6/2018
www.iot-design.de
TeDo Verlag GmbH
Dezember
€ 7,80

+++ Wie sicher sind Permissioned Blockchains? S.16 +++

Datenmanagement:
Dank kurzer Reaktionszeiten stehen Daten an jedem Ort zu jeder Zeit zur Verfügung S.28

IoT DESIGN

Smarte Systeme für das Internet of Things

IOT SOFTWARE FRAMEWORK

SUSiEtec: vom Sensor bis in die Cloud

S.8

s&t

kontron
S&T Group

Multiple Clouds vs. Multi-Cloud

RICHTIG UNTERSCHEIDEN

S.16


Bild: © jamesstoehart/iStockphoto.com

Sicheres Netz S.30
Wie funktioniert Netzwerksicherheit mit 5G?

Security & Leistung
In der Cloud
S.34

» Himmlisches IoT

Das Internet of Things in der Luftfahrt S.36

HIER KOSTENLOS DOWNLOADEN!

JETZT BEI Google Play

Laden im App Store

Editorial

Die Aufgabe von Anwendungsentwicklern im Embedded Bereich ist eigentlich klar: Sie sollen eine umrissene Funktion für ein Gerät zur Verfügung stellen. Doch die Komplexität der Aufgabe hat in den vergangenen Jahren immer weiter zugenommen und ein Ende dieser Entwicklung ist nicht in Sicht. Da stellt sich die Frage: Make or Buy? Stellt man also alle notwendigen Systembestandteile immer noch selbst zusammen oder setzt man auf ein 'Rund-um-Sorglos'-Paket. Und: Gibt es das überhaupt?

Klar ist: Für das Geschäftsmodell müssen die Lebenszykluskosten betrachtet werden, auch wenn das nicht immer ganz einfach ist. Das fängt schon bei Wahl der Hardware an. Die Lebenszyklen bestimmter Prozessoren werden immer kürzer und die Abkündigungspraktiken diesbezüglich rigoroser. Ein Neudesign nach Abkündigung soll dann möglichst kostensensibel möglich sein. Dazu gehört also nicht nur das Board mit seiner CPU, sondern auch die dafür benötigten Erweiterungen und natürlich die entsprechenden Treiber.

Auch die Bedienoberfläche unterliegt immer kürzeren Zyklen, die beim Produktdesign – je nach Aufgabenstellung – berücksichtigt werden müssen. So fordern immer mehr Anwendungen die Einbindung von Touch oder gar Multitouch-Displays, was die bisherige Bedienphilosophie in der Regel völlig über den Haufen wirft.

Bei der Kommunikation mit der Außenwelt, und damit ist nicht nur die lokale Kommunikation gemeint, sondern auch das Internet der Dinge, wechseln die Anforderungen ständig, weil die Anzahl der Möglichkeiten immer weiter steigt. Mit LoRaWAN, Sigfox, NB-IoT und demnächst TSN und 5G kommen immer mehr Technologien hinzu, die ihre jeweiligen Besonderheiten haben und mit denen Entwickler sich beschäftigen müssen.

Und mit der Kommunikation in die Außenwelt werden auch die Security-Funktionalitäten zu einer immer weiter wachsenden Aufgabe in der Entwicklung. Und weil wir wissen, dass Sicherheit kein Zustand ist, sondern ein Prozess, bedeutet dies, dass es in Bezug auf die Anwendungsentwicklung eine Daueraufgabe ist.

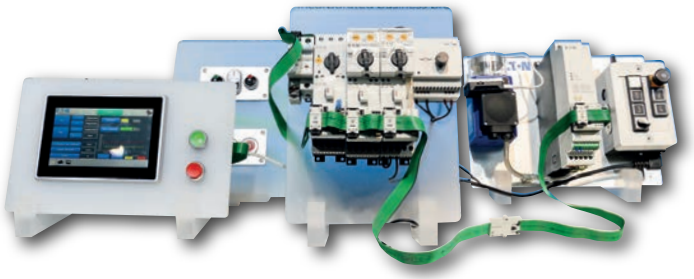
Es wird also nicht langweilig in der Embedded Welt und schon gar nicht einfacher. Mit jeder Ausgabe der IoT Design wollen wir genau diese Welt immer ein bisschen transparenter machen.

In diesem Sinne wünsche ich Ihnen viel Spaß beim Lesen.

Ihr

Kai Binder, Chefredakteur IoT Design
kbinder@iot-design.de

Inhalt 6/18



40

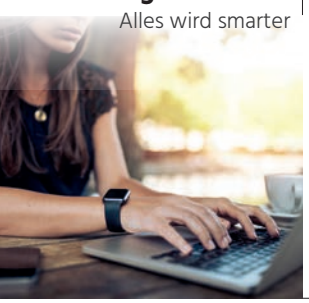
Mittelstand: Welche IoT-Lösungen werden genutzt?

