

03/2018
www.iot-design.de

TeDo Verlag GmbH
April
€ 7,80

+++ Sichere industrielle Infrastruktur S.36 +++

Sinnvolle Synergie: Microsoft
Windows 10 IoT Core
für i.MX 6- und i.MX 7-
Applikationsprozessoren

S.17

IoT DESIGN

Smarte Systeme für das Internet of Things



Pushing Performance



Intelligenz von Anfang an S.17 Leiterplatte 4.0



Transport 4.0

- Fahrerlose
Transportsysteme S.44



- Asset
Tracking
via BLE S.46



S.38



Marktübersicht
Tischmultimeter

LoRa
Grundlagen &
Einsatz in der
Landwirtschaft
S.25

RTOS in Embedded Devices

S.14

Sind diese 11 Mythen richtig oder falsch?

Blockchain

Was ist dran an
der Technologie?
Interview plus
Praxisbericht

S.48

**DER NEUE MASSSTAB FÜR
INDUSTRIAL ETHERNET.**

Mit dem fido5000 ist es ein Leichtes, unterschiedliche Industrial Ethernet Protokolle auf ein und derselben Plattform zu unterstützen. Der Switch ist bereits heute auf TSN ausgelegt und gewährleistet, dass die Anforderungen der Industrie 4.0 spielerisch umgesetzt werden können – heute und in Zukunft.

fido5000 ÄNDERT DIE SPIELREGELN FÜR INDUSTRIAL ETHERNET DESIGN.

Besuchen Sie uns auf der
Hannover Messe vom 23.-27. April 2018
Halle 9, Stand H23

VIDEOS, TECHNISCHE ARTIKEL UND WEITERE
INFORMATIONEN ZUM fido5000 REM:
analog.com/industrial-ethernet



#ADlahead

 **ANALOG
DEVICES**

fido
5000 



Mikroelektronik im Boom

Wohin man auch schaut: Alles wird intelligent. Nach dem furiosen Auftakt des Branchenjahres mit der Embedded World in Nürnberg hat auch die gerade zu Ende gegangene Weltmesse für die Gebäudetechnik Light + Building deutlich gezeigt, wohin die Reise beispielsweise im Wohn- und Zweckgebäude geht. Und auch die Hannover Messe wirft in dieser Hinsicht ihre Schatten voraus: Integration ist das Schlüsselwort der Zeit.

Der Boom der smarten Systeme beschert den Elektronikherstellern volle Auftragsbücher. Jüngst hat der ZVEI seine Konjunkturzahlen für den Welt-Mikroelektronikmarkt veröffentlicht. Demnach konnte dieses Segment im Jahr 2017 um 21 Prozent auf 412 Mrd.Us\$ zulegen. Das sei das größte Wachstum seit der Jahrtausendwende. Umsatztreiber waren zwar vor allem Speicherchips, aber auch ohne dieses Segment lag das Plus des Weltmarkts bei fast zehn Prozent.

Europäer sind führend bei Halbleitern für die Segmente Automobilelektronik und Industrieelektronik. Mit Portfolioanteilen von 33 und 24 Prozent sind wir Europäer im weltweiten Vergleich am stärksten auf diese Wachstumsfelder fokussiert. Der Mikroelektronik-Trendanalyse des ZVEI zufolge lassen diese Segmente in den kommenden fünf Jahren weiter hohe Zuwächse erwarten. Abnehmer seien hier vor allem die Hersteller von Automobilelektronik und die Unternehmen der Automation. Immer mehr Fahrerassistenzsysteme und die Elektromobilität sind dabei die Treiber im Bereich Automobilelektronik. Industrie 4.0 und das Internet of Things sind die Herausforderungen der Industrieelektronik.

Indes hat der europäische Markt – verglichen mit anderen Weltregionen – insgesamt mit einem Jahresumsatz von 38Mrd.US\$ (ca. neun Prozent) eher eine bescheidene Größe. Asiens Weltmarktanteil war 2017 mit gut 61 Pro-

zent dominierend. Allein auf China entfielen 131Mrd.US\$ von den insgesamt 412 Mrd.US\$. Die USA liegen mit knapp 82Mrd.US\$ auf Platz zwei.

Dass die Anwendung der Embedded Systeme auch in Europa große Wertschöpfungspotenziale bietet zeigt sich in unzähligen Anwendungen. Am Ende ist eine einzelne Komponente heute nichts mehr. Vielmehr muss aus vielen Teilnehmern ein funktionierendes Ganzes entwickelt werden – eben Integration betrieben werden. Und zwar sicher, zuverlässig und nachhaltig. Und davon verstehen wir in Deutschland und Europa eine ganze Menge. Von dieser Aufgabe und deren Lösung berichten wir in jeder Ausgabe der IoT Design. In diesem Sinne wünsche ich Ihnen auch mit dieser Ausgabe wieder viel Spaß beim Lesen.

Ihr


Kai Binder
Chefredakteur IoT Design



— Anzeige —



PCIM Europe Halle 7 Stand 229

© eiSos



REDEXPERT. Die einzigartige Online-Plattform von Würth Elektronik zur Auswahl elektronischer und elektromechanischer Bauelemente.
www.we-online.de/redexpert

- Weltweit genauestes AC-Verlustmodell für Speicherinduktivitäten
- Filtermöglichkeit für über 20 elektrische und mechanische Merkmale
- Simulation der Induktivität im DC/DC-Wandler
- Vergleichbarkeit anhand interaktiver Messkurven (Induktivität/Strom und Erwärmung/DC-Strom)
- Verfügbar in sieben Sprachen
- Messwertbasierte Online-Plattform
- Kein Login notwendig
- Integrierte kostenlose Musterbestellung
- Direkter Zugriff auf Produktdatenblatt

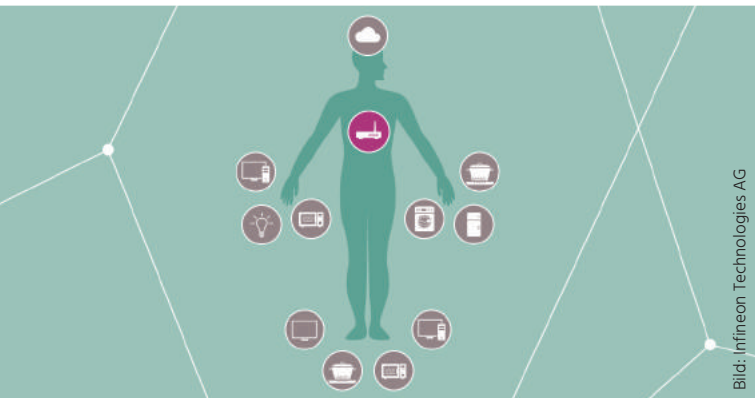
#REDEXPERT

*WE speed up
the future*



Leiterplatte 4.0

06 Die intelligente Leiterplatte kann jetzt sprechen und denkt mit – ideal für smarte Produkte von heute...



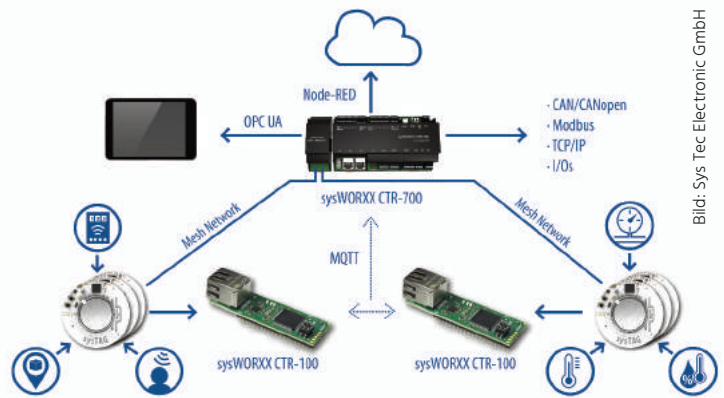
Immunsystem für das IoT

18 Gehackte Firmware ist die neue Herausforderung für die Securityabteilung. Dabei gibt es geeignete Abwehrmaßnahmen...



Der Alltag von morgen

28 Die clevere Nutzung von Daten aus vernetzten Dingen treibt unsere Entwicklung voran. Wir zeigen die größten Auswirkungen...



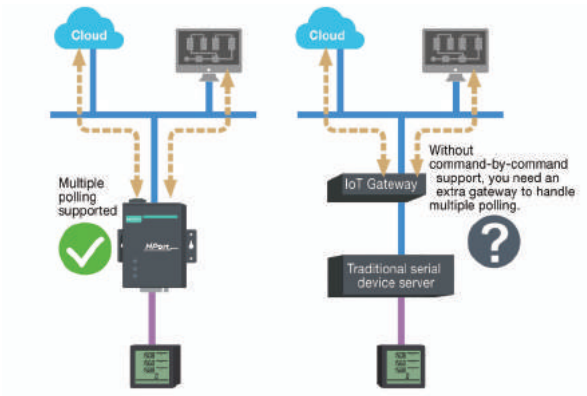
Voll vernetzt

42 Mit einer neuen Produktfamilie zeigt Sys Tec Electronic den Weg ins Internet der Dinge...



Sichere industrielle Infrastruktur

36 Wir stellen ein geschütztes Framework für IoT-Lösungen im industriellen Umfeld vor...



Mehrwert durch Integration

34 Oftmals müssen Geräte mit serieller Schnittstelle für moderne Datennetzwerke fit gemacht werden. Wir zeigen wie...

IoT Must Haves

- 9 Modulare Gateway-Plattform
- 9 Funk-Chip und Modul für IoT
- 9 DC/DC-Wandler mit niedriger Stromaufnahme
- 10 LAN-Übertrager als Gigabit-Version
- 10 Kühlkörper für Leistungselektronik
- 10 Box-PC mit ULV-CPU
- 11 Hardware für CAN-Bus-Anwendungen
- 11 Hardware für Box-PCs
- 12 Daten-Flatrate für das IoT
- 12 Tools für Deep Learning
- 12 Robustheitsstests mit Fuzzing-Werkzeug

30 Produktübersicht Embedded Systeme

38 Marktübersicht Tischmultimeter

Ratgeber

- 6 Intelligenz von Anfang an – Leiterplatte 4.0
- 13 Nachbericht embedded world
- 14 RTOS: Elf Mythen
- 17 Softwareunterstützung für i.MX 6 und i.MX 7
- 18 Immunsystem für das IoT
- 20 Embedded Cloud und TSN

- 22 Tools zum Managen von Industrie 4.0
- 25 Datenübertragung im Internet der Dinge
- 28 Der Alltag von morgen
- 32 Vision-Systeme mit Framegrabbern beschleunigen
- 34 Serielle Geräte in das IoT integrieren
- 36 Secure Industrial Visibility (SIV) für eine sichere industrielle Infrastruktur
- 40 Geräteanschlüsse und Elektronikgehäuse
- 42 Steuerungen für vorausschauende Wartung
- 44 Steuerungsrechner für fahrerlose Transportsysteme (FTS)
- 46 Asset Tracking über Bluetooth LE (BLE)
- 48 Embedded Systems und Blockchain: Interview mit M. Barr, Mitbegründer und CTO von der Barr Group
- 50 Hafen Rotterdam im Internet of Things

IoT News

- 16 Sensor+Test 2018
- 16 TÜV für Künstliche Intelligenz
- 16 Produktkataloge 2018
- 47 Sigfox Connect 2018
- 47 Neue Mitglieder im VDE-Präsidium

Service

- 3 Editorial
- 49 Impressum / Inserentenverzeichnis

- Anzeige -

Jeder spricht über das IIoT

... wir setzen es einfach um.

Netzwerke und Computer für eine „smartere“ Industrie.

- Leistungsstarke Computer für Ihre Bedürfnisse designt
- Sichere und verlässliche Netzwerke – immer und überall
- Vertikale Integration von SCADA bis zu Feldgeräten

Moxa. Wo Innovation passiert.



www.moxa.com



MOXA
Reliable Networks ▲ Sincere Service

Intelligenz von Anfang an Leiterplatte 4.0



Leiterplatten sind ein Kernstück von allen **Elektrogeräten**, Autos, Robotern, und Smartphones, Tablets und Co. Eine Leiterplatte muss daher zuverlässig sein, den steigenden **Qualitätsansprüchen** gerecht werden und dennoch müssen die **Herstellkosten** sinken bei steigender **Komplexität** des Endproduktes. Logisch, dass sich die Leiterplatte und deren Herstellung wandelt. Die Leiterplatte kann jetzt **sprechen** und **denkt mit**...

OLAF WILMSMEIER, Business Development Manager RFID, Harting

Eine Bestellung über eine Steuerplatine wird bei einem der MES-Dienstleister in Deutschland platziert. Nach Erfassung wird der Auftrag eingeplant, die Produktion wird gestartet und alle relevanten Fertigungs- und Qualitätsdaten werden im Backend System (einer Datenbank) abgespeichert. Der komplette Prozess wird zentral aus dem führenden Backend System gesteuert. Die Leiterplatte wird zwar bei der Fertigung eindeutig, eventuell mit einem gelaserten 2D-Code, erkannt, aber Prozessparameter oder Qualitätsmerkmale kennt die Leiterplatte selbst nicht. Wenn auch stark vereinfacht dargestellt, ist dies der klassische Prozess wie eine Leiterplatte entsteht.

Lebenszykluskosten betrachten

In Zukunft wird dies jedoch deutlich anders aussehen, denn – auf den Lebenszyklus bezogen – ist diese vorgehensweise viel zu teuer und unflexibel. In einer Leiterplatte steckt daher viel mehr Industrie 4.0 als sich viele vorstellen. Bereits bei der Herstellung der Rohleiterplatte, erhält sie ein Gedächtnis. Darüber kann sie aktiv mit auf alle weiteren Prozesse Einfluss nehmen – nicht nur in der Fertigung, sondern über den gesamten Lebenszyklus hinweg. Ein kleiner UHF RFID Chip mit einer kleinen Antennenstruktur macht dies möglich. Eingebettet in die Leiterplatte fällt dieser gar nicht auf. Der Platzbedarf ist vergleichbar mit einem 2D-Code. Von jetzt an kann bereits die Rohleiterplatte Fertigungsdaten jederzeit abrufbar abspeichern – vielleicht das Herstellungsdatum und Charakteristika wie Dicke und Anzahl Layer. Und selbstverständlich kann sie eindeutig identifiziert werden. Dies sogar im Pulk und über relativ große Entfernungen; Reichweiten von größer als einem Meter sind nicht unrealistisch. Lagerlogistikprozesse können daher durch eine automatisierte (Pulk-) Erfassung bereits optimiert werden.

Über Unternehmensgrenzen hinweg

Kommt die Leiterplatte zum MES-Dienstleister, dem Bestücker, und schließlich an die SMD-Fertigungsline, meldet sich die Leiterplatte oder der Nutzen an der Fertigungsline an. Fertigungsmaschinen mit integrierter UHF RFID-Technik machen dies möglich. Leiterplatten können erkannt, die gespeicherten Informationen ausgelesen, aber bei Bedarf auch aktualisiert bzw. ergänzt werden. Wann? Auf welcher Maschine? Mit welcher Produktionszeit? Das sind nur einige Parameter, die abgelegt werden können. Aber auch Sonderereignisse, wie relevante Störungen innerhalb einer Fertigungsmaschine können erfasst werden. Wird die Leiterplatte oder der Nutzen manuell nach dem Ab Stapeln einem neuen Fertigungsprozess zugeführt, kann die Leiterplatte mitteilen, ob sie hier richtig ist – oder vielleicht erst noch einen anderen Prozessschritt durchlaufen muss.

UHF RFID-Reader Ha-VIS von Harting

Dies alles wird mit modernster UHF RFID Technik ermöglicht. Dank der Koaxialkabel basierten Ha-VIS Locfield Antenne und des flexiblen UHF RFID Reader Ha-VIS RF-R350 von Harting ist die Realisierung mit geringem Aufwand möglich. Die Locfield ist eine platzsparende Antenne, die die Datenkommunikation mit den Leiterplatten innerhalb der Fertigungsstraße ermöglicht. Das Antennenfeld folgt hierbei einem Koaxialleiter und ermöglicht daher, bei voller Fertigungsgeschwindigkeit eine Kommunikation mit mehreren Platinen in einem Platinen-Nutzen. Dank der flexiblen und Standard-Konformen Datenverarbeitung des UHF RFID Lese-/Schreibgeräts können die Daten direkt im Reader vorverarbeitet werden. Reader und Antenne können problemlos in Neu- und Altanlagen

integriert werden. Die kompakte Bauform und die hohe Schutzart IP67 erleichtert das Nachrüsten ebenfalls. Eine datentechnische volle Integration in die Fertigungsanlagen ist hierbei jederzeit möglich, aber nicht zwingend nötig. Selbstverständlich können und sollen auch bestehende Back-End Systeme integriert werden. Die Lösung kann einfach und flexibel mit den Ansprüchen und Ideen des Leiterplatten-Bestückers und deren Kunden mitwachsen. Die Datenhaltung auf dem RFID-Chip der Leiterplatte folgt hierbei ISO Standards und bereits aus dem Güterverkehr im Handel bekannten GS1 Standards. Hier ist nicht nur die ID der Leiterplatte selbst gemeint, sondern auch die Prozess- und Fertigungsdaten, die im sogenannten User-Memory des RFID-Chips abgelegt werden. Alles ist also transparent und kann somit auch später von Dritten problemlos genutzt werden. Das Einbetten des UHF RFID Chips direkt in die Roh-Leiterplatte ist sicherlich die eleganteste Lösung, aber nicht die Einzige. Mit dem eingebetteten Chip, welcher dank eines Verfahrens der Firma Beta Layout vollautomatisiert in die Leiterplatte eingesetzt wird, lässt sich der komplette Lebenszyklus und die komplette Fertigungskette direkt in der Leiterplatte abbilden. Auch beim Bestückprozess kann der Chip als SMD Bauteil auf die Leiterplatten aufgebracht werden. Die Firma Murata bietet mit dem Magicstrap entsprechende UHF RFID Chips bzw. Transponder an.

Neue Produktionsprozesse nutzen

Einmal mit der UHF RFID Technik ausgerüstet, kann diese natürlich bei Bedarf ein ganzes Leiterplattenleben genutzt werden. Neben Lagerlogistik Anwendungen, denn auch eine Pulk-Erfassung mehrerer Platinen auf einmal ist möglich, können z.B. Reparaturprozesse optimiert werden. Auch wenn die Leiterplatte nicht mehr funktioniert, also nicht mehr eingeschaltet werden kann, können abgespeicherte Informationen, wie ausgelieferte Firmwareversionen noch abgefragt werden. Außerdem lassen sich die Informationen auch problemlos abfragen, wenn die Platine bereits in einem Fertigprodukt eingebaut wurde. Solange das Gehäuse nicht komplett aus Metall ist und gewisse physikalischen Grundprinzipien eingehalten werden, kann die im RFID Chip enthaltenen Informationen weiterhin genutzt und aktualisiert werden. Bis zur Entsorgung der Leiterplatte stehen die Möglichkeiten der UHF RFID Technik zur Verfügung und können diverse Anwendung ermöglichen und verbessern. Ist dies alles nun blanke Theorie oder wird dies schon reell umgesetzt? Die Firma Nokia nutzt die Vorteile der UHF RFID gestützten Leiterplattenfertigung bereits in ihrer neuen modularen Industrie 4.0 Fertigungsstraße, welche auf der Hannover Messe gezeigt wird. Die ersten dort produzierten Produkte sind schon mit UHF RFID Transponder ausgerüstet. Die verwendeten Maschinen diverser Hersteller, u.a.

eine Lötanlage der Firma Rehm Thermal Systems, sind mit den beschriebenen UHF RFID Produkten von Harting ausgerüstet und erfüllen so die Ansprüche einer Industrie 4.0 fähigen Leiterplattenfertigung. Auch die Firma ASM Assembly Systems GmbH & Co. KG integriert die RFID Technik in ihre Maschinen. Doch nicht nur die Maschinen und die Leiterplatten können mit der RFID Technik ausgerüstet werden. Auch Verbrauchsmaterialien wie Reinigungsrollen, die in den Lotpastendruckern verwendet werden, können automatisiert erkannt werden. Entsprechende Produkte bietet die Firma Vliesstoff Kasper an. Die Zollner Elektronik AG zeigt die Möglichkeiten dieser Technik bereits seit längerem in ihrem Technikum in Cham. Ein Kundenevent, organisiert und begleitet von diversen Größen der Branche, die sich in einem Konsortium zusammengeschlossen haben, fand Anfang April dieses Jahres statt. Ideen, die UHF RFID Technik noch vielseitiger zu nutzen, haben die Mitstreiter in dem Konsortium viele. Unter anderem engagieren sich auch die TU-Dresden, um ganz neue Baugruppenentwicklungen voran zu bringen. Die UHF RFID-Technik macht die Leiterplattenbranche also noch vielseitiger, die Fertigungsprozesse flexibler und sicherer und ermöglicht ganz neue Anwendungsszenarien, bis hin zur Verbesserung eines nachhaltigen Umgangs mit den Rohstoffen einer Leiterplatte durch fachgerechte Entsorgung. Harting hat bereits weitere Ideen und wird gemeinsam mit seinen Partnern an deren Umsetzung arbeiten. www.harting.com ■

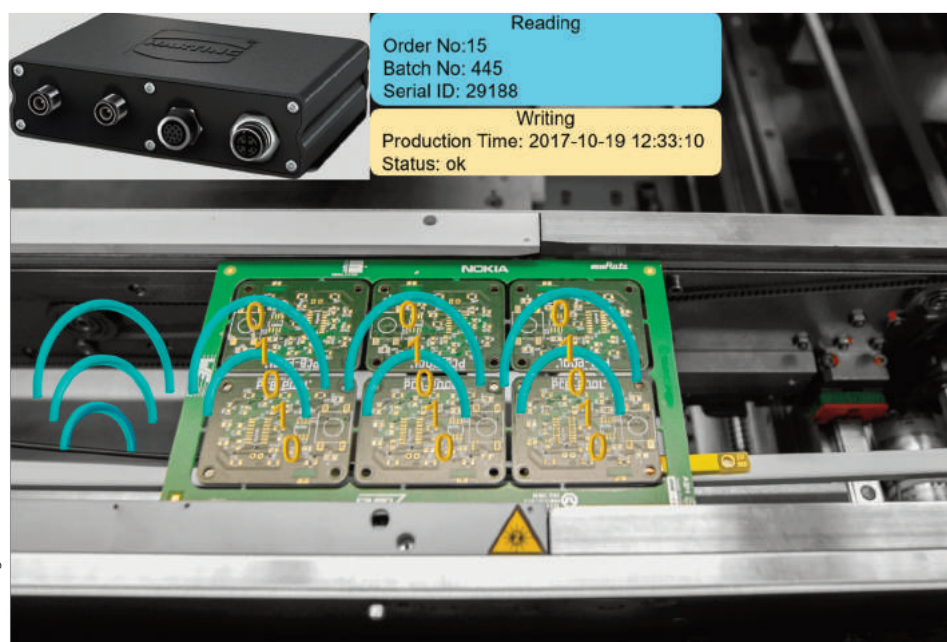


Bild: Harting



Bild: Harting

Bidirektionale Kommunikation direkt mit der Leiterplatte, die dank UHF RFID ein Gedächtnis erhält (links). Der MICA basierte Reader RF-R300 ermöglicht dank Vorverarbeitung der Rohdaten direkt an der Maschine eine einfache Kommunikation mit einem MES genauso wie mit der Maschinensteuerung (rechts).



INDUSTRIAL MANAGEMENT NEWS

INDUSTRIE 4.0

TECHNIK // ARBEITSWELT // GESELLSCHAFT

INDUSTRIE 4.0-MAGAZIN –

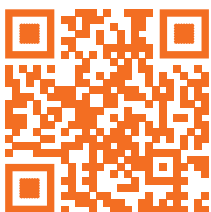
Die Zeitschrift für die vierte industrielle Revolution

Technik, Arbeitswelt,
Gesellschaft – das digitale

INDUSTRIE 4.0-MAGAZIN

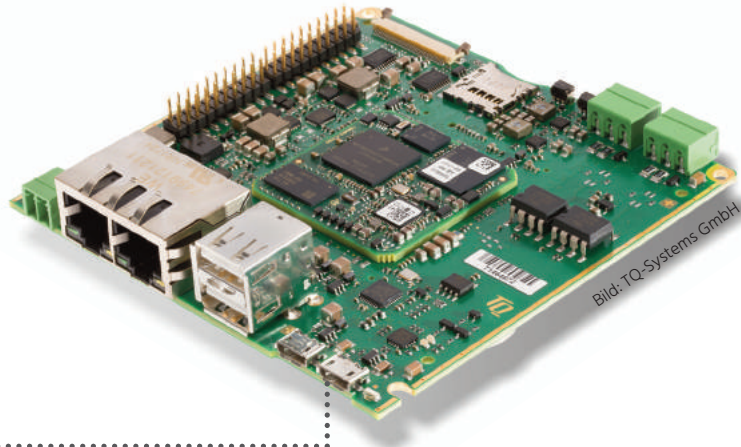
zeigt das ganze Bild!

Verständlich, umfassend
und übersichtlich zusammen-
gestellt. So sichern Sie sich
Ihren Wissensvorsprung!



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

www.tedo-verlag.de | info@tedo-verlag.de



IoT MUST HAVES

Modulare Gateway- Plattform

TQ hat das CPU-Modul TQMa6ULxL vorgestellt. Es setzt mit den i.MX6UL und i.MX6ULL auf eine Cortex-A7-CPU von NXP. Der Datenlogger bzw. das Gateway bieten dem Anwender auf dem 10x10cm großen Basisboard eine Vielzahl von Schnittstellen inklusive RS232, 2xCAN (galvanisch getrennt), 2xUSB2.0 und 2xEthernet. Weiter ist ein MicroSD-Interface zur Speichererweiterung verfügbar. Neben den Standardschnittstellen ist das Board über zwei Mini-PCIe-Steckplätze mit SIM-Card-Interface auf USB2.0-Basis erweiterbar, die Funklösungen wie UMTS/GPRS, Wi-Fi, Bluetooth sowie LoRa-Wan ermöglichen. Über ein Grafikinterface lassen sich Displays in den Diagonalen von 3,5 bis 7" inklusive Touch ohne Zusatzaufwand realisieren. Somit kann das Mainboard auch als Grundlage für HMI-Geräte benutzt werden. Typische Einsatzgebiete für die langzeitverfügbare Plattform sind Gebäudeautomation, Smart Metering, Smart Home, Sicherheit und Überwachung, Industrieautomation, Prozesskontrolle und Service Management.

www.tq-group.com

Funk-Chip und Modul für IoT



Hy-Line Computer Components zeigt ein-On-a-Chip-Produkt, das sich über WiFi mit dem WLAN verbindet: das FC9000 von Silicon Motion. Es ist als Chip und Modul mit Peripherie, wie Antennenstecker, erhältlich. Besondere Merkmale sind eine niedrige Leistungsaufnahme trotz permanenter Verbindung mit dem Router, eine hohe Reichweite durch den empfindlichen HF-Eingang und eingebaute Security-Funktionen. Dadurch ist es für Anwendungen geeignet, die lange im Batteriebetrieb laufen müssen. Je nach Anforderungen soll ein Batteriewechsel erst nach mehr als einem Jahr fällig sein. Ein eingebauter ARM-Kern wickelt alle Netzwerkprotokolle ab, der Host-Prozessor bleibt davon entlastet und ist so auch für IoT im Bereich Home Automation vorgesehen.

www.hy-line.de

DC/DC-Wandler mit niedriger Stromaufnahme

Rohm bietet mit dem BD70522GUL einen Ultra-Low-Power-DC/DC-Wandler mit integriertem Mosfet, der aufgrund seiner geringen Stromaufnahme von 180nA die Anforderungen des IoT-Marktes hinsichtlich langer Batterielaufzeit von bis zu zehn Jahren mit einer Knopfzelle erfüllen soll. Der Wandler bietet Abmessungen von 1,76x1,56x0,57mm und Schaltfrequenzen zwischen 0 und 1MHz. Er arbeitet mit Versorgungsspannungen von 2,5 bis 5,5V und die Genauigkeit der Ausgangsspannung beträgt $\pm 2\%$ (bei 10mA), der maximale Ausgangsstrom 500mA. Der Betriebstemperaturbereich liegt zwischen -40 und $+85^{\circ}\text{C}$, daher soll sich der DC/DC-Wandler insbesondere für kompakte und mobile Geräte eignen.

www.rohm.de

Bild: Rohm Semiconductor GmbH



LAN-Übertrager als Gigabit-Version

Würth Elektronik erweitert seine vollautomatisch gefertigte WE-LAN-AQ-Serie. Die neue Gigabit-Bauform zeichnet sich durch die elektrischen Eigenschaften und eine kompakte Bauform aus, außerdem sind die bisherigen Ringkerne durch SMD-lötbare Transformer und Common-Mode-Choke-Elemente ersetzt. Der LAN-Übertrager ist für den Temperaturbereich von -40 bis $+85^{\circ}\text{C}$ ausgelegt und kompatibel zu gängigen LAN-Produkten. Mit einer Höhe von 4mm bei der 10/100-Base-T-Variante und 4,25mm bei der 1000-Base-T-Variante stehen pin- und pad-kompatible Bauteile für gängige Standardbauformen zur Verfügung.

www.we-online.de

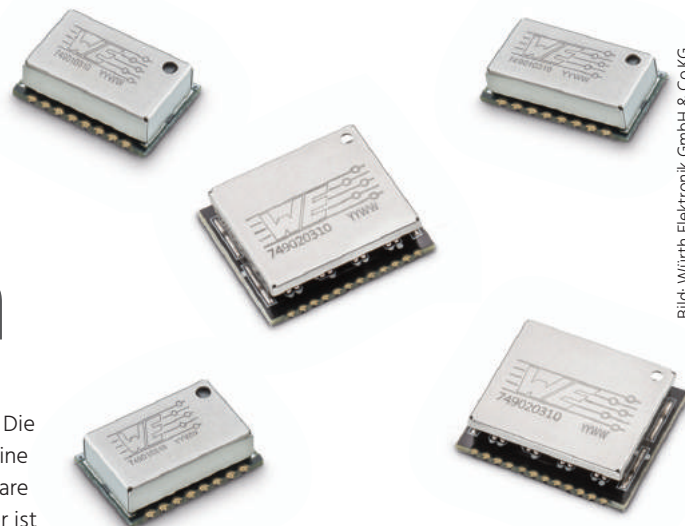


Bild: Würth Elektronik GmbH & Co.KG

Kühlkörper für Leistungselektronik

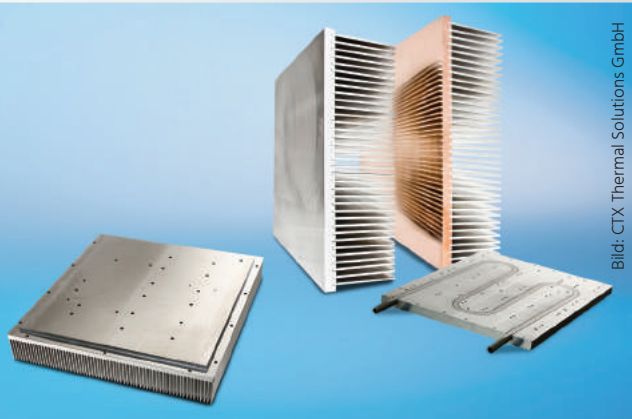


Bild: CTX Thermal Solutions GmbH

Auf der PCIM zeigt CTX Kühllösungen für Anwendungen und Anforderungen im Bereich der Leistungselektronik. Im Fokus des Messeauftritts stehen vor allem die Hochleistungskühlkörper des Unternehmens sowie Produkte mit Flüssigkeitskühlung. Die SuperFins-Hochleistungskühlkörper mit Kupfer- oder Aluminiumbodenplatten und eingepressten Rippen sollen vor allem in Applikationen zum Einsatz kommen, bei denen eine starke Wärmeentwicklung auftritt, wie in der Rundfunktechnik, bei der Stromübertragung oder bei UPS-Systemen. Eine Alternative zu Flüssigkeitskühlkörpern bietet der Hersteller mit den SuperPower-Hochleistungskühlkörpern. Diese sollen dieselben technischen Eigenschaften und eine vergleichbare Kühlleistung wie herkömmliche Stranggussprofile bei niedrigeren Abmessungen und Kosten bieten.

www.ctx.eu

Box-PC mit ULV-CPU

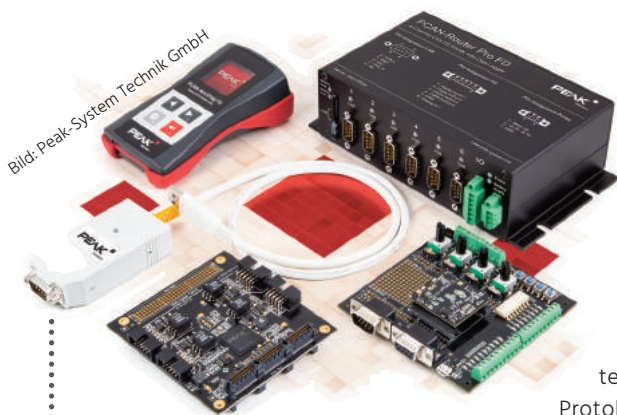


Bild: Efcotec Electronics GmbH

Efcotec hat den Embedded-Box-PC SmartMod vorgestellt. Zum Lieferumfang gehört eine PoE-Option. Das Embedded-System ist mit einem Kaby-Lake-Core-ULV-Prozessor der siebten Generation von Intel ausgestattet und ist für verschiedene industrielle Anwendungen einsetzbar. Die ULV-Prozessoren eignen sich für Anwendungen mit hohen Anforderungen an die Verarbeitungsleistung, wie z.B. industrielle Steuerungssysteme, Überwachungssysteme, Machine-Vision-Systeme, automatische optische Inspektionssysteme sowie Prüf- und Messausrüstungen. Der Box-PC verfügt über sechs Gigabit-Ethernet-Ports (davon vier mit PoE-Option), vier USB-Schnittstellen (4xUSB3.0 und 1xUSB2.0), einen HDMI- oder VGA-Port, einen DisplayPort-Anschluss, 16bit isolierte GPIOs, vier RS-232/422/485-Schnittstellen, zwei RS-232-Interfaces, zwei Mini-PCIe-Anschlüsse mit SIM-Sockel sowie einen Mini-PCIe-Stecker (PCIe und USB).

www.efcotec.com

Hardware für CAN-Bus-Anwendungen



Peak-System Technik stellt die stapelbare Steckkarte PCAN-PCI/104-Express FD vor, die bis zu vier CAN-FD-Kanäle aufweist. Für die Anbindung an LIN-Netzwerke veröffentlicht das Unternehmen den PLIN-USB, ein einfach zu handhabendes PC-USB-Interface. Es unterstützt das LIN-Protokoll gemäß ISO17987 und erfüllt alle LIN-Spezifikationen bis Version 2.2.

