwickelt und inspiriert neue Entwicklungen in zahlreichen Branchen. Doch welche Mechanismen liegen der Schwarmrobotik zugrunde, welche Merkmale kennzeichnen intelligente Schwarmalgorithmen und welche Modelle und Anwendungsmöglichkeiten gibt es aktuell?

Algorithmen in der Schwarmrobotik

Dem Modell eines intelligenten Schwarms liegt ein kooperativer Algorithmus als Schlüsselkomponente zugrunde, der Verhaltensweisen und Interaktionen kontrolliert. Roboterschwärme basieren auf der Grundlage verschiedenster Algorithmen,

die Grundfunktionen wie die einfache Verteilung von Objekten oder Robotern im Raum oder Funktionen zur komplexen Zusammenarbeit wie die Bildung einer Kette regeln können.

Die grundlegenden Ziele der Schwarmrobotik zielen häufig auf die Miniaturisierung von Hardware oder Kosteneffizienz ab. Vier der wichtigsten Merkmale von Schwarmintelligenz sind Koordination, Gruppenbildung, Optimierung und Pfadplanung. Typische Eigenschaften von Schwarmalgorithmen sind:

- Geringe Komplexität: Einzelne Roboter folgen einfachen Regeln.
- Skalierbarkeit: Die Auslegung des Systems erfolgt für eine beliebige Anzahl von Robotern.
- Dezentralisierung: Schwarmroboter sind autonom und folgen keinen externen Befehlen.

und begibt sich dorthin, um die vorhandene Nektarmenge zu sichten. Alte Nahrungsquellen werden durch die von Kundschafterinnen entdeckten neuen Nahrungsquellen ersetzt. Die beste Nahrungsquelle und die damit verbundene Position werden so konserviert.

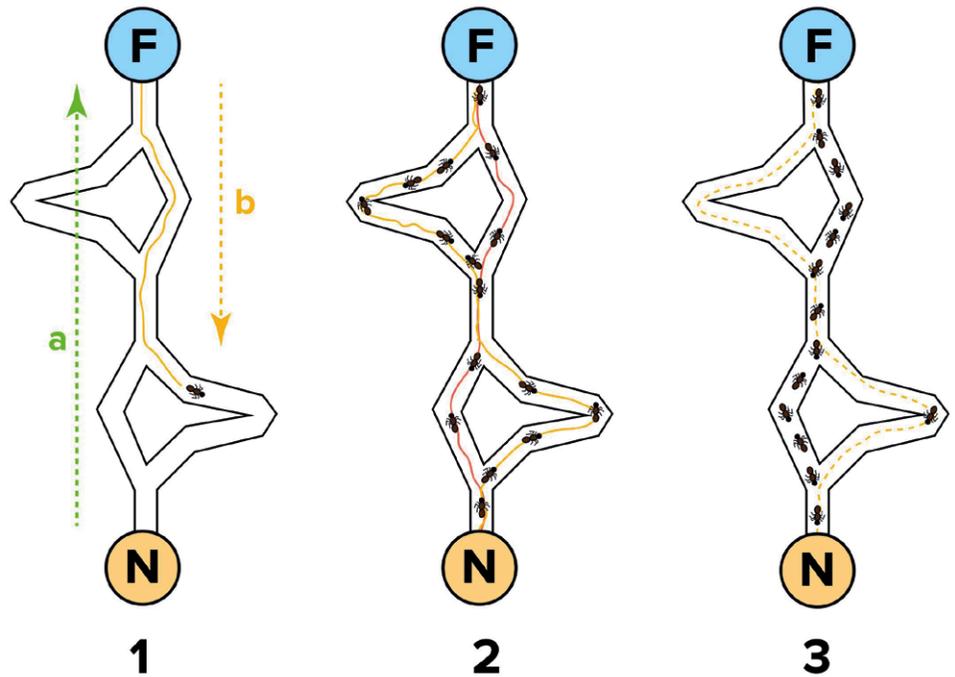
Die Position einer Nahrungsquelle stellt das ‚Ziel‘ dar. Die in diesem Bereich gefundene Nektarmenge entspricht der ‚Qualität/Quantität‘, auch Fitness oder ‚Associated Solution‘ genannt. Die Anzahl der Arbeiterinnen entspricht somit der Anzahl der ‚Associated Solutions‘ innerhalb des Schwarms.

Ein anschauliches Beispiel für einen ABC-Algorithmus findet sich in der Landwirtschaft. Die Schwarmrobotik eignet sich insbesondere im Bereich Precision Farming, etwa bei großen Einsätzen in der Landwirtschaft, bei denen Drohnen für topografische und thermografische Zwecke eingesetzt werden.

In der Landwirtschaft liefert die Thermografie wichtige Informationen über die Umgebungsbedingungen, die auf andere Art und Weise schwer zu gewinnen sind. Wird eine Drohne mit einer Thermokamera ausgestattet, lässt sich die Temperatur im untersuchten Gebiet mit erstaunlicher Präzision messen. Dabei stehen verschiedene Temperaturwerte für unterschiedliche Merkmale der pflanzlichen Entwicklung. Der Einsatz von Drohnen im Precision Farming führt zu einer hohen Produkteffizienz und ermöglicht den Einsatz minimaler Ressourcen und damit Einsparungen.

Boids - Bird-oid Objects

Boids steht für eine Simulation künstlichen Lebens, die 1986 von Craig W. Reynolds entwickelt wurde. Es handelt sich dabei um



Beim ACO-Algorithmus wird das Optimierungsproblem durch Suche des kürzesten Pfades in einem gewichteten Graphen gelöst.

Bild: Johann Dréon

einen Optimierungsalgorithmus, der vom natürlichen Verhalten von Schwarmvögeln inspiriert ist. Boids ist ein einfacher Algorithmus mit drei Regeln, die komplexes Verhalten in der Schwarmrobotik möglich machen: Zusammenhalt (Cohesion), Ausrichtung (Alignment) und Trennung (Separation).

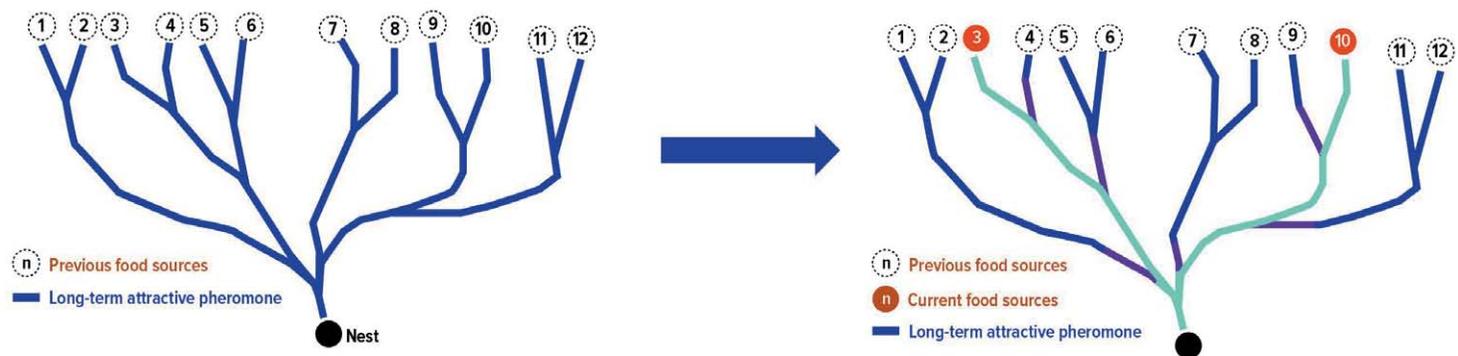
Zusammenhalt (Cohesion): Dieses Verhalten veranlasst Agenten dazu, die mittlere Position (den Massemittelpunkt) innerhalb der benachbarten Agenten aufzusuchen. Auf diese Weise bewegen sich die Boids immer innerhalb eines bestimmten Bereichs.

Ausrichtung (Alignment): Dieses Verhalten veranlasst einen bestimmten

Agenten dazu, seine Position relativ zu weiteren Agenten in der Umgebung auszurichten und in dieselbe Richtung wie seine Nachbarn zu steuern. Genutzt wird eine Formel zur Definition der eigenen Geschwindigkeit aus den Geschwindigkeiten der Nachbarn in der Umgebung.

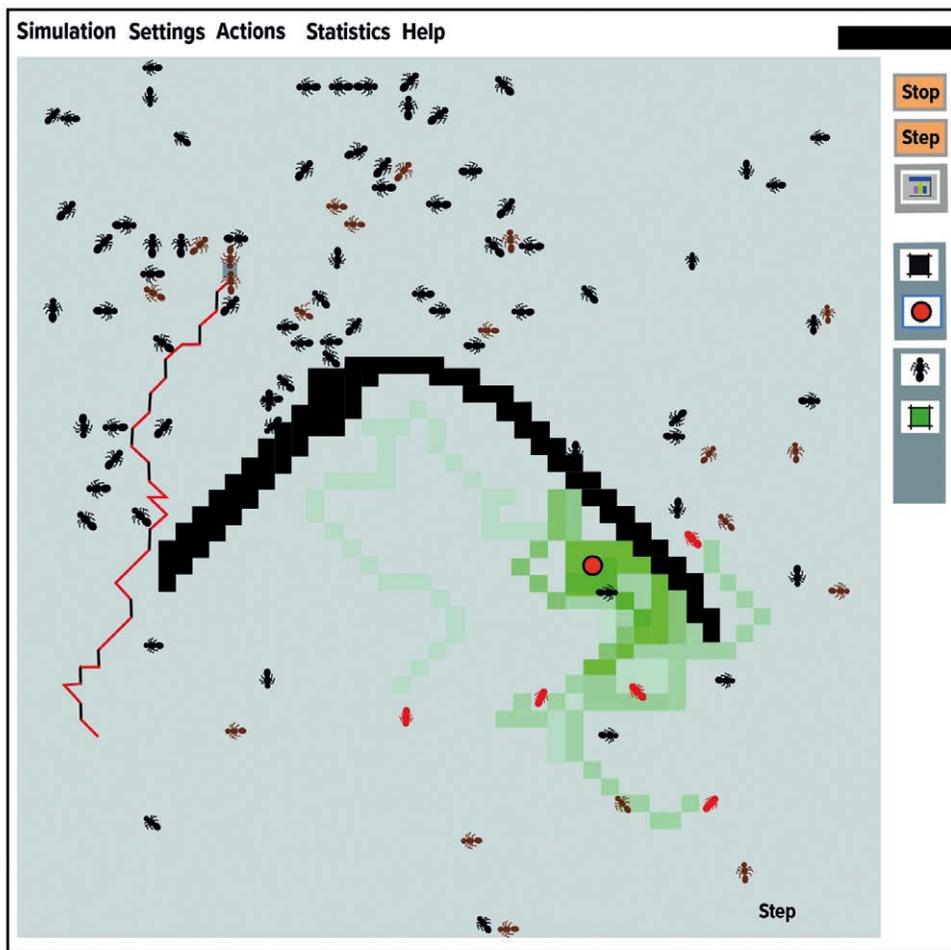
Trennung (Separation): Dieses Verhalten veranlasst einen Agenten dazu, sich vom Nachbarn wegzubewegen, wenn der Abstand zwischen ihnen zu gering wird, um einen Zusammenstoß zu vermeiden. Dies garantiert zudem einen Mindestabstand zwischen allen Agenten.

Mit diesen einfachen Regeln ist es möglich, das Schwarmverhalten zu simulieren. Da sie allein jedoch oft nicht ausreichen,



Eine künstliche Visualisierung der Pheromon-Intensität. Diese Art der Kommunikation ist eine der effektivsten in der Natur.

Bild: A Multiple Pheromone Communication System for Swarm Robotics and Social Insects Research



Simulation einer Ameisenkolonie auf der Suche nach einer Nahrungsquelle anhand des ACO-Algorithmus.

kann dieses Schwarmverhalten durch weitere, individuelle Regeln ergänzt werden, um eine komplexere oder sinnvollere Bewegung zu erreichen. Alle möglichen Formen allgemeinen Verhaltens können als Anziehung und Abstoßung von bestimmten Dingen modelliert werden, zum Beispiel ‚starker Wind‘, ‚Geschwindigkeitsbegrenzungen‘ oder ‚Hindernisvermeidung‘. Werden beispielsweise die drei Basis-Verhaltensweisen durch die Regel der Hindernisvermeidung ergänzt, wechselt der Schwarm seine Richtung, um auf dem Weg zum Zielpunkt Hindernisse zu vermeiden.

Einer der häufigsten Anwendungsfälle dieser Art von Algorithmen sind Suchaufgaben: Eine bestimmte Anzahl kleiner Drohnen mit Selbstlokalisierungs- und Messfunktionen übernimmt Suchmissionen in ländlichen, natürlichen oder komplexen Umgebungen, in denen der Zugang von Menschen oder großen Flugzeugen nur eingeschränkt möglich oder gefährlich ist. Die Eigenschaften der Schwarmintelligenz

werden genutzt, um auf skalierbare Weise Probleme kooperativ zu lösen. Das Ausführen derselben Aufgabe durch eine einzelne Drohne würde mehr Zeit in Anspruch nehmen. Zudem müsste diese einzelne Drohne komplexer aufgebaut sein, was die Kosten erhöhen würde.

ACO - Ant Colony Optimization

ACO ist eine probabilistische Technik, die Marco Dorigo 1992 entwickelt hat, um Computerprobleme nach dem Vorbild des Futtersuchverhaltens von Ameisen zu lösen. Das Modell basiert auf dem Ansatz, dass unabhängige Einheiten mit einfachen und unvorhersehbaren Verhaltensweisen miteinander kooperieren. Ziel jeder Ameise ist es, den optimalen Weg vom Nest zu einer oder mehreren Futterquelle(n) zu finden. Die Ameisen schwärmen willkürlich in unterschiedliche Richtungen aus und kehren zu ihrem Nest zurück, sobald sie eine Futterquelle gefunden haben. Auf ihrem Weg hinterlassen sie Pheromone auf

dem Boden. Andere Ameisen folgen der ersten Ameise auf unterschiedlichen Wegen. Dieser Prozess wird solange wiederholt, bis nach einiger Zeit auf dem kürzesten Weg eine höhere Menge an Pheromonen zu finden ist als auf den anderen. Die Wahrscheinlichkeit steigt, dass dieser Weg eingeschlagen wird: Am Ende nehmen alle Ameisen den kürzesten Weg.

Der ACO-Algorithmus bietet sich für komplexe Optimierungsprobleme wie das Traveling Salesman-Problem (TSP) oder das Vehicle Routing-Problem (VRP) an. So lässt sich die effizienteste Route zwischen zu besuchenden Punkten und Orten bestimmen. Der ACO-Algorithmus ist vor allem dann von Nutzen, wenn sich der Graph dynamisch verändert. Daher wurde dieser Algorithmus in der Vergangenheit bereits auf viele kombinatorische Optimierungsprobleme angewandt und trägt dazu bei, die jeweils optimale Lösung zu finden.

Für die Nutzung von Schwarmrobotik sind die Art der Kommunikation, die Komplexität des Algorithmus im Hinblick auf die Berechnung und damit verbunden das Identifizieren möglicher Anwendungsfälle wichtig. Diese drei Punkte sind unterschiedlich komplex und stellen den Anwender vor diverse Herausforderungen. Die bisher genannten Anwendungsmöglichkeiten haben Beispielcharakter. Denn die aktuelle Forschung und Entwicklung zeigt, dass künftig viele weitere Anwendungsszenarien in Bereichen wie Verkehr – sowohl auf der Straße als auch in der Luft –, dem Überwachen und Kontrollieren großer Gebiete sowie dem Ausführen von Aufgaben in Gefahrenbereichen denkbar sind. ik



PIETRO FERRARA
ist Senior Consultant Concept bei Reply in Turin.



DR. CHRISTIAN KOETSCHAN
ist Practice Lead Swarm Robotics bei Reply in München.

Der Roboter als Edge-Gerät

Die besten Automatisierungsstrategien innerhalb der Industrie 4.0 beruhen auf der Erkenntnis, dass die Stärken von Robotern ideal zur Geltung kommen, wenn sie neben und nicht in Abwesenheit von Menschen arbeiten. Dabei kann es helfen, den Roboter als Edge-Komponente wahrzunehmen. Eine Einschätzung von Ian Ferguson.