Internet der Dinge 2019: Im Vergleich zum letzten Jahr hat sich die Zahl der IoT-Projekte mehr als verdoppelt.

NEWS Seite 40

42

Vielseitiger dank IoT
Alles wird smarter



SERVICE

NEUHEITEN

FACHWISSEN

8

TITELSTORY: SUSIEtec
Ein IoT Software Framework vom Sensor bis in die Cloud

14

DER WEG ZUR SMART FACTORY
Diese vier Missverständnisse halten Unternehmen von der Entwicklung ab...

44

KI FÜR DIE PRODUKTION NUTZBAR MACHEN
WGP möchte mit einem Standpunktpapier den Einstieg in KI erleichtern...

12

DER WEG ZUR ROBUSTEN EMBEDDED-PLATTFORM
Diese drei Möglichkeiten bieten sich Unternehmen ...

26

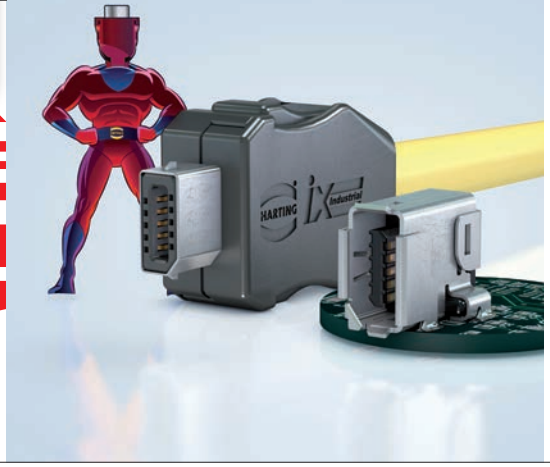
DER HERSTELLER ALS DIENSTLEISTER
Der Weg von Produktionsunternehmen zu Service-Anbietern...

22

AUTOMATISIERUNGSCHIP FÜR DAS IOT
Das bringen Hilschers neue netX 90-Chips...

21

CONNECTIVITY-LÖSUNGEN FÜR DAS IIOT
So bleibt die Infrastruktur für kommende Anwendungen kompatibel...



IoT NEWS

Chip on Computer/Module
Alle Highlight-Produkte auf einen Blick

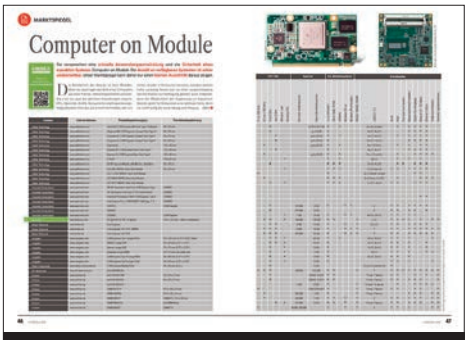


Bild: ©tam/Fotolia.com, Microchip Technology Inc.

KLEIN, ABER OHO

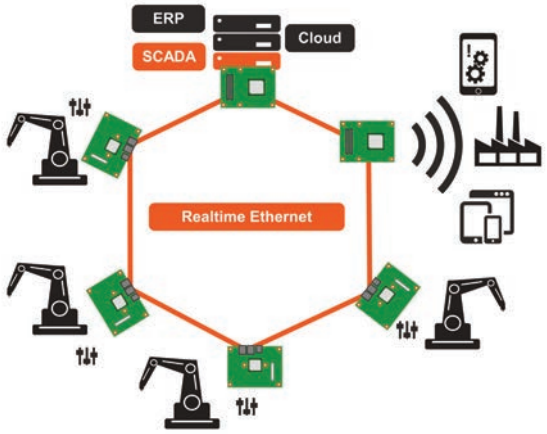
Microchip stellt seine hochintegrierte LoRa-System-in-Package-(SIP)-Serie (SAM-R34/35-SIP) in einem 6x6mm Gehäuse mit einem stromsparenden 32-Bit-Mikrocontroller, Sub-GHz HF-LoRa-Transceiver und einem Software-Stack vor. Zusammen mit dem Entwicklungsboard ATSAMR34-XPRO (DM320111) und dem Softwareentwicklungskit Atmel Studio 7 lassen sich damit Prototypen schnell erstellen. Die SIPs eignen sich vor allem für stromsparende IoT-Anwendungen mit geringer Baugröße.