Außerdem wird das Einsteckmodul PCAN-MicroMod FD für die Entwicklung eigener Hardware mit CAN-FD-Anschluss und I/O-Funktionalität angeboten. Ebenfalls erhältlich ist der PCAN-Router Pro FD, der mit sechs CAN-FD-Kanälen individuell oder einer Windows-Software konfiguriert werden kann. Ebenfalls im Portfolio des Herstellers zu finden ist das kompakte Diagnosegerät PCAN-MiniDiag FD, das Übertragungsraten erkennt, Error-Frames zählt und Terminierung sowie Buslast misst.

www.peak-system.com

Hardware für Box-PCs

Unter dem Namen Smartcase fasst Fujitsu seine Bausätze für Boxed-Industrial-PCs zusammen. Sie richten sich an Systementwickler, die ohne hohen Engineering- und Testaufwand kompakte Industrie-PCs konzipieren möchten. Dazu gehören Tiny-PCs mit Mainboards in den Formaten Mini-ITX (170x170mm) und Mini-STX (147x140mm). Entwickler erhalten neben Mainboard und Gehäuse auch Kühlkörper, Riser-Karten und Adapterkabel, außerdem interne AC-Adapter und Grafikkarten. Alle Bestandteile der Cases wurden hinsichtlich Klimateigenschaften getestet und zertifiziert. Erhältlich ist das S500 für die Industrie-Mainboards der Reihe DS3544-S im Format Mini-STX, die für die neue Generation der Low-Power-Prozessoren der Intel Gemini-Lake-Familie ausgelegt ist. Der Hersteller verwendet ein flaches Design mit 36mm Bauhöhe und einem Gehäuse von 0,9l Volumen. Das zweite Smartcase S700 eignet sich für die Mainboards der Serie D3543-S im Format Mini-ITX, die ebenfalls die neuen Gemini Lake-CPU's unterstützen. Dieses Case verfügt über einen Low-Profile-Erweiterungssteckplatz, der u.a. Platz für einen AC-Adapter oder eine Low-Power-Grafikkarte bietet.

www.tds.fujitsu.com



Bild: Fujitsu TDS GmbH

Embedded-PC Gehäuse

- funktionelle Aluminiumgehäuse für verschiedenartige Embedded Formfaktoren
- wahlweise integrierte Kühlrippen zur effizienten Entwärmung von Embedded Mainboards
- Tragschienen- und Monitorbefestigungen
- EMV-gerechte Ausführungen
- kundenspezifische Anfertigungen mit individuellen Gestaltungsmöglichkeiten



Mehr erfahren Sie hier:
www.fischerelektronik.de

Fischer Elektronik GmbH & Co. KG

Nottebohmstraße 28
 58511 Lüdenscheid
 DEUTSCHLAND
 Telefon +49 2351 435-0
 Telefax +49 2351 45754
 E-mail info@fischerelektronik.de



Wir stellen aus:
 „HIGH END“ in München
 10.5 - 13.5.2018
 Halle 3, Stand L13

Daten-Flatrate für das IoT

1NCE hat sein Connectivity-Modell für IoT-Anwendungen vorgestellt. Mit der Lifetime Fee zahlen Kunden einmalig 10€ und können über eine Laufzeit von zehn Jahren auf eine Daten-Flatrate zugreifen. Bereits in den ersten Tagen nach Markenstart trafen laut Anbieter Vorbestellungen für SIM-Karten im hohen sechsstelligen Bereich ein. Das Lifetime-Fee-Preismodell ermöglicht den Kunden durchgängige IoT-Konnektivität über eine Laufzeit von zehn Jahren zum einmaligen Preis von 10€. Damit verbunden ist eine Daten-Flatrate, die bis zu 500MB für den gesamten Lebenszyklus eines Geräts abdeckt. Nach heutigem Stand repräsentiert dieses Inklusivvolumen den Grundbedarf der meisten Low-Bandwidth-Applikationen. Darüber hinaus ist die Lösung geeignet, 'Connectivity as a feature' sowohl bei OEMs als auch bei IoT-Modul- und Gateway-Herstellern sowie IoT-

Plattformanbietern zu integrieren. Dadurch wird es möglich, konnektierte Gesamtlösungen im Sinne einer End-to-End-Lösung anzubieten. Der Vertriebsstart für die Connectivity-Lösungen ist für August 2018 geplant. Ab diesem Zeitpunkt wird auch die Connectivity-Management-Plattform zur Verwaltung und Steuerung der SIM-Karten bereitstehen. Unter der Website des Unternehmens können sich Interessenten bereits in Kürze registrieren und größere Mengen an SIM-Karten vorbestellen. Die Connectivity-Lösungen sind zunächst innerhalb der Europäischen Union sowie in der Schweiz und Norwegen verfügbar. Parallel dazu werden in den kommenden Monaten Strukturen aufgebaut, um das Angebot auch in ausgewählten Märkten außerhalb Europas anzubieten.

www.1nce.com

Tools für Deep Learning

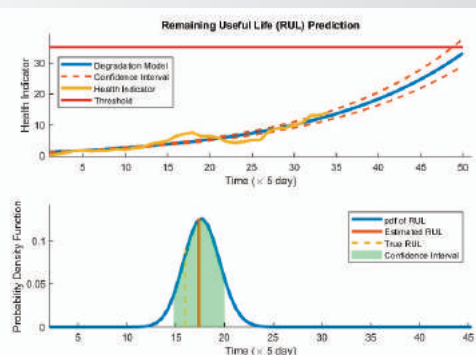


Bild: MathWorks GmbH

Mathworks hat das Release 2018a mit einer Reihe neuer Funktionen in Matlab und Simulink vorgestellt. Es enthält u.a. die Predictive-Maintenance-Toolbox zum Entwerfen und Testen von Algorithmen für die Zustandsüberwachung und vorausschauende Wartung sowie das Vehicle Dynamics Blockset für die Modellierung und Simulation von Fahrzeugdynamik in einer virtuellen 3D-Umgebung. Mit der Toolbox können Ingenieure Daten kennzeichnen, Zustandsindikatoren entwerfen sowie Störfälle bei Maschinen voraussagen und vermeiden. Zur Analyse können Maschinendaten aus lokalen Dateien, Cloud-Storage und verteilten Dateisystemen importiert werden. Die Box enthält Referenzbeispiele für Motoren, Getriebe, Batterien und andere Maschinen, die Richtwerte für die Entwicklung eigener prädiktiver Wartungs- und Zustandsüberwachungsalgorithmen zur Verfügung stellen.

www.mathworks.de

Robustheitstests mit Fuzzing-Werkzeug

Bestorm von Hitex ist ein Werkzeug zur Durchführung von Robustheitstests und bedient sich der Fuzzing-Testmethodik, bei der zufällig erzeugte Daten an das Testobjekt geschickt werden, um ein Fehlverhalten zu provozieren. Das System unterstützt eine Vielzahl von Protokollen aus unterschiedlichen Anwendungsbereichen und kann für proprietäre und andere Protokolle erweitert werden. Um Fehlverhalten zu entdecken, wird ein Monitor eingesetzt, der das Testobjekt überwacht und die ordnungsgemäße Funktion sicherstellen soll. Diese Überwachung ist individuell vom Testobjekt abhängig und kann unterschiedliche Aussagekraft haben. Meldet der Monitor ein abnormales Verhalten an das System, erstellt es ein Python-Skript, mithilfe dessen das abnormale Verhalten reproduziert werden kann. Der Quellcode der überprüften Anwendung kann dabei in einer beliebigen Programmiersprache geschrieben sein.

www.hitex.de



Bild: Hitex GmbH

Auf Rekordjagd

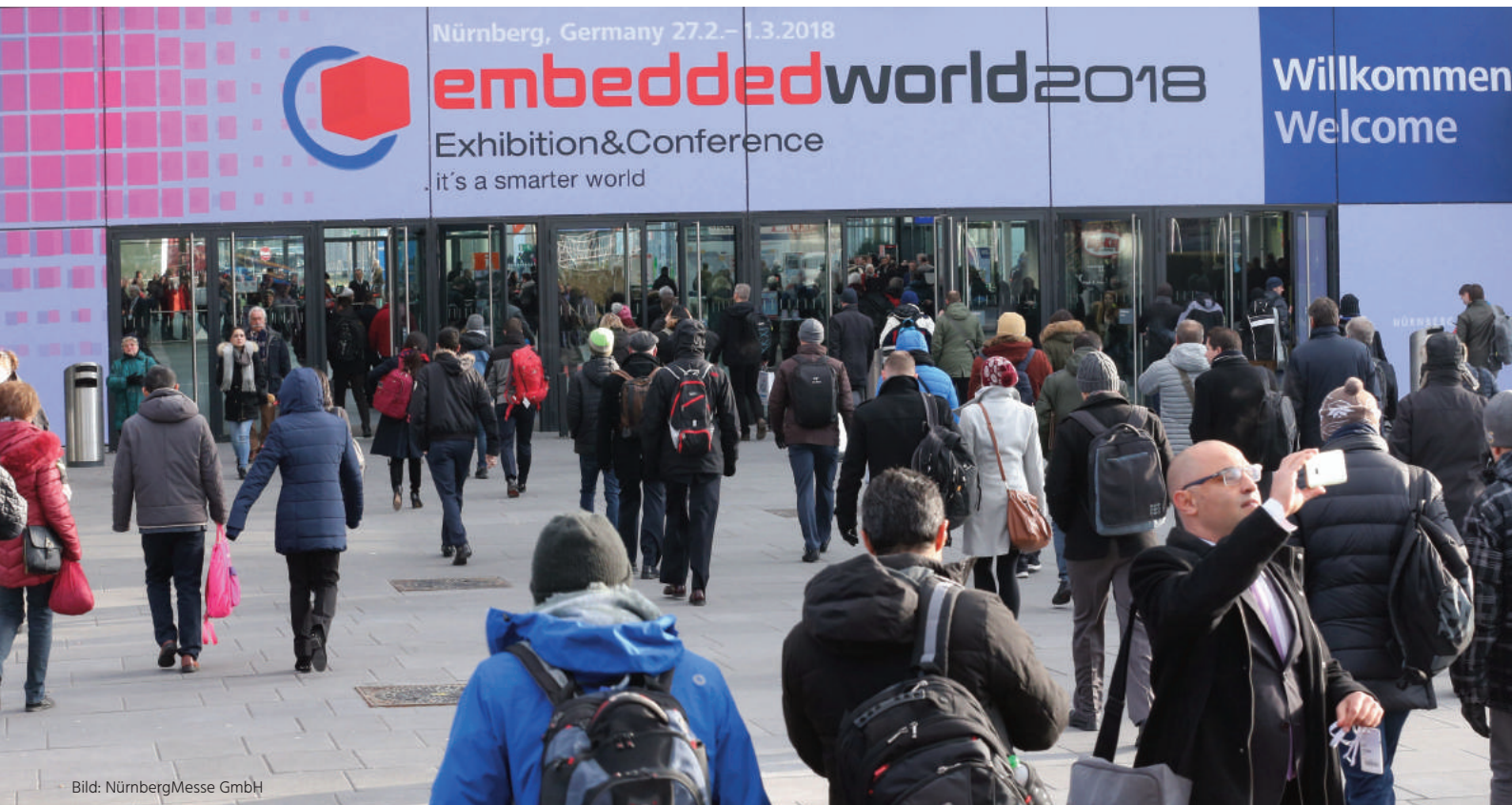


Bild: NürnbergMesse GmbH

Im 16. Veranstaltungsjahr stellt die **embedded world** ein weiteres Mal unter Beweis, dass sie die Leitmesse der internationalen Embedded-Community ist. **1.021 (+1 Prozent) Unternehmen aus aller Welt** zeigten den **32.217 (+7,3 Prozent) Embedded-Experten** aus **78 Ländern** in sechs Hallen wo die Reise im Internet der Dinge und der zunehmend digitalisierten Welt hingeht. Innovative und visionäre Produkte wurden zum 14. Mal mit dem **embedded award** prämiert.

NürnbergMesse GmbH

1.021 Unternehmen aus 38 Ländern präsentieren sich auf der embedded world. Das ist die bis dato stärkste Beteiligung. Und wir sehen nach wie vor enormes Potential. Auch zur 16. Veranstaltung wächst sie in den wichtigen Messeparametern Besucher, Aussteller und Fläche. Die Innovationskraft der Ingenieure, die Digitalisierung, die ohne Embedded-Technologien ebenso wenig möglich wäre wie das Internet der Dinge, die beiden Konferenzen und die Nachfrage eines weltweiten Marktes sind Motoren der Branche“, so Richard Krowoza, Mitglied der Geschäftsleitung, NürnbergMesse.

Zufriedene Aussteller und Fachbesucher

Auch dieses Jahr überzeugte die embedded world ihre Community. 97 Prozent der Fachbesucher gaben noch während der Laufzeit der Messe an, 2019

wieder teilzunehmen. 96 Prozent waren mit der embedded world zufrieden. Ebenso positiv sehen dies die ausstellenden Unternehmen: 95 Prozent werden laut eigener Aussage auch 2019 wieder ausstellen, ebenso viele haben ihre Zielgruppen erreicht und neun von zehn erwarten ein Nachmessegeschäft.

Die Gewinner stehen fest

Die Gewinner des embedded awards 2018 stehen fest: Antenna ist mit der Antenna Robusta SR4G031 Sieger in der Kategorie Hardware. Embedded Trend überzeugt mit byET-engine in der Kategorie Software. Data I/O Corporation gewinnt mit SentiX in der Kategorie Tools. Die Preise wurden von Prof. Dr.-Ing. Matthias Sturm, Vorsitzender der Jury, und Dr. Roland Fleck, Geschäftsführer der NürnbergMesse, überreicht. Die Gewinner finden Sie auch unter: www.embedded-world.de/award. www.embedded-world.de ■

```

_save_thread_context:
    MRS     R12,PSP                ; Pickup thread's stack pointer
    STMDB   R12!,{R4-R11}         ; Save thread context
    LDR     R0,=_current_thread    ; Pickup current thread pointer address
    LDR     R1,[R0]               ; Pickup current thread pointer
    STR     R12,[R1]              ; Save thread's stack pointer
    MOV     R12,#0                ; Build NULL value
    STR     R12,[R0]              ; Clear current thread pointer
    B       _scheduler            ; Look for next thread to execute

...

_scheduler:
    LDR     R0,=next_thread        ; Pickup next thread pointer address
    LDR     R1,[R0]               ; Pickup next thread to schedule
    CBZ     R1,_scheduler          ; If no thread, continue checking
    B       _restore_thread_context

...

_restore_thread_context:
    LDR     R0,=_current_thread    ; Pickup current thread pointer address
    STR     R1,[R0]               ; Setup current thread pointer
    LDR     R12,[R1]              ; Pickup thread's stack pointer
    LDMIA   R12!,{R4-R11}         ; Recover thread context
    MSR     PSP,R12               ; Setup thread stack pointer
    MOV     LR,#0xFFFFFFF0        ; Setup return to thread on PSP

```

RTOS: Elf Mythen

Die UBM **Embedded Developer-Umfrage** des Jahres 2015 ergab, dass **mehr als 60%** der **aktuellen Projekte Echtzeitfähigkeiten bieten** und dass mehr als ein Drittel mit einer grafischen Benutzeroberfläche (GUI) ausgestattet ist. Mehr als 70% der Befragten gaben an, dass sie ein Echtzeit-Betriebssystem (RTOS) oder einen Scheduler verwenden. Von den verbleibenden 30%, die kein RTOS nutzen, wurde mit 79% als wichtigster Grund hierfür genannt, dass die Anwendung kein RTOS erforderte. Dennoch ranken sich die **verschiedensten Mythen um die Gründe für die Verwendung (oder auch Nichtverwendung) eines RTOS.**

WILLIAM E. LAMIE, Co-Founder and CEO, Express Logic

Mythos Nr. 1: Die meisten IoT-Geräte brauchen kein RTOS.

Die Embedded-Industrie registriert bereits eine intensive Abkehr von 8- und 16bit-Mikroprozessoren, was sowohl an den Forderungen nach verbesserter Geräte-Funktionalität als auch am attraktiven Preis-Leistungs-Verhältnis der neuen 32bit-Mikroprozessoren liegt. IoT-Geräte benötigen eine Netzwerkanbindung und eine GUI und verlangen deshalb generell nach 32bit-Mikroprozessoren, allein schon um über den nötigen Adressraum und hinreichend Verarbeitungsleistung verfügen zu können. Ähnliche Entwicklungen vollziehen sich bei der Software. Allein die gesteigerten Vernetzungs-Anforderungen erfordern die Verarbeitung von Kommunikations-Protokollstacks auf dem 32bit-Embedded-Prozessor, was die Verwendung eines RTOS zwingend erforderlich macht. Auch die GUI-Design- und Laufzeit-Software von Drittanbietern stützt sich meist auf RTOS-Dienste.

Mythos Nr. 2: Eine Polling-Loop-Architektur funktioniert genau so gut wie ein RTOS.

Viele ältere 8- und 16bit-Bausteine nutzen eine Polling-Loop-Software-Architektur, um die Verarbeitungszeit auf die verschiedenen Threads zu verteilen. Diese Technik ist zwar leicht zu verstehen und eignet sich gut für einfache Geräte. In komplexeren Anwendungen stößt sie aber an ihre Grenzen. Das Problem besteht darin, dass die Reaktionszeit eines jeden Threads in der Schleife von der Verarbeitung der übrigen Polling-Schleife abhängig ist, sodass als Worst-Case-Reaktionszeit entsprechend die größtmögliche Verarbeitungszeit durch die Schleife angesetzt werden muss. Wenn sich die Verarbeitung in der Polling-Schleife dynamisch ändert, verändert sich die Reaktionszeit eines jeden Threads genauso. Je mehr Komplexität zu der Pollingabfrageschleife hinzugefügt wird, umso schwieriger wird es, die Echtzeitanforderungen vorher-

zusagen und einzuhalten, was wiederum Auswirkungen auf die Zuverlässigkeit von IoT-Geräten hat. Im Gegensatz dazu ist die Reaktionszeit bei der Verwendung eines RTOS konstant. Darüber hinaus koordiniert das RTOS im Hintergrund die Zuweisung des Prozessors zu den Thread-Prioritäten, sodass sich die Anwendungssoftware nicht darum kümmern muss, wieviel Verarbeitungszeit jeder Thread beansprucht. Nicht zuletzt haben Änderungen in den Verarbeitungs-Verantwortlichkeiten eines bestimmten Threads keine Auswirkungen auf die Reaktionseigenschaften von Threads mit höherer Priorität.

Mythos Nr. 3: Ein RTOS bringt einen Mehraufwand mit sich, der mein IoT-Gerät überfordern würde.

Selbstverständlich verursacht ein RTOS einen gewissen Overhead im Zusammenhang mit API-Aufrufen und Kontextwechseln. Dieser Mehraufwand ist jedoch gering, außerdem konstant und wahrscheinlich geringer als der Aufwand einer komplexen Polling-Schleife. So erfordern RTOS-Kontextwechsel auf einem Cortex-M typisch weniger als 120 Zyklen (diese Zahl kann von Architektur zu Architektur und von RTOS zu RTOS variieren). Damit eine Polling-Schleife (oder eine andere RTOS-Alternative) hier besser abschneidet, müsste sie vorhersagen und garantieren können, dass die Worst-Case-Verzögerung beim Aktivieren eines Threads weniger als 120 Zyklen beträgt (das sind etwa 50 bis 60 Zeilen C-Code). Für das Prüfen jedes Threads in der Schleife und die Ausführung des Codes für jeden aktiven Thread dürfen somit weniger als 60 Instruktionen notwendig sein. Selbst wenn kein anderer Thread etwas zu tun hätte, würde allein das Abfragen jedes Threads Zyklen beanspruchen, bis schließlich der Thread, der die Bearbeitung angefordert hat, abgefragt wird. Dies mag bei Schleifen mit fünf bis zehn Threads noch funktionieren, doch bei größeren Schleifen lassen sich die besagten 60 Instruktionen nicht mehr einhalten. In einer Worst-Case-Analyse muss all den intervenierenden Threads Verarbeitungszeit zugewiesen werden, sodass Echtzeit-Eigenschaften selbst bei einer minimalen Schleife mit zwei Threads praktisch unmöglich zu realisieren sind.

Mythos Nr. 4: Ein RTOS macht die Entwicklung komplexer.

Kleine Gerätefirmware-Projekte mit einem Gesamt-Speicherbedarf von meist weniger als 32KB lassen sich problemlos von einem oder zwei Firmwareentwicklern bewältigen. Beide müssen das Laufzeitverhalten und die Anforderungen des Geräts in ihrer Gesamtheit verstehen, weil die Logik zur Zuweisung des Prozessors auf den gesamten Applikations-Code verteilt ist. Wenn jedoch der Funktionsumfang eines solchen Geräts wächst, indem beispielsweise Protokolle für die Cloud-Kommunikation hinzukommen, wird das Entwicklerteam größer, sodass nicht mehr jeder die Verarbeitungsanforderungen der Firmware versteht. In diesem Fall muss die Kommunikation unter den von den verschiedenen Teammitgliedern entwickelten Codemodulen so gestaltet und umgesetzt werden, dass eine Synchronisation der Threads untereinander und ein Informationsaustausch möglich ist. Ein RTOS dagegen macht die Entwicklung einfacher, wenn die Funktionalität zunimmt. Mit einem RTOS kann sich jeder Firmwareentwickler auf seinen spezifischen Abschnitt

der Firmware konzentrieren, ohne sich um die Verarbeitungsanforderungen der übrigen Firmware des Geräts zu kümmern. Darüber hinaus gibt es effiziente, konsistente und genau definierte Dienste für die Inter-Thread-Kommunikation (Messaging, Semaphoren usw.).

Mythos Nr. 5: Mit einem RTOS wird das Hinzufügen neuer Features zu meinem Gerät schwieriger.

Ein RTOS nimmt sich im Hintergrund der Prozessorzuweisungs-Logik an, sodass sich die Echtzeit-Performance einer hochprioritären Task problemlos garantieren lässt – ganz gleich, ob die Firmware 32KB oder 1MB groß ist oder wie viele Threads es in der Applikation gibt. Allein dies vereinfacht das Pflegen der Applikation und das Hinzufügen neuer Features zu einem Gerät. Hinzu kommt, dass die meisten kommerziellen RTOS-Lösungen einen umfangreichen Bestand an fertig integrierter Middleware mitbringen, mit dem sich das Hinzufügen von Netzwerk-Features, Dateisystemen, USB und GUIs vereinfacht.

Mythos Nr. 6: Ein RTOS erschwert das Portieren von Applikationen.

Anwendungen mit RTOS greifen über ein API auf ihre Dienstfunktionen zu, wodurch das RTOS plattformunabhängig wird. Der Wechsel auf einen anderen Prozessor wird vereinfacht, da keine der Dienst-Referenzierungen der Applikation geändert werden muss. Anders ausgedrückt: die Applikation läuft überall dort, wo auch das RTOS läuft, und das heißt bei den meisten kommerziellen und Open-Source-RTOS-Produkten, dass sie auf praktisch jeder 32bit-Prozessorarchitektur lauffähig ist. Bei nur geringen Änderungen an ihrem Code profitieren Entwickler also von der Portierbarkeit ihrer Applikationen.

Mythos Nr. 7: Ein RTOS belegt zu viel Speicher.

Ein RTOS benötigt für seinen Betrieb sowohl Befehlsspeicher (meist Flash) als auch Datenspeicher (RAM). Ein gutes kommerzielles RTOS aber braucht nur wenig von beidem: meist sind es rund 2KB Befehlsspeicher und 1KB RAM. Selbstverständlich sind diesbezüglich auch die Anforderungen der Applikation zu erfüllen, wodurch es noch vorteilhafter ist, wenn das RTOS mit wenig Speicher auskommt.

Mythos Nr. 8: Ein RTOS benötigt zu viele Verarbeitungszyklen.

Tatsache ist, dass ein RTOS Verarbeitungszyklen für Kontextwechsel, API-Aufrufe usw. benötigt, jedoch stehen diese Zyklen in direktem Zusammenhang mit dem, was die Applikation verwendet. Wenn etwa

Sensor+Test 2018: Willkommen zum Innovationsdialog

Die Messtechnik-Messe Sensor+Test (26. bis 28. Juni 2018) bringt Angebot und Nachfrage zusammen: Wer zum Innovationsdialog in der Sensorik, Mess- und Prüftechnik etwas beizutragen hat, ist dabei – und wer an Sensorik, Mess- und Prüftechnik Bedarf hat, kommt dort hin. In zwei Messehallen ist die gesamte messtechnische Systemkompetenz für Mess-, Prüf- und Überwachungsaufgaben aller Branchen vertreten. Darüber hinaus finden parallel die 19. ITG/GMA-Tagung 'Sensoren und Messsysteme' und der Kongress ETTC 2018 statt.

TÜV für Künstliche Intelligenz

Das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) und TÜV Süd starten eine Kooperation, um Systeme mit Künstlicher Intelligenz (KI), die beim autonomen Fahren im Einsatz sind, zu zertifizieren und um einen 'TÜV für Algorithmen' zu entwickeln. Dazu erforschen die Experten das Lernverhalten der KI-Systeme, um deren Reaktionen kontrollieren zu können. Kernstück ist die Entwicklung einer offenen Plattform für OEM, Zulieferer und Technologieunternehmen, die Module mit Künstlicher Intelligenz validieren soll.

Produktkataloge 2018

Bicker Elektronik hat zwei neue Produktkataloge veröffentlicht: 'Power Solutions for Industrial and Medical Systems' mit aktuellen Stromversorgungs- und USV-Lösungen sowie 'Power+Board Solutions for Professionals' mit ausgewählten Power+Board-Bundles, Systemkomponenten und Zubehör. Direktlink zu den Produktkatalogen (Bestellung oder PDF-Download): www.bicker.de/index.php/bicker/Support/Download/Kataloge.

Bild: Bicker Elektronik GmbH



eine bestehende Polling-Schleife unverändert aus einem einzigen Thread in einem RTOS ausgeführt wird, entsteht keinerlei Mehraufwand, und die Schleife wird genau so verarbeitet wie zuvor. Zusätzlicher Verarbeitungsaufwand durch das RTOS entsteht erst dann, wenn RTOS-Dienste genutzt werden. Hinzu kommt, dass ohne ein RTOS die Applikation selbst für alle erforderlichen Verarbeitungsaufgaben verantwortlich ist, einschließlich der Zyklen, die für das Polling, die Funktionsaufrufe und die Interruptverarbeitung aufgewendet werden. Wenn man also von ganz einfachen Anwendungen absieht, ist es wahrscheinlich, dass das RTOS weniger Zyklen benötigt als die Applikation, wenn sie alle Aufgaben allein bewältigen müsste.

Mythos Nr. 9: Ich habe nicht die Zeit, die Verwendung eines RTOS zu erlernen.

Der Aufwand zur Einarbeitung in ein RTOS ist proportional zu dem, was von der Applikation genutzt wird. Z.B. würde für das Verlegen einer bestehenden Polling-Schleife in einen einzelnen Thread praktisch kein zusätzlicher Lernaufwand entstehen. Die Fallstricke, die bei der Verwendung einer Polling-Loop-Architektur lauern, sorgen aber dafür, dass das Studieren und erneute Untersuchen der Leistungsfähigkeit der gesamten Firmware den Aufwand zum Erlernen eines RTOS sehr schnell bei weitem übersteigt, besonders wenn man den ursprünglichen Code nicht selbst geschrieben hat. Die meisten Anbieter guter kommerzieller Echtzeit-Betriebssysteme bieten außerdem Vor-Ort-Schulungen und äußerst umfangreiche Dokumentation an. Abgesehen davon ist ein gutes kommerzielles RTOS auch einfach zu verstehen und anzuwenden.

Mythos Nr. 10: Ein kommerzielles RTOS kann ich mir nicht leisten.

Das alte Sprichwort, das man das bekommt, was man bezahlt, gilt auch für RTOS-Produkte. Bei kostenlosen oder Open-Source-RTOS-Produkten besteht nicht das garantierte Eigeninteresse an Kompaktheit, Effizienz und einfacher Anwendung. Das Fehlen stetiger Einnah-

men bringt auch einen Mangel an Forschung und Entwicklung, Produktrevolution und – was am wichtigsten ist – Fähigkeit zur umfassenden Unterstützung des Kunden mit sich. Ein RTOS ohne zielgerichteten Support zu nutzen, ist jedoch genauso, als würde man die Zahlenfolge '1234' als Passwort für alles verwenden: es kann funktionieren, aber irgendwann holt es einen ein. Die Kosten für die meisten kommerziellen RTOS-Lizenzen beginnen in der Größenordnung von 10.000 US-Dollar für eine Non-Royalty-Lizenz mit komplettem Quellcode und vollwertiger Unterstützung. Dies stellt einen enormen Wert dar und kostet doch nur einige Monate Gehalt eines typischen Embedded-Firmware-Entwicklers. Außerdem ist es ein einmaliger Lizenzkauf, so dass die Lizenz anschließend unbegrenzt lange genutzt werden kann. Ein entsprechender Entwickler kostet dagegen jeden einzelnen Monat zwischen 5.000 und 10.000 US-Dollar.