Sicherlich gibt es Rollen, die Roboter effektiver ausführen können als Menschen, dazu zählen sich wiederholende, monotone Aufgaben, das Handhaben von schweren Lasten oder Aufgaben in für Menschen gefährlichen Umgebungen. Im Moment machen Roboter nur das, wozu sie programmiert wurden. Die Fähigkeit, zu denken und in Echtzeit situative Entscheidungen zu treffen, ist dem Menschen vorbehalten. Künstliche Intelligenz hat noch einen weiten Weg vor sich, bevor sie dies annähernd replizieren kann.

Das Aufkommen von kollaborativen Robotern, sogenannten Cobots, die mit

Menschen in einem gemeinsamen Raum interagieren oder in unmittelbarer Nähe sicher arbeiten sollen, ist ein wichtiger Schritt in die Richtung Mensch-Roboter-Zusammenarbeit. Cobots stehen in Gegensatz zu traditionellen Industrierobotern, die autonom arbeiten und deren Sicherheit durch die Isolation vom menschlichen Kontakt gewährleistet wird. Mittlerweile beginnen Fertigungsbetriebe, Prozesse neu zu überdenken, um Menschen und Roboter gemeinsam effizienter zu nutzen.

Cobots benötigen eine viel engere Kontrolle für die Echtzeit-Umsetzung von komplexen Entscheidungen in Co-Work-

king-Umgebungen. Künstliche Intelligenz kann hier helfen.

Schnelle Entscheidung an der Edge

Die komplexen Entscheidungen müssen aber vom Roboter als Edge-Gerät getroffen werden. Als Edge-Komponente kann er die benötigte Geschwindigkeit und Latenz erreichen, um die zunehmende Datenmenge von IoT-Sensoren abzuarbeiten.

Dazu muss jedoch geklärt werden, was ‚Edge‘ bedeutet. Ein Edge-Gerät ist eine Komponente, welche mehrere Datenströme analysiert und auf dieser Datenbasis Entscheidungen trifft. Es kann also ein



Bild: iStock.com/JIRARAJ PRADITCHAROENKUL

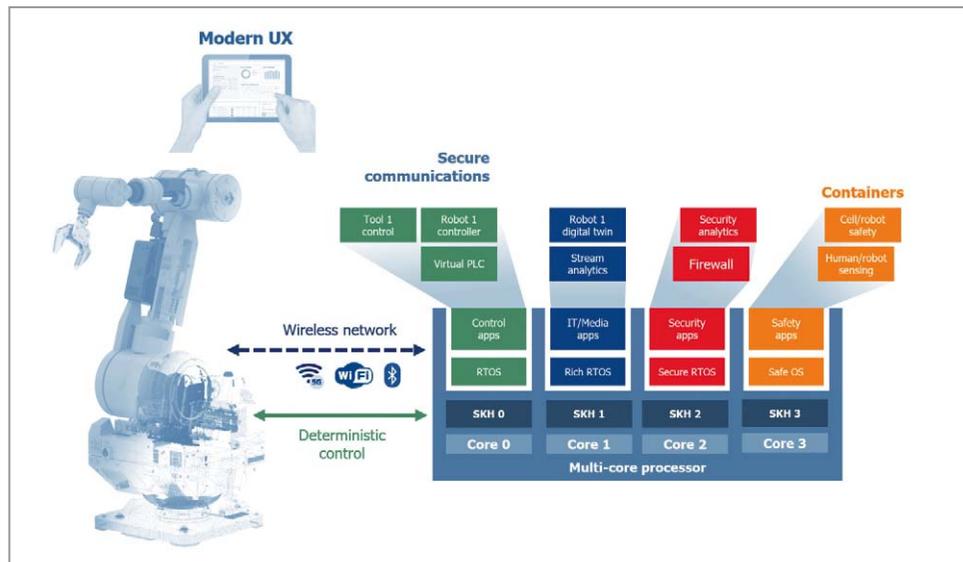
Server-Blade sein, in dem mehrere Informationsströme zusammenlaufen, ein einfaches Gateway oder aber es ist ein Roboter.

Taucht man tiefer in die Architektur dieser Roboter ein, so basieren diese Produkte auf Multicore-Prozessoren. In einer Reihe von Fällen sind die Verarbeitungsfunktionen denen eines Smartphones sehr ähnlich. Einer der Hauptunterschiede bei Robotern besteht darin, dass sie ihre Funktionen in einer sehr vorhersehbaren, kurzen Zeit ausführen müssen. Befinden sich Roboter in der Nähe von Menschen und/oder sehr teuren Materialien, muss der Roboter innerhalb von 100 bis 200 μ s auf ein Ereignis reagieren. Dies ist relativ einfach zu realisieren, sollte dies die einzige Aufgabe für den Prozessor sein.

Echtzeit-Systeme in der Industrie basieren meist auf einem Single-Core-Prozessor (SCP). Für die Entwicklung solcher Systeme hat die Industrie einen Prozess eingeführt, der auf der Annahme der konstanten maximalen Laufzeit (Worst Case Execution Time, WCET) basiert. Diese besagt, dass die gemessene maximale Laufzeit einer Software-Task – sollte diese allein auf einem einzelnen Kern ausgeführt werden –, gleich bleibt, wenn diese Task zusammen mit anderen Tasks ausgeführt wird.

Anforderungen an gemischt-kritische Systeme

Da die Industrie zu sogenannten ‚Mixed Criticality‘-Systemen übergeht – solche, die Echtzeit-Tasks in Verbindung mit weniger zeitkritischen Anwendungen ausführen –, ist die Annahme einer konstanten WCET für Single-Core-Chips korrekt. Für aktuelle Multicore-Prozessoren trifft sie aufgrund von Interferenzen zwischen den Cores beim Zugriff auf gemeinsame Ressourcen nicht zu. Ohne auf tiefe Hardware-Details einzugehen, weisen aktuelle Multicore-Prozessoren nicht-deterministische Speicherzugriffsverzögerungen auf, wenn sie um gemeinsam genutzte Ressourcen konkurrieren. Störungen können sowohl durch Konkurrenz auf Hardware- als auch auf Software-Ebene verursacht werden. Dieser Beitrag konzentriert sich auf die Auswirkungen von Hardware-Interferenzen und der sogenannten Interferenzkanäle, die sich in verschiedenen Aspekten von Multicore-Architekturen manifestieren.



Systemarchitektur für den sicheren Einsatz von Anwendungen mit gemischter Kritikalität in einem verteilten missionskritischen Edge-Kontext.

Das Problem der Multicore-Interferenzkanäle ergibt sich typischerweise durch eine Mischung aus:

- Time separation – Eine zeitliche Trennung unterstützt durch einen Scheduling-Algorithmus, der Cores über nicht überlappende Zeitintervalle aktivieren kann, oder durch Bandbreiten-Partitionierung für den Zugriff auf gemeinsam genutzte Speicherressourcen.
- Space separation – Räumliche Aufteilung gemeinsam genutzter Ressourcen auf den Cores, um Konflikte um gemeinsam genutzte Ressourcen zu vermeiden oder zu reduzieren.

Eine weitere Anforderung für diese gemischt-kritischen Systeme ist die Virtualisierung. Bei der Hardware-Virtualisierung wird eine Software-Umgebung geschaffen, die die zugrundeliegenden Hardware-Fähigkeiten widerspiegelt, damit Betriebssysteme selbst in einer anderen Hardware-Umgebung als der ursprünglichen laufen können. Die Software-Programme, die solche Fähigkeiten bereitstellen, sind Hypervisoren. Ein Hypervisor abstrahiert die Fähigkeiten der Hardware und ermöglicht die Ausführung mehrerer, potenziell heterogener Betriebssysteminstanzen auf einer einzigen Hardware-Plattform.

Es gibt zwei Haupttypen von Hypervisoren:

- Typ 1 (Bare Metal) – Der ‚Typ 1‘-Hypervisor läuft direkt auf der Hardware und hat die vollständige Kontrolle über die Plattform.
- Typ 2 (gehostet) – Der ‚Typ 2‘-Hypervisor läuft auf einem Host-Betriebssystem und ist für die Steuerung der Hardware vom Host-Betriebssystem abhängig.

Sicherheitsfunktionen auslagern

Für eine hohe Zuverlässigkeit eines Robotersystems muss darauf geachtet werden, verschiedene Systeme voneinander zu isolieren, damit eine Anwendung nicht versehentlich oder absichtlich den Ausfall anderer Systemteile verursachen kann. Effektiv wird für jedes Betriebssystem, das gerade ausgeführt wird, ein isolierter Kontext erstellt. Die zunehmende Zahl von Cyber-Angriffen hat gezeigt: Kann ein Wurm auf ein herkömmliches Betriebssystem zugreifen, so erhält er auch Zugriff auf die ‚Kronjuwelen‘ des Systems. Daher ist der Ansatz von Lynx, die Sicherheitsrichtlinien und Hardware-Berechtigungen in eine separate virtuelle Maschine auszulagern.

Ein Beispiel: Ein Hypervisor weist verantwortlich zu, auf welche Hardware eine bestimmte virtuelle Maschine zugreifen kann. Die Hardware, welche für die Internet-Konnektivität sorgt, kann deswegen keinen Zugriff auf die Netzwerk-Schnittstelle erhalten, die Zugang zu unternehmenskritischen Maschinen ermöglicht.

Sobald diese Konfigurationen definiert sind, müssen sie unveränderbar sein. Es darf keinen Root-Zugriff im System geben, um Dinge zu verändern. In ähnlicher Weise werden andere Systemgeheimnisse so partitioniert, dass nur vertrauenswürdige Anwendungen auf sie zugreifen können. Einige Anwender erstellen Bare-Metal-Anwendungen, um diese Funktionen auszuführen, wobei sie Speicher verwenden, der für andere Anwendungen unzugänglich ist.

Mehr Sinne für Roboter

Ein Weg, wie sich Roboter weiterentwickeln werden, ist die Integration von Sensoren in Industrieroboter. Heute nutzen die Roboter meist nur Vision-Systeme. Gestenerkennung wird zum Teil schon eingesetzt. Bald werden Roboter aber auch andere Sinne nutzen. So werden Roboter in der Lage sein, auf Sprachbefehle zu reagieren und Geräusche zu erkennen, die auf Fehlfunktionen in der Produktionsanlage hinweisen. Denkbar wäre auch, dass sie durch Berührung bestätigen, ob ein bestimmtes Produkt glatt genug ist. Mit Hilfe spezieller Sensorik könnten sie die Mischungen bestimmter Verbindungen ‚geschmacklich‘ testen. Künstliche Intelligenz wird dabei helfen: In Zukunft werden sich die Fähigkeiten der Roboter verbessern, je mehr sie in eine Fabrikumgebung eingebunden werden. Sie werden lernen, Szenarien zu erkennen und darauf zu reagieren.

Viele geplante Cobot-Installationen der nächsten Generation haben eine Verbindung zu einer öffentlichen oder privaten Cloud. Systeme, die sich nur mit lokalen Rechenressourcen verbinden, erhöhen zwar einerseits die Sicherheit, erschweren aber die selbstlernenden Prozesse der KI. Die richtige Balance ist eine Kombination aus lokalem Lernen in Verbindung mit der Nutzung der Skalenerleistung, die durch das in der Cloud akkumulierte, aggregierte Lernen erreicht wird. ag



IAN FERGUSON
ist Vice President Strategic Alliances und Marketing bei Lynx Software Technologies.

Greifer

Kleinteilegreifer-Serie erweitert

Die ‚GEP2000‘-Greifer der Zimmer Group sind eine elektrisch angetriebene Kleinteilegreifer-Serie, die vor allem für Montageaufgaben und das Handling von Kleinteilen konzipiert wurde. Für diese Aufgaben bietet die Serie, die in vier Baugrößen verfügbar ist, einstellbare Greifkräfte zwischen 80 und 500 N und Backenhöhe zwischen 6 und 16 mm. Nun wurde die Serie mit der Umstellung auf -B optimiert und um die Greifer-Variante -03 erweitert. So kommen zu den bisherigen Merkmalen – programmierbare 32 Werkstückdatensätze, Teile-Erkennung (im Bereich von ±0,05 mm) und einstellbare Greifkraft – zwei Funktionen hinzu. *GEP2000-B*-Version verfügt über eine freie Positionierbarkeit, wodurch sich der Hub flexibel an das Werkstück anpassen lässt. Neu ist zudem die Funktion der Werkstückverlustkontrolle: Sollte ein Werkstück durch äußere Einflüsse verloren gehen, erkennt der Greifer dies und informiert die Steuerung. Alle Greifer der Serie sind mit einer integrierten Steuerung und einer mechanischen Selbsthemmung ausgestattet und stehen in drei Ansteuerungsvarianten zur Verfügung.



www.zimmer-group.de

Roboter

7. Achse um die Ecke geführt

Die 7. Achse von Expert-Tünkers kann durch eine Drehstation mit integriertem Drehtisch um eine ‚8. Achse‘ erweitert und damit um die Ecke geführt werden, was die Reichweite und Beweglichkeit von Robotern erweitert. Dank Modulbauweise lassen sich mehrere Achsen mit individuellen Abtriebswinkeln und Längen bis 30 m nach Kundenwunsch kombinieren.



Die Basis besteht aus einem massiven Grundrahmen mit geschliffenen und gehärteten Führungsschienen, die den darauf befindlichen Wagen bewegen. Die Übertragung auf eine zweite Achse erfolgt ebenso reibungslos. Je nach Konfiguration kann die Anlage mittels einer Adapterplatte die gängigen Robotersysteme, Schweißzangen oder andere Handling-Geräte mit einem Gewicht bis 4 t aufnehmen und transportieren. Dies erfolgt mit einer Beschleunigung von 1,5 bis 3,8 m/s² und einer Geschwindigkeit von 1,5 bis 2,5 m/s. Die Anlage lässt sich mit gängigen Robotersystemen und deren Steuerungen verbinden. Eine speziell entwickelte Energiekette sorgt für die Energieversorgung auf der gesamten Strecke, auch bei Integration von Drehstationen.

www.expert-tuenkers.de

A *Computer &* **AUTOMATION**

Sonderheft **SAFETY & SECURITY**

genua.

Künstliche Intelligenz
**KI-Klassifikation für
Safety**

Seite 50

Kollaborative Robotik
**Die Evaluierung der
physischen Sicherheit**

Seite 52

Verschlüsselung
**Schutz für
geistiges Eigentum**

Seite 64

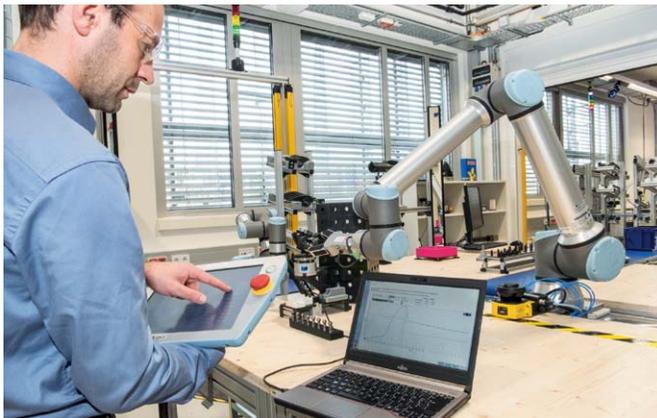


OT Security ist kein Feenstaub



KI-Klassifizierung nach Anwendungslevel

Künstliche Intelligenz in Sicherheitsapplikationen



SAFETY

- 50 KI-Klassifikation für Safety**
Wie KI für Sicherheitsaufgaben verwendet werden kann
- 52 Die Evaluierung der physischen Sicherheit**
Eckdaten für das Zusammenarbeiten von Mensch und Roboter
- 55 Sicherheit für den Einrichtbetrieb**
Die Funktion ‚Sicher begrenzte Geschwindigkeit bei geöffneter Schutztür‘
- 59 Produkte**

Das eigene Know-how schützen

Quellcode sicher verschlüsseln



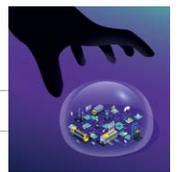
52

Sichere Mensch-Roboter-Kollaboration

Gefahrsituationen erfolgreich vorbeugen

SECURITY

- 60 Titel: OT Security ist kein Feenstaub**
Der Weg zu Cyberresilienz in der Produktion
- 64 Schutz für geistiges Eigentum**
Ideen der Hersteller von KI-Anwendungen wirkungsvoll absichern
- 66 Produkte**



RUBRIKEN

- 49 Editorial**



KI und Sicherheit

Künstliche Intelligenz dringt immer mehr in unseren Alltag ein, sei es in Form einer Benutzeroberfläche wie Alexa oder eines intelligenten Chatbots. Im industriellen Umfeld gilt die Technologie als interessanter Lösungsansatz für verschiedenste Problemstellungen. Doch welche Auswirkungen auf die Sicherheit von Mensch, Maschine oder Anlage hat der Einzug von KI in Produktion und Intralogistik?