MICROCHIP TECHNOLOGY INC. · WWW.MICROCHIP.COM

Heiter bis wolkig

IIoT-Cloudlösung verbindet IT und Feldebene. Mit kompakten Lösungen für das Internet der Dinge verbindet ICPDAS die Feldebene mit der IT-Ebene. Dazu bietet der IIoT Communication Server UA-5231 viele Technologien in einem Gerät. Neben den Datenerfassungs- und Steuerungsfunktionen, verfügt er über einen integrierten OPC-UA-Server und MQTT-Broker. Dank nativem Datenbank-Client können Daten ohne Umwege in Datenbanken geschrieben werden. Mit wenigen Klicks lassen sich Verbindungen mit MES, ERP, Scada und Clouddiensten herstellen. Sämtliche Einstellungen erfolgen über die Weboberfläche mit Funktionsassistent.

ICPDAS Europe GmbH, www.icpdas-europe.com



Industrie-4.0-Fabrikvernetzung in **Echtzeit**

Congatec präsentierte zur Electronica World die Leistungsfähigkeit der harten Echtzeitkommunikation über GBit Ethernet. Die Demo-Installation zeigte erfolgreich, wie Echtzeitdaten zeitsynchron übertragen werden können.

Congatec AG, www.congatec.com

»Gateways

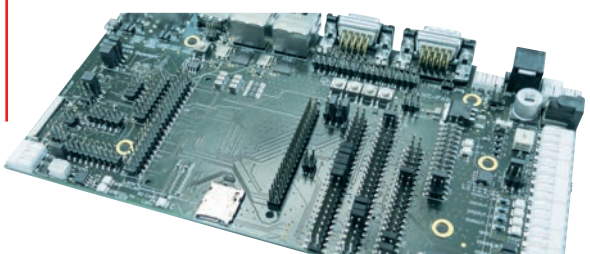
DIE GATEWAY-FAMILIEN ANYBUS COMMUNICATOR IIOT UND ANYBUS X-GATEWAY IIOT VON HMS ERMÖGLICHEN DANK MQTT UND OPC UA DEN EINFACHEN EINSTIEG INS IIOT UND DECKEN IN RICHTUNG FERTIGUNGSEBENE ALLE GÄNGIGEN INDUSTRIELLEN KOMMUNIKATIONSSTANDARDS AB. DER VORTEIL IST, DASS VON NAHEZU ALLEN GERÄTEN DATEN EINFACH UND SICHER IN IT-SYSTEME UND IOT-SOFTWARE ÜBERTRAGEN WERDEN KÖNNEN.

HMS Industrial Networks GmbH, www.hms-networks.de

SBC Development Board basierend auf Raspberry Pi

Kontron bietet ein Development Kit für die Entwicklung von Produkten **basierend auf Raspberry Pi für die Industrie an.** Das Kit umfasst ein Entwickler-Board nach SBC-Spezifikationen, ein Raspberry-Pi-Computermodul 3 Light sowie eine SD-Card mit Raspian Betriebssystem.

Kontron S&T AG, www.kontron.de



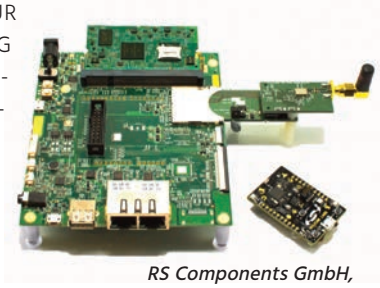
Embedded Server

Kontron stellt den neuen Embedded Server Zinc Cube SKD vor. Der Embedded Server basiert auf Intel Xeon D-2100 Prozessoren (12C 75W/8C 65W/4C 60W) mit vier bis zwölf CPU-Kernen, seine acht DIMM-Sockel unterstützen bis zu 256GB ECC Speicher.

Kontron S&T AG, www.kontron.de

Cloud inklusive

DAS URSALEO UL-NXP1S2R2-KIT VON RS COMPONENTS ENTHÄLT EIN SILICON LABS THUNDERBOARD 2-SENSOR-MODUL, DAS FÜR DIE VERBINDUNG MIT DER PLATTFORM VON URSALEO IN DER GOOGLE CLOUD VORBEREITET IST. SO LÄSST SICH WESENTLICH SCHNELLER ENTWICKELN.



RS Components GmbH, www.rs-components.de

Schnelles und präzises Tracking

Sigfox stellte auf der Sigfox Connect die vernetzte Bubble vor, mit der man weltweit Assets lokalisieren kann. Bubbles sind kleine, innerhalb weniger Sekunden überall installierbare Transmitter zum Tracking von Sigfox-Devices, deren Sendeleistung die Lokalisierungsreichweite definiert. **Sobald ein Gerät in den Sendebereich eintritt, kann es die ID zusammen mit seiner eigenen Identifikation an die Cloud übertragen.** Assets lassen sich so mit hoher Präzision lokalisieren. Die Lokalisierungsgenauigkeit kann über die Cloud von unter einem Meter bis zu hundert Meter angepasst werden.