Mythos Nr. 11: Ein RTOS wäre ein Overkill für meine Anwendung.

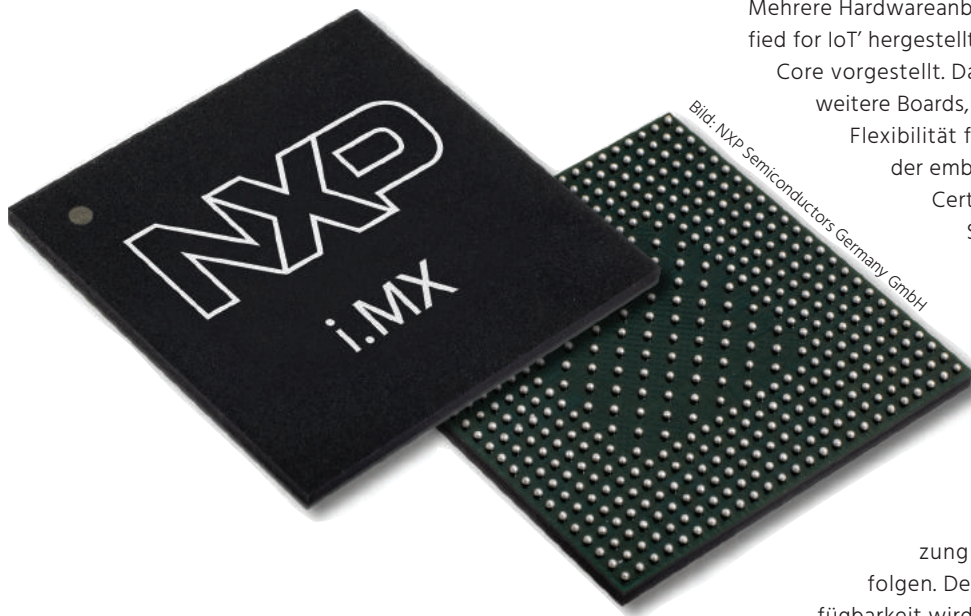
Die Kriterien, ab wann sich ein RTOS lohnt, lassen sich nur schwierig präzise angeben. Wenn aber ein Gerät insgesamt weniger als 16KB Speicher (ROM und RAM zusammen) enthält, ist die Wahrscheinlichkeit groß, dass ein RTOS tatsächlich ein Overkill wäre. Solche Geräte dienen meist einem ganz bestimmten Zweck und sind überwiegend mit einem 8- oder 16bit-Mikroprozessor bestückt. Sobald die Firmware für ein Gerät mehr als 32KB Speicher umfasst oder ein Kommunikations-Protokoll (wie alle IoT-Geräte) oder eine GUI enthält, ist ein RTOS nahezu unverzichtbar. Doch auch ein 32KB großes, für einen bestimmten Zweck und nicht für das IoT vorgesehenes Gerät kann von einem RTOS profitieren, einfach um Vorder- und Hintergrund-Tasks in zwei separate Threads gliedern zu können. Eine solche Konfiguration würde nur 32KB zusätzlichen Speicher für das RTOS erfordern, während im Gegenzug die Firmware deutlich einfacher würde und sich künftig leichter erweitern ließe. Angesichts des rapiden Wachstums des IoT und der neuen Geräte, die es nutzen sollen, wird es immer wahrscheinlicher, dass auch Entwickler, die bisher ohne RTOS entwickelt haben, schon in naher Zukunft die Verwendung eines RTOS ins Auge fassen werden.

www.rtos.com ■

Sinnvolle Synergie

Mit **Microsoft Windows 10 IoT Core** wird die **Softwareunterstützung für i.MX 6- und i.MX 7-** Applikationsprozessoren über die bisherigen Linux- und Android BSP-Angebote hinaus **weiter ausgebaut**.

PATRICK STILWELL,
Product Line Manager für i.MX-Applikationsprozessoren, NXP



Windows 10 IoT Core, eine Variante von Windows 10, ist speziell für die Realisierung intelligenter Dinge konzipiert und wurde für den Einsatz in intelligenten Edge-Produkten wie IoT-Gateways, Robotern oder Konferenzraumsteuerungen ausgelegt. Die NXP i.MX 6- und i.MX 7-Prozessoren zählen zu den weitverbreitetsten IoT-Prozessorfamilien. Mit der geplanten kommerziellen Unterstützung können IoT-Entwickler leistungsstarke und energiesparende Produkte nach Industriespezifikation realisieren. Damit entsteht mehr Flexibilität bei der Entwicklung Cloudbasierter Systeme für das Hardwareportfolio. Der Ausbau des Angebots für die i.MX 6- und i.MX 7-Familien stellt einen großen Schritt hin zur Realisierung eines Betriebssystems für alle vernetzten Produkte dar.

Alleinstellungsmerkmale

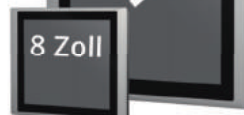
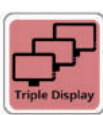
Eines der Alleinstellungsmerkmale ist Trusted I/O. Dafür nutzt NXP Windows 10 IoT Core zusammen mit einer besonderen Funktion des Prozessors zur Steuerung von I/O-Pins über eine TrustZone. Anlagen in der Fertigung oder kritische Infrastrukturprodukte können auf diese Weise sicher betrieben werden, was sich insbesondere im IoT-Bereich positiv auswirkt. Die Trust-Technologie ist heute nur auf Windows 10 IoT Core im Zusammenspiel mit i.MX 6 und i.MX 7 möglich. NXP freut sich, den geplanten kommerziellen Support mit Windows 10 IoT Core für die NXP i.MX6- und i.MX 7-Produktlinien ankündigen zu können. Mehrere Hardwareanbieter haben bereits nach 'Microsoft Azure Certified for IoT' hergestellte Produkte auf i.MX 6-Basis mit Windows 10 IoT Core vorgestellt. Dazu zählen SoMs (System-on-Module) wie auch weitere Boards, die interessierten Herstellern mit ihren Optionen Flexibilität für die Realisierung ihrer Produkte eröffnen. Auf der embedded world waren i.MX 6-basierte, nach 'Azure Certified for IoT' konzipierte Boards an folgenden Ständen zu sehen:

- Aaeon PICO-IMX6
- Advantech RSB-4411
- Keith und Koep pConXS mit Trizeps VII
- Kontron SMARC-sAMX6i
- SolidRun Hummingboard Edge

Im Laufe des Jahres wird NXP zusammen mit Microsoft weitere Lösungen zur Unterstützung der Prozessoren mit Windows 10 IoT Core veröffentlichen. Der endgültige Zeitplan für die kommerzielle Verfügbarkeit wird noch bekannt gegeben. www.nxp.com ■

- Anzeige -

Flexibler Panel PC – CV-1000-Serie



PC-Modul



www.comp-mall.de

Immunsystem für das IoT

Eiskalt erwischt hat es im Sommer 2014 über 17 Millionen Menschen, die sich der 'ALS Ice Bucket Challenge' stellten. Die Aktion galt der Erkrankung 'Amyotrophe Lateralsklerose' (ALS) und wurde zum weltweiten Phänomen in den sozialen Netzwerken. Die Erfolgsbilanz: 115 Millionen US-Dollar Spendengelder in nur sechs Wochen für die Entwicklung von ALS-Heilmitteln. Die Erkrankung zerstört Nervenzellen, schwächt die Muskeln und beeinträchtigt grundlegende Funktionen. Die Teilnehmer der Aktion kippten sich einen Eimer eiskalten Wassers über den Kopf, luden die Videos davon im Internet hoch – und waren vor allem um eine Erfahrung reicher: Wie es sich anfühlt, wenn Körperfunktionen wie die Atmung aussetzen. Eine Lähmung des Nervensystems für den Bruchteil einer Sekunde.

STEVE HANNA, Senior Principal, Infineon Technologies AG

Netzwerkgeräte: Das Nervensystem der verbundenen Welt

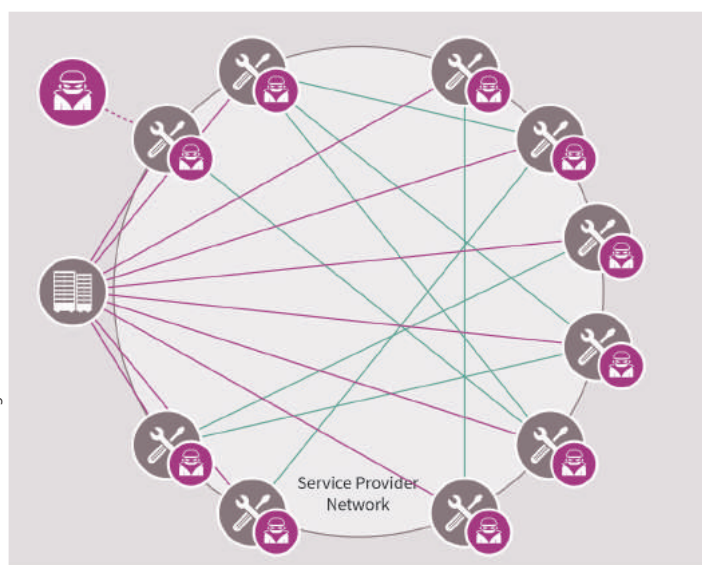
Im Herbst 2016 waren Millionen von Internetusern vom Vorfall mit dem Mirai-Botnetz betroffen. Angreifer hatten ein IoT-Botnetz bestehend aus mehr als einer halben Million kompromittierter Standardrouter und anderen IoT-Geräten genutzt, um bekannte Websites wie Twitter, Netflix und Airbnb auszuschalten. Eine Lähmung des Internets für einige Stunden. Vergleiche zwischen dem menschlichen Körper und einem IoT-System drängen sich durchaus auf, wenn es um die Risiken hinter dem aktuellen Trend des Internets der Dinge (IoT – Internet of Things) geht. Ein IoT-System ist ein ungeheuer komplexer Organismus. Wie der menschliche Körper funktioniert es nur, wenn alle verbundenen Schnittstellen harmonisch zusammenarbeiten. Stellt man die einzelnen 'Organe' der beiden „Systeme“ IoT-Gerät – Mensch gegenüber, ergibt sich eine faszinierende Parallelität von Cloud und Gehirn, Stromversorgung und Herz, Kameras und Augen, Temperatur-/Druckmessern und fühlender Haut, Mikrofonen und Ohren, einem Netzwerk aus Routern und Switches einerseits und dem Nervensystem andererseits. Erstaunlich eigentlich, wie wenig Aufmerksamkeit dieses Nervensystem des IoT bislang bekam. Seine Integrität ist schließlich wesentlich für das Funktionieren eines jeden IoT-Systems. Wie der menschliche Körper muss auch ein IoT-Organismus von innen heraus – konzeptionell – vor äußeren Gefahren geschützt sein. Es genügt nicht, das Gehirn abzuschotten, während die peripheren Nerven angreifbar sind. Genau das passiert aber häufig, wenn Attacken festgestellt wurden: Die Hersteller korrigieren lediglich die Software ihrer Produkte. Anders bei Infineon. Dessen Sicherheitshardware zielt darauf ab, ein IoT-System von innen heraus widerstandsfähiger zu machen und das Immunsystem des Organismus zu stärken, damit Angriffe ins Leere gehen.



Bild: Infineon Technologies AG

Bedrohtes Wachstum

„Wo viel Licht ist, ist auch viel Schatten“ – was J. W. von Goethe vor fast 250 Jahren schrieb, spiegelt auch der IoT-Markt heute mit seinen Chancen, aber auch Risiken wider. Laut IDC wächst das IoT bis 2020 auf eine Datenmenge von 50 Billionen GB an, die durch 25 Milliarden eingebettete und intelligente Systeme fließt und vier Milliarden Menschen verbindet. Hinsichtlich Ertragspotenzial ist das IoT mit geschätzten 4 Billionen US-Dollar eine der interessantesten Entwicklungen des 21. Jahrhunderts. Analysten sagen voraus, dass die IoT-bezogenen Erträge der Lieferanten dreimal so schnell wachsen werden wie die übrigen herkömmlichen Ausgaben für die Informations- und Kommunikationstechnologie. Doch dem stehen Risiken wie kompromittierte Netzwerke und zunehmende Cyberattacken sowie Datenpannen gegenüber. Sie können den eindrucksvollen Aufstieg des IoT bremsen und die Kommunikations- und Informationstechnologie beeinflussen. Mangelnde Sicherheit kann ein IoT-basiertes Netzwerk völlig lahmlegen, wie der oben erwähnte Vorfall mit dem Mirai-Botnetz der Öffentlichkeit drastisch vor Augen führte. Dies war ein Szenario aus dem wirklichen Leben, gerade mal zwölf Monate nach einem weiteren erschüt-



Verlaufsskizze des Mirai-Angriffs

ternden Fall: Die Sicherheitsfachleute Charlie Miller und Chris Valasek hatten ihr Auto ferngesteuert entführt und von der Straße gelenkt. Zwei verschiedene Anwendungen mit dem gleichen alarmierenden Ergebnis: Sobald Angreifer durch das Netzwerk und die Cloud Zugriff erlangt haben, kontrollieren sie das gesamte System in beunruhigendem Ausmaß. Ein ungeschütztes manipuliertes Nervensystem lässt Aggressoren quasi über die Hintertür ins Gehirn des IoT-Systems.

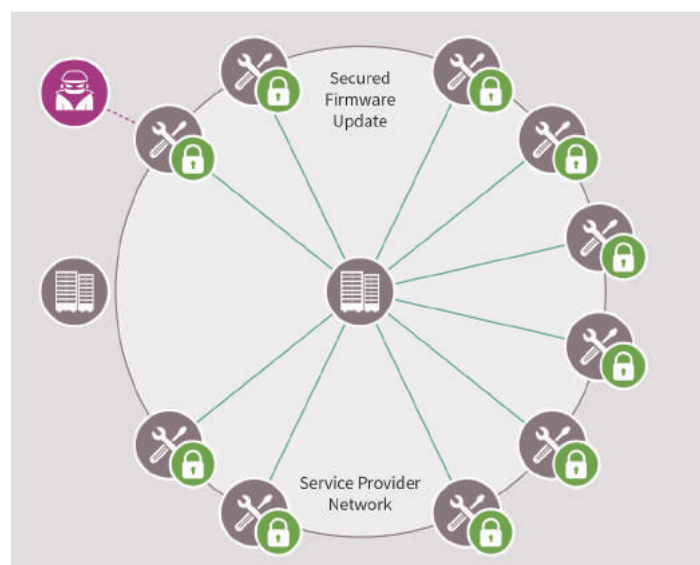
Das Nervensystem des IoT von innen schützen

Sicherheitsbedrohungen sind Realität und damit rücken angreifbare Schwachstellen in den Fokus der Aufmerksamkeit – vor allem mit Blick auf die vielen neuen Applikationen, die den Markt überschwemmen. Entscheidend ist, dass ein Benutzer alle Geräte, die mit seinem privaten oder geschäftlichen Netzwerk verbunden sind, in einem Bestandsverzeichnis listet. Viele Sicherheitsunternehmen bieten dafür Lösungen an. Infineon behält den IoT-Organismus im Auge und konzipiert Sicherheit bereits mit ein, und zwar Hardware-basiert. So ist sie bereits Teil der Gesamtarchitektur des Systems und umfasst Router, Switches sowie die Cloud und die verbundenen Geräte – der beste Weg zu einem tragfähigen Schutz gegen Angriffe von außen. Andernfalls können sich Unternehmen einem hohen Risiko aussetzen. Unglücklicherweise werden diese Probleme in einer zunehmend stärker vernetzten Welt größer: An-

greifer nutzen Schwachstellen aus, um die Kontrolle über Geräte zu erhalten, und bewegen sich dann weiter vor zu den wertvollen Daten und Systemen. Mit einem Zugriff auf die Cloud sind sie bereits im Gehirn des IoT. Sobald es 'stirbt', bleiben die verbundenen Dinge nutzlos zurück. Die Betreiber und die Akteure des Netzwerks und der Cloud unterscheiden sich oft. Doch sie alle müssen eine sichere Infrastruktur bereitstellen, um IoT-Netzwerke zu schützen.

Softwareschutz allein reicht nicht aus

Die meisten Cyberangriffe zielen darauf ab, die Kontrolle zu erlangen – über Hardware, Software und Daten. Sie können jede Organisation, egal welcher Größe und welcher Branche, im Visier haben. Im Falle erpresserischer Software verschlüsseln die Angreifer den Datenbestand nehmen ihn quasi als Geisel und verlangen Lösegeld. Früher nutzten Angreifer meistens eine Schwachstelle in der Software oder an einem Endgerät als Schlupfloch. Als Gegenwehr setzte man Softwarefehlerkorrekturen und Antivirus-Updates ein. Doch inzwischen sehen Angriffe anders aus. Was verursacht mehr Schaden als der kurzfristige Zugriff auf ein System und die durchlaufenden Daten? Wenn er andauernd und im Verborgenen abläuft. Wir haben es mit einer neuen Art von Attacken zu tun: Sie reichen tiefer als bis zur Betriebssystemebene und in die aktuelle Firmware der Geräte hinein. Softwaremaßnahmen sind dagegen hilflos. Mit dem Kompro-

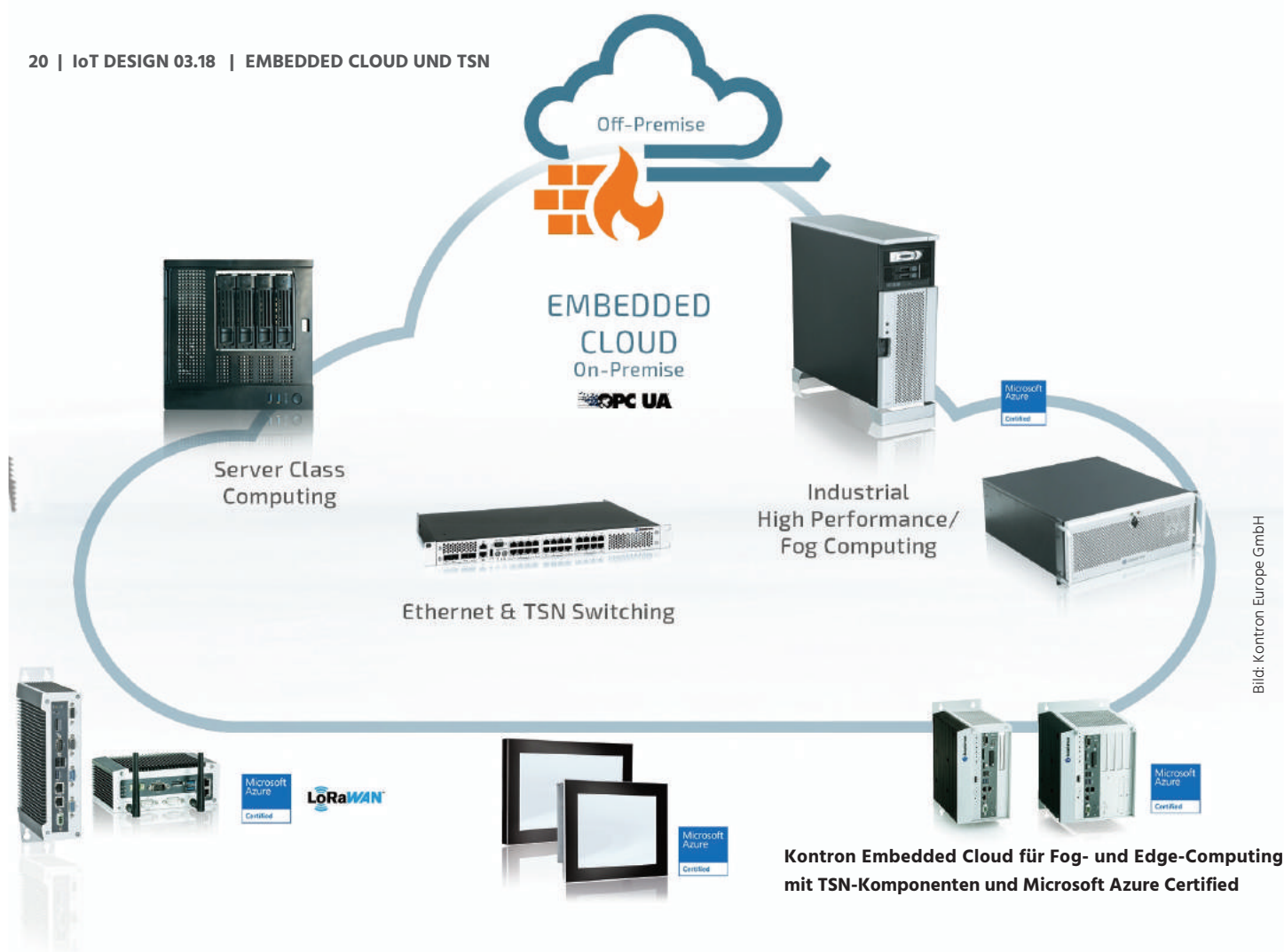


Abwehr des Mirai-Angriffs

mittieren der Firmware erlangt der Eindringling dauerhafte Kontrolle, ohne noch eine Abwehrmöglichkeit zuzulassen. Cyberangriffe sind inzwischen ein hochprofitables, kriminelles Geschäft. Auf dem Markt ist das entsprechende Material allgemein zugänglich, bis hin zu den neuesten Spionagewerkzeugen, entwickelt von Staaten. So können Angreifer auf Netzwerkrouter öffentlicher und privater Bereiche mit sensiblen Daten zugreifen – eine riesige Herausforderung für die Hersteller von Netzwerkgeräten und IoT-Systembetreiber. Für sie stehen nicht nur Gewinne auf dem Spiel, sondern auch ihr Ruf.

Wie eine Hardwarebasierte Lösung eingeführt wird

Die gute Nachricht: Hardware-basierte Sicherheitslösungen wie das Optiga TPM (Trusted Platform Module) geben Netzwerkschutz gegen Firmwareangriffe ab. Gesicherte Halbleitertechnologie wird unter aktuellen Sicherheitsaspekten überprüft. So kann Infineon gemeinsam mit spezialisierten Partnern die Gerätehersteller und Netzbetreiber dabei unterstützen, ihre eigenen Anlagen und die ihrer Kunden vor Cyberangriffen zu schützen. Der Einsatz von Hardware-sicherheit reduziert Schwachstellen und maximiert die Tragfähigkeit. Wie war das doch gleich mit dem menschlichen Körper? Besser das Immunsystem stärken, als später die Antibiotika-Kanone auffahren zu müssen. Chipbasierte Sicherheitslösungen sind die besten Immunstimulanzien für IoT-Systeme. www.infineon.com/cms/de ■



Embedded Cloud und TSN Aufbruchstimmung

Im Gegensatz zu den Konzepten der Public und Private Clouds orientiert sich die **Embedded Cloud** besonders an den **Anforderungen der Smart Factory**, der vernetzten Produktion. Ziel ist es, durch die Echtzeit-Analyse aller im Unternehmen vorhandenen Daten die **Fertigung zu verbessern**. Gefordert ist dafür eine **produktionsnahe und sichere Cloud**, deren Komponenten die Anforderungen der Industrie erfüllen. Eine Embedded Cloud will die **Industrie 4.0** voranbringen. Rückgrat dafür sind **TSN** und **OPC UA**.

NORBERT HAUSER, Vice President Marketing, Kontron S&T AG

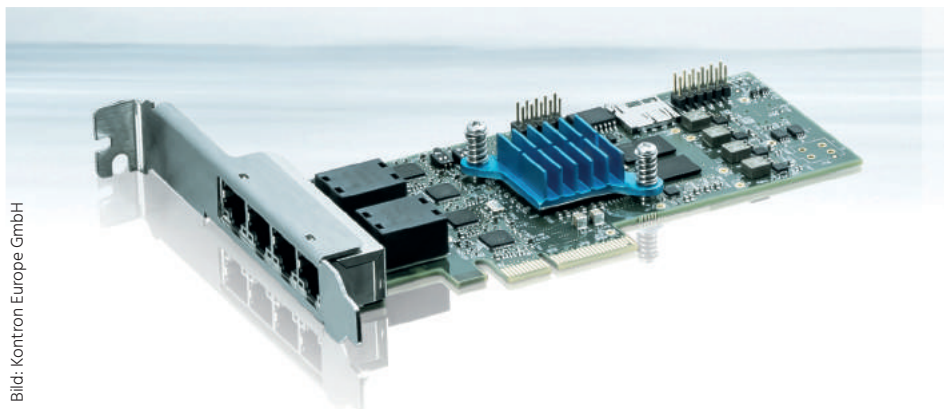
Große Systeme für Business Intelligence (BI) oder Big-Data-Auswertungen werden bereits heute meistens in der Cloud betrieben, entweder als Private Cloud im Firmeneigentum oder als Public Cloud, wie sie z.B. von Amazon, Google, Microsoft oder Oracle bereitgestellt wird. BI-Systeme liefern die Grundlagen für Geschäftsentscheidungen des Managements. Ihre Zahlen und Analysen werden meist nur tages- oder wochenaktuell benötigt. Eine Alternative für eine vernetzte Maschinensteuerung sind diese Clouds aufgrund verhältnismäßig hoher Latenzen durch Standard-Internetverbindungen und nicht ausreichend garantierter Verfügbarkeiten nicht. Beide Nachteile der Public Clouds greift deshalb das Kontron-Konzept der Embedded (Private) Cloud auf. Dafür werden die an der Fertigung beteiligten

Systeme auf dem Firmengelände in einem privaten Verbund zusammengeschlossen, der sogenannten Embedded Cloud. Sie befindet sich vor Ort, also On-Premise. Hier werden die Anwendungen der betrieblichen IT und der OT zusammengeführt.

Embedded Cloud für den Shopfloor

Eine Embedded Cloud, so wie sie Kontron versteht, besteht aus drei Geräteklassen.

- Industrielle Computerplattformen für die Gerätesteuerung und als Edge-/Gateway-Systeme mit einer typischen Rechenleistung von ein bis vier



Die Standard-Netzwerkkarte von Kontron umfasst einen integrierten Switch für redundante Netzwerke mit zwei oder vier Gigabit-Ethernet-Ports. Sie erfüllt alle Spezifikationen gemäß IEEE802.1 und ist insbesondere für raue Industrieumgebungen geeignet.

CPU-Kernen: Sie übernehmen Mess- und Steuerungsaufgaben vor Ort, extrahieren und filtern Daten und verfügen meist über proprietäre Schnittstellen und Feldbusse zur Anbindung der Peripherie vor Ort.

- Hochleistungsfähige industrielle Computerplattformen für Fog-Computing: Mit einer typischen Rechenleistung von vier bis acht CPU-Kernen und einer Speicherkapazität von mehreren Terabyte übernehmen diese leistungsstarken Plattformen vor Ort das Maschinenmanagement bis hin zur Steuerung von Bildgebungssystemen mit Optionen für mehrere Grafikprozessoren, FPGA-Karten, Feldbusschnittstellen und TSN Interface.
- Embedded Cloud Server: Mit einer typischen Rechenleistung von mehr als 16 Cores und einer Speicherkapazität über 100TB übernehmen diese Cloud-Storage-Server die Datenkoordination von Maschinen an einem Standort.

Ohne Standards läuft nichts

Die Anbindung an die Embedded Cloud regelt eine echtzeitfähige Datenkommunikation, beispielsweise per Industrial Ethernet. Auf der Basis von OPC UA (IEC62541 OPC UA) und der entsprechenden TSN-fähigen Hardware wird nun vieles denkbar. Denn TSN (IEEE802.1 TSN) gleicht die bisher fehlende Echtzeitfähigkeit

von Ethernet aus. TSN beginnt damit, den klassischen Feldbus-Spezifikationen Konkurrenz zu machen und hat sogar das Potential, diese mittelfristig zu ersetzen. TSN ermöglicht konvergente Ethernet-basierende Netzwerke, auf denen parallel zum IT-Datenverkehr auch zeit-synchronisierte, deterministische Kommunikation möglich ist. Diese ist bei zeitkritischen Maschinensteuerungen und Prozessen unabdingbar. Die Spezifikationen des TSN sorgen dafür, dass Datenpakete garantiert zeitgerecht und hoch verfügbar zugestellt werden. Im industriellen Umfeld kann konvergentes, Ethernet-basiertes TSN mit garantierter Latenz und Quality of Service (QoS) mit Zeitsynchronisation ohne proprietäre Feldbussysteme nahtlos bis in die IT-Ebene kommunizieren. Damit wird echtes IIoT bzw. Industrie 4.0 basierend auf Ethernet-Protocol-Standards möglich.

Einstieg ins TSN leicht gemacht

Bereits auf der embedded world präsentierte Kontron ein Starterkit für Time Sensitive Networking, das ab April 2018 verfügbar ist. Damit können Unternehmen eine nahtlose Verbindung zwischen der Feldebene, Operational Technology (OT) und Informationstechnologie (IT) herstellen. Mit der Standard-PCI-Express-

Netzwerkkarte einschließlich der dazugehörigen Netzwerk- und Switch-Treiber für Linux können Industriecomputer mit einem TSN-Netzwerk verbunden werden. Um einen Standard zu etablieren, braucht es aber auch Player auf Hersteller- und Anwenderseite, die zielgerichtet und intensiv daran arbeiten, den Markt dafür zu bereiten. Die großen IT-Anbieter, allen voran Microsoft mit seinem Cloudangebot Azure IoT Edge, drängen immer weiter an die Basis der Automatisierungspyramide vor. Kontron hat sich deshalb entschlossen, viele seiner Embedded PCs und Workstations – teilweise auch als Embedded Server – für das Fog- und Edge-Computing mit Microsoft Azure zertifizieren zu lassen; derzeit handelt es sich um rund 20 Produkte und die Zahl wird laufend erweitert. Auf der Seite der Standards setzt Kontron voll auf OPC UA und TSN.