Bereits einfache KI-Applikationen stellen eine Herausforderung bei der Nachweisführung zur Sicherheit dar. Daher werden mögliche Vorgehensweisen in den Normungsgremien diskutiert. Ganz am Anfang aber steht die Klassifikation von KI für Sicherheitsaufgaben. Ab *Seite 50* fasst Holger Laible die aktuelle Situation zusammen und stellt ein Klassifikationsschema für KI in Sicherheitsanwendungen vor.

Durch den Einzug von KI in Safety-Applikationen ist der Schutz der Algorithmen von höchster Bedeutung. Häufig nutzen Entwicklerinnen und Entwickler zum Programmieren der ML- und KI-Algorithmen die Programmiersprache Python. Da dieser Quellcode in KI-Applikationen aber als einfache Text-Datei

ausgeliefert wird und daher im Klartext gelesen werden kann, ist er nicht vor Änderungen, Manipulation oder Kopie geschützt. Das geistige Eigentum liegt offen für jedermann da. Wie sich die Software mittels Vorkompilierung und Verschlüsselung sichern lässt, erfahren Sie ab *Seite 64*.

Andrea Gillhuber
Chefredakteurin

PS: Sie sind auf der Suche nach passenden Safety- oder Security-Lösungen? Dann empfehle ich Ihnen unsere interaktiven Marktübersichten. Diese bieten Ihnen den schnellen Überblick über Produkte und Systeme sowie deren Anbieter unter <https://www.computer-automation.de/marktuebersicht/>



Der richtige Zug – mit Sicherheit

Dezentrale Sicherheitstechnik verlagert Personenschutz in die Nähe der Gefahrenstellen und bietet neue Freiheitsgrade für modulare Produktion

TURCK
Your Global Automation Partner

MEHR ERFAHREN



www.turck.de/da-safety

KI-Klassifikation für Safety



Künstliche Intelligenz wird in vielen Bereichen bereits verwendet und gilt als Lösungsansatz für aktuelle Herausforderungen in den verschiedensten Lebensbereichen. Die Politik fördert KI, möchte aber gleichzeitig die Technikfolgen abschätzen und gegebenenfalls regulieren. Nachfolgend wird der Einsatz von KI für Sicherheitsaufgaben betrachtet.

Der Begriff der KI hat sich über die Jahrzehnte seit dem Erstauftreten sehr gewandelt. Wo früher eine geschickte Verschachtelung von ‚if-then-else‘-Statements bereits als KI galt, werden heute Mechanismen wie Machine Learning (ML) oder Knowledge-Graphen verstanden. Verschiedene Gremien haben sich mit dem Thema einer KI-Definition auseinandergesetzt, doch mit einer praktischen Beschreibung überrascht die Wikipedia mit einem interessanten Ansatz: „Meist bezeichnet künstliche Intelligenz den Versuch, bestimmte Entscheidungsstrukturen des Menschen nachzubilden, indem zum Beispiel ein Computer so gebaut und programmiert wird, dass er relativ eigenständig Probleme bearbeiten kann. Oftmals wird damit aber auch eine nachgeahmte Intelligenz bezeichnet, wobei durch meist einfache Algorithmen ein ‚intelligentes Verhalten‘ simuliert werden soll.“

Festzustellen ist, dass es sich im Jahre 2021 bei angewandter Künstlicher Intelligenz immer noch um einen Versuch handelt, bestimmte Entscheidungsstrukturen

nachzubilden, und im konkreten Anwendungsfall sogar nur eine Nachahmung von intelligentem Verhalten sein könnte. Diese Vorzeichen sind für einen Einsatz im sicherheitstechnischen Umfeld (Sicherheit steht in der Folge für das englische Safety und nicht für Security, also Informationssicherheit) eher ungünstig, da dort evidenzbasiert die risikominimierenden Eigenschaften zu bewerten sind. Somit stellt sich beim erstmaligen Einsatz von KI in Sicherheitsapplikationen – wie in anderen Bereichen bei Verwendung neuer Technologie auch – zuerst die Frage nach der Verhältnismäßigkeit.

Diese Überlegungen bedeuten zunächst Stabilität für bestehende Lösungen. Damit erhöht sich allerdings der Druck auf Lösungsansätze mit KI für aktuelle komplexere Problemstellungen (siehe *Bild 1*).

Während es für Sicherheitsfunktionen bisher in der Regel ausreichend war, Schaltzustände, Ströme oder Spannungen auszuwerten, stehen nun Fragen zur Erkennung von verschiedenen Hindernissen im Raum oder gar deren Charakterisierung. Die Zunahme dieser systematischen Komplexi-

tät geht einher mit der Verwendung von Sensoren, wie CCD-Kameras, die bisher nicht sicherheitsgerichtet eingesetzt wurden. Diese erschwerte Aufgabenstellung soll mit KI bewältigt werden, wobei selbst einfache KI-Applikationen eine Herausforderung bei der Nachweisführung zur Sicherheit darstellen. Der Einsatz von KI für einfache Anwendungen, etwa einer Auswertung von sicheren elektronischen Signalen, ist aber hinsichtlich des Marktes und der Forschung weniger attraktiv, auch wenn dies zur Erarbeitung von geeigneten Methoden anfangs angezeigt wäre.

Im Rahmen der Normung werden daher mögliche Vorgehensweisen diskutiert und sollen im technischen Bericht (ISO/IEC TR 5469 der JTC 1/SC 42/WG 3) beschrieben werden.

Klassifikation von KI für Sicherheitsaufgaben

Ausgangspunkt der Betrachtungen bleibt die Risikoanalyse, welche angemessen auf die Gegebenheiten in verschiedenen Einsatzbereichen angewandt werden kann. Zusam-

men mit der vorgeschlagenen Klassifizierung (nach Bild 2) zum sicherheitstechnischen Kontext der KI können gezielt Empfehlungen hinsichtlich der Evaluation zugeordnet werden.

Die KI-Klassifizierung stellt den Kontext des Einsatzes von KI-Methoden/Techniken bezogen auf das E/E/PE-System (electrical and/or electronic and/or programmable electronic system; nach IEC 61508) dar, und zeigt die Bereiche auf, für welche KI nach bestehenden Regeln der Technik begutachtungsfähig ist, oder in denen noch Kriterien und Anforderungen zu erarbeiten sind.

Die Anwendungslevel A bis D sollen bei der Zuordnung von Anforderungen zum jeweiligen Einsatzzweck helfen:

- Die Anwendungslevel C und D verwenden bestehende Sicherheitskonzepte zur Risikoreduktion. Künstliche Intelligenz spielt hier noch keine Rolle.
- Der Anwendungslevel B bezeichnet den Einsatz von KI im Rahmen der Entwicklung von Safety-Systemen.
- Anwendungslevel A steht für den direkten Einsatz von KI in einer Sicherheitsfunktion. Die angefügten Kennzahlen ‚1‘ und ‚2‘ bezeichnen die Entscheidungshoheit der KI, wobei zum Beispiel ‚A1‘ für den direkten Einsatz im sicherheitsrelevanten Hauptkanal und ‚A2‘ für einen indirekten Einsatz, etwa im Rahmen von Diagnosen, steht.

Die KI-Klassen sind nicht technologiebezogen zu sehen, das heißt, bestimmte Techniken wie neuronale Netze oder Machine Learning gehören nicht automatisch in eine bestimmte Klasse:

KI Klasse I bezieht sich beispielsweise auf bestehende klassische Verfahren, ein sicheres ‚intelligentes System‘ zu entwickeln, zum Beispiel nach IEC 61508. Dabei ist der zugrundeliegende Code und dessen Wirkung vollständig nachvollziehbar und für den Entwickler verständlich.

Bei KI Klasse II handelt es sich nun um ein System, welches sich KI-Methoden/Techniken bedient, die nicht in allen Punkten zu vom Menschen nachvollziehbaren Ergebnissen führt, aber es trotzdem durch erweiterte Maßnahmen möglich ist, angemessene Kriterien und Anforderungen zu erfüllen. Diese Kriterien sind noch zu erarbeiten.



Bild 1. Bekannte strukturierte Szenarien für Sicherheitsapplikationen mit KI zu erschließen, wäre der nächste logische Schritt im Rahmen der evolutionären Entwicklung von Technologie. Als Beispiel ist die Objekterkennung bei Fahrzeugen zu nennen.

	KI Klasse I Begutachtung möglich	KI Klasse II Begutachtung teilweise nicht möglich, aber mit zusätzlichen Maßnahmen anwendbar	KI Klasse III Begutachtung nicht ausreichend möglich, zusätzlich Maßnahmen nicht ausreichend
Anwendungslevel A KI im E/E/PE-System zur Diagnose (A2) oder sogar Steuerung (A1)	Bestehende Normen zur risikominimierenden Maßnahmen der Funktionalen Sicherheit können angewandt werden.	Bereich der zu erarbeitenden Kriterien und Anforderungen	Nicht empfohlener Einsatz
Anwendungslevel B1 oder B2 KI in der Entwicklung eines E/E/PE-System als Support Tool (B2) oder sogar Validierungs-Tool (B1)			
Anwendungslevel C KI nicht sicherheitsrelevant, aber mit Rückwirkung			
Anwendungslevel D KI nicht sicherheitsrelevant, ohne Rückwirkung	Bestehende risikominimierende Maßnahmen der Funktionalen Sicherheit können angewandt werden.		

Bild 2. KI-Klassifizierung entsprechend den derzeitigen Normungsprojekten.

Die KI Klasse III liegt außerhalb der Möglichkeiten der Klasse II und ist letztlich nur bei Systemen des Anwendungslevel D einsetzbar, die sich hinsichtlich der Sicherheit nicht auf die KI verlassen müssen.

Der Mensch als intelligente Instanz

Die Tabelle zeigt, dass es durchaus angemessen sein kann, zur Bewertung bestimmter Applikationen bestehende Normen wie die IEC 61508 zu verwenden. Und zwar immer dann, wenn es sich um eher klassische Verfahren von simulierter Intelligenz (KI Klasse I) handelt. Denn was ein Mensch als intelligentes Verhalten eines Systems ansieht, unterliegt ohnehin der Subjektivität und stellt auch die anfangs diskutierte Schwierigkeit bei der Definition von KI dar.

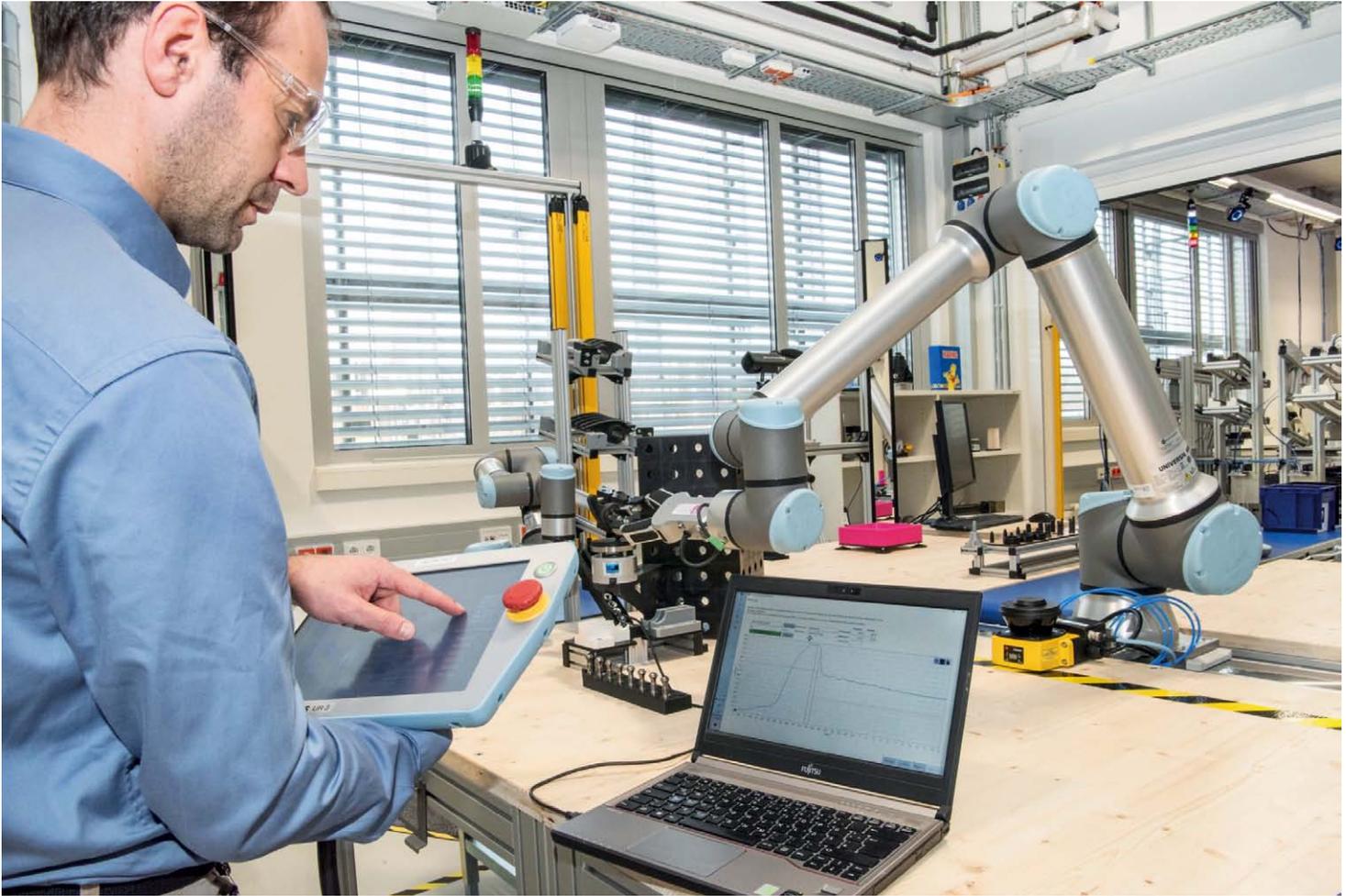
Diese Klassifizierung der KI-Applikationen kann im Rahmen der Risikoanalyse helfen geeignete Räume für den KI-Einsatz, auch im sicherheitstechnischen Zusammenhang, zu eröffnen, wobei der bestehende Stand der Technik berücksichtigt wird. Herausfordernd wird die Erarbeitung konkreter Anforderungen sein, um die KI Klasse II mit geeigneten Methoden für

bestimmte KI-Technologien ausreichend sicherheitstechnisch bewerten zu können.

Abschließend bleibt festzuhalten, dass bei allen Betrachtungen zu KI der Mensch als intelligente Instanz relevant ist, sowohl bei der Definition des Einsatzes und der Auswahl der zugrundeliegenden Daten, als auch bei der Ausarbeitung des KI-Algorithmus selbst. Wäre dies nicht mehr der Fall, wäre der Mensch auch für die weitere Evolution irrelevant geworden. Soweit ist die Entwicklung der KI allerdings noch nicht absehbar, jedoch sind die Auswirkungen der menschlichen Entscheidungen im Rahmen der Entwicklung und des Betriebs der KI deutlich weitreichender, als dies in der Breite wahrgenommen wird. ag



HOLGER LAIBLE
ist Senior Safety Expert bei Siemens.



Die Evaluierung der physischen Sicherheit

Kommen Roboter als kollaborative Assistenzsysteme in einer modernen Produktion zum Einsatz, werden sie ohne Schutzzaun betrieben. Beim Fehlen einer solchen trennenden Schutzeinrichtung spielt die physische Sicherheit für die beteiligten Arbeiterinnen und Arbeiter eine sehr wichtige Rolle.