Sigfox Germany GmbH, www.sigfox.com

Mit der Cloud alles im Blick

Die neue Version der Wago Cloud geht voraussichtlich im ersten Quartal 2019 an den Start. Neben Funktionen wie Controllerstatusverwaltung und Dashboards wird die neue Version eine moderne, übersichtliche Appstruktur sowie weitere Funktionen wie einen leichten Fernzugang bieten. Als Benutzeroberfläche des Clouddienstes wird ein Webportal dienen.

Wago Kontakttechnik GmbH & Co. KG, www.wago.com

Mehr GigE-Ports für Xeon-CPU-Karten

Ab sofort sind alle auf Intel Xeon basierenden CompactPCI-Serial-CPU-Karten von EKF mit zusätzlichen vier M12-X-GigE-Frontbuchsen erhältlich. Untergebracht auf der SCL-Rhythm Side Card, werden diese vier Ports über jeweils einen eigenen I210-IT 1000Base-T Controller versorgt.

EKF Elektronik GmbH, www.ekf.de

SUSiEtec:
Ein IoT Software Framework vom Sensor bis in die Cloud

Bild: © alphaspirit / Fotolia.com

Die zunehmende **Vernetzung industrieller Computersysteme** stellt Systemintegratoren vor **neue Aufgaben und Herausforderungen**. Bei SUSiEtec von der S&T Technologies handelt es sich um ein **IoT Software Framework**, das **als 'Klebstoff' die sichere Verbindung** der Geräte untereinander und mit der Cloud herstellt. **SUSiEtec fügt die IoT-Infrastruktur** – vom Sensor bzw. Aktor über den **Edge Computer** und die **Embedded Cloud** bis zur Private oder Public Cloud – **wie Puzzleteile zusammen** und verbindet diese **zu einem Gesamtpaket**.

TEXT: Bernhard Günthner, Geschäftsführer bei S&T Technologies **BILDER:** Kontron S&T AG

Verbindung zwischen Hardware, IT und Fabrik

Die S&T war bis zur Übernahme von Kontron im Jahr 2017 ein klassisches Systemhaus mit Fokus auf IT-Dienstleistungen. Da Cloud Computing und Connected Devices in der IT schon länger etabliert sind, konnte die S&T in diesem Bereich bereits jahrelang Erfahrungen sammeln. Diesen Erfahrungsschatz im Bereich Software und Vernetzung vereint nun die S&T Technologies als Entwickler und Anbieter des IoT Software Frameworks SUSiEtec. Als weitere Tochter der S&T Gruppe profitiert nun auch Kontron als Anbieter industrieller Embedded/IoT Module, Boards und Systeme, einschließlich der zukunftsweisenden offenen Standards TSN und OPC UA für die deterministische und sichere Kommunikation von der Cloud über Edge bis zur Feldebene hiervon. Die Zusammenarbeit der beiden Konzernschwestern schafft die Verbindung zwischen der etablierten Embedded Computer Technologie und der Unternehmens-IT, einschließlich Cloud. Die Fähigkeit, OT (Operational Technology) und IT (Information Technology) im Zeitalter von Industrie 4.0 aus einer Hand anbieten zu können, ist enorm selten, sehr gefragt – und wird mit SUSiEtec adressiert. Die Vorteile

von Public Clouds wie Microsoft Azure oder Amazon Web Services liegen auf der Hand: Unternehmen müssen sich, wenn sie sich für diese Cloudanbieter entscheiden, nicht selbst um den Aufbau und Betrieb der Infrastruktur kümmern. Damit entfallen rund 50 Prozent des Aufwands. Aber die großen Cloud Provider sind nicht darauf eingestellt, für ihre Kunden individuelle Anpassungen vorzunehmen. Sie bieten nur ein Basisprodukt; ein indvidueller Zuschnitt auf die Kundenwünsche und -bedürfnisse ist nicht vorgesehen. Hier kommen Kontron und die S&T Technologies mit SUSiEtec ins Spiel. Was bei Betriebssystemen das Board Support Package ist, ist bei der Cloud die Netz-Adaption, die Kontron bzw. S&T Technologies mit SUSiEtec übernehmen. Hierbei kann der Kunde auf das modular aufgebaute Software Framework zugreifen und dabei nur diese Elemente einsetzen, die für seine individuelle Lösung benötigt werden. Die Nutzung einer Public Cloud erfordert eine realistische, differenzierte Betrachtung, und ihre Eignung hängt sehr von der Anwendung ab. Das gilt insbesondere für Branchen, in denen Bruchteile von Sekunden bei der Maschinensteuerung ausschlaggebend sind oder Echtzeitauswertungen von Daten für schnelle Entscheidungsprozesse, die z.B. im Rahmen von Machine Learning an der Maschine gefragt sind. Die etablierten Clouds weisen mittlerweile ein sehr großes Leistungsspektrum auf. Limitierungen in puncto Bandbreite und Latenzzeiten bleiben jedoch noch auf absehbare Zeit bestehen. Das Konzept der 'Digital Twins' in der Cloud für Maschinen ist sicher zukunftsweisend, aber derzeit für die meisten Branchen noch keine echte Alternative zur Maschinensteuerung vor Ort. Zudem fühlen sich viele Unternehmen, nicht nur in Deutschland, nach wie vor sicherer, wenn sie ihre Daten traditionell auch physisch im Haus behalten. Anstatt alles in die Cloud auszulagern, gilt bei vielen Unternehmen das Motto: Nur Daten, die nicht sicherheitsrelevant und zeitkritisch sind kommen in die Cloud.