In Siebenmeilenstiefeln zur Industrie 4.0

Für ihre Industrie-4.0-Projekte benötigen Anwender eine integrierbare, skalierbare und vernetzbare On-Premise Lösung, also den Embedded Server. Kontron bietet bereits heute alle wesentlichen Komponenten für die Embedded Cloud. Das bedeutet in der Praxis, dass die Rechen- und Speicherleistung von Cloud Servern und die Robustheit von Industrial Servern kombiniert werden müssen. Erste serienmäßige, industriefähige Embedded Server für die Embedded Cloud und das Edge- und Fog-Computing hat Kontron ebenfalls auf der embedded world in Nürnberg präsentiert. Es handelt sich dabei um den Nachfolger der 'Cube' Evaluierungsplattform mit einem Single-Intel-Xeon-Prozessor in einer kompakten und kostenoptimierten Bauform mit erweiterten Storage-Funktionen. Im Verbund mit S&T bietet Kontron seinen Kunden mit der Embedded Cloud auf Basis von Standards wie OPC UA und TSN das Fundament für die Smart Factory aus einer Hand. Datenverarbeitung in Echtzeit und die uneingeschränkte Sicherheit von Fertigungs- und Produktionsdaten sind eine wichtige Voraussetzung für den Erfolg im digitalisierten Industrieumfeld. www.kontron.de ■

- Anzeige -

From Board to System

www.portwell.eu



WUX-3350



MEDS-BS200

 **Portwell**
Leading in embedded technology

Tools zum Managen von Industrie 4.0

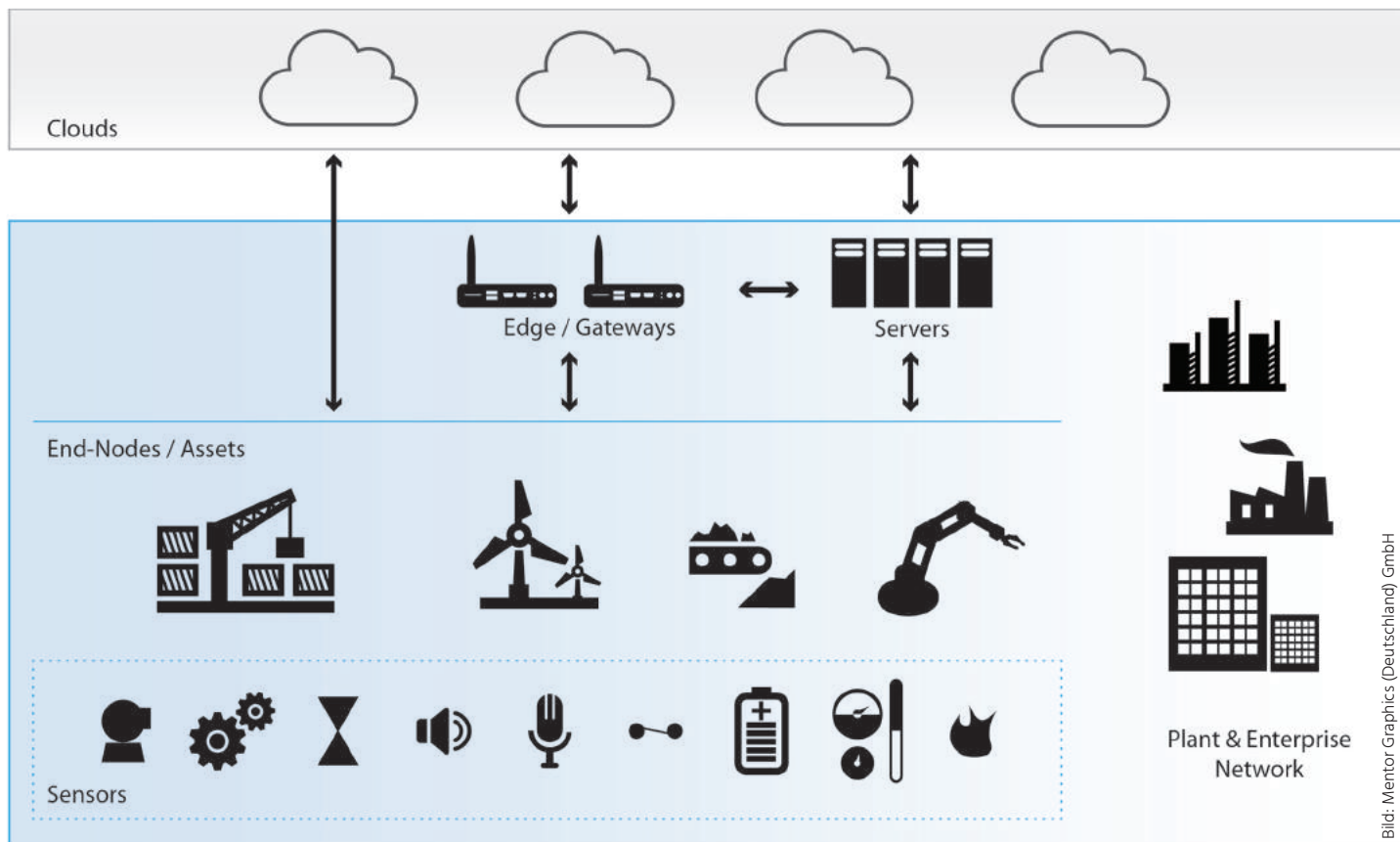


Bild: Mentor Graphics (Deutschland) GmbH

Die Vernetzung der heutigen IloT-Architektur – von winzigen Endknoten und Sensoren über das Smart-Gateway bis hin zur Cloud.

Der Artikel beschreibt drei **Schlüsselkategorien von Werkzeugen**, die den **IoT-Architekturen der nächsten Generation** helfen sollen, ihre **Versprechen** einzuhalten. Zwar beginnt die **Industrie**, diese Anforderungen (wenn auch fragmentiert) in Angriff zu nehmen, doch müssen **Gerätehersteller** diese Anforderungen ganzheitlicher betrachten. Zu diesen drei Werkzeugkategorien gehören sichere **Updates** für Betriebssystem, Firmware und Anwendungen der Geräte, **Ferndatendiagnose** und Systemzustandsüberwachung sowie der **Digitale Zwilling** der Geräte.

KATHY TUFTO, Senior-Product-Manager bei Mentors Embedded Systems Division, MENTOR

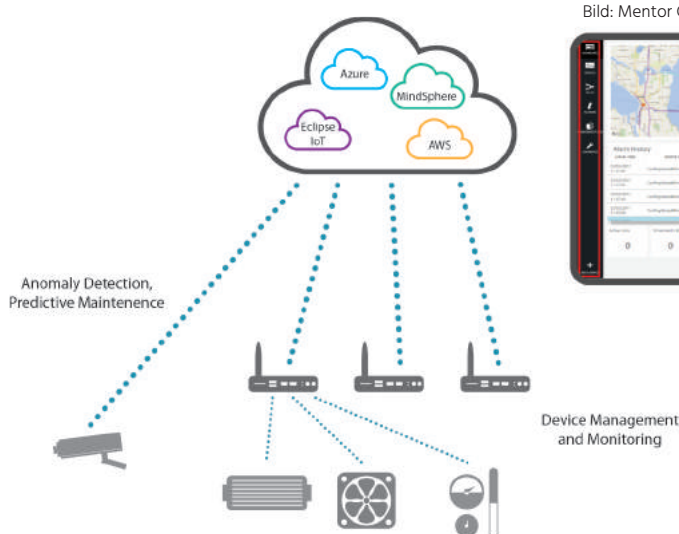
Die Anpassung an Industrie 4.0 bedeutet, dass alles verbunden werden muss. Gateways, Edge-Devices, intelligente Sensoren, einfache Sensoren, Endknoten und sogar lokale Server: Alle sind bis zu einem gewissen Grad damit beschäftigt, Daten zu sammeln, zusammenzufassen, zu verarbeiten und an einzelne oder mehrere Cloud-Backends zu senden (Bild 1). Mit zunehmender Anzahl und Art der ange-

schlossenen Geräte steigt die Komplexität der IloT-Topologien. Die Implementierung und Verwaltung eines IloT-Systems wird dadurch zu einer echten Herausforderung, bei denen Tools wichtige Hilfestellung leisten. Für die Zwecke dieses Artikels nehmen wir an, dass die grundlegenden Elemente einer IloT-Architektur existieren und funktionsfähig sind. Zu diesen Elementen gehören die sichere Konnektivität und das Onboarding

von Geräten sowie grundlegende Aufgaben wie die Konfiguration des Geräts für den Basisbetrieb (Benennung, Einstellung der lokalen Sprache und Zeitzone usw.) und die Ausführung grundlegender Steuerbefehle wie Remote-Reset, Konfigurations-Download und Wiederherstellung der Werkseinstellungen. Außerdem gehen wir davon aus, dass diese Fähigkeiten vollständig in der gesamten IIoT-Topologie implementiert sind (Bild 2).

Sichere Updates

Sobald eine Funktion zum Management der Geräte vollständig implementiert ist, muss der Anwender komplexere Operationen wie Geräte-Updates und -wartung in Betracht ziehen. Dazu gehören Anwendungs- und Betriebssystem-Updates, Patches, Firmware-Rollbacks und Flotten-Rollouts. Tools für sichere Updates beinhalten eine Kombination aus Entwicklungs- und Testwerkzeugen für das Embedded-Gerät, die in Verbindung mit den Backend-Aktualisierungs-Tools arbeiten. Wenn der Anwender Linux als Laufzeitplattform verwendet, gibt es bestimmte Funktionen, die er zu seinem Vorteil nutzen kann. Da Linux Open Source Software (OSS) ist, bietet es eine reiche Auswahl an Möglichkeiten. Z.B. verfeinern aktive Communities ständig den Linux-Kernel, wenn es um Betriebssystem-Updates und Patches geht. Die Hersteller wollen für ihre Geräte relevante Patches, Korrekturen bei Sicherheitsfehlern und Anwendungs-Updates bereitstellen, die leistungsstarke Entwicklungs- und Debugging-Tools erfordern. Um die Sicherheit zu gewähr-



Eine Gerätemanagementstrategie muss alle Gateways, Endgeräte und möglicherweise mehrere Cloud-Backends berücksichtigen. Idealerweise würde die Lösung eine Art Dashboard für die Benutzeroberfläche enthalten, um Interaktionen einfach zu überwachen.

Bild: Mentor Graphics (Deutschland) GmbH



Cloud-based Dashboard: Device Management, Monitoring, Device State

leisten, benötigen sie Tools, mit denen sie Code signieren und verschlüsseln können, um ihn herunterzuladen, zu authentifizieren, zu validieren und auf dem Embedded-Gerät zu installieren. Standardinfrastruktur innerhalb des Linux-Kernels wie der SWUpdate-Agent, ermöglicht es, sichere Software-Updates an einzelne Geräte in der gesamten IIoT-Infrastruktur zu senden. Viele Cloud-Backend-Anbieter stellen ein Embedded-SDK mit Software-Hooks zur Verfügung, die, sobald sie auf dem Embedded-Gerät implementiert sind, von den Backend-Tools genutzt werden können.

Ferndatendiagnose und Systemzustandsüberwachung

Das Ziel jedes Unternehmens ist es, die Anforderungen ihrer Kunden zu erfüllen und gleichzeitig den Gewinn zu steigern. Hierfür müssen Gerätehersteller in der Lage sein, installierte Geräte auf mögliche Probleme zu überwachen (Systemzustandsüberwachung) und Probleme zu diagnostizieren oder vorherzusagen, so dass sie bei planmäßigen Wartungsarbeiten behoben

— Anzeige —

Schluss mit endlosen Entwicklungszeiten – individuelle Elektronik in nur 6 Wochen

SBC^{Plus} – kostengünstig, schnell, industrietauglich

- Steuerungen, Bedieneinheiten und Gateways auf Basis vorgefertigter Funktionsblöcke
- Kundenspezifische Schaltungsteile und Platinenformate möglich
- Inklusive Linux Board Support Package mit Schnittstellen-Anpassung
- Zusatzleistungen von Gehäuse bis Zertifizierung
- Entwicklung und Fertigung in Mainz

Sprechen Sie mit uns über Ihr Projekt. Machen Sie uns zum Teil Ihres Entwicklungsteams. Wir legen direkt los – versprochen!

Treffen Sie das PHYTEC Team: SENSOR+TEST | Halle 5 – 135

PHYTEC



SENSOR+TEST
DIE MESSTECHNIK - MESSE
The Measurement Fair
Nürnberg, Germany
26. – 28.6.2018

PHYTEC MESSTECHNIK GMBH
contact@phytec.de
www.phytec.de
+49 (0) 6131 / 9221-32

Das Mentor Embedded IoT Framework ergänzt und erweitert SDKs von Cloud-Anbietern und ermöglicht die Integration und Portierbarkeit der zugrundeliegenden Plattform.

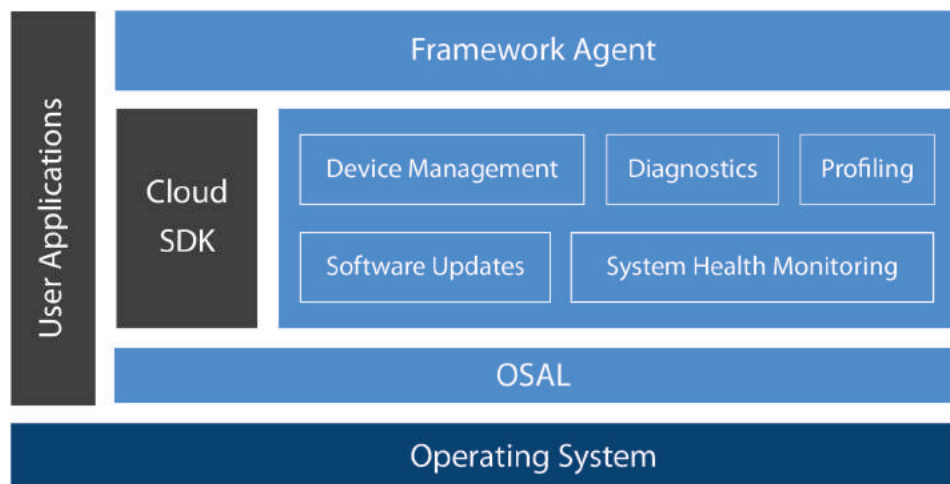


Bild: Mentor Graphics (Deutschland) GmbH

werden können. Beispiele für die Überwachung des Systemzustands sind das Beobachten der CPU-/Speicher-/Netzwerknutzung oder die Überwachung von Watchdog-Daemonen und anderen Funktionen auf Systemebene. Wenn es zu einer Verschlechterung oder einem Ausfall des Systems kommt, gibt es eine Vielzahl von Systemdiagnosefunktionen, die per Fernzugriff auf dem Edge- oder Endknoten-Gerät durchgeführt werden können, um dem Gerätehersteller nützliche Informationen zur Verfügung zu stellen. Letztendlich kann die Fernüberwachung und -diagnose des Systemzustands die Verfügbarkeit des IIoT-Systems und die Kundenzufriedenheit verbessern und gleichzeitig die Kosten des Geräteherstellers für Wartung, Service oder Austausch von Geräten senken. Mentors Sourcery-Analyzer-Tool ist ein gutes Beispiel dafür, wie Softwareentwickler ein neues Level der Datendiagnose und Systemzustandsüberwachung in ihre IIoT-Infrastruktur einbringen können. Der Sourcery-Analyzer ermöglicht es, den Zustand und den Betrieb der Embedded-IIoT-Plattform aus der Ferne zu analysieren. Der Systemzustand kann überwacht werden, indem Funktionen und Dämonen auf Systemebene aktiviert werden und Daten über sichere Telemetrie-Kanäle an Zeitreihen-Datenbanken im Cloud-Backend gesendet werden.

Digitale Zwillinge

Das Versprechen von Industrie 4.0 geht tief und umfasst das, was oft als 'digitales Unternehmen' bezeichnet wird. Der digitale Zwilling ist für Siemens „der Inbegriff der Digitalisierung von Maschinen und Anlagen – die virtuelle Kopie einer realen Maschine oder Anlage“. Bauteile werden seit Jahren vor dem Prototyping und der

Fertigung digital konstruiert. Heute können Teile sogar auf Abruf durch additive Fertigungstechniken hergestellt werden. Aber digitales Design beschränkt sich nicht nur auf physikalische Komponenten. Aus Software-Perspektive existieren Techniken, um Software auf virtueller Hardware zu entwickeln. Das sind im Wesentlichen Simulatoren, die Prozessoren, Komponenten, Boards und sogar ganze Systeme imitieren. Entwickler können Software auf virtuellen Instanzen dieser Systeme entwickeln und testen, bevor die Software finalisiert und auf die eigentliche Hardware 'geflasht' wird. Glücklicherweise ist die Nützlichkeit dieser simulierten Systeme noch lange nicht erschöpft. Durch die Verwendung von Statusinformationen und Daten, die von diesen angeschlossenen Geräten gesammelt wurden, können Unternehmen digitale Zwillinge zum Validieren von Software, Testen und Diagnostizieren von Problemen benutzen. Der Einsatz von digitalen Zwillingen kann daher zu Effizienzsteigerungen und neuen Möglichkeiten führen, indem Gerätemanagement, Software-Updates, Ferndiagnose und Systemzustandsüberwachung zu einer vollständigen Digitalisierungsstrategie verknüpft werden.

Eine IIoT-Lösung für alle

Das Problem besteht darin, eine IIoT-Architektur zu finden, die verschiedene Geräte, Betriebssysteme, Hardware-Plattformen und das Cloud-Backend integriert. Gebraucht wird ein zusammenhängendes, hochfunktionales IIoT-Ökosystem. Ein Ökosystem, das auch die Werkzeuge berücksichtigt, die für den Betrieb und die Wartung aller beweglichen Teile heute, morgen und in ferner Zukunft benötigt werden. Das Mentor Embedded IoT Framework (MEIF) (Bild 3) ersetzt

keine Technologien und Investitionen, die bereits von Cloud-Anbietern bereitgestellt werden, sondern füllt die Lücken, indem es diese Technologien ergänzt bzw. erweitert und Funktionen vollständig in die Edge- oder Endknoten-Geräteplattformen integriert. Das MEIF-Design ermöglicht die Integration der von den Cloud-Anbietern zur Verfügung gestellten Embedded-SDKs mit einem klar definierten Satz von MEIF-Geräte-APIs, ergänzt durch Tools für Gerätemanagement, sichere Updates, Ferndatendiagnose und Systemzustandsüberwachung.

Schlussfolgerung

Unternehmen, die in IoT investiert haben, erkennen die Vorteile einer solchen Strategie und implementieren nun komplexere und expansivere IIoT-Architekturen. Die Gerätehersteller stehen daher vor neuen Herausforderungen in Bezug auf die für das Gerätemanagement erforderlichen Tools, unbekannte/mehrere Clouds, Portabilität, Skalierbarkeit und die Notwendigkeit, Geräte aus der Ferne zu überwachen und zu diagnostizieren. Das Mentor Embedded Portfolio, zusammen mit dem Mentor Embedded IoT Framework, ergänzt und erweitert die großen Investitionen der Cloud-Anbieter. Es stellt umfassende IoT-Tools und -Features zur Verfügung, die bis hinunter zur Hardware von Edge- oder Endknotengeräten implementiert und über Plattformen und Clouds portiert werden können. www.mentor.com ■

Datenübertragung im Internet der Dinge

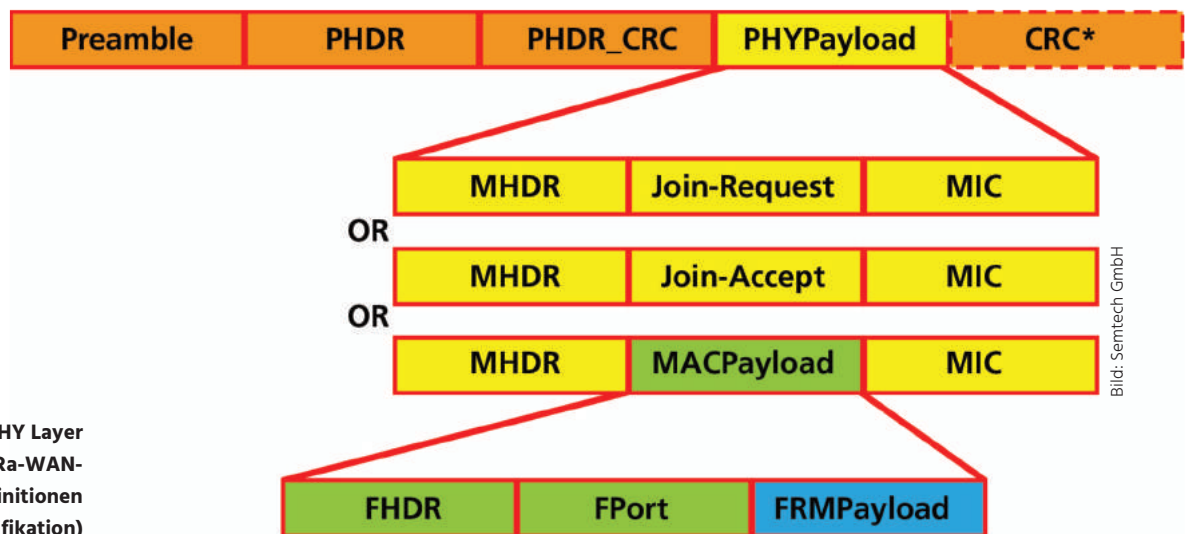


Abbildung 1: LoRa-PHY Layer Packet-Struktur und LoRa-WAN-MAC- und Frame-Definitionen (LoRa-WAN 1.0.2 Spezifikation)

Bild: Semtech GmbH

IoT-Netzwerke müssen **geringe Datenmengen** häufig, über **große Reichweiten** oder in dichten Gebäuden bei **geringem Stromverbrauch** übertragen. Die **Sensoren** im Netzwerk und deren Wartung dürfen dabei **nicht allzu viel kosten**. Keine geringe Rolle spielt aber auch die Sicherheit der Datenübertragung vom Sensor an das Gateway. Wie all diese Anforderungen **erfolgreich gemeistert** werden können, erläutert der folgende Beitrag.

VIVEK MOHAN, Director of Wireless Products bei Semtech Corporation

Das Internet der Dinge ist in aller Munde – es stellt aber auch besondere Anforderungen an Netzwerke: wie hohe Reichweite, hohe Frequenz der Datenübertragung und geringen Stromverbrauch. Mit entsprechenden Verfahren und Protokollen erschließt es aber auch neue Anwendungsmöglichkeiten – von der intelligenten Straßenbeleuchtung bis hin zur modernen Landwirtschaft.

Verfahren der Datenübertragung

Als für diese Anforderungen geeignetes Netzwerk basiert z.B. ein LoRa-WAN-Netzwerk auf der LoRa (Long Range, Low Power)-Technologie, die Daten über eine drahtlose Radiofrequenz-(RF)-Technologie überträgt. LoRa regelt dabei auf dem physikalischen Layer des OSI-Schichtenmodells die Übertragung der Signale über die Luft auf RF-Frequenzen bidirektional zwischen RF-Transmitter in einem IoT-Gerät und dem RF-Empfänger an die Gateways. Die Gateways sind dann über die zentrale Managementplattform in der Cloud an die Applikationen angebunden. Ein LoRa-WAN-Proto-

koll ist die dazu gehörige offene Low-Power-Wide-Area-Network (LPWAN oder auf Deutsch Niedrigenergie weitverkehrsnetzwerk)-Spezifikation für drahtlose batteriebetriebene Systeme in einem regionalen, nationalen oder auch globalen Netzwerk. Die LoRa-Technologie und ihr Datenübertragungsverfahren mit proprietären Frequenzspreizungsverfahren und Modulation gewährleisten eine stabile Datenübertragung, egal wie weit sich ein Sender etwa von den empfangenden Gateways befindet – bei möglichst geringem Stromverbrauch. Z.B. wird ein Sensor, der sich in der Nähe eines Gateways befindet, mit einem niedrigen Spreizfaktor senden, da dann nur eine sehr geringe Leistungsübertragungsbilanz – das sogenannte Link Budget – benötigt wird. Damit lässt sich viel Energie sparen. Ein Sensor, der sich mehrere Meilen von einem Gateway entfernt befindet, muss mit einem viel höheren Spreizfaktor senden, da dieser zu einer höheren Empfängerempfindlichkeit führt. Im Ergebnis wird im zweiten Fall die notwendige höhere Reichweite realisiert, wobei die Datenrate im Gegenzug sinken muss. Das Modulationsverfahren ermöglicht durch die Vervielfachung der Datensignale mit einem Spreading Code zur Spreizung eine optimale Sendeleistung bei

möglichst niedriger Leistungsaufnahme durch den Transmitter. Je nach Spreizungsfaktor ermöglicht die Signalmodulation unterschiedliche Übertragungsgeschwindigkeiten und Bitraten über verschiedene Reichweiten. (siehe Abbildung 3). Ein hoher Spreizungsfaktor senkt z.B. zwar die Bitrate und die Signale brauchen natürlich länger für Ihren Weg zur Gateway. Aber Daten können z.B. beim Faktor SF10 über eine Entfernung von bis zu acht Kilometern gesendet werden. Die Tabelle zeigt die vier Spreizfaktoren, die für Uplink-Übertragungen auf einem 125kHz-Kanal im LoRa-Verfahren ausgewählt werden können. Für den 500kHz-Downlink stehen sechs Spreading-Faktoren zur Verfügung. Die Reichweite kann dabei vom Gelände abhängen. In ländlichen Gegenden etwa mit wenigen störenden architektonischen Elementen lassen sich noch deutlich höhere Reichweiten erzielen als in städtischen Umgebungen. Die LoRa-Modulation hat aber noch einen weiteren Vorteil. Signale, die mit verschiedenen Spreizungsfaktoren moduliert wurden und über denselben Frequenzkanal übertragen werden können, stören sich nicht gegenseitig. Ein Baseband-Prozessor kann also bis zu sechs Signale mit verschiedenen Spreizfaktoren aus einem Kanal gleichzeitig verarbeiten, da die verschiedenen Signale für den jeweiligen Empfänger nur als Rauschen wahrgenommen werden. LoRa-Signale sind zudem sehr robust sowohl gegen In-Band- als auch gegen Out-of-Band-Interferenzen. Ihre Unempfindlichkeit gegen Mehrwegeempfang oder Fading sorgt auch in städtischen oder sub-

urbanen Gebieten für eine hohe Reichweite. Dopplerverschiebungen sind kein Problem. Sie verursachen eine vernachlässigbare Verschiebung in der Zeitachse des Baseband-Signals. Diese Toleranz verringert zudem die Notwendigkeit nach einem strengen Referenztaktsignal, so dass sich LoRa-Sensoren und Geräte auch für den mobilen Einsatz eignen. Die Sensoren nutzen zur Datenübertragung zudem unlicenzierte ISM-Bänder, so dass die Kosten der Datenübertragung entweder ganz entfallen oder – bei Einsatz eines externen Providers – gering ausfallen.

Netzwerkprotokolle

Für die LoRa-Übertragung ist eine grundlegende Packet-Struktur auf dem Link-Layer durch LoRa-Transceiver von Semtech festgelegt (Abbildung 2). Diese Struktur ermöglicht die Point-to-Point-RF-Übertragung von Daten und Befehlen. Anwender können in einer solchen LoRa-Lösung die Datenprotokolle frei definieren. Mit LoRa-WAN steht aber auch ein Layer-3-Netzwerkprotokoll zur Verfügung. LoRa-WAN ist ein offenes Low-Power-Wide-Area-Networking-Protokoll, das für den Betrieb sensor-basierter Applikationen bei niedrigem Stromverbrauch und hoher Reichweite optimiert ist. Das Netzwerk ermöglicht den Aufbau eines Netzes in Sterntopologie. IoT-Geräte werden über eine Over-the-Air-Activation (OTA)-Anfrage authentifiziert und in das Netz

aufgenommen. Die Verwaltung des Netzes leistet dann eine zentrale Cloud-basierte Instanz, die u.a. das Verhältnis von Übertragungsstärke und Spreading-Faktoren mit Hinblick auf Optimierung des Stromverbrauchs festlegt. Die Managementeinheit routet auch die Daten weiter an den jeweiligen Anwendungsserver in der Cloud. Die Abbildung 1 zeigt, wie die einzelnen LoRa-WAN-Parameter innerhalb des (orange gefärbten) LoRa-Pakets enthalten sind. Das LoRa-WAN-Protokoll versieht die Pakete mit einem MAC-Header (MHDR), einer MAC-Payload und einem Message Integrity Code (MIC). Die eigentliche MAC-Payload besteht aus Frame Header, Frame Port und den tatsächlichen zu übertragenden Daten. Die Sterntopologie der LoRa-WAN-Netzwerk-Architektur (Abbildung 2) eignet sich ideal für Netzwerke, deren Betrieb auf batteriebetriebenen Sensoren basiert. Ein Netz in Sterntopologie überträgt nämlich pro Endknoten tatsächlich nur die für die Verbindung relevanten Daten, während in vermaschten Netze zusätzlich Strom für die Weiterleitung von Nachrichten von und zu benachbarten End-Knoten verbraucht wird. Auch die Gateways sind so einfach wie nötig gehalten. Das Gateway empfängt dabei alle LoRa-modulierten Radio-Nachrichten und leitet diese weiter. Jede Nachricht mit einem korrekten CRC-Code wird dann in einem IP-Frame an die Netzwerkservers weitergeleitet. Gateways können an die Netzwerkservers drahtlos über Ethernet-LAN oder auch über eine Mobilfunk-

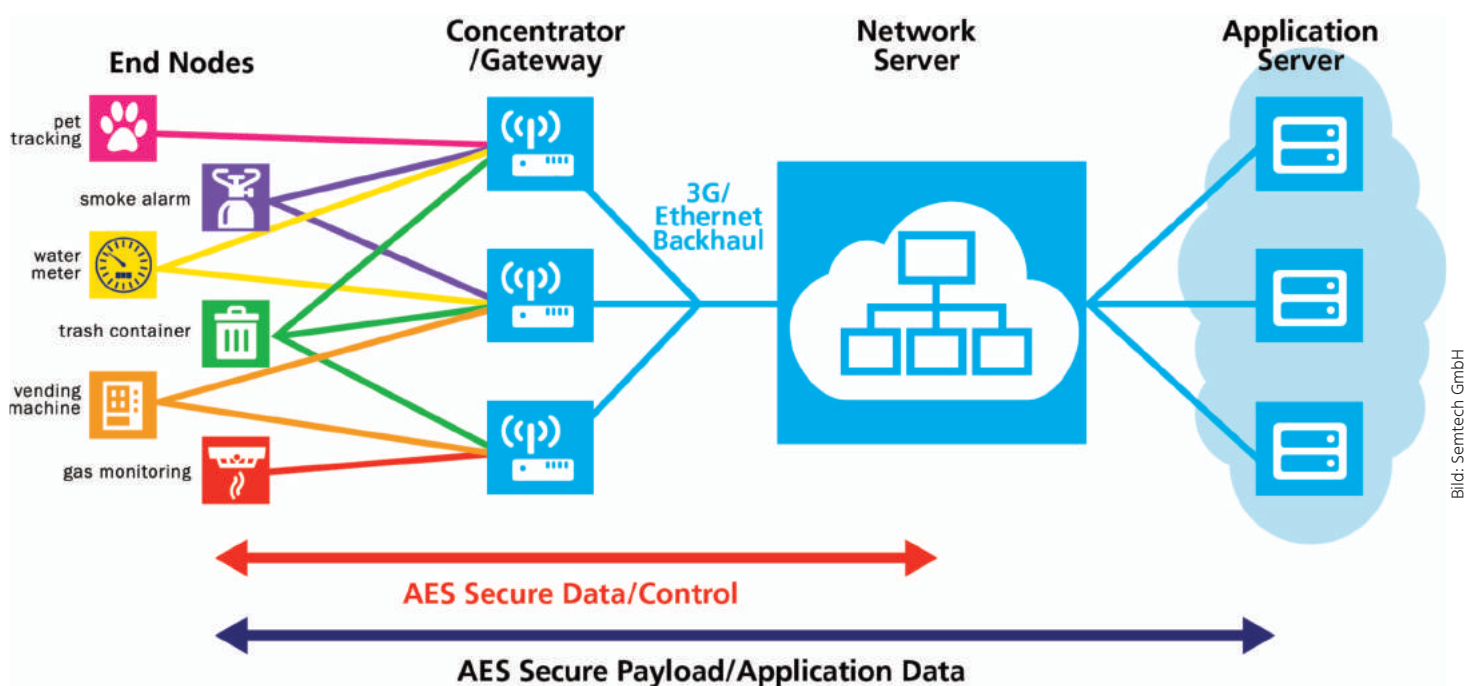


Abbildung 2 LoRa-WAN-Stern-Topologie

Spreading Factor [for UL at 125KHz]	Bit Rate	Range [dependent on terrain conditions]	Time on Air for an 11-byte payload
SF10	980 bps	8 km	371 ms
SF9	1760 bps	6 km	185 ms
SF8	3125 bps	4 km	103 ms
SF7	5470 bps	2 km	61 ms

Abbildung 3 LoRa-WAN-Spreizungsfaktoren und Übertragungsdauer für ein 11-Byte-Payload

verbindung angebunden werden. Ein Netz besteht dabei zum einem aus Macro-Cell-Gateways mit 64 Kanälen für die Übertragung über größere Entfernungen – etwa über eine Stadt hinweg. Zum anderen ermöglichen Pico-Cell-Gateways mit acht Kanälen die Datenübertragung in dicht bebauten Gebieten oder auch schwer auszuleuchtenden Arealen wie Untergeschossen. Eine höhere Anzahl der Pico-Gateways in einem Netz erhöht die Lebensdauer der Sensorbatterien. Denn die geringere Distanz zwischen End-Knoten und Gateway ermöglicht die Übertragung der LoRa-Radio-Pakete mit einem geringeren Spreizungsfaktor und verkürzt die Dauer der Übertragung.