Für die Digitalisierung und Automatisierung in der Produktion benötigt es moderne Robotersysteme, die ihre Aufgaben nicht nur richtig, sondern auch für

den Menschen gefahrenfrei ausführen. Besonders wichtig wird die Sicherheitsfrage, wenn diese Systeme nicht nur in speziell für Roboter vorgesehenen Produktionsbereichen zum Einsatz kommen, sondern als sogenannte ‚Cobots‘ operieren. Anders als klassische Industrieroboter operieren diese speziell für die Zusammenarbeit mit Menschen entwickelten Roboter mit ebendiesen in einem Arbeitsbereich, um auch gemeinsam Produktionsschritte erledigen zu können. Aufgrund der engen Zusammenarbeit kann nicht ausgeschlossen werden, dass es zu ungewollten physischen Kontakten zwischen Roboter und Mensch kommt.

Um die Sicherheit einer Mensch-Roboter-Kollaboration zu definieren, braucht es

klar strukturierte Regeln. Neben der EG-Maschinenrichtlinie 2006/42/EG definieren harmonisierte Normen und Vorschriften für Robotersicherheit den regulativen Rahmen für ein sicheres Zusammenarbeiten von Menschen und Roboter im industriellen Anwendungskontext – insbesondere die ISO 10218:2011 (Industrieroboter-Sicherheitsanforderungen) und die ISO/TS 15066:2016 (Roboter und Robotikgeräte – Kollaborierende Roboter). Das Besondere bei Cobots sind deren erweiterte Ausstattung mittels zusätzlicher, hochzuverlässiger Sensorik sowie ihre Fähigkeit, sicherheitsbewertete Funktionen realisieren zu können, die über den verpflichtenden Not-Halt hinausgehen. Beispielsweise kann der

Roboter mit einer erhöhten Zuverlässigkeit seine Position und Geschwindigkeit überwachen und begrenzen.

Teil 2 der ISO 10218, der sich mit der Sicherheit von Robotersystemen beschäftigt, beschreibt die relevanten sicherheitstechnischen Maßnahmen für einen kollaborativen Roboterbetrieb. Hierfür werden vier klar umrissene Szenarien für die physische Kollaboration zwischen Menschen und Roboter definiert. Eine vorab festgelegte Aufgabenausführung, die Aktivierung aller erforderlichen Schutzmaßnahmen sowie die Verwendung eines für den kollaborierenden Betrieb konstruierten Roboters (Cobot) stellen die Ausgangsbasis für diese Interaktionsszenarien dar. Die vier Möglichkeiten sind:

- Sicherheitsbewerteter überwachter Halt (und Wiederanlauf)
- Handführung
- Geschwindigkeits- und Abstandsüberwachung
- Leistungs- und Kraftbegrenzung

Für moderne Roboteranwendungen sind vor allem die letzteren zwei Betriebsarten von großem Interesse.

Physische Robotersicherheit und deren Evaluierung

In klassischen Robotersystemen werden bauliche und funktionale Sicherheitsmaßnahmen genutzt, um ein ungewolltes Aufeinandertreffen von Mensch und Roboter zu verhindern. Diese Vorkehrungen sind vor allem dann notwendig, wenn bewegte Teile des Roboters sowie die Roboterumgebung nicht sicherheitsbewertet überwacht werden und diese Objekterfassung zur Kollisionsvermeidung herangezogen wird. Aufgrund der unzureichend verfügbaren sicherheitsbewerteten Sensorik zur validen Umgebungserfassung stößt die Betriebsform ‚Geschwindigkeits- und Abstandsüberwachung‘ momentan noch an ihre Grenzen in der Anwendbarkeit. Dies ist auch einer der Hauptfaktoren, weshalb diese Kollaborationsform meist noch im Laborumfeld im Zuge von Forschungsarbeiten untersucht wird und nur vereinzelt im industriellen Kontext Einsatz findet.

Im Gegensatz dazu stellt die Betriebsart ‚Leistungs- und Kraftbegrenzung‘ aktuell die am weitesten verbreitete kollaborative Betriebsform dar. Wie die Bezeichnung

Das Prüflabor

Das Robotics Evaluation Lab (REL) – <https://rel.joanneum.at/> – ist ein speziell eingerichtetes Mess- und Prüflabor der Joanneum Research Forschungsgesellschaft am Institut Robotics mit Standort Klagenfurt am Wörthersee. In diesem Labor können biofidele Belastungen bei Kontaktsituationen in Roboterapplikationen rückführbar und valide gemessen und bewertet werden. Hierfür werden kalibrierte Messmittel am neuesten Stand der Technik verwendet und der gesamte Prüfprozess unter qualitätssichernden Maßnahmen nach ISO/IEC-17025 durchgeführt. Als erste und einzige Prüfstelle in Europa konnte das Robotics Evaluation Lab die Akkreditierung zur Messung der potenziellen Kraftereinwirkung in der Mensch-Roboter Kollaboration erlangen. Die Prüfungen werden je nach Kundenspezifikation in den Räumlichkeiten des REL oder direkt vor Ort an der Anlage des Kunden durchgeführt. Zudem unterstützt das Prüflabor die Wirtschaft und Industrie mit Dienstleistungen und Services rund um die Themen projektbegleitende Beratungsleistungen, eigenständig durchgeführte Sicherheits- und Risikobeurteilungen sowie kompetenzsteigernde Weiterbildungen im Bereich der Robotersicherheit. Durch die Mitarbeit in nationalen und internationalen Normungsgremien sind die Expertinnen und Experten des Prüfteams über die Entwicklung dieses Themenkomplexes stets am neuesten Stand und können auf Basis ihres praxisrelevanten Know-hows Trends aktiv mitgestalten. Unter dem Motto ‚Safety as a Service‘ werden maßgeschneiderte und praxisorientierte Dienstleistungspakete für den gesamten Entwurfs- und Lebenszyklus von Roboteranlagen angeboten.

schon gut beschreibt, werden dabei die Leistungsparameter der elektrischen Antriebe in den Roboterjunkten sowie die Sensitivität der Regelung in Form einer Kraftbegrenzung derart eingestellt, dass im Fall einer Mensch-Roboter-Kontaktsituation die vom Roboter zum Mensch übertragene Stoßenergie unterhalb der normativen Vorgaben liegt.

Identifikation potenzieller Gefahrensituationen

Als erster Schritt müssen also potenziell gefahrbringende Kontaktsituationen im Rahmen der bestimmungsgemäßen Verwendung des Robotersystems sowie bei vorhersehbarer Fehlanwendung in einer entsprechenden Risikobeurteilung identifiziert werden. Dabei sind die Mindestvorga-

Funktionale Sicherheit – Wireless Safety

Bidirektionales sicherheitsgerichtetes Funksystem



Funk-Sicherheits-system UH 6900

SAFEMASTER W

- Übertragung von Not-Halt und Steuerfunktionen
- Für Sicherheitsanwendungen bis Kat. 4 / PL e
- Hohe Verfügbarkeit bei großer Reichweite bis 800 m
- Zweikanalige Sicherheitseingänge und -ausgänge



Die Robotics Hands-on Area ist eine modular aufgebaute Test- und Verifikationsplattform, in der unterschiedlichste industrielle Anwendungsfälle nachgestellt sowie deren physische Sicherheit nachgewiesen werden kann.

ben der Maschinenrichtlinie sowie die Grundsätze der Normen ISO 12100 und ISO 10218 einzuhalten. Identifizierte mechanische Gefährdungen können in Form von Quetsch- oder freien Stoßsituationen auftreten. Bei Quetschsituationen – sogenanntem quasistatischen Kontakt – wird ein Körperteil (zum Beispiel Hand oder Arm) zwischen einem bewegten Roboterteil und einem starren Umgebungsobjekt eingeklemmt. Bei freien Stoßsituationen – dem sogenannten transienten Kontakt – ist die Belastung nur von kurzer Dauer, da das am Stoß beteiligte menschliche Körperteil (zum Beispiel Schulter) zurückweichen kann.

Laut den Anforderungen der Sicherheitsnorm für kollaborative Robotik ISO/TS 15066 müssen genau diese beiden Belastungsarten – also ein quasistatischer Belastungswert für den Fall einer Klemmung und ein transienter Belastungswert für den Fall einer Stoßbelastung – für die laut Risikobeurteilung gefahrbringenden physischen Kontaktsituationen evaluiert werden.

Für die Evaluierung einer Mensch-Roboter-Kontaktbelastung müssen sowohl die Kontaktkraft als auch der zugehörige Kontaktdruckwert erfasst werden. Die Norm ISO/TS 15066 enthält für eine Kon-

formitätsbewertung eine Vergleichstabelle mit aus entsprechenden Studien ermittelten Grenzwerten für den menschlichen Schmerzeintritt bei Kraft- und Druckbelastung an unterschiedlichen Körperstellen. Die gemessenen quasistatischen beziehungsweise transienten Kraft- und Druckwerte werden unter Berücksichtigung der Messunsicherheit mit diesen Vorgaben verglichen. Werden die Grenzwerte überschritten, müssen risikomindernde Maßnahmen getroffen werden. Im Fall einer zu hohen Kraftbelastung sind dies typischerweise eine Reduktion der Bewegungsgeschwindigkeit oder eine Erhöhung der Robotersensitivität bezüglich des Abschaltverhaltens bei zu hoher Drehmomentbelastung der Gelenkantriebe. Bei zu hoher Druckbelastung führt meist eine bauliche Modifikation des Roboterwerkzeuges oder einer Werkstückhalterung zur Erhöhung der Kontaktfläche zum Erreichen der geforderten Grenzwerte – etwa durch das Abrunden oder Polstern von scharfen Kanten.

Messtechnische Verifikation

Während der Entwurfsphase können für den Nachweis der physischen Robotersicherheit, also der Konformität von potenziellen transienten und quasistatischen

Kontaktbelastungen, rechnergestützte Werkzeuge wie Simulation, virtuelle Inbetriebnahme und digitale Abbilder der Anlage einen wertvollen Beitrag leisten. Aber: Derzeit kann noch keine Simulationssoftware eine messtechnische Evaluierung direkt an der realisierten kollaborativen Roboteranlage ersetzen. Zudem ist diese messtechnische Untersuchung unerlässlich, um die Gewissheit zu liefern, ob es sich um ein zuverlässiges und somit sicheres Verhalten des Robotersystems handelt.

Bei der messtechnischen Verifikation werden potenzielle Kollisionen von Mensch und Roboter im Sinne eines zerstörungsfreien Crash-Tests mittels einer sogenannten biofidelen Messanordnung untersucht. Biofidel bedeutet, dass die Messgeräte (Kraft- und Druckmessinstrument) so ausgestattet werden, dass die Nachgiebigkeitseigenschaften der am Kontakt beteiligten Körperstelle technisch nachgebildet werden. Realisiert wird dies über eine Kombination aus Stahlfedern und Dämpfungselementen aus Kunststoff. Anschließend wird die Messanordnung entsprechend im Arbeitsraum des Roboters positioniert und die zu evaluierende Kontaktsituation durch die Ausführung des entsprechenden Steuerprogramms herbeigeführt. Dabei werden Kraft- und Druckbelastungen ermittelt sowie deren Konformitätsbewertung gegenüber normativen Vorgaben, wie oben beschrieben, durchgeführt. Um die Validität der Ergebnisse zu garantieren, sollen qualitätssichernde Maßnahmen nach ISO 17025 (Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien) eingehalten werden. Dies umfasst zyklische und akkreditierte Kalibrierungen von Messmitteln, Eignungsprüfungen und Teilnahme an Ringversuchen, adäquate Dokumentation von Mess-Ergebnissen in Prüfberichten und die Abhandlung von Prüfprojekten durch ein geeignetes QM-System. *ik*



MICHAEL RATHMAIR

ist Leiter der Kompetenzgruppe Robotics Evaluation Lab bei der Joanneum Research Forschungsgesellschaft in Klagenfurt, Österreich.

Sicherheit für den Einrichtbetrieb



Für den Einrichtbetrieb oder die Störungsbeseitigung an Maschinen ist die Sicherheitsfunktion ‚Sicher begrenzte Geschwindigkeit bei geöffneter Schutztür‘ relevant. Nachfolgend eine exemplarische Sicherheitslösung mit redundantem Drehgeber und Sicherheitssteuerung.

Bei größeren Maschinen oder Anlagen – zum Beispiel in der Verpackungsindustrie – ist der Bediener in der Regel durch einen Schutzzaun oder eine Umhausung vor gefährlichen Bewegungen geschützt. Ein Zugang zum Gefahrenbereich ist über eine Tür möglich. Unter dem Gesichtspunkt der Maschinensicherheit muss dabei neben den Sicherheitsfunktionen ‚Schutz vor unerwartetem Anlauf‘ und ‚Stillsetzen über Not-Halt-Einrichtung‘ oft eine weitere Sicherheitsfunktion gewährleistet sein: die ‚sicher begrenzte Geschwindigkeit (SLS) bei geöffneter Schutztür‘. Die SLS-Funktion vereinfacht es für den Bediener, eine Fertigungsanlage einzurichten oder eine Störungsbeseitigung durchzuführen.

Ein aktuelles Whitepaper von Schmersal und Wachendorff stellt eine exemplarische Sicherheitslösung für eine solche Anlage vor, zu der unter anderem ein redundanter Drehgeber sowie eine Sicherheitskleinsteuerung gehören, und gibt eine Hilfestellung für die Bewertung der sicherheitstechnischen

tauglichkeit dieser Lösung. Um das geforderte Sicherheitsniveau zu bestimmen und zu belegen, wird bei diesem Beispiel die Normenreihe EN ISO 13849 angewendet. Für die betrachtete Maschine hat die Risikobewertung einen Performance Level (PLr) von d ergeben. Dieser lässt sich auf verschiedene Arten umsetzen. Für die technische Realisierung bietet sich zumeist die Kategorie 3 an. Sie fordert eine Einfehlersicherheit, die typischerweise durch eine konsequent zweikanalige Auslegung erreicht wird.

Zur Messung der Geschwindigkeit bietet sich die Verwendung eines Drehgebers an. Neben dem Drehgeber, der Auswertelogik – etwa der Sicherheitssteuerung ‚PSC1‘ von Schmersal – und dem Antrieb selbst muss meistens die Überwachung der Schutztür in die Betrachtung einfließen, da die SLS-Funktion im Allgemeinen mit dieser Schutztür aktiviert wird.

In dieser Struktur ist insbesondere die Betrachtung des Drehgebers zur Geschwindigkeitserfassung relevant.

Am einfachsten ließe sich die geforderte Zweikanaligkeit durch zwei separate Geber realisieren, die an verschiedenen Stellen montiert sein müssten, um auch mechanisch zweikanalig zu sein. Allerdings gestaltet sich dies in der Praxis oft aufwendig und schwierig. Praktikabler ist es, nur eine Montageposition verwenden zu müssen. Der Drehgeber der Firma Wachendorff vereint diese beiden Eigenschaften: Er besteht aus zwei voneinander vollständig unabhängigen Gebern unterschiedlicher Technologien in einem Gehäuse. Neben der dadurch vereinfachten Montage erlaubt es die interne Redundanz zudem, die Anforderungen der Kategorie 3 zu erfüllen.

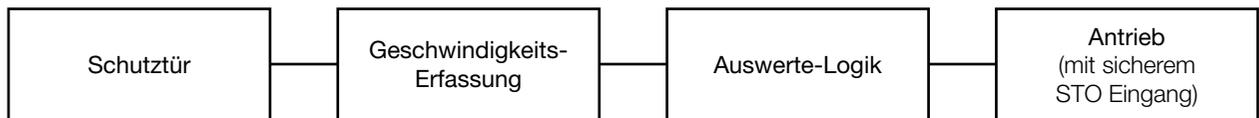
Fernstudium SPS

Nach IEC 61131. Inkl. STEP 7, TIA-Portal, CODESYS

FERNSCHULE WEBER

Tel. 0 44 87 / 263 - Abt: D73

www.fernschule-weber.de



Eine exemplarische Struktur der Sicherheitsfunktion: Neben dem Drehgeber zur Erfassung der Geschwindigkeit, der Auswertelogik, wie zum Beispiel der Sicherheitssteuerung ‚PSC1‘ von Schmersal, und dem Antrieb selbst muss zumeist auch die Überwachung der Schutztür mit in die Betrachtung einfließen, da die SLS-Funktion im Allgemeinen mit dieser aktiviert wird.