Schnell, sicher und flexibel: 'From Edge to Fog to Cloud'

Mit SUSiEtec wird der 'From-Edge-to-Fog-to-Cloud'-Ansatz unterstützt. Das heißt, Unternehmen werten ihre Daten genau dort aus, wo es nötig ist. Weitergehende Auswertungen oder historische Daten werden – sofern keine Sicherheitsbedenken dagegen sprechen – in die Cloud verlagert. Am Rande des Netzwerks, der sogenannten Edge, werden Daten erfasst und durch intelligente IoT-Devices und Edge Analytics für die Maschinensteuerung ausgewertet und gefiltert. Nur für die weitere Auswertung werden wichtige Daten in die Embedded Cloud, also die produktionsnahe firmeninterne private Cloud, weitergeleitet. Sofern dann noch notwendig, können gefilterte und weniger zeitkritische Daten in eine Public Cloud ausgelagert werden. Kontron hat Microsoft Azure als bevorzugte Plattform für IIoT-Lösungen gewählt. SUSiEtec hebt damit die herkömmlichen Grenzen zwischen Datenerfassung, -verarbeitung und -bereitstellung auf, wodurch die Integration von IT und OT möglich wird. SUSiEtec ist komplett in den Gateway-, Fog-Computing- und Server-Plattformen von Kontron integriert, von denen die meisten bereits heute 'Azure Certified for IoT' sind.

Mit Microsoft Azure IoT Edge und SUSiEtec wird Kunden die nahtlose Skalierbarkeit der Rechenleistung zwischen Computing-Ressourcen am Device, in der Embedded Cloud, im On-Premise-Rechenzentrum oder in der Public Cloud ermöglicht. Hierdurch können sie beispielsweise dynamisch entscheiden, wo die Datenanalyse erfolgen soll; je nachem, welches Sicherheits- oder Leistungniveau erwünscht ist. Für die Anpassung der Applikations-Landschaft an den 'From-Edge-to-Fog-to-Cloud'-Ansatz beim Kunden nutzen Kontron und S&T Technologies die Container-Technik. Bei dieser Technik, z.B. mit Docker als Technologiebasis, wird die Anwendung mitsamt ihrer Abhängigkeiten isoliert und kann dann wie eine Datei von System zu System verschoben werden und unabhängig von der Hardware laufen. SUSiEtec übernimmt dabei auch die 'Containerisierung' bestehender Anwendungen.

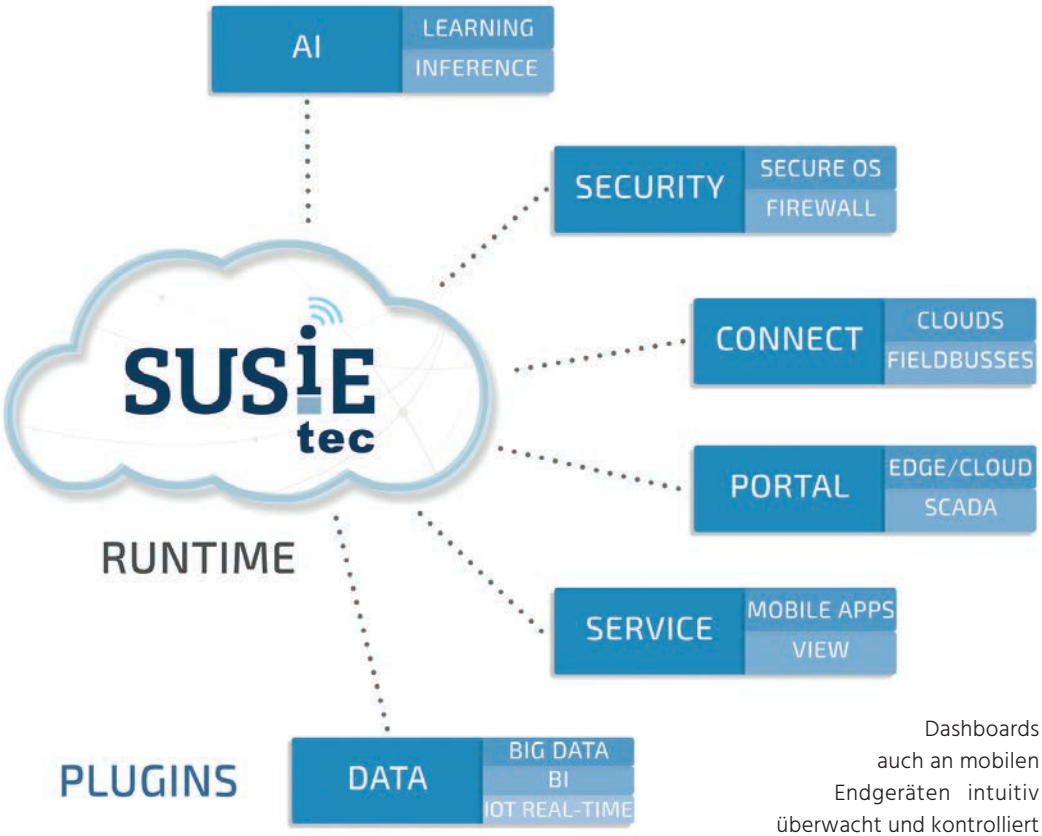
Auf der diesjährigen SPS IPC Drives gaben Bernhard Günthner (Geschäftsführer S&T Technologies) und Russel Agrusa (CEO Iconics) die Partnerschaft der Unternehmen bekannt. Bestens bewährte Scada-Funktionen werden nun in Verbindung mit SUSiEtec cloudfähig gemacht.