Sicherheit

Sicherheit wird auch bei Internet-of-Things-Netzen immer wichtiger – und damit auch bei LoRa-WAN. Denn falsche, nicht übertragene oder abgehornte Daten führen zu Schäden durch das Treffen falscher Entscheidungen oder auch zu Spionage. Eine wichtige Rolle spielt dabei die Verschlüsselung der Daten, wobei aber nicht jede Verschlüsselung wirkliche Sicherheit garantiert. Ein richtig implementiertes Verschlüsselungsverfahren wie etwa 128Bit AES bietet hinreichende Sicherheit. Dessen weit verbreiteten Algorithmen sind jahrelang praxiserprobt und von Communities optimiert. Wichtig ist die Verwendung im standardisierten CRT-Modus, der XOR-Crypto-Operationen für eine verstärkte Verschlüsselung durchführt. Bei der Datenübertragung im Internet der Dinge genügt es aber nicht, Daten beim Transport over the air zu verschlüsseln und dann im Kernnetzwerk des Betreibers unverschlüsselt zu übertragen. Echte Sicherheit bietet nur die End-to-End-Verschlüsselung der Daten auf dem gesamten Weg vom Endgerät

zum Applikationsserver – und damit auch während der Übertragung innerhalb des Core-Netzwerkes des Betreibers. Protokolle, die die Übertragung im Kernnetz nicht verschlüsseln, verlangen für eine sichere Übertragung über die ganze Strecke eine VPN-Verbindung oder eine zusätzliche Verschlüsselungsebene wie TLS, was aber zu höherem Stromverbrauch führt. Dieser würde die Lebensdauer der Sensorakkus verringern. Wichtig ist die wechselseitige Authentifizierung der Sensoren und des zugehörigen Netzwerks. Jeder Sensor verfügt beim LoRa-WAN-Protokoll über seinen eigenen 128-Bit-AES-Key, den Appkey. Im Join-Prozess eines Sensors überprüft die Over-the-Air-Aktivierung durch den für jedes Netzwerk eigenen Identifier die Zugehörigkeit des Sensors zum Netz. Auch der Join-Server eines Netzwerkes verfügt über einen weltweit individuellen Identifier. Die Überprüfung, ob beide Teilnehmer denselben Appkey kennen, erfolgt durch Berechnung eines AES-CMAC (Cipher-based Message Authentication Code) sowohl für die Join-Anfrage des Sensors als auch durch den Backend-Empfänger. Bei erfolgreicher Authentifizierung werden dann für jede Datenübertragungssession zwei Schlüssel abgeleitet: Der AppSKey sichert die End-to-End-Verschlüsselung des Anwendungspayloads. Der sogenannte NWSKey sichert die Integrität und Verschlüsselung der Kommandos und des Anwendungspayloads. Die Verwendung beider Schlüssel stellt auch die Integrität der Datenübertragung sicher. Ein z.B. beim LoRa-WAN-Protokoll bei jeder Verschlüsselung berechneter Frame Counter verhindert zudem ein Packet Replay durch einen anderen, nicht autorisierten Sensor. Ein berechneter Message Integrity Code (MIC) verhindert die Manipulation der Daten im Verlauf der Datenübertragung und gewährleistet zudem, dass nur ein authentifiziertes Endgerät einen gültigen Frame erzeugen kann.

Einsatzszenarien in der Landwirtschaft

IoT-Netze, die auf LoRa-WAN basieren, können unbegrenzt eingesetzt werden. Deren flexible Architektur ermöglicht dies. Das LoRa-WAN-Protokoll sieht z.B. drei Klassen von Endknoten – also Sensoren – vor. Endknoten der Klasse A übertragen einen Uplink – also eine Nachricht vom Endknoten an das Gateway – zu einer zufälligen Zeit automatisch weiter – so die Mülltonne in einem Smart-City-Netzwerk, wenn sie voll ist und geleert werden kann. Danach fährt der Sensor in den Ruhezustand und verbraucht so sehr wenig Energie. Eine Klasse-B-Endknoten kann Uplinks zu jeder Zeit übertragen, hat aber auch Slots in der er auf Downlink-Nachrichten von der Zentrale wartet. Das ist etwa der Fall bei der Steuerung einer Bewässerungsanlage. Die funktionsreichsten Klasse-C-Endknoten können jederzeit Downlinks empfangen – was eine noch bessere Steuerung ermöglicht. Dafür verbraucht der Sensor aber viel Strom und verfügt in der Regel über eine eigene Stromversorgung – etwa bei Straßenbeleuchtungen, die permanent gesteuert werden sollen. Von der Produktion über die Logistik, Smart Cities oder Smart-Buildings können Anwender leistungsstarke Netze aufbauen. Das gilt auch für Bereiche, an die man zuerst gar nicht denkt – wie die Landwirtschaft. Gerade die moderne Landwirtschaft kann ihre Leistungsfähigkeit durch IoT-Geräte, moderne Sensoren, Chips und die Analyse der gelieferten Daten durch Anwendungen steigern. So ist die Überwachung einer Kuhherde durch Sensoren kein Luxus, sondern spart Ressourcen ein. Ein Sensor pro Kuh kostet dabei nur zwischen 10 und 50 US-Dollar, eine verlorene oder gestohlene Kuh ist um einiges teuer. In der Erprobung finden sich sogar Sensoren, die die Körpertemperatur einer Kuh messen und so im Zuchtbetrie den Zeitpunkt des Eisprungs melden. Auch kranke Tiere lassen sich so durch ihr Fieber früh erkennen und Tierärzte können sich auch über die Cloud ein Bild der Tiere machen. Wichtig sind auch Bewässerungssensoren für eine intelligente Steuerung der Wasserzufuhr. Ein Sensor kann den Grundwasserstand, den Eisenanteil des Wassers oder den Salzgehalt des Bodens messen und so Entscheidungsgrundlagen für eine optimale Bewässerung liefern. Solche Sensoren des Unternehmens WaterBit wurden bereits in großen Betrieben in Kalifornien eingesetzt und ermöglichen den Anbau von Mandeln und Artischocken auch in dürrer Umgebungen.



Der Alltag von morgen

2020 wird ein wichtiges Jahr für den **technologischen Fortschritt**: Das Mooresche Gesetz verliert seine Gültigkeit; autonome Elektroautos bestimmen in zunehmendem Maße Transport und Verkehr. Die vielen Möglichkeiten und vor allem die **clevere Nutzung der Daten** aus vernetzten Dingen treiben diese Entwicklungen voran. In den folgenden **fünf Bereichen** werden sich **die größten Auswirkungen** zeigen.

WIM STOOP, Senior Product Marketing Manager, Cloudera

1- Predictive Maintenance

Vor allem in den Branchen Fertigung, Bergbau, Öl und Gas ist eine ordnungsgemäße Wartung und Pflege der Maschinen sehr wichtig. Aber eine rein auf Erfahrungswerten der Vergangenheit basierende Wartung kann Maschinenausfälle nicht vermeiden. Zahlen aus der Automobilbranche verdeutlichen das Problem: Autohersteller schätzen die Investitionen für ungeplante Auszeiten in Fertigungsanlagen pro Minute auf bis zu 22.000\$ bei einer Gesamthöhe von mehreren Millionen Dollar pro Vorfall. Vernetzte und mit IoT-Sensoren ausgestattete Maschinen ermöglichen es, den Zustand der Ausrüstung kontinuierlich zu überwachen und mit Hilfe von Data-Science- und Machine-Learning-Modellen Hinweise auf Funktionsstörungen aufzuspüren, bevor der Schadensfall eintritt. Ausfallzeiten lassen sich so um bis zu 50 Prozent reduzieren, Ersatzteilbestellungen und -auslieferungen sowie die Verteilung von Personal und Ressourcen effizienter und effektiver gestalten.

keiten neuer Anwendungsfälle: etwa soziale Navi-Tools wie Waze, die Informationen über den Verkehr, Hilfe bei der Suche nach einem freien Parkplatz und vielem mehr liefern. Beim Thema Sicherheit helfen neue Tools mit Funktionen wie Kollisionsvermeidung, Notruffunktionen und Vorwarnung bei Gefahr. Versicherungsgesellschaften nutzen schon jetzt Telematik, um auf der Grundlage des Fahrverhaltens und der individuellen Bedürfnisse des Versicherten eine personalisierte Police anzubieten. Behörden und Organisationen mit Sicherheitsaufgaben verwenden Fahrzeugdaten in Verbindung mit anderen Informationen, um Verkehrsmuster zu verstehen, Risiken zu erkennen und diese Einsichten in die Stadtplanung mit einzubeziehen. Welche positive Auswirkungen das haben kann, zeigt folgendes Praxisbeispiel: Durch die Überwachung tausender Speditionslastwagen mittels IoT-Schlüsseldaten reduzierte die Firma Navistar die Anzahl außerplanmäßiger Reparaturen und Ausfallzeiten um bis zu 40 Prozent. Darüber hinaus sanken die Wartungskosten deutlich: Diese betragen jetzt 0,03\$ pro Meile statt der branchenüblichen 0,12 bis 0,15\$

2 - Connected Car

2020 werden 75 Prozent aller produzierten Neuwagen über Internetkonktivität verfügen. Die Anzahl der Sensoren an einem Auto wird sich von derzeit 60 bis 100 auf 200 verdoppeln. Damit steigen auch die Möglich-

3 - Smart Infrastructure

Großstädte und Infrastrukturprojekte boomen – aber das Wachstum hat seinen Preis. Dreckige Luft, hohe Verbrechensraten und Verkehrs-



könnte auch bessere Produkte und Dienstleistungen herstellen und anbieten. Doch diese Informationen zu sammeln und zeitnah darauf zu reagieren, stellt Unternehmen bisher vor gewaltige Herausforderungen. Klassische Umfragen sind zu teuer und vor allem langsam. Bis die Daten ausgewertet sind, ist es meist zu spät, die erlangten Einsichten noch in die laufenden Produktionszyklen einfließen zu lassen. IoT-fähige Anwendungen und -Produkte dagegen verfügen über integrierte Analysefähigkeiten, mit deren Hilfe Organisationen erschließen können, wie ihre Kunden ihre Produkte nutzen. So können Unternehmen schnell auf aktuelle Probleme reagieren, neue oder zusätzliche Funktionen in die Produkte integrieren sowie letztendlich das Kundenerlebnis positiv beeinflussen. Die Firma GoPro kann beispielsweise in Echtzeit herausfinden, welche Kunden welches Modell und welche Version ihrer Kameras zu welchem Zweck (Video, Standbild, Teilen auf Sozialen Medien, etc.) einsetzen. Das erlaubt ihnen, gezielt und zeitnah Produktverbesserungen und neue Produktfunktionen zu entwickeln.

chaos sind nur drei der vielen Probleme, die Millionenmetropolen, U-Bahnen und Flughäfen zu meistern haben. Kein Wunder also, dass man überall beginnt, die Grenzen des technologisch Machbaren mittels IoT, Big Data, Mobile Computing und Analytics auszutesten. Ein Beispiel aus UK zeigt, wie so etwas funktionieren kann. Milton Keynes, eine der am schnellsten wachsenden Städte im Vereinigten Königreich, hat zusammen mit BT Global Services eine Lösung entwickelt, die Verkehrsteilnehmer auf der Suche nach einer Parkmöglichkeit zu einem freien Platz leitet. Das spart der Stadt nicht nur Millionen Pfund, weil keine neuen Parkplätze gebaut und instand gehalten werden müssen, sondern verringert auch die Emissionen, da der Suchende gezielt zu einem Parkplatz geleitet wird.

4 - Connected Healthcare

Chronische Krankheiten wie Herzerkrankungen, Krebs, Typ-2-Diabetes oder Arthritis und ihre Begleitscheinungen sind die am weitesten in den USA verbreiteten und vor allem kostenintensivsten Gesundheitsprobleme. Eine erfolgreiche Behandlung basiert meist auf der regelmäßigen Überwachung der wichtigsten Gesundheitswerte des Patienten. Das

Problem ist, durch vermehrte Kontrollbesuche in den Krankenhäusern steigen die Kosten der Behandlung weiter. Genau an dieser Stelle können IoT-Lösungen ansetzen. Ein chronisch Kranker könnte mit mehreren vernetzten IoT-Geräten ausgestattet werden. Diese zeichnen kontinuierlich die wichtigsten Gesundheitswerte auf und senden sie an eine auswertende Softwarelösung. Mittels Machine Learning und auf Basis der gesammelten Daten erkennt diese gefährliche Abweichungen und informiert den zuständigen Arzt. Vorreiter ist hier die Michael J. Fox Foundation. Gemeinsam mit Intel hat sie Tausende von Parkinson-Patienten mit Wearables ausgestattet, die über ein Mobiltelefon mehr als 300 Beobachtungen pro Sekunde zu Symptomen wie Bewegungsverlangsamung, Zittern oder Schlafqualität in die Cloud hochladen können. Diese steigende Datenmenge bietet Spezialisten die Möglichkeit, Muster zu erkennen und so die Krankheit besser zu erforschen.

5 - Connected Products & Analytics

Wenn Firmen wüssten, wie genau die Kunden ihre Produkte nutzen, dann ließe sich nicht nur mehr Umsatz erzielen, sondern man

Getting there

Das Internet der Dinge wird uns viele neue Möglichkeiten und Innovationen bringen. Schwierig ist jedoch noch das 'Getting there' – aber auch das ändert sich. Auf Open-Source basierende Software hat die Innovationsrate bereits beschleunigt und völlig neue, auf Daten basierende Anwendungen in den Unternehmen ermöglicht. Kein Wunder also, dass immer mehr Unternehmen auf den IoT-Zug aufspringen. Sichtbar wird dies z.B. bei den Mitgliedern der 'Eclipse IoT Working Group', was sich wie ein 'Who is Who' der wichtigsten IT-Unternehmen liest. Sie alle arbeiten zusammen, um Open-Source-Software und -Architektur zu entwickeln, um die IoT-Revolution zu beschleunigen. Die oben aufgeführten fünf Bereiche sind nur Beispiele, die zeigen, wo und wie das Internet der Dinge die Gesellschaft in den kommenden Jahren prägen wird. Aber damit ist das Potential noch lange nicht ausgeschöpft. Um jedoch optimal davon profitieren zu können, reicht es nicht, IoT-Sensoren einfach nur überall zu implementieren, denn das führt lediglich zu einer Datenflut; viel wichtiger ist künftig die Kontextualisierung der IoT-Daten, denn darin liegt der Schlüssel zu noch besseren Services. www.cloudera.com ■

Embedded Systeme

Embedded Systeme sind lange vor dem IoT – dem Internet der Dinge – die Plattform für viele nützliche Anwendungen. Doch ihre Vernetzung über das Internet macht neue Anwendungen möglich, die andere Geschäftsmodelle hervorbringt.

In einem Premiumauto laufen heute für ein reibungsloses Fahrerlebnis bis zu 100 Mio. Codezeilen in kleinen verteilten Embedded Systemen. Zum Vergleich: Die Facebook-Implementierung wird auf ca. 50 Mio. Zeilen Quellcode geschätzt. Nicht erst seit dem Internet der Dinge leisten die Kleinen erstaunliches. Aber durch das IoT kommen auf sie neue Aufgaben zu, insbesondere in puncto Kommunikation und Cloudanbindung. Hier liegen neue Anwendungen und Geschäftsfelder und die Embedded Systeme bilden das Rückgrad der IoT-Infrastruktur. (kbn)

www.i-need.de ■



Aaronn Electronic GmbH
82178 Puchheim | Tel.: +49 89 894577 0
info@aaronn.de
www.aaronn.de

Kontron FlatClient HMI-Produktserie

Mit der FlatClient HMI-Produktserie, die als ECO und PRO Version erhältlich ist, bietet Kontron höchstmögliche Flexibilität hinsichtlich Design und Montage. Die Frontausführung ist wahlweise mit PCAP Touch, resistivem Touch oder Sicherheitsglas erhältlich



FlatClient:

Maximale Vielseitigkeit und Flexibilität

- Displaygrößen von 10,4" bis 23,8" im Breitbild- und Standardformat
- Frontausführungen: PCAP Touch, resistiver Touch oder Schutzglas
- Erhältlich als ECO (Intel Atom® Quad Core™) und PRO Version (Intel® Core™ i5)
- Industrietauglich – robust, zuverlässig und wartungsfrei
- Flexible Anbringungsmöglichkeiten: Einbauversion oder als stand-alone/VESA im Vollmetallgehäuse



FlatClient XXL (Neu!)

Eine neue Dimension der Visualisierung

- Displaygrößen von 32" – 75" mit oder ohne Touch
- ECO Version (Intel Atom® Quad Core™) und PRO Version (Intel® Core™ i5)
- Industrietauglich: robust, zuverlässig und wartungsfrei
- Langzeitverfügbarkeit



Aaronn Electronic GmbH
82178 Puchheim | Tel.: +49 89 894577 0
info@aaronn.de
www.aaronn.de

Die neue Generation modularer BOX PC:

Advantech UNO-2484G:

Kompaktes, lüfterloses und robustes Design

- Modular Box IPC Plattform für Intel Core i7/i5/i3 Prozessor bis zu 2,6 GHz, 8 GB DDR4 eingebautem Speicher (Bis zu 16GB)
- 4x GbE, 4x USB 3.0, 1x HDMI, 1x DP (4K), 4x RS232/422/485
- 2. Layer für bis zu 4 iDoor Erweiterungen
- Optional TPM2.0 für Cyber Security
- Diverse System I/O's erweiterbar über die Advantech iDoor Technologie, z.B. PROFIBUS, PROFINET, EtherCat, Ethernet/IP, CANOpen, COM-Ports, Digital I/O. Wireless und viele mehr



Unterstützt
30+ iDoor
Kombinationen!

Technologiepartner:

ADVANTECH

Enabling an Intelligent Planet



kontron

Kontron S&T AG
86156 Augsburg | Tel. +49 821 4086-0
info@kontron.com
www.kontron.com

SMARC 2.0

DIE NÄCHSTE GENERATION FÜR
EMBEDDED IoT APPLIKATIONEN



- ▶ Ermöglicht mobile, vernetzte, embedded Lösungen
- ▶ Skalierbare Building Blocks
- ▶ Optimierte Pin-out Definitionen für vielseitige Architekturen
- ▶ Ultra low-power, low profile Lösungen
- ▶ Geeignet für raue Industrieumgebungen

Jetzt mehr Erfahren!





Kontron S&T AG
86156 Augsburg | Tel. +49 821 4086-0
info@kontron.com
www.kontron.com

INDUSTRIE COMPUTER PLATTFORM
FÜR EDGE/GATEWAY ANWENDUNGEN

KONTRON KBox A-203



- ▶ Intelligentes IoT Gateway für Edge Analytics, Datenerfassung, Remote Monitoring
- ▶ Intel Atom® x5-E3930 Prozessor
- ▶ Vielzahl an Schnittstellen und Erweiterungsmöglichkeiten
- ▶ Wartungsfrei
- ▶ Unterstützt Security Solution Kontron APPROTECT



Kontron S&T AG
86156 Augsburg | Tel. +49 821 4086-0
info@kontron.com
www.kontron.com

LEISTUNGSSTARKE INDUSTRIE COMPUTER
PLATTFORMEN

KONTRON KBOX C-102 SERIE



- ▶ Basierend auf 6th Gen Intel® Core™ oder XEON® E3-1500 Prozessoren für anspruchsvolle Steuerungsaufgaben
- ▶ Modulares Systemkonzept - Forever Young
- ▶ Wartungsfrei
- ▶ Security Solution Kontron APPROTECT
- ▶ Hoch skalierbar und erweiterbar



Schubert System Elektronik GmbH
78579 Neuhausen | Tel.: +49 7467 9497-200
info@schubert-system-elektronik.de
www.primecube.de

CUSTOMIZED COMPUTER SYSTEMS



NICHT VON DER STANGE. SONDERN VON VORTEIL.
IPC-Lösungen von Prime Cube®. Für Sie gemacht.

Widescreen quer/hoch · Multi-/Glastouch · CPUs bis Intel i5/i7 · 6th gen., AMD eKabini · Windows 8/10 und Linux · Look & Feel der Smartphone-Geräte · Anbau-/Einbau-Panel, Box-PCs · Individuelle Anpassung in Performance, Funktion und Design

Erfahren Sie mehr unter www.primecube.de

Anlagenbau, Industrie und Gebäude

SCHALTSCHRANKBAU

Methoden - Komponenten - Workflow

Immer aktuell!

Die neuen Normen und
Normenentwürfe der DKE **VDE DIN**



Das Magazin 'Schaltschrankbau' berichtet als erste Fachzeitschrift über relevante Technologien, Produkte, Normen und Trends für Hersteller von Schaltschränken und bietet aktuelles Wissen für Unternehmen aus Handwerk und Industrie.

ssb-magazin.de



Bild: © alphaspirit/Fotolia.com

Beschleunigen!

In der **industriellen Automatisierung** mit **Bildverarbeitung** gilt es, den höchstmöglichen **Produktionsdurchsatz** zu erreichen. **Steigende Sensorauflösungen** und **Bildraten** der Kameras **helfen** dabei, stellen jedoch auch neue Anforderungen an die Datenübertragung. Schnittstellen wie CoaxPress, 10GigE sowie Embedded-Systeme stellen viele Vision-Anwender vor die Frage, wie sie ihre Kamera am besten konfigurieren. Die **Verwendung von Framegrabbern** für industrielle Anwendungen in Hochgeschwindigkeit bietet dabei spezifische **Vorteile in Bezug auf Geschwindigkeit, Datensicherheit und die verlässliche Synchronisation** mehrerer Kameras.

DR. FREDERIK SCHÖNEBECK, Field Application Engineering, Framos GmbH

Um besser zu verstehen ob ein Framegrabber für ein Bildverarbeitungssystem oder eine Anwendung vorteilhaft ist, ist ein Blick auf die Funktionen und den Zweck eines Framegrabbers wichtig. Durch spezielle Synchronisationsfunktionen erfasst und überträgt ein Framegrabber hochauflösende Bilder mit sehr hohen Geschwindigkeiten in Echtzeit. Ein Framegrabber verwaltet die Bilddaten, die von der Kamera über den PCI-Bus in den Speicher des PC hochgeladen werden. Durch den Direct Memory Access (DMA) des Framegrabbers wird eine CPU-Überlastung durch Bildübertragungsvorgänge vermieden, indem die Bilddaten direkt in den RAM-Speicher des PC verschoben werden. Der Framegrabber übernimmt alle notwendigen Tasks und Prozesse zum Verschieben dieser Daten in den und aus dem Speicher, sodass die CPU für andere Aufgaben zur Verfügung steht. Außerdem kann er vorab die komplette Bildverarbeitung und eventuell weiteres Onboard-Processing der Bilddaten erledigen. Ein Framegrabber akzeptiert schnelles Triggering und/oder Encodersignale zur nahtlosen

Synchronisation bei Bildaufnahmen bewegter Objekte oder über multiple Kameras. Framegrabber ermöglichen verschiedene Bildaufnahme-Modi und unterstützen eine verzögerte Bildverarbeitung im Hintergrund des Gesamtprozesses. Der Framegrabber kann ein allgemeines 'bildbereit'-Signal an die SPS oder andere angeschlossene Geräte übermitteln, sodass er in der Automatisierung beispielsweise als Output-Manager genutzt werden kann.

Die Vorteile von Framegrabbern

Die wichtigsten Vorteile eines Framegrabbers liegen darin, in einem Bildverarbeitungssystem die Ergebnisse bei hoher Geschwindigkeit zu erzielen und damit vom höchstmöglichen Durchsatz zu profitieren.

- Übernahme der gesamten Bilderfassung und des I/O-Management von einem einzigen Gerät

- Management aller externen Geräte und deren Triggering und Synchronisierung
- Hohen Datenraten von bis zu 25GB/s
- All-in-One-Verwaltung mit zahlreichen erweiterten Bildverarbeitungsfunktionen
- Framegrabber übernimmt gesamte Vorverarbeitung und Bildvorbereitung wie beispielsweise Debayering oder Farbkorrekturen
- CPU steht derweil für andere Aufgaben zur Verfügung
- Dual-Triggering ermöglicht Signalsynchronisation bei Line-Scan-Anwendungen
- Latenzen unter 1µs möglich

Durch diese Merkmale und Funktionen sind Framegrabber eine einfache Lösung zur Verwaltung und Synchronisation von Bildverarbeitungssystemen in Echtzeit mit einer oder mehreren Kameras und der gleichzeitigen Unterstützung verschiedener Triggermodi. CoaXPress-Modelle wie der Euresys Coaxlink Quad 3D-LLE mit Onboard-IP übernehmen beispielsweise die 3D-Laserlinienextraktion und Triangulation, so dass eine präzise Abstimmung der Laserlinien bei exakten Messaufgaben möglich ist.

Framegrabber nutzen

Auch heute noch sind Framegrabber die beste Möglichkeit, eine Erhöhung der maximalen Geschwindigkeit und Auflösung der an eine Anwendung angeschlossenen Kameras zu erreichen. CoaXPress-Modelle mit bis zu vier Kanälen und 25GBps stellen hierbei die schnellste Möglichkeit zur Verbindung von Kameras und PC dar und unterstützen sehr hohe Auflösungen nahezu ohne Latenz in der Übertragung. Andere Lösungen mit hoher Bandbreite und direkter Verbindung, wie beispielsweise 10GigE-basierte, sind bedeutend langsamer und basieren vollständig auf Netzwerkkarten. Bei der Verwendung eines Framegrabbers entfällt das Risiko, dass Daten verloren gehen. Onboard-Puffer speichern die Bilddaten vorübergehend, sodass der Framegrabber die Bilder vor der Übertragung an den Host-PC rekonstruieren oder spiegeln kann. Die Bilder, die direkt in den RAM-Speicher übertragen werden, stehen sofort für CPU- oder GPU-Aufgaben zur Verfügung. Wichtig ist auch, dass alle Schnittstellen, Geräte und Parameter für mehrere Kameras und Systeme je nach Positions- und Timing-Parametern korrekt synchronisiert werden können, und zwar gleichzeitig mit der Onboard-Bildverarbeitung. Damit verringert sich wiederum die Belastung der CPU, die somit für andere Aufgaben frei bleibt.

Vier Kriterien für die Auswahl des richtigen Framegrabbers

Die individuellen Eigenschaften jedes Framegrabbers sind entscheidend für die Auswahl des richtigen Modells für eine Anwendung, um eine gelungene Bildleistung und Systemintegration zu erzielen. Bei der Auswahl eines Framegrabbers für eine spezifische Applikation sollten insbesondere vier Kriterien berücksichtigt werden:

- **Kameratyp**
 1. **Schnelligkeit:** Wie schnell ist der Kamerasensor? Ist es ein Flächen- oder Zeilensensor?
 2. **Farbigkeit:** Erfolgt die Bildaufnahme in Schwarz-Weiß oder Farbe? – Farbige Bilder beanspruchen aufgrund ihrer höheren Bildgröße normalerweise mehr Bandbreite.
 3. **Anwendungsumgebung:** Wo soll der Framegrabber verwendet werden?
- **Kamera-Schnittstelle** – Je nach Schnittstelle und Anschlussart gibt es verschiedene Modelle und Optionen.
- **Anzahl der Kameras** – Wie viele Kameras sollen ans System angebunden werden? Insbesondere wenn mehrere Kameras synchronisiert werden oder ein bereits installiertes System erweitert wird, empfiehlt sich ein Framegrabber.
- **Software** – Der Framegrabber muss softwareseitig kompatibel mit der Anwendungsumgebung sein.

Alle notwendigen Informationen, um den geeignetsten Framegrabber für eine bestimmte Anwendung auszuwählen und die jeweils

unterstützten Funktionalitäten sind den Datenblättern der Hersteller zu entnehmen.

Typische Anwendungen

Framegrabber werden meist dazu eingesetzt, die maximale Bandbreite und Datenübertragungsrate in Hochgeschwindigkeitsanwendungen zu erzielen. Die industrielle Inspektion, Broadcasting- und Sportanwendungen profitieren von der latenzarmen Synchronisation mehrerer Kameras, um die bestmögliche Bildanalyse aus verschiedenen Winkeln und Perspektiven zu erhalten. Die Qualitätsprüfung an Produktionsbändern mit sehr hoher Geschwindigkeit zählt zu den gängigsten und besten Beispielen, bei denen Framegrabber überzeugen, da sie die Bildaufnahmen mit den ankommenden Triggern synchronisieren und gleichzeitig die Bilder vorverarbeiten können. Auf diese Weise können die Pass-/Fail-Kriterien eines Produkts zuverlässig bestimmt und entsprechende Signale an die SPS gesendet werden, wobei die CPU deutlich entlastet wird und damit für weitere Aufgaben verfügbar ist.

Warum ein Framegrabber sinnvoll ist

Ein Framegrabber stellt innerhalb eines Bildverarbeitungssystems Funktionen für die Bilderfassung von hochauflösenden Bildern in Hochgeschwindigkeit bereit. Applikationsingenieure können damit ein Bildverarbeitungssystem mit deutlich erweiterten Aufnahmemöglichkeiten erstellen und gleichzeitig eine hochzuverlässige und konsistente Imaging-Pipeline ohne die Gefahr von Datenverlusten aufbauen. Mit Framegrabbern lassen sich Kameras bequem und zuverlässig mit dem PC verbinden, gerade in hochauflösenden Anwendungen, bei denen schnelle Datenübertragungs- und Trigger-Funktionen erforderlich sind.



Mehrwert durch Integration

An vielen industriellen Standorten arbeiten die **vorhandenen seriellen Geräte** noch immer **sehr effizient**. Das **volle Potenzial** vieler serieller Geräte ist jedoch **weitgehend noch nicht ausgeschöpft**. Um einen Mehrwert aus solchen Geräten zu generieren, werden die **von ihnen erfassten Daten in der Cloud gespeichert**. Das dient zur weiteren Analyse und dazu, bisher unbekannte Informationen zu erhalten, die breitere Möglichkeiten für die Verschlinkung des Betriebs eröffnen. Hierfür müssen die **bestehenden seriellen Geräte** zunächst **in ein Netzwerk integriert** werden.

CASPER YANG, Produktmanager, Moxa

Um serielle Altgeräte an ein Ethernet-basiertes Netzwerk anzubinden, können seriell-zu-Ethernet-Konverter, auch serielle Geräteserver genannt, installiert werden. Serielle Geräteserver unterstützen zwei Schnittstellen: eine serielle auf der einen Seite, eine Ethernet-Schnittstelle auf der anderen. Außerdem unterstützen sie virtuelle COM-Ports, sodass sie als bestehende COM-Ports im Scada-System dienen. Das bedeutet, dass ein bestehendes Scada-System genutzt werden kann – das spart die Kosten für eine Neuentwicklung. Darüber hinaus unterstüt-

zen serielle Geräteserver auch den so genannten Rad-Socket-Betrieb, der serielle Daten transparent in TCP oder UDP konvertiert. Die meisten Scada-Systeme und OPC-Server unterstützen Ethernet-Kapselungstreiber, die mit seriellen Geräteservern arbeiten, um proprietäre Protokolle zu empfangen. Das Protokoll muss zwar wie zuvor manuell gehandhabt werden, der Geräteserver hilft aber, die Daten mühelos an ein Ethernet-Netzwerk weiterzuleiten. Bevor Daten von seriellen Altgeräten empfangen werden können, müssen die Geräte korrekt konfiguriert werden. Die meisten nutzen proprietäre Protokolle, also muss man überlegen, wie sich die seriellen Daten in Ethernet-Pakete umwandeln lassen. Dabei müssen verschiedene Faktoren bedacht werden, damit die seriellen Geräteserver IoT-Cloud-Anwendungen unterstützen können.