Der redundante Drehgeber

Ein redundanter Drehgeber besteht im Grundsatz aus zwei komplett autarken Standard-Drehgebern, wodurch der gesamte elektronische Teil des Drehgebers als zweikanaliges System zu betrachten ist. Einzig der mechanische Aufbau, bestehend aus Welle und Lagerpaket, ist einkanalig ausgeführt. Die Norm für elektrische Antriebe EN 61800-5-2 sieht die Betrachtung des Fehlerfalls durch das Lösen der mechanischen Verbindung zwischen Drehgeber und Antrieb vor. In vielen Fällen wird ein Fehlerausschluss benötigt, da die Steuerung einen derartigen Fehler nicht zwingend aufdecken kann. Dieser Fehlerausschluss lässt sich erreichen, indem die Anbauelemente entsprechend stark dimensioniert ausgelegt werden und eine 100 % zuverlässige mechanische Verbindung genutzt wird.

Die Drehgeber von Wachendorff setzen auf das Prinzip der Diversität. Dies bedeutet, dass gezielt die Ausfallsicherheit erhöht wird, indem verschiedene Messprinzipien eingesetzt und dadurch so wenig baugleiche Komponenten verwendet werden wie möglich. Grundgedanke dabei ist, dass die unterschiedlichen Sensorik-Plattformen auch verschieden empfindlich beziehungsweise unempfindlich auf Störungen jeglicher Art reagieren und dadurch nicht zeitgleich ausfallen, sodass die nachgeschaltete Elektronik diesen möglichen Ausfall sicher erkennen kann.

Der redundante Standarddrehgeber stellt diversitäre (magnetisch und optisch) Signale zur Verfügung, die vollständig unabhängig voneinander erzeugt werden, aber dennoch in Korrelation zueinander gebracht werden können. Selbst die Versorgungsspannung ist für jede Sensoreinheit separat vorhanden.

Subsystem ‚Geschwindigkeitserfassung‘

Die von Kategorie 3 geforderte Einfehler-sicherheit ist durch die durchgängige Zweikanaligkeit der Geschwindigkeits-/Rich-

tungserfassung im Drehgeber gegeben. Die ebenso geforderte Fehleraufdeckung (DC) ist nicht in den Geber integriert, muss also in der Auswertelogik erfolgen.

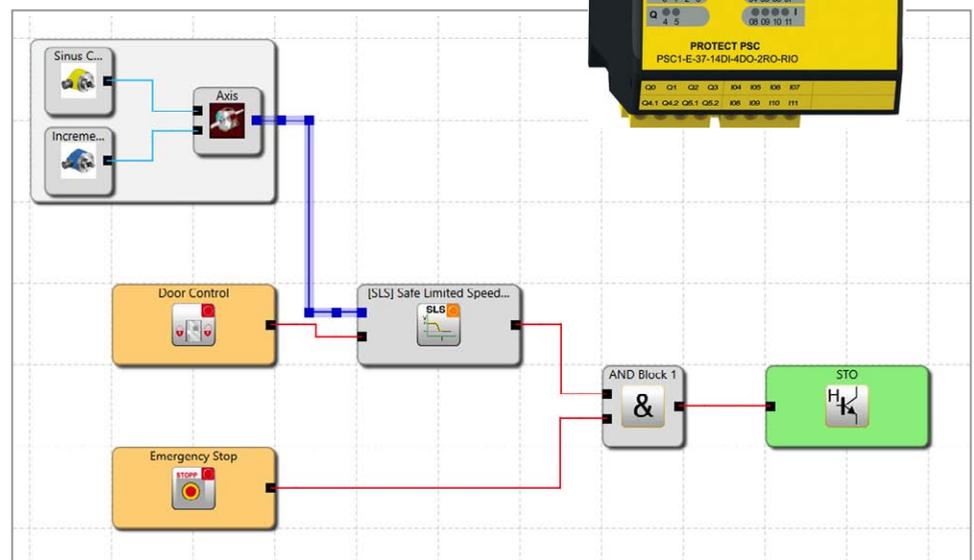
Exemplarisch steht hier die Sicherheitssteuerungs-Reihe ‚PSC1‘ von Schmersal. Mit ihr können – wenn es die Applikation erfordert – bis zu zwölf Achsen sicher überwacht werden. Hierbei lassen sich die Drehgeber einfach über D-Sub-Schnittstellen anschließen. Durch Kreuzvergleich der beiden Gebersignale oder im Fall von sin-cos-Gebern durch Auswertung der Relation $\sin^2 + \cos^2 = 1$ werden auftretende Fehler erkannt und eine Fehlerreaktion eingeleitet. Zudem sind im Programmierool ‚SafePLC2‘ der ‚PSC1‘ bereits Funktions-

blöcke für die wichtigsten Überwachungsfunktionen entsprechend der DIN EN 61800-5-2 vorhanden, beispielsweise SLS, SOS (Safe Operating Stop) oder SCA (Safe Cam, sichere Positionsüberwachung). Diese lassen sich einfach in das Programm der Sicherheitslogik integrieren.

Fehlerausschluss

Besondere Aufmerksamkeit gilt der mechanischen Kopplung zwischen Geber und Antrieb, die prinzipbedingt nur einkanalig ausgeführt ist. Dies macht einen Fehlerausschluss auf Versagen dieser Verbindung notwendig, da hier bereits der einzelne Fehler eine gefährliche Situation herbeiführen würde.

Die Sicherheitsteuerung PSC1 und die Programmierung der Anwendung in SafePLC2. Die Kategorie 3 fordert unter anderem Fehleraufdeckung (DC). Diese erfolgt in dem beschriebenen Beispiel über die Sicherheitsteuerung ‚PSC1‘. Im Programmierool ‚SafePLC2‘ der ‚PSC1‘ sind bereits Funktionsblöcke für die wichtigsten Überwachungsfunktionen integriert und aufgrund der einfachen Programmierung wird die Wahrscheinlichkeit von Fehlern minimiert.



Neben einem Nachweis der maximalen Belastbarkeit der Verbindung fordert die Norm EN ISO 13849, dass für diesen Fehlerausschluss eine FMEA (Fehlermöglichkeits- und -Einflussanalyse) durchgeführt wird.

Zu den weiteren Aspekten, die gemäß EN ISO 13849 zur Erfüllung der Kategorie 3 notwendig sind, zählen Maßnahmen zur Vermeidung von Ausfällen gemeinsamer Ursache (CCF Common Cause Failure), die Vermeidung systematischer Ausfälle in der Software der Sicherheitskleinsteuerung, die Berechnung einer Ausfallwahrscheinlichkeit der Steuerungslösung auf Basis von MTTFD-Werten (Mean time to failure dangerous) und/oder eine höherwertige Diagnose (DC – Diagnostic Coverage). Unter Einbeziehung dieser Aspekte wird im Whitepaper schließlich der Performance Level für diese exemplarische Sicherheitslösung berechnet. Siehe dazu auch:

<https://bit.ly/2R7hqiN>

Mit der beschriebenen Struktur lässt sich ein Performance Level von d erreichen. Begrenzt wird der mögliche PL in der Beispielrechnung im Wesentlichen durch den PL des Frequenzumrichters. Trotz des teilweisen Einsatzes von Standardkomponenten ist es also möglich, ein hohes Sicherheitsniveau zu erzielen. Die Verwendung des redundanten Gebers erleichtert die Montage. Und in Verbindung mit der Sicherheitskleinsteuerung ‚PSC1‘ ist auch die Realisierung weiterer Sicherheitsfunktionen wie Not-Halt oder die Überwachung weiterer Sicherheitskreise mit nur einem Gerät möglich. ik



CHRISTIAN LUMPE

ist Produktmanager Steuerungen bei der Schmersal Gruppe in Wuppertal.



STEFFEN NEGELI

ist Produktmanager und Mitarbeiter im technischen Vertrieb bei Wachendorff Automation in Geisenheim.

STORMSHIELD



STORMSHIELD

Konrad-Zuse-Platz 8

D-81829 München

Germany

Tel. +49 89 8091 3578 – 0

dach@stormshield.eu

Firmenprofil / Firmenausrichtung

Stormshield ist ein europäisches, auf Cybersicherheit für kritische Infrastrukturen und Daten spezialisiertes Unternehmen des Airbus-Konzerns. Mit den über zwanzig Jahren Erfahrung in der Entwicklung von einander ergänzenden Lösungen zur Absicherung von Unternehmens- und Industrietzwerken (Stormshield Network Security), Arbeitsplätzen und Servern (Stormshield Endpoint Security) und Daten (Stormshield Data Security) verfolgt der Hersteller einen ganzheitlichen, kollaborativen Security-Ansatz zum erfolgreichen Schutz von sensiblen IT- und OT-Infrastrukturen auch gegen unbekannte Bedrohungen.

Die Cybersicherheitslösungen von Stormshield sind nach den höchsten europäischen Standards zertifiziert (EU RESTRICTED, NATO, ANSSI EAL3+/EAL4+) und werden über ein solides Partnernetz in über 40 Ländern weltweit vertrieben. Die innovativen, verhaltensbasierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und sichern strategische Informationen von Unternehmen aller Größen, sowie Behörden und militärischen Organisationen weltweit ab. Die Netzwerksicherheitslösungen für die Industrie sind speziell darauf ausgelegt, die IT/OT-Konvergenz zu fördern und beide Umgebungen zu schützen. Die Industrie-Firewalls sind in der Lage, in Echtzeit die Legitimität von Informationen und Befehlen zu überprüfen, die von Steuerungssystemen direkt an Maschinen gesendet und sowohl über IT- als auch Industrieprotokolle übertragen werden. Jedes abnormale Verhalten im Datenfluss, das auf eine mögliche Manipulation der Befehle oder auf einen Cyberangriff hinweist, wird in Echtzeit signalisiert und/oder blockiert.

Impresum

Anschrift des Verlages

WEKA FACHMEDIEN GmbH
Richard-Reitzner-Allee 2
85540 Haar
Telefon: 089.255 56 - 10 00
Telefax: 089.255 56 - 16 70
www.weka-fachmedien.de

Redaktion

redaktion@computer-automation.de

Assistenz

Simone Schiller
Telefon: 089.255 56 - 10 84
E-Mail: SSchiller@weka-fachmedien.de
www.weka-fachmedien.de

Chefredakteur/in

Dipl.-Ing. (FH) Andrea Gillhuber (ag) verantw.
Telefon: 089.255 56 - 10 39
E-Mail: AGillhuber@weka-fachmedien.de

Senior Advisory Editor

Dipl.-Ing. (FH) Meinrad Happacher (hap)
Telefon: 089.255 56 - 10 85
E-Mail: MHappacher@weka-fachmedien.de

Chefin vom Dienst

Elisabeth Skowronek
Telefon: 089.255 56 - 13 34
E-Mail: ESkowronek@weka-fachmedien.de

Redaktion

Inka Kruschke M.A. (ik)
Telefon: 089.255 56 - 13 73
E-Mail: IKruschke@weka-fachmedien.de

Freier Mitarbeiter

Dipl.-Ing. (Univ.) Peter Stiefenhöfer (ps)

Herstellung/Leitung

Marion Stephan, 089.255 56 - 14 42

Herstellung/Sonderdrucke

Andreas Hofner
Telefon: 089.255 56 - 14 50
E-Mail: AHofner@wekanet.de

Urheberrechte

Die in der Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Alle Rechte, insbesondere das der Übersetzung in fremde Sprachen, vorbehalten. Kein Teil dieser Zeitschrift darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form – durch Fotokopie, Mikrofilm oder andere Verfahren – reproduziert oder in eine von Maschinen, insbesondere von Datenverarbeitungsanlagen, verwendbare Sprache übertragen werden. Auch die Rechte der Wiedergabe durch Vortrag, Funk- oder Fernsehendung, im Magnettonverfahren oder ähnlichem Wege bleiben vorbehalten. Fotokopien für den persönlichen und sonstigen eigenen Gebrauch dürfen nur von einzelnen Beiträgen oder Teilen daraus als Einzelkopien hergestellt werden. Der Autor erklärt mit der Einreichung, dass eingereichte Materialien frei sind von Rechten Dritter. Eine Haftung für die Richtigkeit der Veröffentlichung kann trotz sorgfältiger Prüfung durch die Redaktion vom Verlag nicht übernommen werden. Für unverlangt eingesandte Manuskripte, Fotos, Grafiken und Datenträger wird keine Haftung übernommen, Rücksendung erfolgt nicht. Die Zustimmung zum Abdruck wird vorausgesetzt.

Printed in Germany. Imprimé en Allemagne.
© 2021 für alle Beiträge bei WEKA FACHMEDIEN GmbH

Verlagsleitung

Peter Eberhard

Sales Director

Tiffany Dinges verantw. 089.255 56 - 13 63
E-Mail: tdinges@weka-fachmedien.de

Key Account Manager

Christine Gässler 089.255 56 - 13 08
E-Mail: cgaessler@weka-fachmedien.de

Mediaberatung

Andreas Zepf 089.255 56 - 13 64
E-Mail: azepl@weka-fachmedien.de

Disposition

Nadine Ziegler 089.255 56 - 14 73
DISPO.ComputerundAutomation@wekanet.de
Anzeigenpreise nach Preisliste vom 1. 1. 2021
Media-Information auf Anforderung

Druck L.N. Schaffrath GmbH & Co. KG
Marktweg 42-50, 47608 Geldern

Vertriebsleitung

Marc Schneider (089.255 56 - 15 09)
E-Mail: mschneider@weka-fachmedien.de

Bestell- und Abonnement-Service

WEKA FACHMEDIEN GmbH
c/o Zenit Pressevertrieb GmbH
Postfach 810640, 70523 Stuttgart, Tel. 0711.7252.210
E-Mail: abo@weka-fachmedien.de

Erscheinungsweise: 12 Ausgaben

Jahresabonnement Print Inland

78,40 €, davon 49,00 € Heft, 29,40 € Versand

Jahresabonnement Print Ausland

88,60 €, davon 49,00 € Heft, 39,60 € Versand

Einzelausgabe Print

7,50 €, zzgl. 3,00 € Versand
Preise jeweils inkl. der aktuellen MwSt.

Jahresbezug digitales E-Paper

(Inland/Ausland) 24,99 €
inkl. der aktuellen MwSt., ohne Versandkosten

Einzelausgabe digitales E-Paper

(Inland/Ausland) 2,99 €
inkl. der aktuellen MwSt., ohne Versandkosten

Geschäftsführung

Kurt Skupin, Matthäus Hose

ISSN 1615-8512

Vertriebskennzeichen B 49163

VERLAGSVERTRETUNGEN

Benelux, Skandinavien, Frankreich:
Huson International Media, Kingsfordweg 151,
1043 GR Amsterdam, The Netherlands
Tel. +31.20.491.77.44, Fax +31.20.491.77.45
Great Britain: Huson European Media, Mr. Gerald
Rhoades-Brown, Cambridge House,
8 Gogmore Lane, Chertsey, Surrey, KT16 9AP,
phone: +44 (0) 1932.564.999,
fax: +44 (0) 1932.564.998
USA: Huson European Media, Mr. Ralph Lockwood,
Pruneyard Towers, 1999 South Bascom Avenue,
Suite 510, Campbell, CA 95008,
Tel. 1.408.879.66.66, Fax 1.408.879.66.69



Inserentenverzeichnis

A Analog Devices GmbH www.analog.com 1	K Kontron Europe GmbH www.kontron.com 26
B Beckhoff Automation GmbH & Co. KG www.beckhoff.com 13	N NetModule AG www.netmodule.com 24
C Christ Electronic Systems GmbH www.christ-es.de 26	S Schurter AG www.schurter.ch 25
D Digi-Key Electronics www.digikey.de 2	SEW-EURODRIVE GmbH & Co. KG www.sew-eurodrive.de 17
E E.Dold & Söhne GmbH & Co. KG www.dold.com 53	Spectra GmbH & Co. KG www.spectra.de 27
ESCHA GmbH & Co. KG www.escha.de 5	spstiger UG www.spstiger.de 26
F Fernschule Weber www.fernschule-weber.de 55	STEGO Elektrotechnik GmbH www.stego.de 7
Fiessler Elektronik GmbH & Co. KG www.fiessler.de 59	Stormshield www.stormshield.com 57
G CARLO GAVAZZI GmbH www.gavazzi.de 24	T TR-Electronic GmbH www.tr-electronic.de 11
genua GmbH www.genua.de 47	Hans TURCK GmbH & Co. KG www.turck.com 49
H HMS Industrial Networks GmbH www.hms-networks.de 24	W Wachendorff Prozesstechnik GmbH & Co. KG www.wachendorff-prozess- technik.de 27
I Indu-Sol GmbH www.indu-sol.com 24	Weidmüller GmbH & Co. KG www.weidmueller.de 9
	WEKA FACHMEDIEN GmbH www.weka-fachmedien.de 30, 40
	Z Ziehl-Abegg SE www.ziehl-abegg.de 68

Abonnementbestellung

Bitte ausschneiden und einsenden an: WEKA FACHMEDIEN GmbH, c/o Zenit Pressevertrieb GmbH, Postfach 81 06 40, 70523 Stuttgart, Tel. 0711.7252.210 oder per Fax an: 0711.7252.333
Ich bestelle Computer&AUTOMATION mit 12 Ausgaben jährlich zum Preis von z. Zt. 78,40 Euro inkl. 7 % MwSt. im Inland. Auslandspreis 88,60 Euro. Ich kann jederzeit kündigen.
Geld für bezahlte, aber noch nicht gelieferte Ausgaben erhalte ich zurück.