Brownfield-Integration als Einstieg ins IIoT

In den meisten Anwendungsfällen gilt es eine bereits im Feld installierte Infrastruktur mit einer zentralen Stelle zu vernetzen. Dies ist auf

Vorteile von SUSiEtec im Einsatz:

- Hard- und Software-integration aus einer Hand
- Breites, ständig erweitertes und gewartetes Funktions-spektrum
- Zugeschnittene Lösung basierend auf erprobten Modulen
- Einfacher und kontrollierter Einstieg
- Schnelle Erfolge bei der Umsetzung
- Flexible Anpassungs- und Erweiterungsmöglichkeiten



Dashboards auch an mobilen Endgeräten intuitiv überwacht und kontrolliert werden. Zudem lassen sich umfangreiche Analyseapplikationen nutzen, um digitalisierte Werte für verschiedene Bereiche wie Qualität, Service und Energie anzuzeigen.

den ersten Blick eine triviale Aufgabenstellung, birgt jedoch im Detail einige Herausforderungen. Hier müssen beispielsweise verschiedene im Feld befindliche Produktvarianten unter Berücksichtigung nicht veränderbarer Bedingungen und Betriebsszenarien sicher ins IIoT gebracht werden. SUSiEtec stellt in derartigen Szenarien in Verbindung mit den Kontron Gateways eine kostengünstige und skalierbare Lösung dar, um diese Anbindung zu realisieren.

SUSiEtec bringt Scada-Funktionen auf mobile Devices

Um Kunden mit SUSiEtec noch umfangreichere Funktionen aus einer Hand anbieten zu können, hat S&T Technologies im November 2018 eine Partnerschaft mit Iconics geschlossen. Damit werden die Industrie-4.0-Kunden einen Schritt weiter in die Cloud gebracht. Bekannte und bestens bewährte Scada-Funktionen werden nun in Verbindung mit SUSiEtec cloudfähig gemacht. Vor allem im Automatisierungsumfeld lassen sich damit komplexe Prozesse in der Cloud visualisieren. Der sichere Zugriff auf Maschinendaten kann damit praktisch über jedes Endgerät erfolgen. Kunden profitieren so von der über 30-jährigen Erfahrung des Partners bei der Visualisierung komplexer Prozesse in Verbindung mit dem IoT Software Framework für IIoT-Anwendungen. Damit können Anlagen über

Das IIoT Starterkit zur einfachen Implementierung

Da sich die Anforderungen an die Vernetzung bei jedem Kunden und von Projekt zu Projekt unterscheiden, ist SUSiEtec kein standardisiertes Produkt, sondern eine Mischung aus Beratung, Entwicklungs-Dienstleistung und Software. Die Herausforderung bei vielen Industrie 4.0- und Cloudprojekten liegt darin, dass die Kunden am Anfang oft selbst noch nicht wissen, wo die Reise einmal hingeht, welche Möglichkeiten eine Cloud bereitstellt und wo welche Daten liegen sollen. Oft tauchen Detailfragen auch erst im Laufe eines Projekts auf und führen dann zu zusätzlichem Aufwand. Auch dies ist ein Punkt, wo die Erfahrung eines Softwareanbieters wie S&T Technologies hilft, den Aufwand realistisch abzuschätzen. Mit einem Startkerkit erleichtert die S&T Technologies Unternehmen den Einstieg in das Edge, Fog und Cloud Computing für den Einsatz in ihrer Fertigung und/oder in ihren Produkten. Das Starterkit umfasst vier Bausteine: Die Erarbeitung eines individuellen Fragenpakets, Analyse und Bestandsaufnahme vor Ort, die Erarbeitung eines konkreten Konzepts sowie die Präsentation von Architekturkonzept, Aufwandsabschätzung und den Zeitplan für eine Realisierung. ■