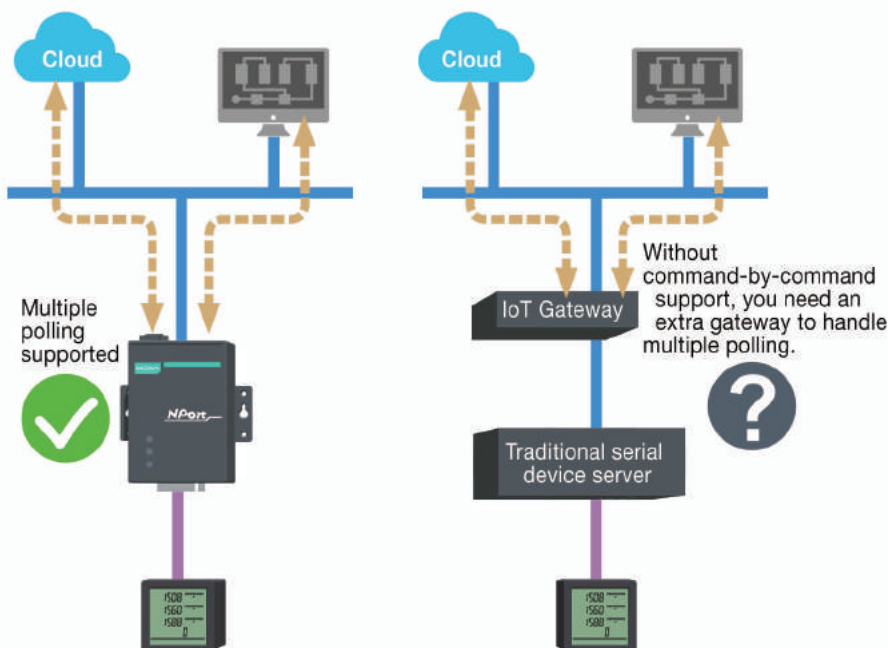
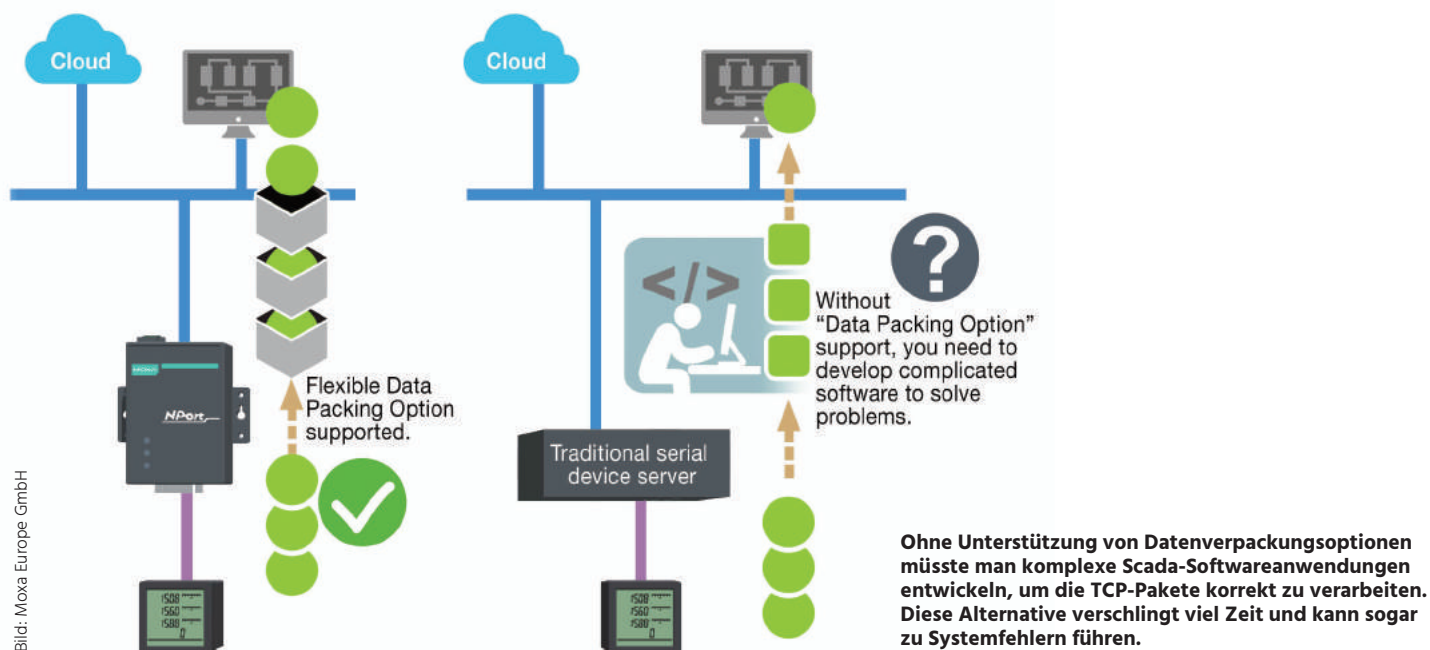


Bild: Moxa Europe GmbH

Multiples Polling

Die Anbindung eines seriellen Geräts an ein Escada-System ist einfach. Im Fall des IIoT ist dieser Vorgang jedoch nicht so unkompliziert, da die Daten in die Cloud vielleicht weitergeleitet werden müssen. Ein Scada-System und eine dezentrale Cloud-Anwendung können über einen seriellen Geräteserver gleichzeitig ein Kommando an ein seriellcs Gerät senden. Deshalb muss der Geräteserver die FIFO- (First In, First Out) Queue unterstützen, damit alle Anfragen verarbeitet werden können. Nur die erste Anfrage wird an ein seriellcs



Gerät gesendet, der Rest wartet in der FIFO-Warteschlange. Sobald der Geräteserver die Antwort eines seriellen Geräts empfängt, sendet er diese an das relevante Scada-System oder die Cloud-Anwendung und bearbeitet dann die nächste Anfrage in der Warteschlange. Diese Form des Befehl-für-Befehl-Abarbeitens ist in IIoT-Anwendungen mit multiplem Polling aufgrund der hohen Anzahl von Geräten mit proprietären Protokollen sehr wichtig. Ohne diese Funktionalität wäre ein extra IoT-Gateway erforderlich, welches multiples Polling unterstützt.

Proprietäre Protokolle über Ethernet

Da viele serielle Geräte proprietäre Protokolle einsetzen, ist die größte Herausforderung deren korrekte Konvertierung in Ethernet-Pakete. Viele serielle Geräteserver unterstützen die Betriebsmodi Raw Socket und TCP, welche diese Art der Konvertierung durchführen können. Das Problem liegt jedoch darin, dass ein serieller Geräteserver nicht zwangsläufig weiß, wie er serielle Daten in TCP-Pakete aufteilen soll. Die Geräteserver verstehen serielle Datenformate nicht, deshalb kann es sein, dass sie die Antwort eines seriellen Geräts in zwei oder mehr TCP-Pakete packen. Ein Scada-System oder eine Cloud-An-

wendung werden diese Pakete als falsche Antworten ablehnen, da sie erwarten, dass ein TCP-Paket einer einzelnen Antwort von einem seriellen Gerät entspricht. Um das zu vermeiden, müssen Geräteserver flexible Datenverpackungsoptionen beherrschen, da die proprietären Protokolle verschiedene Formate aufweisen können. Beispielsweise können feste Datenlängen oder spezielle Begrenzungszeichen genutzt werden, um einzelne Antworten serieller Geräte zu identifizieren. Das bedeutet, dass ein serieller Geräteserver die Daten eines seriellen Geräts so lange empfängt und nicht ans Ethernet weiterleitet, bis er die feste Datenlänge oder ein Begrenzungszeichen empfängt. Ohne Unterstützung von Datenverpackungsoptionen müsste man komplexe Scada-Softwareanwendungen entwickeln, um die TCP-Pakete korrekt zu verarbeiten. Diese Alternative verschlingt viel Zeit und kann sogar zu Systemfehlern führen.

Mehr Verbindungen, mehr Bandbreite

In vielen Anwendungen müssen serielle Geräte Daten an eine Leitstelle oder eine Cloud-Anwendung zurücksenden. Dazu müssen serielle Geräteserver eine dezentrale Verbindung öffnen, bevor sie serielle Daten übertragen können. Ist eine große Anzahl von seriellen Geräten im sel-

ben Netzwerk angebunden, erfordert diese Verbindung in der Leitstelle oder der Cloud-Anwendung viele Ressourcen. Um die vielen dezentralen Verbindungen richtig zu verarbeiten, sollten serielle Geräteserver die flexible Verbindungssteuerung unterstützen. Der beste Weg, um das zu tun, ist es, eine Verbindung nur dann zu öffnen, wenn serielle Daten von einem Gerät empfangen werden. Sobald die Verbindung beendet ist, sollte der Geräteserver die Verbindung so schnell wie möglich wieder schließen. Ohne flexible Verbindungssteuerung muss man Extrazeit investieren, um die Verbindungen in der Leitstelle oder Cloud-Anwendung zu bewältigen.

Das meiste aus einem Geräteserver herausholen

Wenn die Betriebsmodi richtig aufeinander abgestimmt werden, kann ein serieller Geräteserver viel Zeit und Geld sparen. Moxas serielle Geräteserver der NPort-Serie bieten eine Vielzahl von Betriebsmodi, die dabei helfen, verschiedene Arten serieller Geräte im Netzwerk sichtbar zu machen. Darüber hinaus bieten die Geräteserver verschiedene fortschrittliche Funktionen als Bestandteil jedes Betriebsmodus, um Anwender dabei zu unterstützen, ihren Betrieb zu verschlanken und die Vorteile der seriell-zu-Ethernet-Konnektivität vollständig auszuschöpfen.



Bild: Giesecke+Devrient Mobile Security GmbH

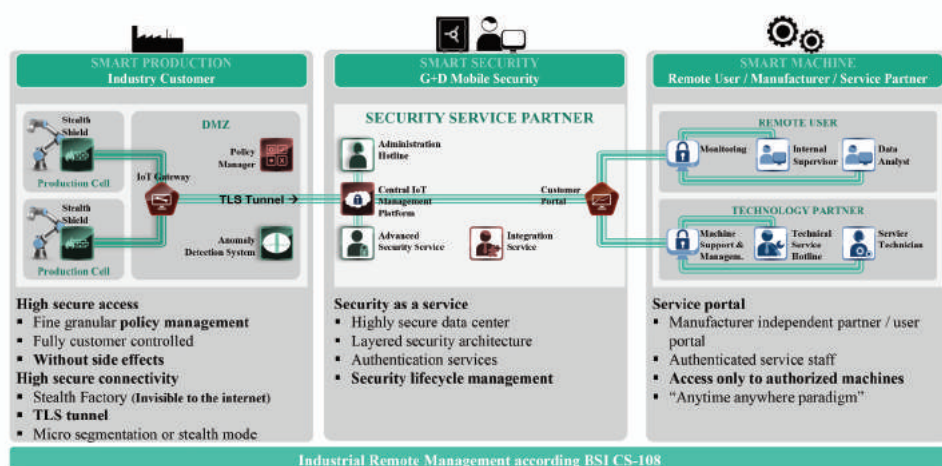
Aufbauend

Anzahl und Schwere der **Cyberangriffe auf Fertigungseinrichtungen** nehmen signifikant zu. Vor diesem Hintergrund hat G+D Mobile Security für seine eigenen Fertigungseinrichtungen (Herstellung von Banknoten, Bankkarten, etc.) lange nach einem **Security-Konzept** gesucht. Letztendlich hat man sich zu einer Eigenentwicklung entschlossen. Diese Lösung wurde mittlerweile dem Markt verfügbar gemacht, und mehr als 60 internationale Kunden profitieren bereits davon. Hersteller erhalten so nicht nur **Hilfestellung beim Aufbau von Cyber-Security**, sondern auch ein **geschütztes Framework für die Umsetzung von IoT-Lösungen im Industrieumfeld**.

DR. CHRISTIAN SCHLÄGER, Group Vice President und Head of Cyber Security, G+D Mobile Security

Im Zuge der industriellen Digitalisierung und der zunehmenden Konnektivität von Maschinen wächst die Gefahr aus dem Internet für Produktionsumgebungen rasant. Herkömmliche Vorgehensweisen wie Antiviren-Software ist für die Sicherung von Industriemaschinen ungeeignet, da Updates Auswirkungen auf die maschineneigene Software haben können. Erschwerend kommt hinzu, dass bei den langen Produktlebenszyklen im Feld in manchen Fällen die Betriebssysteme industrieller Maschinen unzureichend aktualisiert werden. Alle entsprechenden Maschinen und Fertigungsgeräte auf den neusten Stand mit modernen, sicheren Betriebssystemen zu bringen, scheitert an den enormen Kosten. Hinter Secure Industrial Visibility (SIV) verbirgt sich eine smarte, kompakte Box mit sicherem Betriebssystem und einer Software, die den Fernzugriff auf einzelne Maschinen erlaubt und sie gleichzeitig vor Cyberattacken schützt. Dabei wird

grundsätzlich das Produkt (Maschine) von der Security getrennt, indem eine zusätzliche Security-Komponente den Maschinen vorgeschaltet wird und eine Gateway-Funktion übernimmt (Bild 2). Damit entsteht eine kontrollierbare, sichere Schnittstelle. Mit SIV kann man Maschinen segmentieren, also mit einer Firewall regelrecht einkapseln. Die nun smarte Maschine erlaubt Aktualisierungen, Predictive Maintenance – also die vorausschauende Wartung – sowie als Option auch eine Anomalieerkennung (Anomaly Detection Service, ADS). Eine intelligente mit SIV und ADS ausgestattete Fabrik erkennt also eigenständig unberechtigte Zugriffe, weil sie lernt, normale Zugriffe von auffälligem Traffic zu unterscheiden. Hersteller müssen die Interaktion zwischen Maschinen, Produktionssteuerungssystemen und Personen allumfassend sichern. Bis heute noch werden dazu üblicherweise VPN (Virtual Private Network)-Verbindungen eingesetzt, bei denen allerdings die



Mit der SIV-Lösung wird eine zusätzliche smarte Security-Hardware den Maschinen vorgeschaltet. Damit kann der Zugriff auf ältere und neue Maschinen kontrolliert und geschützt werden, ohne Legacy-Produkte zu hohen Kosten austauschen zu müssen.

IP-Adressen der Geräte ungeschützt im Internet aufscheinen. Im Gegensatz zu gängigen VPN-Verbindungen arbeitet SIV im 'Stealth-Modus', das heißt, die IP-Adressen der Maschinen sind von außen nicht erkennbar. Damit wird die Angriffsfläche deutlich reduziert. SIV stellt eine sichere 'Tunnelverbindung' (Bild 2) zwischen den vernetzten Endpunkten her, mit feingranularer Richtlinienverwaltung, die vollständig vom Anwender gesteuert wird. Hierzu ist lediglich ein gewöhnlicher Internetbrowser auf Client-Seite erforderlich – die IP-Adresse bleibt für das Internet unsichtbar. SIV schützt vor Cyberangriffen, entdeckt Angriffe, reagiert auf Angriffe und arbeitet vorausschauend. Auf die einzelnen Fertigungseinrichtungen wird über ein sicheres und intelligentes IoT-Gateway zugegriffen. SIV ist unabhängig vom Anbieter oder Maschinenhersteller einsetzbar und sichert sowohl bestehende (als Nachrüstoption) als auch neue Maschinen in Industrie-4.0-Umgebungen. Damit ist SIV in der Lage eine Vielzahl von Industrie-IT-Systemen sowie das Maschinenservice- und Instandhaltungsmanagement mit High-End-Sicherheitsfunktionen auszustatten und deckt sämtliche Sicherheitsaspekte ab, darunter etwa Zertifikatsprüfungen oder Schwachstellen-Management. So erfüllt SIV schon heute die hohen Sicherheitsanforderungen für die Fernwartung im industriellen Umfeld (BSI CS-108) des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Infrastrukturen sichern

Hersteller profitieren auch von der Transparenz (Visibility) der vernetzten Maschinen und deren Anwendung auf allen Fertigungsstufen. So er-

halten Hersteller und Netzwerkverwalter detaillierte Informationen über die gesamte Wertschöpfungskette. Mit den so verfügbaren Daten können Fertigungs-Performance, Prozesse und Arbeitsabläufe verbessert werden. Dabei wird der Status des kompletten Maschinen-Parks ständig erfasst, was auch die älteren Maschinen einschließt, die nicht ursprünglich für das IIoT ausgelegt wurden. Zu den wesentlichen Einsatzbereichen und Vorteilen von SIV gehören die Fernwartungs-Diagnose, die schnelle Beseitigung von Problemen, das sichere System-Update, die Wartung, Performance-Management und -Reports sowie die verbesserten Systemabläufe. Außerdem ermöglicht die SIV-Lösung eine Verbesserung der Produktivität, eine gesicherte Identifizierung mit vertrauenswürdiger ID für alle Geräte sowie letztendlich

den Schutz der Fertigungseinrichtungen gegenüber Cyberangriffen und Daten-Lecks. Mit der SIV-Lösung können Hersteller verschiedene Fertigungsstätten sowie die Maschinen verschiedener Anbieter verwalten. Dabei haben sie die volle Übersicht und Kontrolle, durch die detaillierten Informationen über alle Fertigungsprozesse, Einrichtungen und Installationen. Remote-Zugriff und Datentransfer nahezu in Echtzeit wie Alarm- oder Fehlermeldungen helfen dabei, die Reaktionszeiten und Wartungskosten zu reduzieren. Auch Kapazitätsplanung und Qualitätssicherung können mit Hilfe von SIV verbessert werden. Letztendlich werden die Betriebskosten gesenkt, indem die langen Lebenszyklen auf der Fertigungsseite von den relativ kurzen IT-Zyklen entkoppelt werden.

Kompakte Security-Hardware

Es stehen zwei leistungsfähige Hardwaremodule zur Verfügung, die als SIV IoT-Gateway und geschützte Firewall direkt an der Maschine eingesetzt werden können. Es sind zwei Module (Base und Advance) mit unterschiedlichem Funktionsumfang und Abmessungen erhältlich. Die SIV Base-Box (Bild 3) misst nur 85x82x35mm und kann so platzsparend an jeder Maschine installiert werden. Beide Module verfügen über ein spezielles Security-Betriebssystem und einen entsprechenden Security-Hardwareanker. www.gi-de.com

Bild: Giesecke+Devrient Mobile Security GmbH



Es stehen intelligente Security-Hardwaremodule in zwei Ausführungen zur Verfügung (hier dargestellt die besonders kompakte Basis-Version), je nach Funktionsumfang und Applikation.

Tischmultimeter

Der Produktkatalog Digitalmultimeter umfasst neben Handgeräten auch Tischgeräte, wobei diese stationär, auf dem Tisch bzw. im Gestell, oder auch mobil verwendbar sind. Letztere besitzen dann einen Tragegriff.

Wie schon die Handgeräte, so unterscheiden sich die Tischgeräte untereinander in vielen Eigenschaften. Da die Tischmultimeter infolge größerer Messbereiche, geringerer Messunsicherheit und zusätzlichen Messfunktionen in einer höheren Preisklasse angesiedelt sind, spielen Schutzfunktionen eine wichtige Rolle. So lassen sich z.B. unbekannte Spannungen und Ströme zunächst in einem Autorange-Modus eingrenzen, bei der manuellen Messbereichseinstellung per Tastendruck könnte aber ein falscher Bereich ausgewählt worden sein. Weitere mögliche Messsituationen, die sogar zu einem Ausfall des Multimeters führen können, sind das Messen von Spannungen, während die Messleitungen für Strommessung eingesteckt sind, oder die Messung von Spannung in der Betriebsart Widerstandsmessung. In diesem Zusammenhang sind auch Eingangsstromsicherungen von Bedeutung. Diese müssen für die Löschung von Hochenergiekurzschlüssen ausgelegt sein, da sich ansonsten ein Lichtbogen über die Sicherungskontakte bilden kann, der neben Geräteschäden auch Personen gefährden kann. Gerade im industriellen Umfeld sind die unterschiedlichen Angaben der Hersteller zur Sicherheit von Multimetern besonders zu beachten.

(ghl) ■



Anbieter	AMC Analytik & Messtechnik GmbH
Produkt-ID	14912
Ort	Chemnitz
Telefon	0371/ 38388-0
Internet-Adresse	www.amc-systeme.de
Produktname	Digitalmultimeter HMC-8012
Einsatzschwerpunkt	Prozessindustrie, Industrielle Wartung und Service, Installationstests
Automatische / Manuelle Messbereichswahl	✓ / ✓
Anzeigeumfang	3 simultane Anz.: z.B. DC + AC + Statistik
Messgrundgenauigkeit in %	0,015%
Schutzklasse nach EN 61010-1	EN 61010-1, EN 61326-1
Spannungsmessbereich DC	0,4 - 1000 V
Höchste Genauigkeit im Spannungsmessbereich DC	
Spannungsmessbereich AC	0,4 - 750 V
Strommessbereich DC	20 mA - 10 A
Strommessbereich AC	20 mA - 10 A
Echte Effektivwertanzeige TRMS bis ... Frequenz	
Gleichzeitige Anzeige von DC und AC Messgrößen	✓
Tiefpassfilter zur Mes. von Spannung und Drehzahl	Nein
Widerstandsmessbereich	400 Ohm - 250 MOhm
Kapazitätsmessbereich	5 nF - 500 µF
Frequenzmessbereich	-
Temperaturmessbereich	PT100, PT500, - PT1000
Logik-, Dioden-, Transistor-, Durchgangstest	Nein, ✓, Nein, ✓
Zuschaltbare Hintergrundbeleuchtung	Nein
Messwertspeicherung im Gerät	Intern: 50.000; ext.: USB Stick Kapazität.
Schnittstellen	USB2.0 (TMC u. CDC/VCP), Ethernet, IEEE-488/GPIB optional

i-need.de
PRODUCT FINDER |

Direkt zur Marktübersicht auf
www.i-need.de/92



Anbieter	Conrad Electronic SE	Fluke Deutschland GmbH	Hacker-DatenTechnik	Keysight Technologies GmbH	Meilhaus Electronic GmbH
Produkt-ID	15619	2787	2791	29498	2774
Ort	Hirschau	Glottal	Bad Breisig	Böblingen	Ailing
Telefon	09604/ 4089-88	069/ 222220200	02633/ 200360	07031/ 464-1955	08141/ 5271-0
Internet-Adresse	www.conrad.biz	www.fluke.de	www.pc-messtechnik.biz	www.keysight.com	www.meilhaus.com
Produktname	Rigol DM3068	Fluke 8846A	PicoTest M3510A - High-Speed	34460A/34461A	Keysight 344xx Serie
Einsatzschwerpunkt	Prozessindustrie	Industrielle Wartung und Service, Labor, Prüffeld	Industrielle Wartung und Service, Installationstests, Prozessindustrie	Industrielle Wartung und Service	Industrielle Wartung und Service, Prozessindustrie
Automatische / Manuelle Messbereichswahl	✓ / Nein	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Anzeigeumfang	2.200.000	199.999		6 1/2 stellig	120.000
Messgrundgenauigkeit in %	±0,0015%	0,0024%	0,012%	0,0075/0,0035%	bis 16 ppm
Schutzklasse nach EN 61010-1	1000 V CAT I bzw. 300 V CAT II	1000 V CAT I bzw. 600 V CAT II	Inst. CAT II, Meas. CAT III bei max. 1000V		CAT II bis 300V, CAT I bis 1000Vdc
Spannungsmessbereich DC	0,1 µV - 1000 V	100 nV - 1.000 V	100 mV - 1000 V	100 mV - 1000 V	100mV - 1000V, je nach Modell
Höchste Genauigkeit im Spannungsmessbereich DC	±0,0015%	(±0,0024 % vom MW ±0,0005 % vom EW)		0,0075 / 0,0035%	±(0,0035%+0,0005%), je nach Modell
Spannungsmessbereich AC	0,1 µV - 750 V	100 nV - 300 kHz - 750 V	100 mV - 1000 V	100 mV - 750 V	100 mV - 750V, je nach Modell
Strommessbereich DC	0,1 nA - 10 A	100 pA - 10 A	10 mA - 10 A	100 µA - 3 A / 10 A	10 mA - 10A, je nach Modell
Strommessbereich AC	0,1 nA - 10 A	100 pA - 10 kHz - 10 A	1 A - 10 A	100 µA - 3 A / 10 A	10 mA - 10A, je nach Modell
Echte Effektivwertanzeige TRMS bis ... Frequenz	TRMS bis 300 kHz	TRMS für AC und DC bis 300 kHz	Integrierte TrueRMS Technologie	300 kHz	300 kHz
Gleichzeitige Anzeige von DC und AC Messgrößen	Nein	✓	✓	✓	Nein
Tiefpassfilter zur Mes. von Spannung und Drehzahl	Nein	Nein	Nein	Nein	Nein
Widerstandsmessbereich	100 µOhm - 100 MOhm	10 µOhm - 1 GOhm	100 Ohm - 100 MOhm	100 Ohm - 100 MOhm	100 Ohm - 100 MOhm, je nach Modell
Kapazitätsmessbereich	1 pF - 100 mF	1 nF - 50 mF	1 nF - 10000 µF	100 nF - 100 µF	1 nF - 10 µF, je nach Modell
Frequenzmessbereich	3 Hz - 1 MHz	1 µHz - 1 MHz	3 Hz - 300 kHz	3 Hz - 300 kHz	2Hz - 300 kHz, je nach Modell
Temperaturmessbereich	-	-200 °C - 600 °C	-250 °C - 2316 °C	Sensorabhängig	-80 °C - 150 °C, je nach Modell
Logik-, Dioden-, Transistor-, Durchgangstest	Nein, ✓, Nein, ✓	Nein, ✓, Nein, ✓	✓, ✓, ✓, ✓	Nein, ✓, ✓, ✓	Nein, ✓, Nein, ✓
Zuschaltbare Hintergrundbeleuchtung	✓	Nein	Nein	✓	✓
Messwertspeicherung im Gerät				1000 / 10.000 Messwerte	je nach Modell
Schnittstellen	RS232, USB, LAN, GPIB	RS 232, IEE-488.2, Ethernet, USB	USB, optional RS232 oder GPIB - IEEE-488.2	LAN, USB, GPIB	USB, LXI, GPIB, RS232

					
ASM Automation Sensorik Messte. GmbH 2731 Moosinning 08123/ 986-0 www.asn-sensor.de Hioki 3237 bis 3239	Chauvin Amoux GmbH 24222 Kehl/Rhein 07851/ 9926-40 www.chauvin-arnoux.de MX5060	CME CompuMess Elektronik GmbH 2747 Unterschleißheim 089/ 321501-10 www.compumess.de Transmille 8081	Conrad Electronic SE 2768 Hirschau 09604/ 4089-88 www.conrad.biz GW Instek GDM-8245	Conrad Electronic SE 2771 Hirschau 09604/ 4089-88 www.conrad.biz Hameg HM 8112-3	Conrad Electronic SE 13416 Hirschau 09604/ 4089-88 www.conrad.biz Votcraft VC650BT
Entwicklung, Forschung, Labor, Fertigungslinien	Industrielle Wartung und Service in der Elektrotechnik und in der Elektronik	Referenzquelle, Kalibration, Industrielle Wartung und Service	Prozessindustrie	Prozessindustrie, Stromverteilung	Industrielle Wartung und Service
✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
199999	60.000 Dig. / Analog-Bagr. mit 31 Segm.	105.000.000	50.000	1.200.000	40.000
0,01% ±2d	0,05%	4 ppm / Jahr	±0,03%	±0,003%	0,03%
1000V CAT I bzw. 600V CAT II	CAT III - 1000V		1000 V CAT I bzw. 500 V CAT II	600 V CAT II	600 V CAT II
200 mV - 1000 V	60 mV (kl. B.) / Aufl. 0,001 mV - 1000 V	10 nV - 1050 V	10 µV - 1000 V	100 nV - 600 V	0,01 mV - 600 V
0,01% ±2d	0,05 % Anz. + 25 D	0,9 ppm / 24 Std.	±(0,03 + 4 Digits)	±(0,003% + 0,0006%)	±(0,03 % + 10 digit)
2000 mV - 700 V	60 mV (kl. B.) / Aufl. 0,001 mV - 1000 V	100 nV - 1000V	10 µV - 1000 V	100 nV - 600 V	0,1 mV - 600 V
200 mA - 2000 mA	6000µA (kl.B.) / A. 0,1µA - 10A / 20A (30s)	0,1 pA - 30 A	10 nA - 20 A	100 pA - 1 A	0,01 µA - 10 A
200 mA - 2000 mA	6000µA (kl.B.) / A. 0,1µA - 10A / 20A (30s)	1 µA - 30 A	10 nA - 20 A	100 pA - 1 A	0,01 µA - 10 A
TRMS 10 Hz - 30 kHz	TRMS AC / DC / AC+DC bis 100 kHz	10 kHz	TRMS bis 50 kHz	TRMS bis 300 kHz	100 kHz
Nein	Nein	Nein	Nein	Nein	Nein
Nein	✓	Nein	Nein	Nein	✓
200 Ohm - 100 MOhm	600 Ohm (kl.B.) / Aufl. 0,01 Ohm - 60 MOhm	0,1 µOhm - 1 TOhm	10 mOhm - 20 MOhm	100 µOhm - 10 MOhm	0,01 Ohm - 40 MOhm
-	6 nF (kl. B.) / Aufl. 0,001 nF - 60 mF	-	1 pF - 50 µF	-	0,001 nF - 40 mF
100 Hz - 300 kHz	60 Hz (kl. B.) / Aufl. 0,01 Hz - 60 kHz	1 Hz - 10 MHz	10 Hz - 1 kHz	0,00001 Hz - 100 kHz	0,001 Hz - 4 MHz
-	-60°C / Aufl. 0,1°C - 1200°C / Aufl. 1°C	-200 °C - 660 °C	-	-270 °C - 1372 °C	-40,0 °C - 1000,0 °C
Nein, ✓, Nein, ✓	Nein, ✓, ✓, ✓	Nein, Nein, Nein, Nein	Nein, ✓, Nein, ✓	Nein, Nein, Nein, ✓	Nein, ✓, Nein, ✓
Nein	✓	Nein	Nein	✓	✓
30 Settings				30.000	1000
RS232, GPIB, ext. I/O	USB	RS232/GPIB/USB		USB, RS232	USB

					
Meilhaus Electronic GmbH 2797 Ailing 08141/ 5271-0 www.meilhaus.de Rigol DM30xx Serie	PCE Deutschland GmbH 23996 Meschede-Freienohl / www.warensortiment.de/messtechnik PCE-DSO8060	Plug-In Electronic GmbH 22469 Ailing 08141/ 3697-0 www.plugin-in.de SDM3055	PSE - Priggen Special Electronic 2790 Steinfurt 02551/ 5770 www.priggen.com Peak Tech 4000	Tektronix GmbH 2798 Köln 0221/ 9477-602 www.tek.com Digitalmultimeter Modell 2100	Tektronix GmbH 25733 Köln 0221/ 9477-277 www.tek.com Graphi. Sampling-Digitalmult. DMM7510
Industrielle Wartung und Service, Prozessindustrie			Industrielle Wartung und Service, Stromverteilung, Installationstests	Industrielle Wartung und Service, Prozessindustrie, Installationstests	Forschung, Design und Fertigung von elektronischen Bauteilen und Geräten
✓ / ✓	/	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
5½ und 6½ Digit bis 0,0035% (DCV, 1 Jahr)		5 1/2 stellig	53.000	1.000.000	7,5 Stellen
CAT I 1000 V, CAT II 600 V o. CAT II 300 V			CAT II 1000V		
200 mV - 1000 V	60 mV - 800 V	200 mV - 1000 V	1 µV - 1000 V	100 nV - 1000 V	10 nV - 1000 V
±(0,0035%+0,0005%)		0,02 %	±0,03% + 6 dgt.	±(0,0038% MW + 0,0006% Bereichsend.)	0,0014%
200 mV - 750 V	60 mV - 600 V	200 mV - 750 V	1 µV - 1000 V	100 nV - 750 V	100 nV - 700 V
200 µA - 10 A	60 mA - 10 A	0,2 mA - 10 A	0,01 µA - 10 A	10 nA - 3 A	1 pA - 10 A
20 mA - 10 A	60 mA - 10 A	20 mA - 10 A	0,01 µA - 10 A	1 µA - 3 A	1 nA - 10 A
100 kHz		10 kHz	TRMS bis 20 kHz	TRMS bis 300 kHz	300 kHz
		✓	Nein	Nein	Nein
		Nein	Nein	Nein	Nein
200 Ohm - 100 MOhm	600 Ohm - 60 MOhm	200 Ohm - 100 MOhm	10 mOhm - 50 MOhm	100 µOhm - 100 MOhm	100 nOhm - 1 GOhm
2 nF - 10000 µF	40 nF - 400 µF	2 nF - 10 mF	0,01 nF - 5000 µF	-	100 nF - 1 mF
20 Hz - 1 MHz	1 Hz - 25 MHz	20 Hz - 1 MHz	5 Hz - 200 kHz	3 Hz - 300 kHz	3 Hz - 500 kHz
-	-50 °C - 50 °C	-200 °C - 1820 °C	-	-100°C - 630°C	-200 °C - 1820 °C
, ✓, ,	, , ,	, ✓, , ✓	✓, ✓, Nein, ✓	Nein, ✓, Nein, ✓	Nein, ✓, Nein, ✓
	✓		Nein		Nein
bis 512 K Rdgs			30	2000	27M
USB, Ethernet/LXI, RS232	USB, Mini USB	USB, Ethernet, GPIB (optional)	USB		GPIB, USB, LXI

Intelligent und passiv

Auch **passive Komponenten** können **elektronischen Geräten** etwas **beibringen**: als **Schnittstelle aller zentralen und dezentralen Kommunikations-teilnehmer** bestimmen Elektronikgehäuse und Leiterplattenanschlüsse maßgeblich, **wie funktional ein Gerät ist** – und wie **flexibel** es in den intelligent vernetzten Automatisierungsstrukturen von morgen **eingesetzt** werden kann.