A015

_____	_____
Firma	PLZ, Ort
_____	_____
Name, Vorname	Telefon*
_____	_____
Abteilung	Beruf
_____	_____
_____	_____
Straße, Nr.	E-Mail*

- Ich bin damit einverstanden, dass die zu entrichtenden Abonnementgebühren
- vierteljährlich halbjährlich jährlich von meinem Konto abgebucht werden.

Kontonummer BLZ Kreditinstitut

Datum, Unterschrift

Ein gesetzliches Widerrufsrecht besteht nicht (§§ 505, 491 Abs. 2 Nr. 1 BGB).
WEKA FACHMEDIEN GmbH, Richard-Reitzner-Allee 2, 85540 Haar, HRB 119806 Amtsgericht München
Hinweis: Ihre Daten werden von uns zur Durchführung des Vertrages und für Direktmarketingzwecke
verarbeitet und genutzt. Mit dem Ausfüllen stimme ich dem Erhalt von Serviceangeboten zu.
Die Zustimmung kann jederzeit durch Löschung der Kommunikationsdaten widerrufen werden.
* (Diese Angaben sind freiwillig.)

Die nächste Ausgabe der

Computer & AUTOMATION

erscheint am

20.07.2021

Anzeigenschluss: 24.06.2021



Seilzugschalter

Sicherer Halt fürs laufende Band

Für die Absicherung von Förderanlagen und Maschinen erweitert Pilz die Produktfamilie der Positions- und Näherungsschalter um den kompakten Seilzugschalter *PSENRope mini*.

Die platzsparende Variante des Seilzugschalters ‚PSENRope‘ ermöglicht die Abschaltung von Funktionsprozessen per manueller Betätigung. Die mechanische Not-Halt-Funktion bei ‚PSENRope mini‘ lässt sich sowohl am integrierten Not-Halt-Taster als auch an jedem Punkt durch Ziehen des Seiles auslösen. Durch die Seillänge von bis zu 30 m können auch ausgedehnte Anwendungen mit nur einem Seilzugschalter bedient und abgesichert werden. Die Varianten des Seilzugschalters mit geradem oder gewinkelten Kopf tragen zu einer flexiblen Montage bei. Muss aufgrund des Maschinendesigns verdeckt eingebaut werden, kommt die Variante mit integriertem Reset-Taster zum Einsatz.



Das robuste Metall- oder Kunststoffgehäuse nach IP67 macht den Seilzugschalter sowohl für Indoor- als auch Outdoor-Anwendungen mit Umgebungstemperaturen von -30 bis +75 °C geeignet.

www.pilz.com

Sicherheits-Drehgeber

Erfüllen SIL 2 und PL d

Der TRK38 von TWK ist ein Singleturn-Magnet-Drehgeber, der mit Blick auf sicherheitsgerichtete Anwendungen entwickelt wurde. Mit einem Durchmesser von nur 38 mm und einer Länge von ebenfalls 38 mm eignet sich der Sensor für die Montage in beengten Bauräumen; er wiegt circa 60 g. Der Safety-Drehgeber erfasst Position und Geschwindigkeit und erfüllt dabei die Anforderungen von SIL 2 (IEC 61508) und PL d (EN 13849). Die sicherheitsgerichteten Signale werden über eine zertifizierte Ethercat-FSoE-Schnittstelle übertragen. Die Positionsauflösung beträgt 16 Bit pro Umdrehung. Über die Ethercat-FSoE-Schnittstelle erfolgt die Übertragung der sicherheitsgerichteten Signale

an die übergeordnete Steuerung beziehungsweise an ein Sicherheitsrelais sowie die Programmierung des Sensors.

Dank dem Aluminiumgehäuse sowie dem gesamten Design arbeitet der Sensor selbst unter ungünstigen Bedingungen wie Vibrations- und Stoßbelastungen.



www.twk.de

Servoantriebe

TÜV-zertifizierte Sicherheit

Synapticon bietet hochkompakte Servo Drives, deren Sicherheit vom TÜV Süd zertifiziert ist. Das jüngste TÜV-Zertifikat bestätigt die funktionelle Sicherheit hinsichtlich STO (Safe Torque Off) und SBC (Safe Brake Control) der *Circulo*-Serie. ‚Circulo‘ ist die aktuellste Klasse der ‚Somanet‘-Reihe. Bei diesen ‚Integrated Motion Devices‘ handelt es sich um komplette Servo-Drive-Lösungen für die Integration am ‚Point of Motion‘. Mit ihrer kreisrunden Form und großen Hohlwellen-Durchmessern von 20 bis 40 mm eignet sich die ‚Somanet Circulo‘-Serie insbesondere für vollintegrierte Achsen, wie sie zum Beispiel bei Cobots, Servicerobotern oder Radnabenantrieben von AGVs zum Einsatz kommen.

Zunächst sind zwei Varianten verfügbar: ‚Circulo 7‘ und ‚Circulo 9‘, die sich durch Größe und Leistung unterscheiden. Beide sind für den Spannungsbereich bis 60 V ausgelegt. Die Servoantriebe verfügen über integrierte Encoder (19 bis 20 Bit) mit einer Multiturn-Option und besonderen Kalibrierungsfunktionen, die die Genauigkeit erhöhen.

www.synapticon.com

produktanzeige

Fiessler Elektronik GmbH & Co.KG

Complete Safety Solutions
FISSLER ELEKTRONIK

unsere Erfahrung für Ihre Sicherheit

ULVT - ULCT
Sicherheits - Lichtvorhänge
Kat. 2 - 4 - PLd - SIL 3



- innovative Sicherheitstechnik
- weitweitere Kunden- und Vertriebservice
- individuelle Kundenlösungen

- große Reichweite bis 60 m
- mit integriertem Schaltgerät
- programmierbare Ausblendfunktion
- montagefreundlich

- Sicherheits-Sensoren
- Sicherheits-Steuerungen
- Sicherheits-Dienstleistungen
- Sensoren für die Fördertechnik
- Steuern, Messen und Regeln

AKAS
Abkantpressenabsicherung



- innovativer Fingerschutz durch Laser-optisches Sicherheitslichtgitter
- Betrieb durch Fußtaster
- innovative Sicherheitstechnologie

NEU FMSC
Sicherheitssteuerung modular und konfigurierbar



- einfachste Programmierung
- kürzeste Reaktionszeiten
- Online-Diagnose
- erweiterbar mit bis zu 17 Modulen
- max 204 Eingänge / 153 Ausgänge
- bis zu 17 Achsen sicher überwachbar

Buchenteich 14 • D - 73773 Aichwald

Tel.: +49-(0)711 91 96 97-0

Fax: +49-(0)711 91 96 97-50

<http://www.fiessler.de> • info@fiessler.de

FISSLER
ELEKTRONIK



OT Security ist kein Feenstaub

Für die Cybersecurity von vernetzten Produktionsumgebungen besteht angesichts der volatilen Bedrohungslage dringender Handlungsbedarf. Eine zeitgemäße Strategie für OT Security kombiniert Regeln, Verfahren und Maßnahmen mit dem Defense-in-Depth-Prinzip und KI-gestützter Angriffserkennung – und berücksichtigt die wichtigsten OT-Security-Schutzziele von Anfang an.

Die zunehmende Vernetzung von Maschinen, Anlagen, industriellen Steuerungssystemen sowie Automatisierungslösungen hebt die bisherige physische Trennung der OT (Operational Technology) von anderen IT-Systemen auf. Für den Schutz der jetzt potenziell auch von außen angreifbaren OT-Netze sind klas-

sische IT-Security-Lösungen oft nicht anwendbar. Häufig wird ein wirksamer Schutz durch veraltete Betriebssysteme, nicht erwünschte Eingriffe in laufende Prozesse, nicht umsetzbare Sicherheits-Updates oder nachträgliche Härtungsmaßnahmen verhindert. Jeder zweite erfolgreiche Angriff führte in der Vergangenheit

zu Produktions- beziehungsweise Betriebsausfällen, so das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Das Defense-in-Depth-Prinzip

Ein wirksamer Schutz für die Vertraulichkeit, Integrität und Verfügbarkeit von OT-Netzen ergibt sich aus dem Zusammenspiel

Bilder: Genua

von Regeln, Verfahren, Maßnahmen und Tools, wie sie unter anderem im Informations-Sicherheits-Management-System (ISMS gemäß ISO/IEC 27000) und der Norm für ‚Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme‘ (IEC 62443) definiert sind sowie unter dem Stichwort ‚Cyberresilienz‘ aktuell diskutiert werden (siehe Kasten: Cyberresilienz: Das neue IT-Security-Paradigma).

In der Norm IEC 62443 definiert das Defense-in-Depth-Prinzip (gestaffelte Verteidigung) den Schutz gegen Cyberangriffe in mehreren Schichten ähnlich einer Zwiebel: Auch wenn eine Sicherheitsschicht überwunden wurde, ist nur ein Teil des Netzes betroffen. Das Gesamtsystem ist durch weitere Sicherheitsebenen geschützt. Diesem Konzept folgend ist es sinnvoll, interne Netzwerke in unterschiedliche Sicherheitszonen aufzuteilen und gestaffelte Schutzlevel zu vergeben. So können besonders sensible Segmente von anderen Bereichen strikt getrennt werden. Die Zonenübergänge und die Kommunikation zwischen den Zonen können durch Industrial Firewalls und entsprechende Filterregeln restriktiv begrenzt werden.

Das Verhalten von Netzkomponenten überwachen

Das Netzmonitoring ist auch für OT-Netze eine geeignete Schutzmaßnahme, um die Anlagenkommunikation zu überwachen und auf Auffälligkeiten zu untersuchen. Hier setzt die KI-gestützte (KI – Künstliche Intelligenz) Anomalie-Erkennung an. „Sie ermöglicht die Erkennung untypischen Verhaltens und somit neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen auf solche Netze“, so die Cyber-Sicherheits-Empfehlung des BSI (BSI-CS 134).

Wer spricht im OT-Netzwerk mit wem? Der KI-gestützte cognitix Threat Defender zeigt aufsummiert, welche Assets in der letzten Stunde oder in den letzten 30 Tagen wie viel Datenverkehr initiiert (Source Assets) beziehungsweise beantwortet (Destination Assets) haben, sowie den Datenverkehr zwischen den Assets. Basierend auf diesen Analysen können Policies festgelegt, überwacht und durchgesetzt werden.

Cyberresilienz: Das neue IT-Security-Paradigma

Interview mit Matthias Ochs, Geschäftsführer des Security-Spezialisten Genua.



Welche Voraussetzungen müssen für eine nachhaltige Cyberresilienz geschaffen werden?

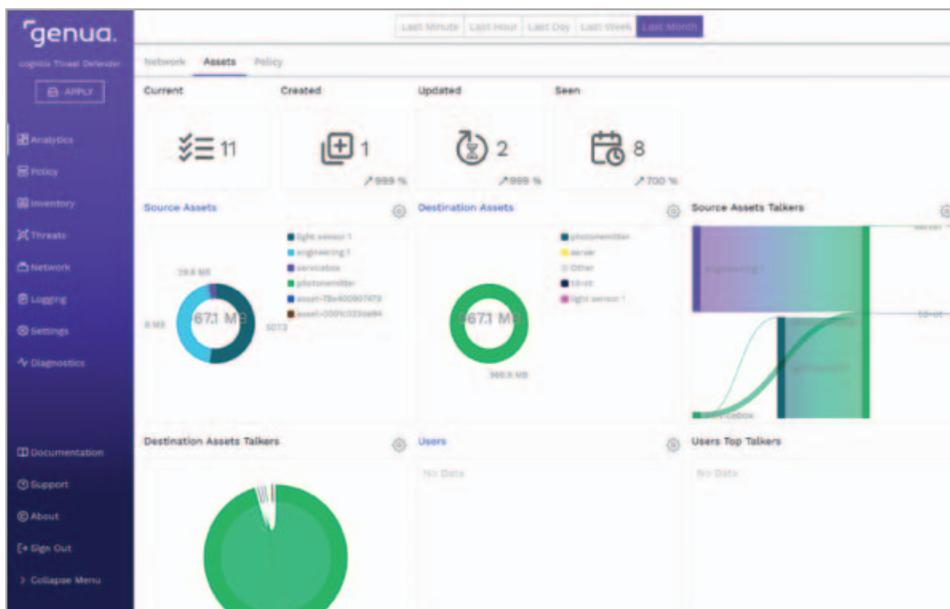
Matthias Ochs: Der Ausgangspunkt auf dem Weg zur Cyberresilienz ist eine fundierte Risikoanalyse der kritischen Geschäftsprozesse und die Definition möglicher Bedrohungen. Darauf aufbauend werden wirksame Maßnahmen zur Minimierung von Bedrohungslagen definiert. Der Fokus liegt dabei nicht auf hundertprozentiger, sondern adäquater Sicherheit. Für Risiken, die mit akzeptablem Aufwand nicht ausreichend zu reduzieren sind, müssen tragfähige Notfallpläne beschrieben werden. Verantwortlichkeiten, Führungsstrukturen und Kommunikationsprozesse werden auf Notsituationen ausgerichtet.

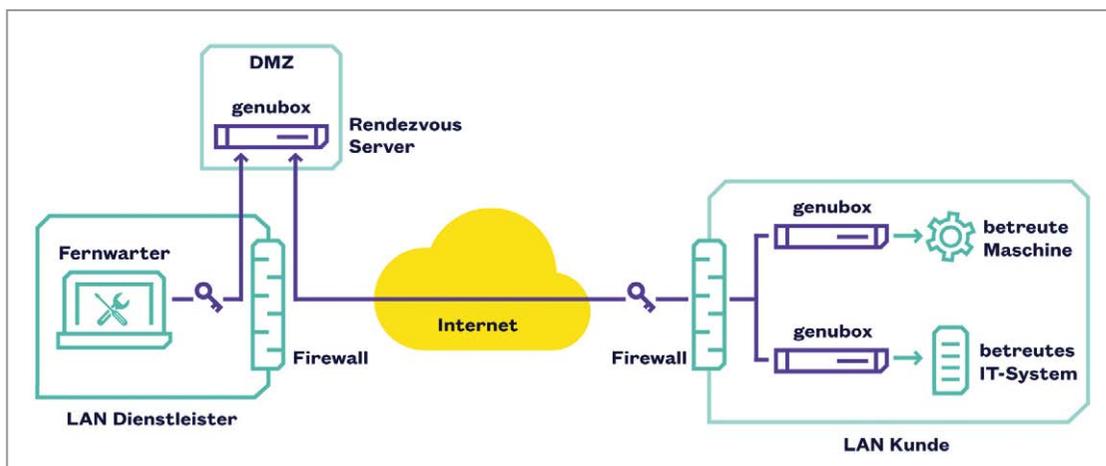
Wie kann dabei die hohe Komplexität beherrscht werden?

Der Schlüssel sind Prävention und frühe Detektion. Die hohe Komplexität macht Prävention zu einer anspruchsvollen Aufgabe, bei der klassische Firewall-Regeln und -Policies an ihre Grenzen kommen. KI-basierte Threat Defender bauen mittels Data-Analytics und Threat-Intelligence eine zweite Verteidigungslinie auf und ergänzen existierende Firewall-Lösungen. Industrie-Firewalls wie unsere genuwall schützen Produktionsnetze hochwirksam gegen Angriffe. Gleichzeitig sollte die Komplexität etwa durch klar definierte, minimale Schnittstellen weiter reduziert werden.