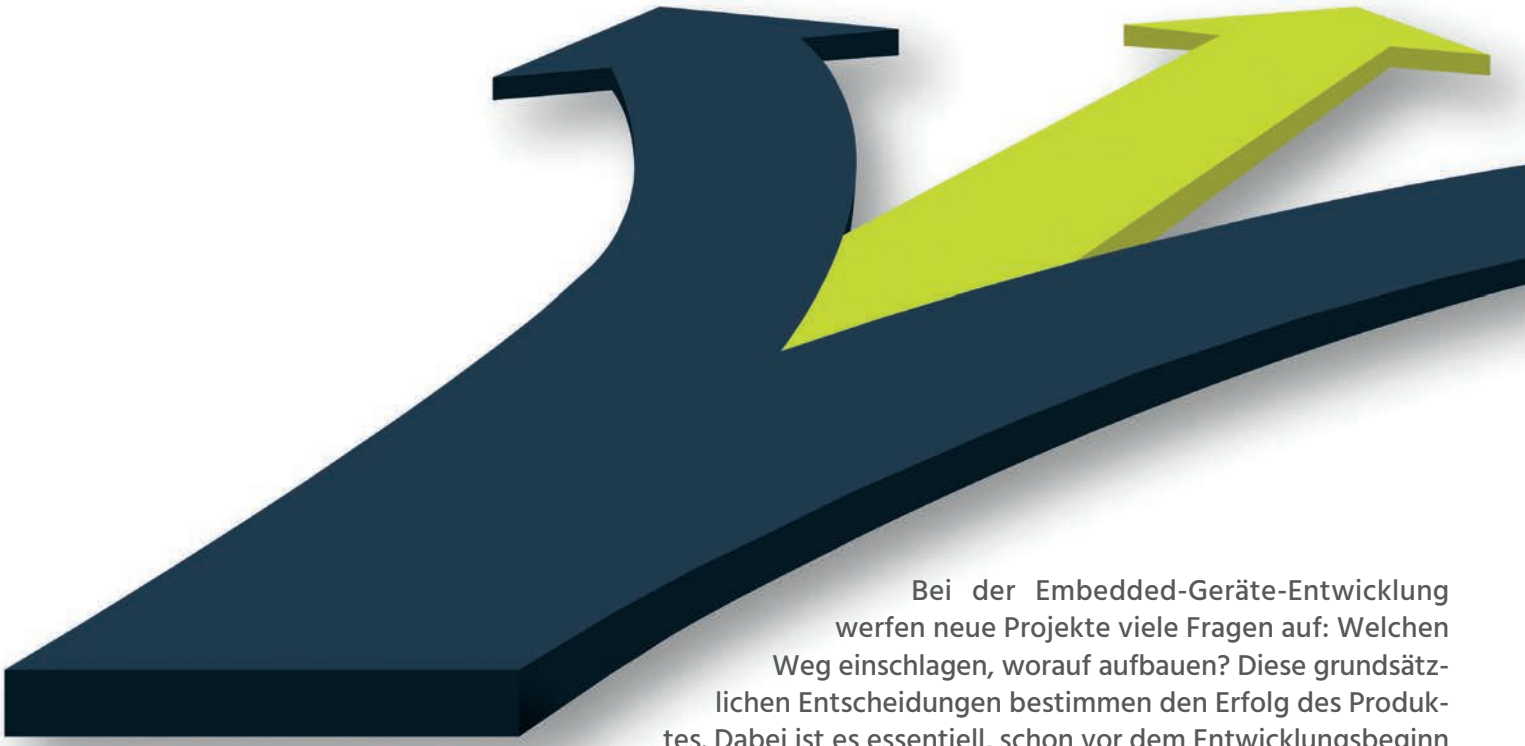
www.kontron.de

Hochfrequenz-RFID-Systeme an Cloud anbinden

Siemens erweitert das Portfolio der Simatic-Ident-Kommunikationsmodule. Die ersten Geräte der neuen Reihe sind Simatic RF185C, RF186C und RF188C. An die am Ethernet/Profinet betriebenen Modelle lassen sich wahlweise ein, zwei oder vier Reader anschließen. So kann immer die benötigte Anzahl von Anschlüssen projektiert werden. **Der Datendurchsatz lässt sich durch die neuen Geräte – abhängig von der Applikation – um bis zu 20 Prozent steigern. Das webbasierte Management und das Engineering im TIA-Portal ermöglicht jederzeit den gesicherten Zugriff auf Konfigurations-, Inbetriebnahme- und Diagnosetools.** Anwender profitieren so von einer flexiblen Visualisierung und reduziertem Projektierungsaufwand. Die Diagnosefunktion im laufenden Betrieb und die im Logbuch verfügbare Historie erhöhen zusätzlich die Anlagenverfügbarkeit. Die Geräte unterstützen OPC UA als IoT-Schnittstelle und kommunizieren über das Datenmodell der OPC-UA-AutoID-Companion-Spezifikation V1.0. Dies ermöglicht die herstellerunabhängige Kommunikation in der Automatisierung sowie eine standardisierte Anbindung an Cloudapplikationen über ein Industrial IoT-Gateway.

Siemens AG • www.siemens.de

Der Weg zur robusten Embedded-Plattform



Bei der Embedded-Geräte-Entwicklung werfen neue Projekte viele Fragen auf: Welchen Weg einschlagen, worauf aufbauen? Diese grundsätzlichen Entscheidungen bestimmen den Erfolg des Produktes. Dabei ist es essentiell, schon vor dem Entwicklungsbeginn alle Kostentreiber und Zeiträuber zu identifizieren.

TEXT & BILDER: Ginzinger electronic systems GmbH

Die Komplexität heutiger Gerätefeatures wird oft unterschätzt. Randthemen wie Lizenzen und Normen werden anfangs selten hinterfragt. Während der Entwicklung explodieren dann aber die Kosten, oft sind es 70 bis 80 Prozent der Gesamtaufwände.

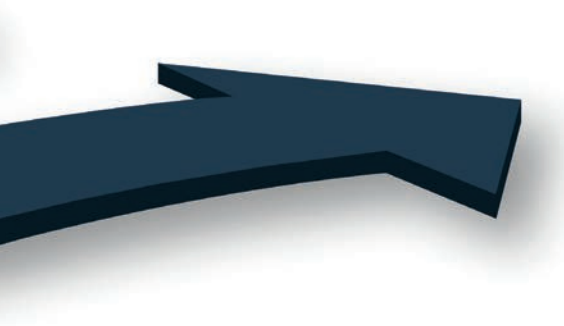
Drei Wege führen zum Ziel