MARCO STAPELMANN, Marketing Communications,
Business Area Device Connectors, Phoenix Contact GmbH & Co. KG

Mit der Anzahl dezentraler Kommunikations- und Automatisierungskomponenten steigt auch die Anzahl der Schnittstellen. Schließlich müssen alle Geräte mit Leistung versorgt und kommunikativ in das Gesamtsystem eingebunden werden. Jeder Privatanwender kennt Steckverbinder – wie etwa HDMI zur Signalübertragung, RJ45 zur Datenübertragung oder Schuko-Stecker zur Übertragung der Leistung. Industrielle Verbindungslösungen müssen aber deutlich höhere Qualitäts- und Sicherheitsanforderungen erfüllen. Letztlich bestimmen diese passiven Anschlusskomponenten, wie funktional ein Gerät ist, wie flexibel es an unterschiedliche Anwendungsbereiche angepasst werden kann und wie ausfallsicher es auch unter extremer Beanspruchung arbeitet. In der Industrie- und Prozessautomation haben sich daher in den vergangenen Jahrzehnten zahlreiche – oft proprietäre – Anschlussarten, Verriegelungstechnologien, Schirmkonzepte und Polbilder etabliert. Eine große Herausforderung der international agierenden Initiativen und Konsortien wird es sein, diese Technologien zu vereinheitlichen und damit weltweit flexibel einsetzbare Verbindungslösungen zu ermöglichen.

Hybrid-Steckverbinder:
Signale, Daten und
Leistung werden
gleichzeitig über eine
einzige Leitung mit
einer einzigen Schnitt-
stelle übertragen

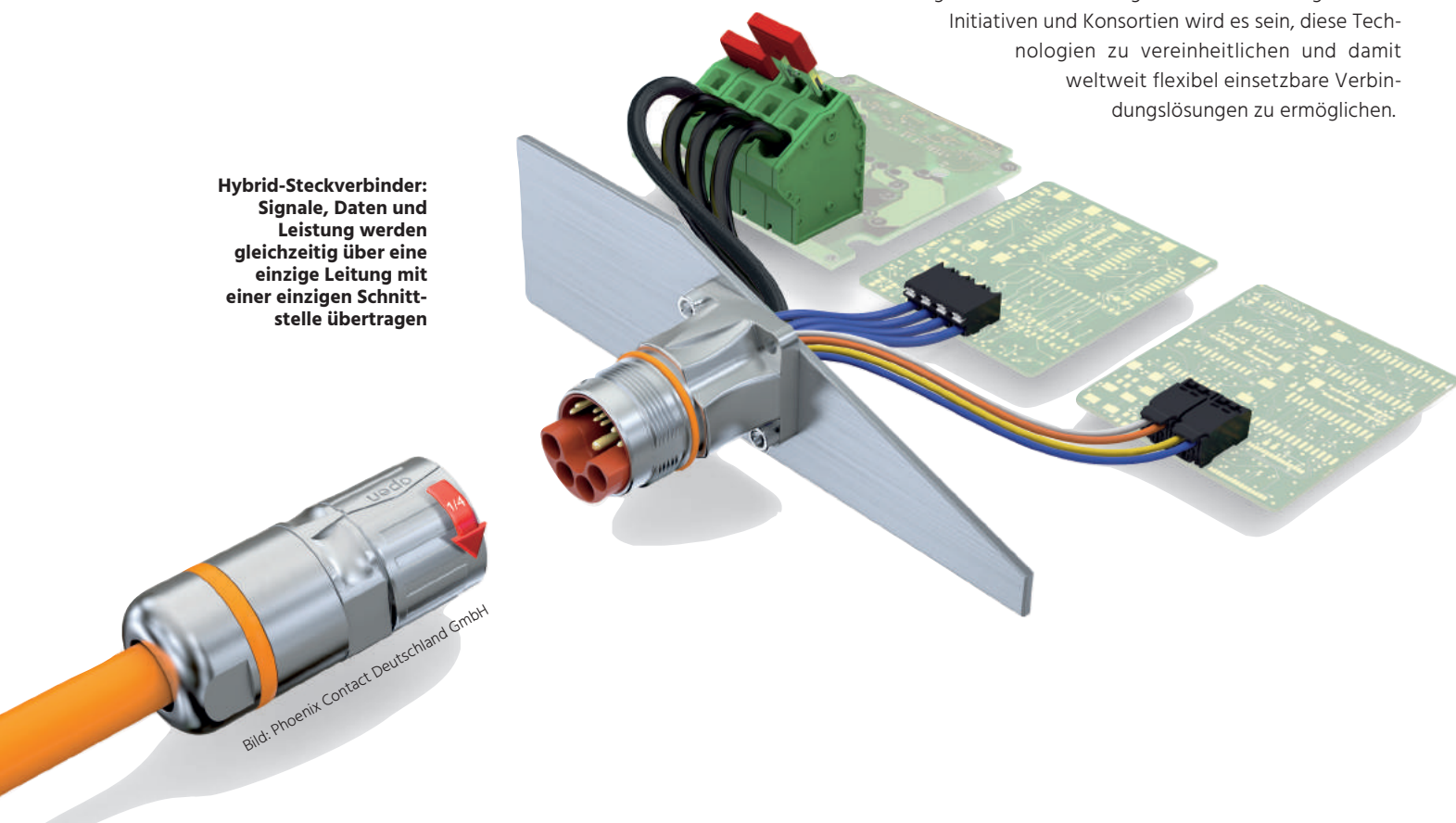


Bild: Phoenix Contact Deutschland GmbH

Flexibilität schaffen

Ein Beispiel für eine derartige Lösung ist die Kooperation der Unternehmen Phoenix Contact, Binder, Molex und Murrelektronik: auf der Hannover Messe 2017 haben diese Anbieter von Rundsteckverbindern die Entwicklung eines neuen Standards für M12-Push-Pull-Steckverbinder angekündigt, und bereits 2018 stellt Phoenix Contact die ersten Produkte vor. Der Vorteil: Einerseits sorgt die werkzeuglose Schnellverriegelung auch unter beengten Einbausituationen oder im rauen Industrieumfeld für sichere Verbindungen. Andererseits können Anwender künftig ihre Feld- und Geräteverkabelung mit – untereinander kompatiblen – Push-Pull-Steckverbindern von vier Herstellern umsetzen. Dies ermöglicht eine weltweit hohe Verfügbarkeit passender Steckverbinder und macht Gerätehersteller und Anlagenbetreiber flexibler in Planung, Design und Logistik. Auf diese Weise wird die eigentlich passive Komponente 'Anschluss-technik' zur Basis intelligent vernetzter und einfach erweiterbarer Systeme.

Intelligent im Feld verkabelt

Eine intelligente Lösung auf Basis etablierter Standards bieten auch Hybridsteckverbinder. Die Steckverbinder erlauben die gleichzeitige Übertragung von Signalen, Daten und Leistung über eine einzige Leitung und mit einer einzigen Schnittstelle. Die hybride Anschlusstechnik reduziert nicht nur den Platzbedarf am Gerät oder im Schaltschrank. Auch die Maschinen- und Anlagenverkabelung wird übersichtlicher, da nur noch eine einzige Leitung verlegt werden muss. Die daraus resultierenden schlankeren Kabelwege reduzieren wiederum die Kosten für Trasse und Kabelkanal (Bild 1). Da bis zu zwei Drittel weniger Kabelverbindungen verlegt werden müssen, können Geräte, Maschinen und Anlagenteile zudem einfacher in Betrieb genommen und gewartet werden. Viele Anlagen- und Maschinenbauer führen beispielsweise Vor-Inbetriebnahmen in der eigenen Fertigung durch. Nach erfolgreichem Abschluss dieser Tests müssen die Anlagen schnell und sicher abgebaut, versandt und beim Endkunden wieder in Betrieb genommen werden. Hier wirkt sich die reduzierte Anzahl anzuschließender Verbindungen unmittelbar auf die Verfügbarkeit und damit auf die Betriebseffizienz aus.



Bild: Phoenix Contact Deutschland GmbH

Vier Grundflächen, zwei Bauhöhen, individuelle Anschlusstechnik: das universelle Elektronikgehäuse bietet zahlreiche Anpassungsmöglichkeiten

Direkt auf der Leiterplatte

Intelligente Anschlusslösungen sind auch im Geräteinneren möglich. Hier stehen nicht der Wartungs- und Bedienkomfort im Feld im Vordergrund, sondern der Anschlusskomfort und die Flexibilität im Leiterplatten- und Gerätedesign. Die Direktstecktechnik Skedd erlaubt erstmals direkt steck- und lösbare Anschlüsse an beliebiger Position. Die Steckverbinder SDDC 1,5 und SDC 2,5 von Phoenix Contact benötigen keine Grundleiste und können direkt von Hand in verzinnte, durchkontaktierte Bohrlöcher gesteckt werden. Bisher mussten die Elektronikhersteller applikationsspezifische Anschlusstechnik wie Leiterplattenklemmen oder Grundleisten in einem irreversiblen Lötprozess mit der Platine verbinden. Damit war die Funktionalität der Leiterplatte und des gesamten Gerätes jedoch weitgehend fixiert. Durch die Skedd-Technik bleiben Leiterplatten- und Gerätehersteller flexibel. In der Leiterplatten-Fertigung müssen lediglich entsprechende Bohrlöcher vorgesehen werden. Je nach Endanwendung des Geräts können dann Anschlüsse für Leistungen bis zu 160V (SDDC 1,5) oder 320V (SDC 2,5) aufgesteckt werden, ohne die bestückte Leiterplatte nochmals thermisch zu belasten.

Universelle Elektronikverpackung

Elektronikgehäuse bieten die passende Verpackung für die bestückten Leiterplatten und

damit die funktionale Hülle für Geräte wie Steuerungen oder Bediengeräte. Die universellen Gehäuse UCS etwa eignen sich besonders für Embedded Systems – also für den dezentralen Einsatz dedizierter Informationstechnologie. Die Elektronikgehäuse bestehen aus zwei identischen Halbschalen in vier unterschiedlichen Größen. Kombiniert mit den herausnehmbaren Seitenwänden in zwei Höhen ergeben sich acht Kombinationsmöglichkeiten zur Unterbringung von Standard- oder individuellen Leiterplatten. Der Clou dabei: das System ist so konzipiert, dass jeweils die größere der beiden Seitenwände als kleine Seitenwand der nächstgrößeren Gehäuse-Variante eingesetzt werden kann. Die für entsprechende Schnittstellen bearbeiteten Seitenwände können also ohne Anpassungen in zwei Gehäusegrößen eingesetzt werden. Elektronikgehäuse bieten unterschiedliche Möglichkeiten, um Leiterplatten zu befestigen. Um für individuelle Elektronik-Layouts die maximale Bestückungsfläche auszunutzen, können die Leiterplatten über die integrierten Schraubdome direkt an den Eckenlegern fixiert werden. Soll auf Basis standardisierter Leiterplatten die Flexibilität steigen, können die Eckenleger auch ohne die integrierten Schraubdome verwendet werden. Die Leiterplatten werden dann auf spezielle Aufnahmen gesetzt, die an der passenden Position der Gehäuseschale eingeklebt werden. Die Kombination aus beiden Befestigungssystemen erlaubt individuelle Gestaltungsmöglichkeiten. Auch zwei Leiterplatten stellen kein Problem dar, denn in jeder Gehäusehalbschale kann die gesamte Grundfläche ausgenutzt werden. Lediglich die Aufbauhöhe der Leiterplatten bildet eine Begrenzung (Bild 2).

www.phoenixcontact.de ■

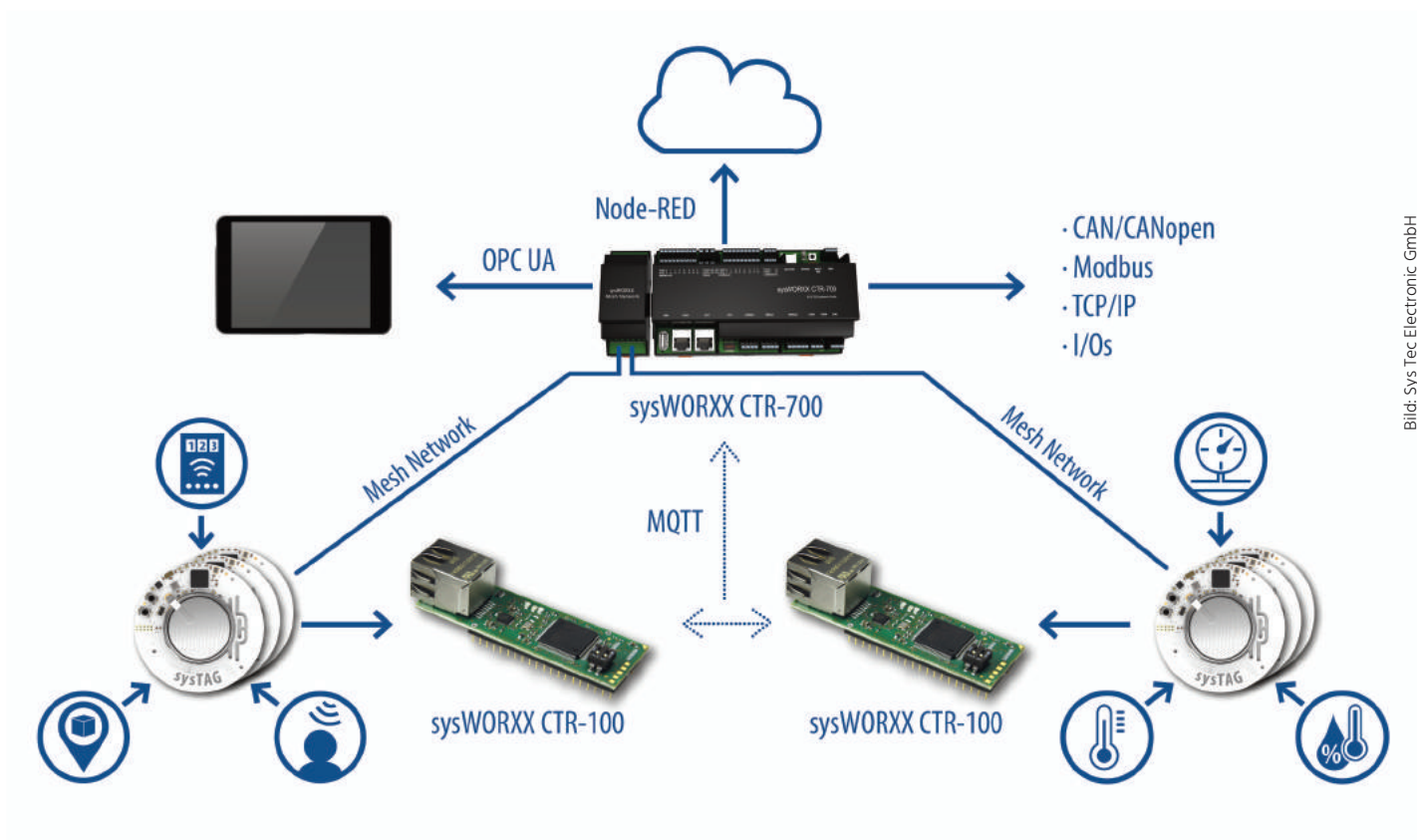


Bild: Sys Tec Electronic GmbH

Voll vernetzt

Mit der neuen Produktfamilie sysWorxx will Sys Tec Electronic den **Weg ins Internet der Dinge** und die **Industrie 4.0 vereinfachen**. Die **Steuerungen** ermöglichen neben **Predictive Maintenance** auch **Condition Monitoring**.

JAN SCHULZE, Head of Communications, Sys Tec Electronic GmbH

Anfang Januar hat es Sys Tec Electronic im wahrsten Sinne des Wortes kalt erwischt. Nach der Produktionspause über Weihnachten und Jahreswechsel wartete eine unangenehme Überraschung: Während des geplanten Produktionsstillstands war die Heizungsanlage ausgefallen. Die Folge: Ungeplanter Stillstand der Produktion – sowohl bei Mitarbeitern wie Maschinen. „Und das uns, die wir die passenden Produkte im Sortiment haben, um so etwas frühzeitig zu erkennen“, lacht Klaus Rupprecht, kaufmännischer Direktor bei Sys Tec electronic, „Jetzt kann uns das nicht mehr passieren.“ Jetzt messen in allen Produktionsbereichen vernetzte Sensoren Temperatur und Luftfeuchtigkeit, erklärt Rupprechts Kollege Thomas Krause, Direktor der Fertigung: „Wenn so etwas erneut passieren sollte, bekommen die Produktionsleiter umgehend eine Nachricht auf ihr Handy und können eingreifen.“ Der unangenehme Zwischenfall, der die Wiederaufnahme der Produktion verzögerte, zeigt Nutzen und Vorteile des Internet der Dinge in der Produktion und die Vorzüge der Industrie 4.0. Beim Einstieg in die moderne Fertigung unterstützt die neue Produktfamilie ‘sysWorxx’ von Sys Tec.

Revolution in der Industrie

Das Internet der Dinge (IoT) ist ein Konzept, nach dem unterschiedlichste Objekte und Rechensysteme über Netzwerke und das Internet verbunden sind, miteinander kommunizieren und Daten austauschen. Das können ganz Fabriken sein. Die kleinsten dieser Dinge sind per Funk angebundene Sensoren wie die, die bei Sys Tec Electronic jetzt Temperatur und Luftfeuchtigkeit überwachen. Das Internet der Dinge bildet wiederum einen Teil der Basis für die Industrie 4.0, ein von Henning Kagermann, Wolf-Dieter Lukas und Wolfgang Wahlster erstmals erwähnter Begriff. Er beschreibt die vierte revolutionäre Entwicklung in der Industrie dank Cyber Physical Systems und massiver Vernetzung. Die erste Revolution war die Einführung mechanischer Wasser- oder Dampfkraft-betriebener Produktionsanlagen im 18. Jahrhundert. Ihr folgte Revolution zwei in Form der Elektrifizierung und der Fließbandproduktion. Als Stufe drei sehen Experten den Einsatz von Elektronik und elektronischer Datenverarbeitung bis hin zu digitalen Maschinensteuerungen. Aus dieser dritten Stufe industrieller Revolutionen bringt Sys Tec Electronic 27 Jahre Erfahrung und Wissen über die Bedürfnisse von



Bild: Sys Tec Electronic GmbH

Neben zahlreichen Schnittstellen wie industriellen Ein- und Ausgängen, TCP/IP, MQTT, Modbus, CANopen, USB, µSD enthält die Steuerung zwei Ethernet-Schnittstellen. Damit wird die Trennung von Enterprise IT und Shop Floor OT gewährleistet.

Industriekunden in die Industrie 4.0. Das Unternehmen bietet dabei von Hardware- über Elektronik- bis hin zu Software-Entwicklungen Lösungen für den Embedded- und Anwendungsbereich – auch mit Cloud-Anbindung. „Wir kommen aus der Tradition der Automatisierungsfunktionen“, erklärt Klaus Rupprecht, „Von daher sind unsere IoT-Lösungen wie die sysWorxx-Familie immer auch verbunden mit Funktionen der Maschinensteuerung.“ Das Unternehmen liefere mehr als nur Gateways, die Daten lediglich durchreichen, ohne sie zu be- oder verarbeiten. Zum Beispiel das CTR-100: Die neue Steuerung bringt unter ande-

rem Signalvorverarbeitung für Bluetooth-Sensoren mit und leitet seine Daten an das ebenfalls neue CTR-700 weiter. Diese größere und leistungsfähigere Steuerung wurde speziell aber nicht nur für Predictive Maintenance und Condition Monitoring konzipiert und kann Daten mehrerer Maschinen verarbeiten und verwalten und dient als Schnittstelle zu Cloud-Servern bzw. Leitwarten. Die vorbereitende Datenverarbeitung direkt an der Maschine ist nötig, weil viele Anwendungen in der Produktion zeitkritisch sind. Sys Tec leitet Daten deswegen nicht einfach in 'eine große Wolke'. „Mit der sysWorxx CTR-100 werden Maschinendaten in der Steuerung bereits vorverarbeitet“, erklärt Thomas Krause, „Wenn dann Abweichungen oder Fehler auftreten, senden wir über die CTR-700 und per Cloud eine Warnung an die Anwender, um darauf hinzuweisen – z. B. dann, wenn Werte außerhalb definierter Grenzen liegen.“

Condition Monitoring mit sysWorxx

Beim IoT und der Industrie 4.0 geht es nicht nur um Warnungen, sondern darum, die Produktion zu verbessern. Rupprecht

beschreibt ein Beispiel: „Viele Hardwareproduzenten haben Lötöfen im Einsatz, die beim Aufheizen extrem viel Energie benötigen, was den Stromtarif in die Höhe treiben kann.“ Ist der Ofen auf Betriebstemperatur, sinkt die benötigte Menge an Energie massiv ab. Mithilfe dezentraler Strommessung, wie sie die Sys Tec mit sysWorxx anbietet, lässt sich das Verhalten beobachten und analysieren. Dazu kommen Bluetooth-basierte vermaschte Sensoren zum Einsatz. Deren Messwerte werden an die sysWorxx-Gateways gesendet und dort exakt ausgewertet. So kann verhindert werden, dass die Spitzenleistung über einen festgelegten Höchstwert hinausgetrieben wird. „Sie können die Öfen nacheinander hochfahren, also den zweiten erst dann, wenn die Werte des ersten Ofens zeigen, dass genug Luft bis zum festgelegten Spitzenwert ist.“ Mit dieser modernen Regeltechnik kann der Anwender verhindern, bestimmte Spitzenwerte innerhalb des Abrechnungszeitraums zu überschreiten und so in einen teureren Tarif seines Energieversorgers zu rutschen. Wer bisher kein solches Monitoring betriebe, könne seine Kosten sogar senken, so Klaus Rupprecht: „Weil Sie Peaks vermeiden können, die sie vorher nur erahnen konnten.“

Vorher wissen was kaputt geht

Mit dem Monitoring wird für Anwender noch ein weiteres Anwendungsfeld aus der Industrie 4.0 möglich: Die vorausschauende Wartung (Predictive Maintenance). Dabei erkennen die Kontrollsysteme minimale Änderungen in den Maschinendaten, die auf Verschleiß oder gar auf mögliche Ausfälle hinweisen. Mit einem Monitoring wie bei den Lötöfen lässt sich Predictive Maintenance realisieren, erklärt Thomas Krause: „Aus den Messwerten, beispielsweise wenn die Öfen länger zum Aufheizen brauchen, können Sie zunehmenden Verschleiß der Heizelemente erkennen. Zeigt die Verlaufsanalyse, dass regelmäßig ungewohnt viel nachgeheizt werden muss, könnte die Isolierung Defekte aufweisen.“ Durch die digitale Überwachung durch die sysWorxx-Familie lassen sich regelmäßige Wartungen verringern. Teilweise kann ganz darauf verzichtet werden und stattdessen vorausschauend dem Verschleiß entsprechend gewartet werden. Mit sysWorxx ermöglicht Sys Tec Electronic den sinnvollen und auf das eigene Unternehmen abgestimmten Einstieg in das IoT und die Industrie 4.0. www.systec-electronic.com



Bild: Sys Tec Electronic GmbH



Zuverlässig vernetzt

Die **Anforderungen** an **Steuerungsrechner** in **fahrerlosen Transportsystemen (FTS)** sind hoch. Die Rechner werden häufig im **Dauerbetrieb** bei **ständigen Vibrationen** eingesetzt. Ungeplante Ausfälle lassen schnell massive Kosten auflaufen. Entsprechend braucht es hier **zuverlässige Industriecomputer** mit **Wireless-Konnektivität**.

PATRIK HELLMÜLLER, Public Relations, Syslogic GmbH

Durch schnelle Entwicklungen im Bereich Wireless-Technologie wird die Automatisierung aktuell stark vorangetrieben. Insbesondere in der Logistikbranche birgt die Automatisierung beträchtliches Einsparpotenzial. Wertvolle Dienste leisten dabei fahrerlose Transportsysteme (FTS). Sie sorgen für einen organisierten Material- und Informationsfluss, was nicht nur für eine bessere Produktivität, sondern auch für eine hohe Transparenz sorgt. Die kalkulierbaren Transportvorgänge erlauben es, die Lagerbestände zu reduzieren. Als weiterer Vorteil lassen sich die Personalkosten senken und Fehllieferungen sowie Transportschäden vermeiden. Entsprechend vielseitig werden FTS eingesetzt, sei es für die Lagerbewirtschaftung, für die Gepäckabfertigung an Flughäfen oder für Logistikaufgaben in Spitälern.

Zuverlässigkeit entscheidend

Moderne Steuerungscomputer lassen sich mittels WLAN-, GPS-, GSM und Bluetooth-Modulen vernetzen und eignen sich damit zur Umsetzung des IIoT. Gleichzeitig kann die Wireless-Technologie aber auch zur Achillesferse werden. Dann, wenn ungeplante Ausfälle einzelner Komponenten ganze Logistiksysteme lahmlegen. Gerade in der Logistik laufen bei solchen Zwischenfällen schnell massive Kosten auf. In den letzten Jahren haben sich immer mehr Industriehersteller dem Consumer-Markt angenähert. Infolgedessen kamen vermeintlich industrielle Produkte auf den Markt, die den Industrieanforderungen nicht gewachsen sind. Damit automatisierte Logistiksysteme zuverlässig funktionieren, braucht es ro-



Steuerungsrechner für
fahrerlose Transportsysteme (FTS)

Bild: Syslogic GmbH



Der Industrie-PC Compact M8 wurde
für den Einsatz in fahrerlosen Transportsystemen (FTS)
oder in Logistiksystemen entwickelt.

tisch. Via Flash Controller werden Daten in einer Matrix aus Zeilen und Spalten direkt auf sogenannte NAND adressiert.

- **Echte Embedded-Prozessorplattformen**
Längst nicht alle Prozessorplattformen, die als industriell bezeichnet werden, eignen sich tatsächlich für den harten Industrieinsatz. Echte Embedded-Prozessoren zeichnen sich durch ihr Low-Power-Design aus. Durch niedrige Leistungsaufnahme erzeugen die Prozessoren eine geringe Abwärme. Damit erreichen sie einerseits sehr hohe MTBF-Werte (Mean Time Between Failures), andererseits wird ein anfälliger Lüfter überflüssig. Die Baytrail- und Apollolake-Prozessorfamilien von Intel Atom werden aktuell erfolgreich für Industrieapplikationen eingesetzt.
- **Erweiterter Temperaturbereich**
Je nach Einsatzgebiet können in der Logistik extreme Temperaturen herrschen. Sei es die Hitze in Produktionshallen oder die Kälte in der Lebensmittelverarbeitung. Echte Industriecomputer sind für den erweiterten Temperaturbereich von -40 bis +85 Grad zertifiziert. Wichtig ist dabei die Art der Zertifizierung, denn viele Hersteller verlassen sich auf ein Screening-Verfahren. Nur wenige Hersteller spezifizieren den Temperaturbereich bereits in der Entwicklungsphase und treffen eine entsprechende Bauteilauswahl. Nur so sind Hersteller in der Lage, einen langfristig zuverlässigen Betrieb unter extremen Temperaturen sicherzustellen.
- **Robuste Stecker**
Gerade in Fahrzeugen wie fahrerlosen Transportsystemen (FTS) sind ständige Vibrationen eine Herausforderung. Zu einem industriellen Board-Design gehören robuste Stecker. M12-Stecker sind mit ihren Crimp-Kontakten beständig gegen Vibrationen und Schocks. Zudem verhindern M12-Stecker, dass über die Schnittstellen Staub oder Feuchtigkeit ins Innere des Industrierechners gelangt.

- **Intelligentes Überwachungssystem**
Neben der robusten Bauweise überzeugen moderne Industrierechner zudem mit cleveren Überwachungssystemen. Bei Syslogic beispielsweise beinhaltet das Überwachungssystem ein intelligentes Power Management, eine Temperaturüberwachung sowie einen Watchdog. Während beim intelligenten Power Management ein zusätzlicher Mikrokontroller das Ein- und Ausschaltverhalten überwacht und damit auch beim Abschalten des Gesamtsystems, beispielsweise einer Anlage oder eines Fahrzeuges, ein definiertes Shutdown-Management des Industrierechners erlaubt, stellt der Watchdog sicher, dass das System im Fall einer Störung automatisch wieder gestartet wird. Mit der Temperaturüberwachung kann der Wärmegrad im System überwacht werden und allenfalls eingegriffen werden. Ein ernstzunehmendes Thema ist auch der Schutz vor Hackerangriffen. Seriöse Anbieter bieten meist Schutzfunktionen, beispielsweise mittels eines Trusted Platform Module (TPM).