Welche organisatorischen Maßnahmen sind dabei wichtig?

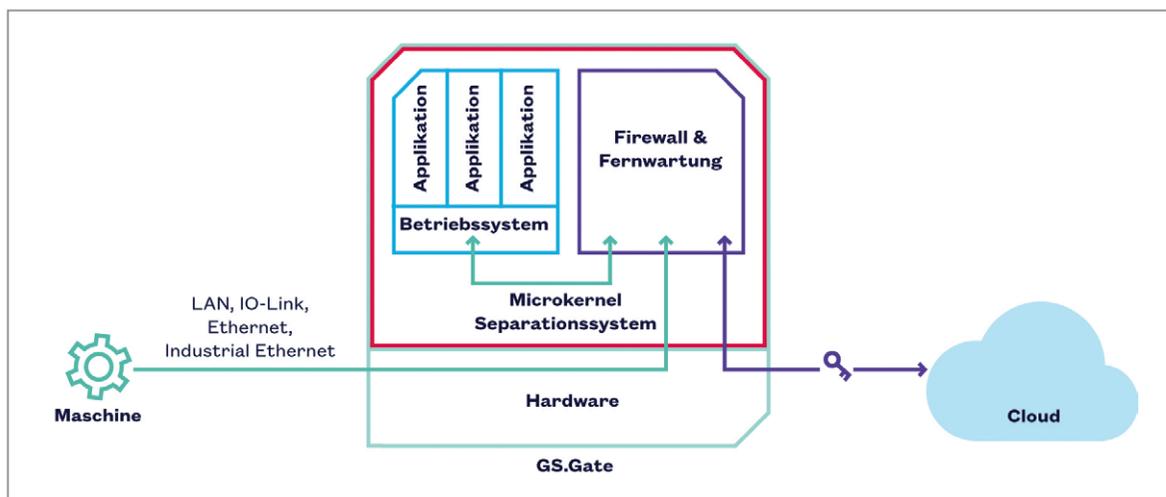
Basierend auf Aufgaben und Verantwortlichkeiten müssen vor allem Sicherheitspolicies definiert werden. Ein Schwerpunkt liegt auf Identitäts- und dienstebasierten Zugriffskontrollen. Und schließlich bedarf es einer auf Cyberresilienz ausgerichteten IT-Sicherheitsorganisation. Ihre Initiierung hat tiefgreifende transformative Auswirkungen auf die gesamte Organisation und ist der Weg zu einem neuen IT-Security-Paradigma.





Das Rendezvous-Konzept einer sicheren Fernwartung. Sichere Fernwartungslösungen erlauben den Zugang nur von innen nach außen und auch nur zu einer Sicherheitszone.

Schaubild zur Datenverarbeitung an der Edge. Sichere Edge-Gateways schützen Sicherheits-Gateway und Edge-Computing, also die Applikation, strikt ab.



Mit einem System zur Anomalie-Erkennung kann nicht nur der gesamte Netzwerk-Verkehr überwacht, sondern auch das Verhalten der Netzkomponenten (Assets) analysiert werden. Threat Defender richten hierfür ein überwacht sicheres Netzwerk ein. Verhaltensmuster von Netzwerk-Geräten werden erkannt, klassifiziert und Regeln entsprechend der Klassifikation angewendet. Dabei werden bisher getrennte Funktionen wie Netzwerk-Analyse, Intrusion Detection, Asset Tracking und eine dynamische Policy Engine in einem System zusammengeführt.

Durch eine Bestandsaufnahme (Asset Tracking) des Netzwerks werden zunächst alle Devices und der gesamte Netzwerk-Verkehr im ‚Grundzustand‘ erfasst. Dabei wird die Kommunikation der Geräte untereinander analysiert und für die zulässige Kommunikation werden nach und nach Regeln angelegt. Wird jetzt eine unbekannte Kommunikation erfasst, muss gebe-

nenfalls die Policy nachjustiert werden. Anderenfalls stellt der neuartige Netzwerk-Verkehr eine Anomalie dar, die auf ein Problem oder gar eine Störung beziehungsweise einen Eindringling hinweist.

Netzwerk-Segmentierung sinnvoll

Darüber hinaus ist es sinnvoll, eine dynamische und transparente Segmentierung des Netzwerkes vorzunehmen. Welche Sicherheitsvorgaben für ein Gerät gelten, bestimmt sich dann nicht mehr nach dem Netzwerk-Port oder dem Switch, an dem das Gerät eingesteckt ist. Wie ein Gerät mit den anderen Teilnehmern des gleichen Netzwerkes oder anderer Netzwerke kommunizieren darf, entscheidet sich nun anhand der Funktion und des Verhaltens. Durch diese Zuordnung der Netzwerkkomponenten können deren Security-Eigenschaften einzeln festgelegt und das Kommunikationsverhalten eingeschränkt werden.

Geschäftskritische Systeme und Prozesse lassen sich jetzt stärker abschotten. So kann beispielsweise der Datenverkehr von Produktionsanlagen mit dem SAP-System als besonders schützenswerter Prozess festgelegt werden. Um das zu erreichen, werden die Produktionsanlagen und Arbeitsstationen als SAP-Devices markiert und für diese Assets Regeln definiert. Darin können beispielsweise Priorisierungen im Datenverkehr, eine maximal Anzahl von Anfragen oder zugelassene Kommunikations-Protokolle festgelegt werden. So werden unerwünschte und problematische Zugriffe auf das SAP-System wirksam blockiert.

Fernwartungszugriffe zuverlässig absichern

Ein besonders sensibler Eingriff in das OT-Netz erfolgt durch die Fernwartung von Maschinen und Anlagen. Eine vertrauenswürdige Fernwartungslösung sorgt deshalb

Bilder: Genua

dafür, dass der Anlagenbetreiber über jeden Zugriff die Kontrolle behält. Sichere Fernwartungslösungen erlauben den Zugang nur von innen nach außen und auch nur zu einer Sicherheitszone. Dies kann mit einem sogenannten Rendezvous-Server mit integrierter Firewall umgesetzt werden, der in der demilitarisierten Zone (DMZ) installiert wird. Durch diese neutrale Zwischenebene wird eine direkte Verbindung mit dem Internet ausgeschlossen. In der DMZ bauen sowohl der Wartungsservice als auch der Maschinenbetreiber zum vereinbarten Zeitpunkt verschlüsselte Verbindungen auf. Erst mit deren Rendezvous auf dem Server in der DMZ und der Hoheit des Empfängers über die Verbindung, zum Beispiel beim initialen Aufbau, entsteht die durchgängige Wartungsverbindung zur betreuten Maschine.

Security für Edge-Computing

Mit Hilfe des Edge-Computing können immer größere Datenmengen beispielsweise von Sensoren maschinennah sofort verarbeitet werden. Zeitkritische Daten müssen nicht mehr komplett über das Netzwerk übertragen werden und sensible Daten können im eigenen Unternehmensnetz verbleiben. Das verkürzt die Reaktionszeit zum Beispiel im Vergleich mit der Datenverarbeitung in einer Big Data Cloud. Für die Absicherung der Daten sorgt ein Edge-Gateway. Sichere Gateways sollten zwei getrennte Bereiche in einer industrietauglichen Hardware bieten, die strikt voneinander abgeschottet sind: eine Computing-Plattform für individuelle Anwendungscontainer und ein Sicherheits-Gateway. Die separierten Bereiche verfügen über jeweils eigene Betriebssysteme sowie fest zugewiesene Hardware-Ressourcen.

Im Bereich der Anwendungsplattform können Maschinenhersteller oder -betreiber mittels Container-Technologie ihre individuelle Anwendung installieren. Die Anwendung ruft über gängige Schnittstel-

len die Zustands- und Leistungsdaten von der Maschine ab und führt eine Vorverarbeitung der Daten durch. Die Einsatzszenarien sind vielfältig. Beispielsweise können Informationen für die sofortige Auswertungen genutzt werden, während andere in die Cloud übertragen werden. Die Informationen werden also gefiltert und nur diejenigen Daten in die Cloud übertragen, die für die Data-Analytics-Auswertungen benötigt werden.

OPC UA verstärkt die Cybersecurity

Der Kommunikationsstandard OPC UA ermöglicht eine starke und abgesicherte Vernetzung. Bisher überwiegend proprietäre herstellerspezifische Protokolle müssen an den Netzgrenzen nicht mehr umgewandelt werden. Mit OPC UA kann vom Sensor bis in die Cloud ein einziges Protokoll verwendet werden. Das Thema Sicherheit spielt im OPC-UA-Standard von Anfang an eine wichtige Rolle. Dazu wurde ein eigener Security-Layer mitspezifiziert. Dieser legt Mechanismen fest, wie sich Dienste oder Geräte authentifizieren lassen, wie Daten verschlüsselt werden und wie deren Authentifizierung gewährleistet ist.

In der Praxis ist der Anwender allerdings von der Qualität der Implementierung des jeweiligen Herstellers abhängig. Für sensible Anlagen und Netzsegmente können daher ergänzende Sicherheitslösungen wie Datendiode sinnvoll sein. Sie lassen nur eine unidirektionale Kommunikation zu, um beispielsweise Daten aus sensiblen Industrieanlagen risikolos in ‚unsichere Umgebungen‘ wie das Internet oder eine Cloud auszuleiten. Ohne Rückkanal haben Angreifer dann in keinem Fall Zugriff auf die Maschinen oder Anlagen.

Geringer Aufwand, hoher Schutz

In der OT-Security kann mit heutigen Technologien ein hohes Schutzlevel gegen Cyber Risiken mit überschaubarem Auf-

Sichere Datenausleitung

Die Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (NAMUR) hat sich mit der ‚NAMUR Open Architecture‘ (NOA) zum Ziel gesetzt, Produktionsdaten einfach und sicher für eine Anlagen- und Geräteüberwachung (Monitoring) und für Optimierungen nutzbar zu machen – auch für bestehende Anlagen. Die NAMUR-Initiative schlägt zur direkten Ausleitung von Prozessdaten zusätzlich zu den vorhandenen Automatisierungsstrukturen einen sicheren One-Way-Kanal vor. Auf diesem zweiten Kanal können die Daten rückwirkungsfrei übertragen werden. Für die Sicherheit des Datentransfers soll eine Diode sorgen, die ungewollte und unkontrollierte Datenströme in Richtung des Senders verhindert. So ermöglicht die ‚cyber-diode‘ von Genua einen solchen sicheren Einbahn-Datentransfer, indem sie per Produkt-Design keine Kommunikation zulässt. Im Sinne des Defense-in-Depth-Prinzips schützt sie mit ihrem hohen Sicherheitsstandard als ergänzende Sicherheitsmaßnahme besonders sensible Netzwerk-Segmente. Diese sind dann de facto von außen nicht mehr angreifbar.

wand erreicht werden. Dabei sollte der Fokus auf einer adäquaten Sicherheit liegen. Cybersicherheit ist allerdings kein Feenstaub, der zum Projektabschluss kurz einmal aufgetragen wird. OT Security ist von Anfang an und in allen relevanten Dimensionen zu berücksichtigen. Und wenn man nachrüsten möchte, sollte dies möglichst herstellerunabhängig geschehen, um einen Vendor Lock-in zu vermeiden. Das Ziel besteht darin, durch technische und organisatorische Maßnahmen gestaffelte Schutzlevel zu schaffen und die wichtigsten Daten und Systeme des Unternehmens besonders zu schützen. Durch diese Cyberresilienz wird darüber hinaus sichergestellt, dass Kernprozesse und Kerninfrastrukturen auch bei Cyberangriffen aufrechterhalten oder zumindest schnell wieder auf die volle Leistung hochgefahren werden können. ag



Für sensible Anlagenbereichen eignen sich Datendiode. Durch ihre One-Way-Architektur erlauben sie eine risikolose Ausleitung von Daten.



STEVE SCHONER
ist Strategic Product Marketing Manager für industrielle Cybersicherheit bei Genua.

Schutz für geistiges Eigentum

Im industriellen Umfeld entsteht umfangreicher Daten-Input aus den unterschiedlichsten Quellen, der oft mit Hilfe von Anwendungen mit Künstlicher Intelligenz verarbeitet wird. Wie lassen sich die guten Ideen hinter diesem Prozess wirksam schützen?

Arbeiten Maschinen, Anlagen, Roboter und Menschen im industriellen Umfeld, sorgen verschiedene Quellen für umfangreichen Daten-Input. Dieser wird oft mit Hilfe von Anwendungen mit Künstlicher Intelligenz (KI) verarbeitet. Zudem können Maschinen – Stichwort Machine Learning (ML) – anhand dieser Daten lernen und ihren Algorithmus dadurch selbst optimieren. So wird beispielsweise über Kameras die Qualität eines Produkts geprüft und mittels KI sowie ML lassen sich Abweichungen präzise und schnell entdecken. Um die Ideen der Entwickler hinter diesem Prozess zu schützen, benötigen Hersteller von Anwendungen für KI und ML, die oft mit der Programmiersprache Python geschrieben sind, einen wirkungsvollen technischen Schutz.

Die Beliebtheit der unterschiedlichen Programmiersprachen hat der Analyst Slash Data in einer Umfrage ‚State of the developer nation‘ untersucht. Im ersten Quartal 2021 wurden dazu über 19.000 Entwickler befragt. Eines der Ergebnisse: Am zweithäufigsten arbeiten die Software-Entwickler mit Python, wobei die Haupteinsatzzwecke Data Science, Machine Learning und Anwendungen für IoT sind.

Angriff auf die Programmiersprache

Aufgrund der wachsenden Bedeutung von KI und ML werden Angreifer verstärkt versuchen, an die guten Ideen der Hersteller zu gelangen und mit geringem Aufwand davon zu profitieren. Typischerweise liegt in Python ein Angriffspunkt, da der Python-Quellcode als einfache Text-Datei

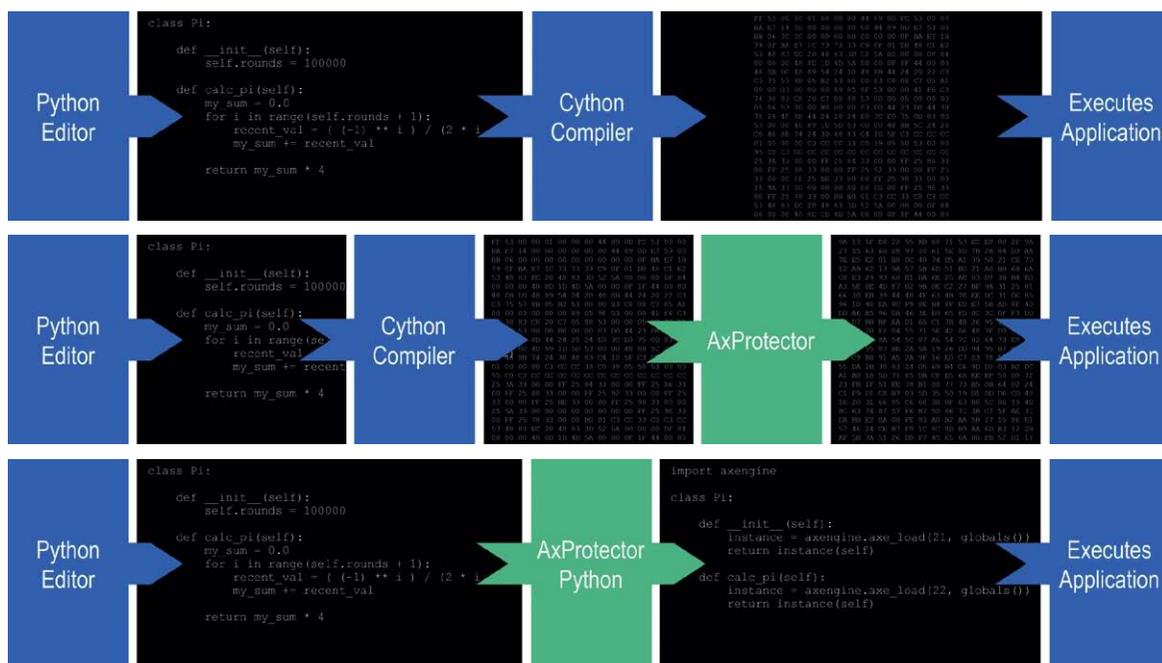
ausgeliefert wird und im Klartext gelesen werden kann, was bei Skriptsprachen üblich ist. So können Anwender – absichtlich oder unabsichtlich – den Quellcode ändern, manipulieren, kopieren und die Idee dahinter, beispielsweise einen KI-Lernalgorithmus, analysieren und unberechtigt nutzen (Reverse Engineering).

Wibu-Systems kennt als Schutz- und Lizenzierungsexperte die Bedeutung der Programmiersprache Python für Hersteller von KI- und ML-Anwendungen. Aus diesem Grund hat das Unternehmen die Verschlüsselungsmöglichkeit ‚AxProtector Python‘ auf den Markt gebracht.

Die ‚CodeMeter‘-Technologie des Anbieters konnte bereits Python-Software über Vorkompilierung der EXE-Dateien mittels Cython-Compiler schützen. Neu ist



Bild: Wibu-Systems / iStock, Serhii Yakovliev



Kompilierung des Python-Quellcodes in eine ausführbare Datei. Das Ergebnis ist plattformabhängig und unverschlüsselt. Die Anwendung kann weiterhin von einem Experten mit einem Disassembler analysiert werden.

Kompilierung des Python-Quellcodes in eine ausführbare Datei und anschließende Verschlüsselung mit AxProtector. Das Ergebnis ist plattformabhängig und verschlüsselt. Die Anwendung kann nicht mehr mit einem Disassembler analysiert werden.

Verschlüsselung des Python-Quellcodes mit AxProtector Python ohne vorherige Kompilierung in eine ausführbare Datei. Das Ergebnis ist plattformunabhängig und verschlüsselt. Die Anwendung kann nicht mehr mit einem Disassembler analysiert werden.

nun die direkte und automatische Verschlüsselung der Python-Software über ‚AxProtector Python‘, was die vorhandenen Tools der CodeMeter Protection Suite erweitert.

Das Grundprinzip aller CodeMeter-Tools ist: Zuerst verschlüsseln die Hersteller ihre Software und danach liefern sie den passenden Lizenzschlüssel an die Anwender. Anschließend können die Anwender die verschlüsselte Software den Berechtigungen gemäß nutzen. Als Träger der Lizenzschlüssel dienen die Schutzhardware ‚CmDongle‘, die softwarebasierte Aktivierungsdatei ‚CmActLicense‘ oder der ‚CmCloudContainer‘, der in der Cloud liegt.

Über Vorkompilierung zur geschützten Software

Der klassische Weg besteht aus zwei Schritten: Vorkompilierung und Verschlüsselung. Über den Cython-Compiler wird die Python-Software in eine ausführbare, in C geschriebene Datei (EXE) umgewandelt, damit dann diese ausführbare Datei über das Standardtool ‚AxProtector‘ verschlüsselt wird. So können Hersteller ihr geistiges Eigentum, das in der Software steckt, verschlüsseln und auch lizenzieren und somit unter dem Stichwort ‚Softwaremonetarisierung‘ zusätzlichen Umsatz generieren. Hersteller können automatisiert verschiedene Lizenzmodelle umsetzen – beispielsweise

Einzelplatzlizenzen, Floating-Lizenz innerhalb eines Netzwerkes oder ein zeitbasiertes Modell. Für die Python-Software wichtige Daten lassen sich über das CodeMeter Core API ebenfalls verschlüsseln sowie signieren. Bei diesem Weg muss der Hersteller für jede einzelne Plattform je eine dafür bestimmte ausführbare Datei erzeugen und ausliefern, was technische Kenntnisse voraussetzt.

Direkte Verschlüsselung

Die Mindestvoraussetzungen zum Einsatz von ‚AxProtector Python‘ sind ‚Python 3‘ und ‚CodeMeter 7.30‘. Das Tool verschlüsselt direkt, ohne die Umwandlung durch ‚Cython‘, und es wird kein nativer Code erzeugt. Da die Python-Software nur einmal verschlüsselt wird, gibt es nur eine einzige ausführbare Datei, die auf den verschiedenen Plattformen Windows, Linux oder macOS läuft. Nur der gerade benötigte Teil wird zur Laufzeit in den Hauptspeicher geladen und dann entschlüsselt, sodass der große Teil der Software immer noch verschlüsselt bleibt. Jede Funktion der ‚Python‘-Software wird einzeln verschlüsselt, sodass Hersteller modulare Lizenzen erzeugen können. Anwender bekommen nur die Lizenzschlüssel für das, was sie gekauft haben. Auch spätere Käufe werden auf diese Weise behandelt.

Will der Hersteller Funktionen und Dateien unverschlüsselt lassen, kann er

Annotationen setzen sowie dies über Einträge in der Schutzdefinition steuern. Die Integration des Schutzes ist mit ‚AxProtector Python‘ viel einfacher, da der Schritt der Vorkompilierung entfällt.

Unterschiedliche Verschlüsselungstools

Ähnlich einem Werkzeugkasten können Hersteller verschiedene Verschlüsselungstools nutzen, um die komplette Software oder nur bestimmte Teile zu verschlüsseln. Zur Auswahl stehen verschiedene ‚AxProtector‘-Varianten, die für unterschiedliche Programmiersprachen optimiert sind und für den automatischen Schutz einer ausführbaren Datei sorgen, ‚AxProtector‘ zur Verschlüsselung einzelner Funktionen und ‚IP Protection‘, um Software vor Reverse Engineering zu schützen, jedoch werden keine Lizenzschlüssel benötigt. ‚AxProtector Python‘ ergänzt die vorhandenen Varianten: den Standard- ‚AxProtector‘, ‚AxProtector Java‘, ‚AxProtector .NET‘ und ‚AxProtector CmE‘ für Embedded-Software. *ik*



RÜDIGER KÜGLER
ist VP Sales & Security Expert
bei Wibu-Systems in Karlsruhe.

Cloud Security

Mit kontextbezogener KI-Technologie

Check Point Software erweitert die Funktionen der Plattform ‚CloudGuard Cloud Native Security‘ um *CloudGuard Application Security (AppSec)*, eine automatisierte Lösung zum Schutz von Web-Anwendungen und APIs. CloudGuard AppSec beseitigt die Notwendigkeit der manuellen Abstimmung und senkt die hohe Rate von Fehlalarmen, die mit herkömmlichen Web Application Firewalls (WAFs) verbunden sind. Die Lösung nutzt kontextbezogene Künstliche Intelligenz, um Angriffe auf Cloud-Anwendungen zu verhindern. Sie blockiert Angriffe gegen Anwendungen, wie Site Defacing, Information Leakage, User Session Hijacking und alle der OWASP Top 10 Sicherheitsrisiken für Webanwendungen. Dabei passt sich die KI-Engine der Lösung permanent an Anwendungsänderungen an und aktualisiert sich selbst, um kontinuierliche Sicherheit zu gewährleisten. Zudem nutzt die Lösung Verhaltensanalysen, um zwischen menschlichen und maschinellen Interaktionen mit Anwendungen zu unterscheiden. So werden Credential Stuffing, Brute-Force-Angriffe und Site Scraping verhindert.

www.checkpoint.com/de

Switches

Bis zu 24 Ports

Belden bringt mit dem High-Port Switch *Bobcat* von Hirschmann ein neues Mitglied der ‚Bobcat‘-Produktfamilie auf den Markt. Der Managed Switch mit bis zu 24 Ports ist eine kompakte Netzwerklösung für das Industrial Internet of Things (IIoT). Zu den wichtigsten Merkmalen der Switches gehören eine hohe Port-Dichte für den Anschluss von Netzwerkgeräten, TSN-Technologie zur gleichzeitigen Unterstützung mehrerer Dienste im Netzwerk und zur Gewährleistung deterministischer Kommunikation, erweiterte Sicherheitsfunktionen wie Wire-Speed Access Control Lists (ACL) und automatischer Denial-of-Service (DoS)-Schutz sowie maximale Ausgangsleistung durch Power-over-Ethernet-Ports (PoE/PoE+), die keine Lastverteilung erfordern.

www.belden.com



Cybersecurity

Tansparenz auf die Cloud ausweiten

Netscout Systems gibt die Bereitstellung von *Netscout Cyber Investigator (NCI)* für AWS bekannt. Er steigert die Effizienz bei der Verwaltung zunehmender Komplexität aufgrund der Verlagerung von Anwendungen in die Cloud. Da sich die Bedrohungsfläche vergrößert, nutzt ‚NCI‘ Paketdaten, um schnell eine ganzheitliche Sichtbarkeit zu gewährleisten, die zur Ursachenfindung von Problemen erforderlich ist. Netscout hat bei der Einführung von ‚VPC Traffic Mirroring‘, ‚VPC Ingress Routing‘ und dem Gateway ‚Load Balancer‘ (GWL) zusammen mit AWS an Lösungen für den Zugang zu Paketdaten gearbeitet. GWLB bietet einen skalierbaren Zugriff auf den Paketverkehr für Sicherheits- und Leistungsmanagement. So können Kunden den Datenverkehr von jeder Virtual Private Cloud (VPC) zu beliebigen Sicherheits- und Überwachungstools leiten, ohne die Cloud zu verlassen. NCI ist in AWS Security Hub integriert.

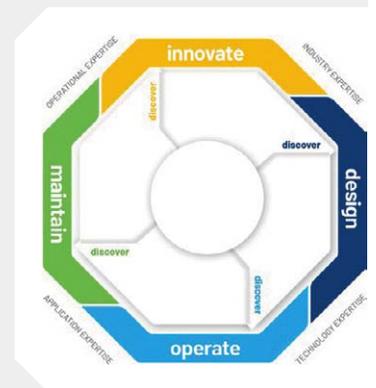


www.netscout.com

Lebenszyklus

Service-Portfolio erweitert

Die Firma Rockwell Automation hat ihre Service- und Lösungskompetenzen weiterentwickelt und führt die Marke *LifecycleIQ Services* ein. Bei ‚LifecycleIQ Services‘ werden digitale Technologien mit menschlichem Know-how kombiniert. Dadurch helfen die Services Unternehmen dem Anbieter zufolge an jedem Punkt ihres Geschäftszyklus, schneller, intelligenter und flexibler zu arbeiten. Die Services unterstützen Unternehmen während der Entwurfs-, Betriebs- und Wartungsphasen. Produzierende Unternehmen können die Services nutzen, um folgende Ergebnisse zu erzielen: Erfolgreiche Gestaltung der Digitalen Transformation, Stärkung der Cybersicherheit, optimale Unterstützung der Belegschaft.



www.rockwellautomation.com

nachgehakt

bei **Marcus Eibach**
Senior Vice President der Deutschen Messe AG



5G in der Halle 9

Siemens wird die Halle 9 auf dem Hannover Messegelände bis September mit einem 5G-Campus-Netz ausstatten, soweit die gemeinsame Mitteilung von Siemens und der Deutschen Messe Mitte Februar. Was dies konkret bedeutet, erläutert Marcus Eibach, Senior Vice President, Deutsche Messe AG im Interview.

In der Mitteilung vom Februar heißt es: „Das Besondere an der Siemens-Infrastruktur: Sie verbleibt dauerhaft in der Messehalle und wird der Deutschen Messe zur kommerziellen Nutzung überlassen.“ Bedeutet dies, dass die Deutsche Messe die Hoheit über die Siemens-Infrastruktur haben wird oder wird das 5G-Netz in Halle 9 ganzjährig von Siemens betreut und betrieben?

Marcus Eibach: Das 5G-Campus-Netz von Siemens in der Messehalle 9 wird nach seiner Fertigstellung ganzjährig gemeinsam mit Siemens betreut und betrieben. In enger Partnerschaft bieten wir als Deutsche Messe zusammen mit Siemens die Nutzung des Campus-Netzes für Test- und Demonstrationszwecke von 5G-Produkten, -Lösungen und -Anwendungen an. Der Fokus dabei liegt auf Industrie Use Cases.

Der Basisbetrieb des Netzes erfolgt dabei durch die Deutsche Messe. Hierzu zählen das Schreiben von SIM-Karten, Anmeldung von Geräten, Ein- und Ausschalten der Anlage. Darüber hinausgehende Themen wie Ausbau hinsichtlich Erweiterung und Upgrades, aber auch die Diagnose bei möglichen Problemen erfolgen dann durch Siemens.

Aussteller können das Netz während laufender Messen für Tests und Feldversuche nutzen. Damit haben Aussteller in Halle 9 zukünftig ein maßgebliches Alleinstellungsmerkmal gegenüber Ausstellern in den anderen Messehallen. Erzeugen Sie damit explizit auf die Hannover Messe bezogen einen Run auf Halle 9? Anders gefragt: Sind die Aussteller in anderen Hallen dann nicht benachteiligt?

Keineswegs. Neben dem Auf- und Ausbau des Industrial-5G-Campus-Netzes von Siemens in der Halle 9 erfolgt auf dem Messegelände die flächendeckende Ausstattung mit dem Mobilfunkstandard 5G. Technologiepartner für diesen Ausbau ist an der Stelle die Telekom. Dieses Campus-Netz realisiert die Telekom als ein hybrides Netz. Wir verfügen somit zukünftig über ein privates Netz, welches es unseren Ausstellern und Gastveranstaltern aller Messen in Hannover ermöglicht, ihre 5G-fähigen Produkte,

Lösungen und Anwendungen live zu präsentieren. Gleichzeitig haben Besucher der Messen eine hervorragende Versorgung mit dem öffentlichen 5G-Netz der Telekom auf dem Gelände.

Wird es so etwas wie ein Testbed in der Halle 9 geben, mit dessen Hilfe Firmen Tests und Erprobungen im Zusammenspiel mit Produkten anderer Firmen durchführen können?

Genau derartige Szenarien wollen wir realisieren, denn das wird die Realität im Produktionsumfeld sein. Diese Notwendigkeiten wurden uns in einigen Vorgesprächen signalisiert und nun sind wir gespannt auf die ersten konkreten Anfragen. Die Größe der Halle ermöglicht es industriellen Anwendern, Applikationen in allen Formaten schon jetzt mit 5G zu testen. So können nicht nur große Unternehmen sondern auch kleine und mittelständische Unternehmen schon sehr früh in der Entwicklung 5G-Technologie testen, ohne in ein eigenes Campus-Netzwerk investieren zu müssen.

Ab September soll es mit dem Betrieb des Campus-Netzes losgehen. Können beziehungsweise haben sich interessierte Firmen schon für die Nutzung des Netzes angemeldet?

Wir konnten im Bereich Smart Mobility bereits einen ersten Kunden für unser 5G Smart Venue gewinnen: Die Firma SMEV hat eine patentierte Innovationstechnologie entwickelt, die zukünftig Einsatzfahrzeugen den schnellstmöglichen Weg zum Einsatzort garantieren soll. SMEV nutzt die 5G-Infrastruktur unseres Smart Venues, um ihre Technologie weiterzuentwickeln und auf den Echteinsatz vorzubereiten.

Durch die Einbindung der Deutschen Messe und des Messegeländes in das Konsortium Testfeld Niedersachsen ermöglichen sich für uns spannende neue Kooperationsmöglichkeiten mit Unternehmen und Forschungseinrichtungen in den Bereichen autonomes Fahren und vernetzte Mobilität. Darüber hinaus sind wir mit Unternehmen unterschiedlichster Branchen in Gesprächen. hap

Die Königsklasse

der Motoren



Zukunft spüren

ECblue – intelligente Hightech-IE5-Motorentechnologie mit einzigartiger Performance.

Klimafreundlich, höchste Effizienz, größtes Energiesparpotential und integrierte MODBUS-Kommunikation. Hochintelligente Sensoren und optionale Bluetooth-Verbindung eröffnen den Weg in die Hochsicherheits-Datenräume unserer **ZABluegalaxy** – der cloudbasierten IoT Plattform – und damit u.a. die Möglichkeit vorausschauender Wartung (Predictive Maintenance). www.ziehl-abegg.de



Zaset –
mobile App



ZABluegalaxy
Cloudbasierte IoT-Plattform für
Produktverwaltung der Zukunft



Die Königsklasse in Lufttechnik, Regeltechnik und Antriebstechnik

Bewegung durch Perfektion

110 Jahre | 110 Years
ZIEHL-ABEGG