Ein weiterer wichtiger Punkt in der Logistikbranche ist die Verfügbarkeit der Steuerungsrechner. Fallen einzelne Komponenten aus und sind nicht mehr lieferbar, kann das für komplexe Logistiksysteme weitreichende Folgen haben. Ein Unternehmen, das seinen Kunden Industriecomputer mit überdurchschnittlich langer Verfügbarkeit bietet, ist Syslogic. Als eines der wenigen Unternehmen in Europa entwickelt und fertigt Syslogic ihre Steuerungsrechner und Touch-Panel-Systeme selbst. Entsprechend achtet das Unternehmen bereits bei der Entwicklung ihrer Produkte auf eine lange Verfügbarkeit sämtlicher Komponenten. Werden Steuerungsrechner bedarfsgerecht evaluiert, leisten sie einen wichtigen Beitrag zur Automatisierung und zur Realisierung des IIoT. Das gilt für die Logistikbranche genauso wie für andere Industriezweige mit hohen Anforderungen an Steuerungskomponenten. www.syslogic.de ■

buste und langlebige Steuerungen. Es gibt einige Unternehmen, die sich kompromisslosen Industriecomputern verschrieben haben. Diese Unternehmen legen ihr Augenmerk insbesondere auf fünf Punkte:

- **Keine anfälligen Bauteile**
Echte Industriecomputer kommen ohne anfällige Bauteile wie Batterien oder rotierende Teile aus. Anstelle herkömmlicher Harddisks werden industrielle Festkörperlaufwerke (Solid State Disk) verwendet. Während konventionelle Harddisks wegen des mechanischen Lesekopfs bei ständigen Vibrationen und Erschütterungen frühzeitig ausfallen, bieten industrielle SSD-Speicher (Solid State Drive) eine wesentlich bessere Haltbarkeit. Im Gegensatz zu den mechanischen Harddisks funktionieren SSD-Speicher statisch, nicht op-

Bild: Syslogic GmbH



Bild: NetModule AG

Immer im Auge

Traceability spielt für **Logistikprozesse** eine **immer wichtigere Rolle**. Die Beförderung soll so wirtschaftlich wie möglich erfolgen, zugleich rückverfolgbar über die gesamte Supply Chain sein. Hier sind **professionelle Konnektivitätslösungen** gefragt, die auch Frachtbedingungen prüfen und somit eine **transparente Logistikprozess-Überwachung** ermöglichen.

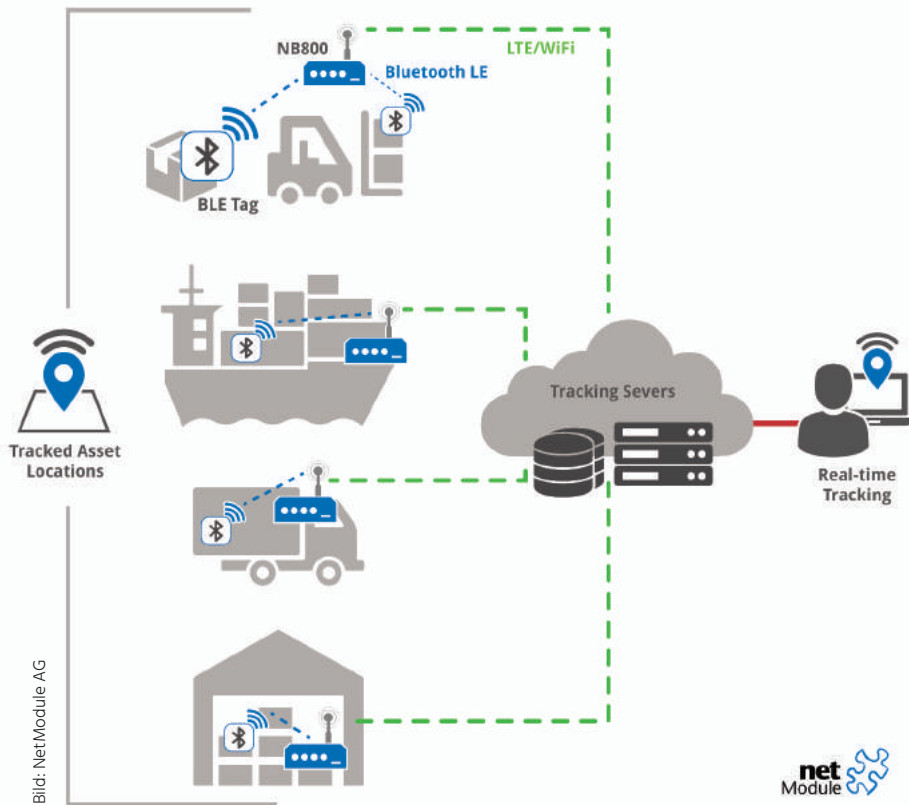
JÜRGEN KERN, CEO, Netmodule AG

Unser Beispiel skizziert den Transport von Motorenblöcken für den Einsatz in Industriemaschinen. Nach deren Produktion werden sie in Containern verladen und per Schiff und LKW an die Zielorte transportiert. Um zu kontrollieren, welche Lieferungen sich im Container und im Lager befinden, ob der Transport pünktlich erfolgt und ob es eine unsachgemäße Handhabung der Fracht gab, einschließlich der Ermittlung des Verursachers, wurde eine Lösung gesucht. Diese sollte einfach installierbar sein, kundenspezifische Sensordaten sammeln und deren Übertragung per Cloud erlauben und Warnmeldungen in Echtzeit liefern. Wegen entfernten Standorten sollte auch Fernwartung möglich sein. Weitere Anforderungen waren größtmögliche Zuverlässigkeit und Netzabdeckung und gute Kosteneffizienz.

Systemkomponenten

Als Lösung entschied man sich für an den Ladungen angebrachte sogenannte 'Smart-Tags', die über Funk eindeutige Kennungen senden, batteriebetrieben sind und erst nach mehreren Jahren ausgetauscht werden müssen. Diese Wegbegleiter enthalten flexibel nutzbare Sensoren,

die sich je nach Transportgut – z.B. verderbliche Ware, sensible Technik, robuste Maschinenteile – unterschiedlich konfigurieren und de-/aktivieren lassen. Sie messen und sammeln Umgebungsdaten wie beispielsweise Temperatur, Luftdruck, Feuchtigkeit, Erschütterungen oder die aktuelle Position. Die Kommunikation basiert auf BLE-Funktechnologie. Sie eignet sich für kurze Entfernungen (10 bis 30m) und punktet mit niedrigem Stromverbrauch und Kosten. Um diese Daten auszulesen und an einen zentralen Server bzw. direkt in ein übergeordnetes ERP-System zu übertragen, braucht es ein Gegenstück – den sogenannten 'Tag-Finder'. Dies ist ein robuster NB800 Industrial Router, der als IoT-Gateway agiert. Er wird an Schlüsselstellen auf dem Schiff, LKW und im Lager installiert, wo der Warentransport vorbeifährt. Mit IP40 oder wahlweise IP65-Gehäuse eignet sich das kleine Gerät (95x75x35mm) sowohl für den Innen- als auch Außenbereich und hält auch mechanischen und thermischen Belastungen stand. Ebenso wie die Smart-Tags basiert der Tagfinder auf BLE, verbraucht also in der Standardversion weniger als 5W Strom unter Volllast. Kommt die mit dem Smart Tag gekennzeichnete Ware in einen Umkreis von 10 bis 30m vorbei, liest er die gesammelten Daten automatisch über BLE aus und überträgt sie über



Jederzeit über den Stand der Ladung informiert sein – die Tag-Finder-Lösung macht es möglich.

WLAN oder via Ethernet über einen VPN-Tunnel an einen zentralen Server oder direkt in ein ERP-System. Wenn das IoT-Gateway bzw. der Tag-Finder an einem entfernten Ort stationiert ist, erfolgt die Übertragung mittels 3G/4G-Mobilfunk. Das ermöglicht auch die Steuerung per Remote aus dem Rechenzentrum oder die ausfallsichere Ausführung von Firmware- und Konfigurationsupdates. Die Integration in ein Netzwerk-Managementsystem kann über die integrierte SNMP-Schnittstelle erfolgen.

Sicherheit

Immer im Zusammenhang mit entfernten Standorten liegt der Fokus auf Sicherheit. Zur sicheren Verbindung der remotevernetzten Tag-Finder bietet die Router-Software viele VPN-Funktionen, zu den verfügbaren Protokollen zählen u.a. OpenVPN und IPsec. Zusätzlich zur verschlüsselten Datenübertragung über VPNs (Virtuelle Private Kanäle) sichern Firewalls den Zugang zu den Endgeräten und dem Server. Für zusätzlichen Schutz vor oft genutzten Angriffsmethoden nutzt die Software des Tag-Finders keine Standardpasswörter oder -zugangsdaten, sondern beim ersten Start-up des Geräts muss das Administrationspasswort individuell eingegeben werden, womit das Root-Passwort automatisch festgelegt ist. Erst danach hat der integrierte Web-Manager die

Möglichkeit, weitere User mit entsprechenden Berechtigungen zu erstellen. Außerdem enthält die Software keine festcodierten Schlüssel oder Zertifikate. Beim Konfigurieren des Tag-Finders muss der Anwender diese zur Sicherstellung von Diensten (z.B. HTTP- und SSH-Server) oder zur Implementierung von Authentifizierung und Verschlüsselung (z.B. für VPN-Tunnel und WLAN-Clients) explizit erstellen. Sollte der Kunde zu einem anderen Zeitpunkt eine noch stärkere kryptografische Absicherung in Betracht ziehen, kann er die Schlüssel mithilfe eines externen RNG (Random Number Generator)-Geräts erstellen oder alle Zertifikate insgesamt auf einem Remote-Zertifizierungsserver verwalten.

Die Tag-Finder-Lösung mit der automatischen Kommunikation via BLE bietet gleich mehrere Vorteile: drahtlose Technologie, niedriger Stromverbrauch, keine teuren Lesegeräte, mobile App, Remote Management, Nachweis jeder Bewegung des Transports von Ausgangs- bis Endpunkt, Überwachung von Umgebungsfaktoren. So könnte etwa ein Container eine unsanfte Landung erlebt haben, wodurch es zu einem Haarriss in einem der Motorenblöcke kam. Eine kleine Ursache mit großer Wirkung, die durch das Asset Tracking rückverfolgbar ist. Damit lässt sich dann auch gleich die Frage der Verantwortung klären.

www.netmodule.de ■

Save the date: Sigfox Connect 2018

Nach der Sigfox World IoT Expo 2017 in Prag mit mehr als 1.200 Besuchern wird die Sigfox Connect 2018 in Berlin zum nächsten Treffpunkt für alle, die sich für das IoT-Business interessieren. Teilnehmer erhalten die Möglichkeit, verschiedene Keynotes und Vorträge zu besuchen, um die technologischen Neuerungen und interessante Anwendungsfälle zu entdecken. Die Veranstaltung richtet sich an Anwender sowie an Gerätehersteller, Modulhersteller, Distributoren, Start-ups, Universitäten und Operatoren sowie alle, die sich für das IoT-Business rund um das Thema LPWAN interessieren.



Bild: Sigfox Germany GmbH

Neue Mitglieder im VDE-Präsidium

Professor Dr. Hans Schotten ist zum neuen Vorsitzenden der Informationstechnischen Gesellschaft (VDE|ITG) und damit zum Mitglied des Präsidiums des Technologieverbandes VDE gewählt worden. Ebenfalls ins Präsidium gewählt wurde Ralf Christian, CEO Division Energy Management bei der Siemens AG in Erlangen.



Bild: VDE Verband der Elektrotechnik

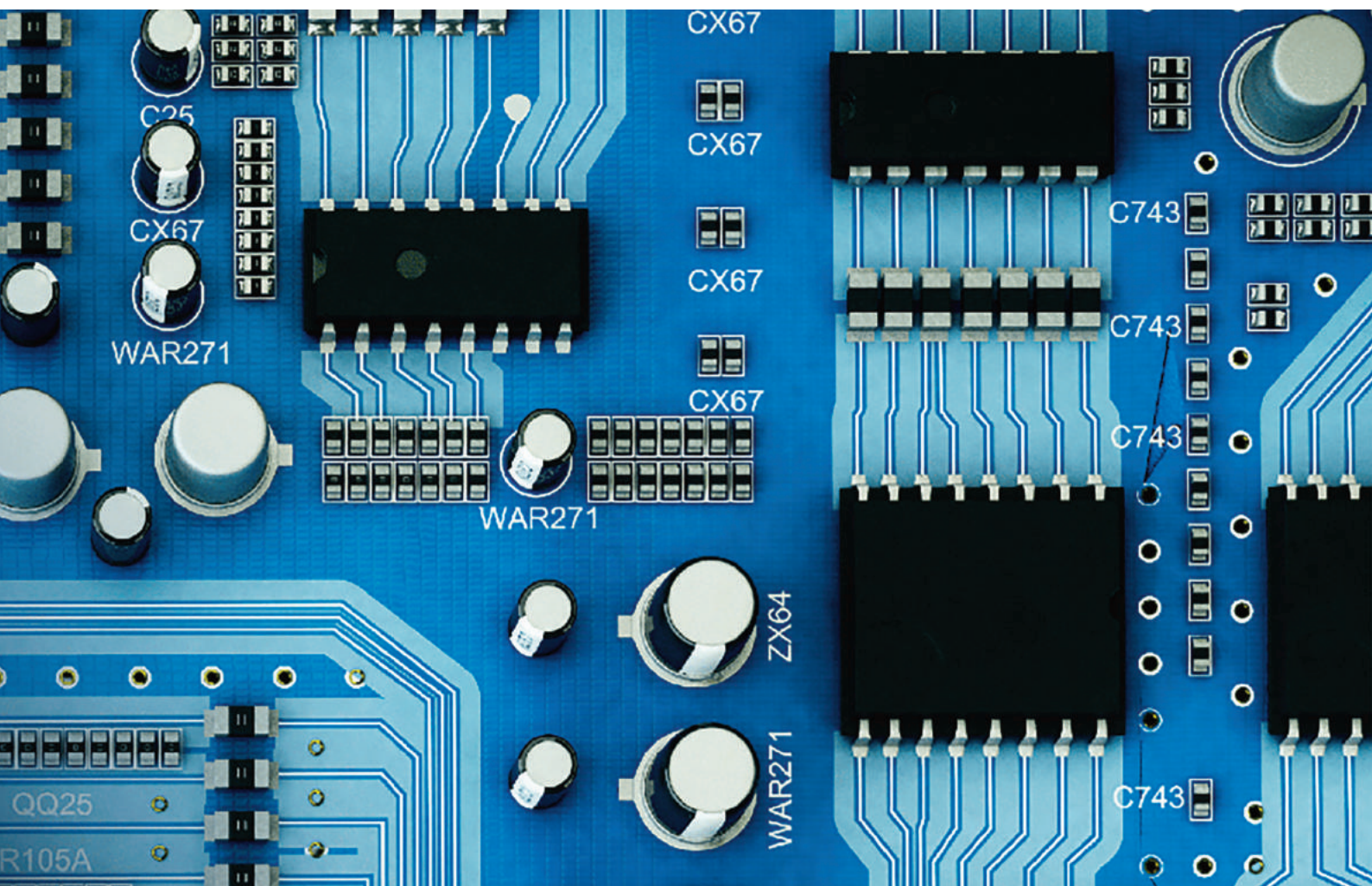


Bild: Barr Group

Wer, wie, was?

War das Thema **Blockchain** zunächst im Finanzsektor angesiedelt, ist es heute auch über die Industriegrenzen hinweg angekommen. Im Gespräch mit Michael Barr, Mitbegründer und CTO der Barr Group, erfahren Sie unter anderem, wie **Blockchains und Embedded-Systeme zusammenhängen** und was das Ganze mit dem **IoT** zu tun hat.

Im Gespräch mit MICHAEL BARR, CTO, Barr Group



Bild: Barr Group

IoT: Herr Barr, was genau ist eine Blockchain?

Michael Barr: Eine Blockchain ist im Prinzip eine Art Datenbank. Embedded-Programmierer arbeiten oft mit Datenbanken und man kann sich eine Blockchain als eine Datenbank der nächsten Generation mit einigen besonderen Eigenschaften vorstellen.

IoT: Und wie setzt man diese Datenbanken ein, wo es sich doch um eine spezielle Datenbank handelt?

Barr: Was eine Blockchain gegenüber anderen Arten von Datenbanken

auszeichnet, ist die Tatsache, dass es sich um eine verteilte Datenbank mit mehreren Kopien aller Einträge handelt. So etwas setzt man in der Regel in einer Umgebung mit mehreren verschiedenen Vertrauensbeziehungen ein – komplizierten Vertrauensbeziehungen, in denen man eine objektive Aufzeichnung von Geschehnissen benötigt. Ein Beispiel wäre eine Reihe von Transaktionen, bei denen ein Teilnehmer einem anderen nicht vertraut. Deshalb findet die Blockchain-Technik auch bei Kryptowährungen wie Bitcoin oder Ethereum Anwendung. Es gibt also bestimmte Sonderfälle, für die diese Art Datenbank geeignet ist.

IoT: Sie erwähnten gerade Bitcoin und Ethereum. Bitcoins haben natürlich eher mit finanziellen Dingen zu tun. Gibt es aber im Bereich des Internet of Things oder der Embedded-Systeme Beispiel dafür, wie sich die Blockchain-Technik sinnvoll einsetzen ließe?

Barr: Selbstverständlich. Dafür muss man zunächst einmal eines an der Blockchain-Technik verstehen: Weil sich eine Blockchain potenziell als sehr umfangreiche Datenbank auf einer Menge verschiedener Computer repliziert und weil die Abstimmung einen enormen Rechenaufwand verursacht, wird die Blockchain selbst häufig in der Cloud implementiert.

IoT: In der Cloud, ich verstehe.

Barr: Das Internet of Things und andere Embedded-Systeme generieren aber häufig Daten, die zum Bestandteil dieser Einträge werden, oder sie interagieren mit Daten in der Blockchain.

IoT: Können Sie ein konkretes Beispiel nennen?

Barr: Natürlich. Denken wir an eine Applikation, die die Historie eines bestimmten Autos verfolgt. Man könnte hier mit Informationen über den Bau dieses Autos beginnen. Zum Beispiel könnte der Motor in Japan gefertigt und in Mexiko in das

Auto eingebaut werden. Als nächstes würde eine bestimmte Version der Firmware in die verschiedenen Prozessoren geladen. Später würde eine der Rechnerkarten ersetzt, bevor das Auto schließlich verkauft und gekauft wird. Man kann sich dies als eine Beziehung mit einem Dienst in der Art von Carfax mit entsprechenden Einträgen und Details vorstellen. Embedded-Systeme könnten während des ganzen Vorgangs einige der Informationen beisteuern und beispielsweise mit den gerade erwähnten Firmware-Updates zu tun haben. Ein Versicherungsunternehmen könnte nun daran interessiert sein zu wissen, ob das Auto jemals mehr als 160km/h gefahren ist. Hier könnte eine Art Trigger existieren, der diese Information zum Bestandteil der Blockchain-Historie dieses Autos macht.

IoT: Und weil diese Blockchain verteilt ist, ist sie theoretisch sicherer. Und die weit verstreuten Partner können den Informationen vom Entstehen des Autos bis zu seiner Verwendung leichter vertrauen?

Barr: Genau, vom nächsten Käufer des Fahrzeugs an. Man kann feststellen, ob die Instandhaltung korrekt durchgeführt wurde, wie vom Verkäufer behauptet, oder dass das Fahrzeug

niemals in eine Überschwemmung geraten ist. Genau, wie es mit Carfax derzeit geht. Ebenso lässt sich prüfen, ob die neuesten Firmware-Versionen aufgespielt wurden.

IoT: Welche Interaktionsmöglichkeiten gibt es noch?

Barr: Eine weitere Möglichkeit der Interaktion von Embedded-Systemen mit der Blockchain-Technik sind elektronische Währungen. Nehmen wir als Beispiel an, Sie entwickeln ein Embedded-System wie etwa eine Set-Top-Box für Apple TV oder ein Gerät, mit dem man verschiedene Streaming-Dienste verfolgen kann. Man kann sich vorstellen, dass ein solches Gerät ein Bitcoin-Wallet enthält, um Einkäufe zu tätigen, Micropayments auszuführen und dergleichen mehr. Vielleicht gibt es im Automobilbereich eine Applikation, die etwas Ähnliches tut, z.B. ein E-Z Pass im Auto, der mit Ihrer Kreditkarte verknüpft ist. Die Karte verfügt über einen bestimmten Kredit im Bitcoin-Wallet und wird zu einem Bestandteil des Bitcoin-Ledgers bzw. der Bitcoin-Transaktion.

IoT: Vielen Dank für das sehr interessante Gespräch.

www.barrgroup.com ■

Inserentenverzeichnis

Aaronn Electronic GmbH	30
Analog Devices GmbH	2
Comp-Mall GmbH	17
Fischer Elektronik GmbH & Co. KG	11
Harting Deutschland GmbH & Co. KG	Titel
Kontron Europe GmbH	30, 31, 52

Moxa Europe GmbH	5
Portwell Deutschland GmbH	21
Phytec Messtechnik GmbH	43
Schubert System Elektronik GmbH	23
WÜRTH Elektronik eiSos GmbH & Co. KG	31

Impressum

VERLAG/POSTANSCHRIFT

Technik-Dokumentations-Verlag
TeDo Verlag GmbH®
Postfach 2140, 35009 Marburg
Tel.: 06421/3086-0, Fax: -180
www.iot-design.de

LIEFERANSCHRIFT

TeDo Verlag GmbH
Zu den Sandbeeten 2
35043 Marburg

VERLEGER & HERAUSGEBER

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

REDAKTION

Kai Binder (Chefredakteur, kbn),
Georg Hildebrand (ghl),
Clara Luise Josuttis (clj)

WEITERE MITARBEITER

Inka Bach, Tamara Gerlach, Anja Giesen,
Frauke Itzerott, Pascal Jenke, Victoria Kraft,
Katharina Kuhl, Kristine Meier, Melanie Novak,
Sarah-Lena Schmitt, Kristina Sirjanow, Florian
Streitenberger, Natalie Weigel

ANZEIGEN

Markus Lehnert, Tel. +49 6421 3086-0
Es gilt die Preisliste der Mediadaten 2018

GRAFIK & SATZ

Anja Beyer, Tobias Götz, Fabienne Hessler,
Kathrin Hoß, Melissa Hoffmann, Ronja Kaledat,
Moritz Klös, Timo Lange, Ann-Christin Lölkes,
Nadin Rühl

DRUCK

Offset vierfarbig
Grafische Werkstatt von 1980 GmbH
Yorckstraße 48, 34123 Kassel

ERSCHEINUNGSWEISE

6 Hefte für das Jahr 2018

BANKVERBINDUNG

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

GESCHÄFTSZEITEN

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

ABONNEMENTSBEZUG

Inland: €36,00 inkl. MwSt. + Porto
Ausland: €42,00 inkl. Porto

EINZELBEZUG:

Einzelheft: €7,80 (inkl. MwSt.)

ISSN

1869-8832

Vertriebskennzeichen (ZKZ)

18427



HINWEISE:

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

Titelbilder: Harting Deutschland GmbH & Co. KG



Hafen Rotterdam im Internet of Things

Bild: IBM Deutschland GmbH

Die **Hafenverwaltung** von Rotterdam und **IBM** gaben kürzlich ihre Zusammenarbeit im Rahmen einer mehrjährigen Digitalisierungsinitiative bekannt, die auf die **Transformation der Betriebsumgebung des Hafens** mithilfe von IoT-Technologien in der **Cloud** abzielt. Profitieren sollen davon der Hafen und alle, die ihn nutzen. Mit der Initiative soll auch das gesamte 42km lange Hafengelände auf die künftige **Abfertigung vernetzter Schiffe** vorbereitet werden. Begonnen wird mit der Entwicklung einer zentralen **Dashboard-Anwendung**, die Wasser-, Wetter-, Sensor- und Kommunikationsdaten in Echtzeit erfasst und verarbeitet, die über die **IoT-Plattform von IBM** analysiert werden. Dies eröffnet dem Hafen zahlreiche Innovationsmöglichkeiten für eine **sicherere und effizientere Steuerung** des Schiffsverkehrs.

RENATE STUECKA, Product Marketing Manager Watson IoT DACH, IBM

„Wir haben in Rotterdam entsprechende Maßnahmen eingeleitet, um zum intelligentesten Hafen der Welt zu werden“, so Paul Smits, Chief Financial Officer vom Hafenbetrieb Rotterdam. „Schnelle und effiziente Abläufe sind für unser Geschäft unerlässlich und erfordern, dass wir alle uns zur Verfügung stehenden Daten nutzen. Dank Echtzeitinformationen über Infrastruktur, Wasser, Luft usw. können wir den Service für alle, die den Hafen nutzen, erheblich verbessern und uns auf die Umstellung auf einen vernetzten, autonomen Schiffsverkehr vorbereiten.“ Als größter Hafen Europas verzeichnet der Hafen Rotterdam, in dem jährlich 140.000 Schiffe abgefertigt werden, einen Güterumschlag von 461 Mio.t pro Jahr. Bislang verließ man sich im Hafen auf die herkömmliche Funk- und Radarkommunikation zwischen Kapitänen, Piloten, Terminalbetreibern und Schleppern, um den Hafenbetrieb zu koordinieren. Im Zuge der eingeleiteten digitalen Transformation des Hafens werden nun auf dem 42km langen Hafengelände, das sich von der Stadt Rotterdam bis zur Nordsee erstreckt, Sensoren entlang der Kai-mauern, Anlegestellen und Straßen des Hafens installiert. Diese Sensoren erfassen diverse Datenströme, einschließlich Wasser- und Wetterdaten über Gezeiten und Strömungen, Temperatur, Windgeschwindigkeit und

– richtung, Wasserstände, Liegeplatzverfügbarkeit und Sichtverhältnisse. Diese Daten werden von den cloudbasierten IoT-Technologien von IBM analysiert und in Informationen umgewandelt, die der Hafen Rotterdam als Entscheidungsgrundlage heranziehen kann, um Wartezeiten zu verkürzen, den optimalen Zeitpunkt für das Anlegen und Be- und Entladen von Schiffen zu bestimmen oder den verfügbaren Platz besser zu nutzen, um noch mehr Schiffe unterzubringen. Beispielsweise kann der Hafen Rotterdam dann anhand des Wasserstandes den optimalen Zeitpunkt für die Ein- oder Ausfahrt von Schiffen ermitteln, um so das maximale Frachtvolumen zu erreichen. Dank der neuen Initiative können die Hafenbetreiber außerdem sämtliche Vorgänge im Hafen gleichzeitig verfolgen und den Prozess auf diese Weise effizienter gestalten. Die Reedereien und der Hafen können die Liegezeiten damit um bis zu eine Stunde verkürzen und so bis zu 80.000US\$ einsparen. Das Projekt zur digitalen Transformation des Hafens wird durch die cloudbasierten IoT-Technologien von IBM ermöglicht und ist auf eine langfristige Zusammenarbeit zwischen dem Hafen Rotterdam und IBM ausgelegt, um weitere innovative Anwendungsbereiche für IoT und künstliche Intelligenz abzudecken. Cisco und Axians sind ebenfalls an diesem Projekt beteiligt.

www.ibm.de ■

NETWORK SCHALTSCHRANKBAU 2018

Neuste Entwicklungen zuerst erfahren und miteinander austauschen!

Essen

01.02.18

Zeche Zollverein
mit 130 Teilnehmern

Hamburg

28.06.18

Hotel Bötcherhof



Berlin

08.05.2018

Hotel Estrel



Frankfurt, Bad Nauheim

16.04.18

Hotel Dolce
Bad Nauheim



Stuttgart

18.09.18

Ingolstadt

25.10.2018

Parkhotel Heidehof



Relevante VDE/DKE-Normen

UL-Normung für den nordamerikanischen Markt

Digitalisierung im Schaltanlagenbau

Planungstools und Software

EMV- und Störlichtbogenschutz

Treffen Sie Kollegen aus Ihrer Branche und pflegen Sie Kontakte in angenehmer Atmosphäre. Freuen Sie sich auf spannende Fachvorträge zu aktuellen Themen rund um den Schaltanlagenbau.



Jetzt Anmelden

ssb-magazin.de/network08

ABB



**PHOENIX
CONTACT**

RITTAL

SIEMENS

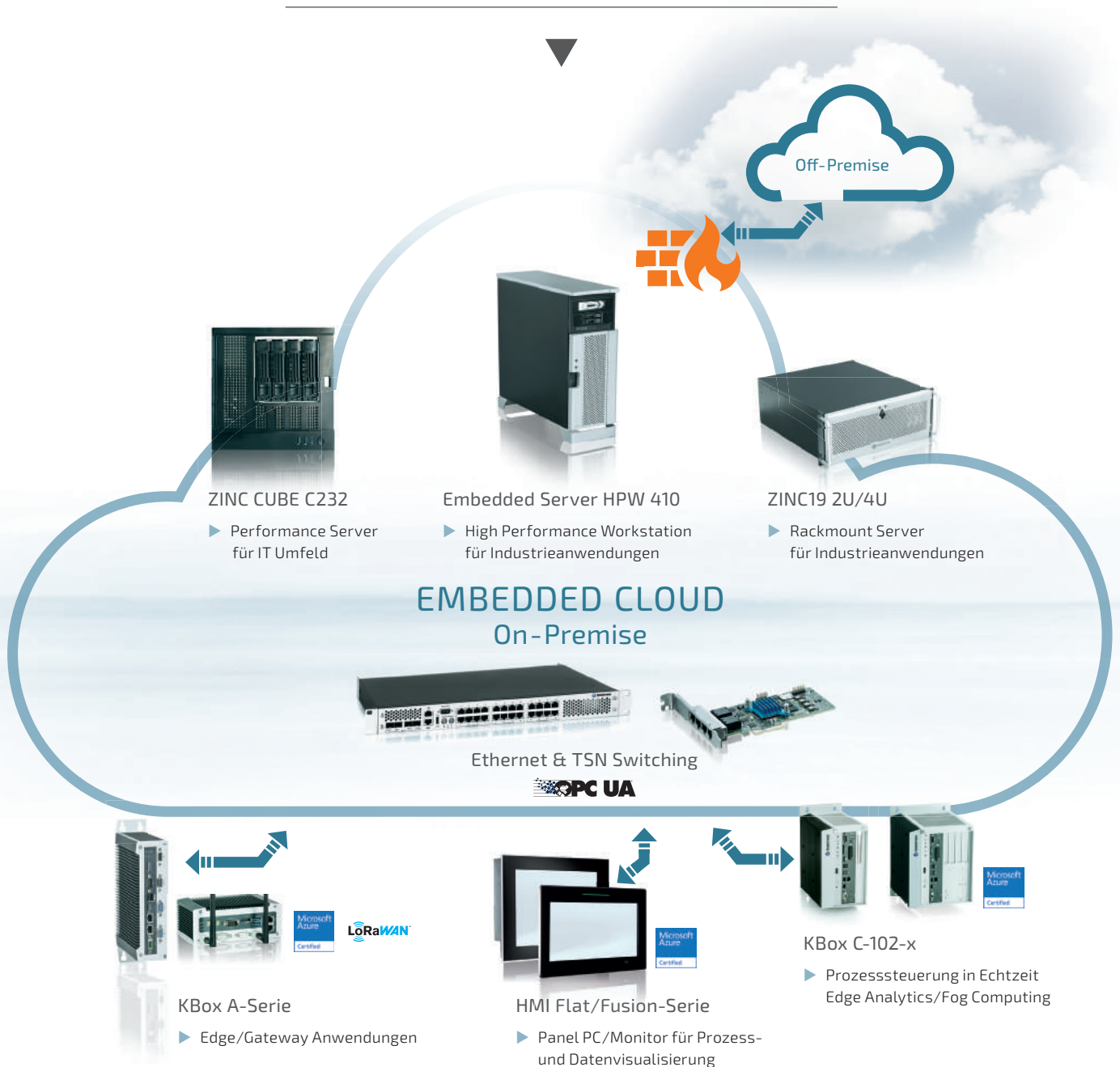
WAGO

Weidmüller

Unsere Industriepartner zeigen in der Ausstellung neuste Entwicklungen und beantworten Ihre Fragen.

INDUSTRIE 4.0 / IIOT EDGE TO FOG TO CLOUD

TSN & OPC UA ENABLED



- Embedded Cloud
- Embedded Software
- Embedded Systems
- Embedded Boards & Modules
- Embedded ODM Services