Um die Komplexität bei Embedded-Projekten in den Griff zu bekommen, ist eine geschickte Auswahl der richtigen Technologie essentiell. Sie muss zweckmäßig und praktikabel sein und mittel- und langfristig unterstützt werden. Dabei kristallisiert sich in den letzten Jahren vor allem Linux als ideales Betriebssystem für Embedded Systeme heraus. Es hat sich in den letzten Jahren stark verbreitet und durch eine breite Palette an Softwarepaketen und Frameworks sehr gut etabliert. Allerdings führen die extreme Flexibilität und Anpassungsfähigkeit von Linux und anderer Open-Source-Software selbst Experten vor schwierige Entscheidungen und zu einer sehr hohen Verantwortung. Grundsätzlich kann man zwischen drei Auswahlansätzen wählen:

1. Die Open-Source-Softwareplattform für das neue Gerät wird komplett selbst entwickelt, konfiguriert und erweitert.
2. Kommerziell erhältliche Software-Distributionen werden eingesetzt, erweitert und punktuell angepasst.
3. Ein externer Komplettanbieter übernimmt die Verantwortung für die gesamte Plattform: Hard- und Software.

Komplette Eigenentwicklung der Plattform

'Selbst ist der Entwickler' lautet hier die Devise. Das bedeutet, bereits vom Linux-Kern weg die eigene Distribution zu erstellen. Building-Tools wie buildroot und Yocto sind dabei hilfreich. Der große Vorteil ist, dass man das komplette



System am Ende auswendig kennt und von Grund auf selbst beherrscht. Nicht zu unterschätzen sind die hohen Ressourcen, die benötigt werden. Startet man 'vom Kernel' weg, muss klar sein, dass alle eigenen Anpassungen sehr zeitaufwändig und fehleranfällig sind. Auch obliegt dem Entwickler die Wartung und Pflege des Systems. Themen wie die Integration, sowie die Tests der Treiber, die Verinnerlichung sämtlicher Chip-Konfigurationen, die Prüfung der optimalen Zusammenstellung der einzelnen Pakete zur Distribution, um nur einige Themen zu nennen.

Aufbau auf bestehenden Software-Distributionen

Alternativ zum kompletten Eigenaufbau können bereits existierende Embedded-Betriebssysteme offen und kommerziell verwendet werden, um darauf aufzubauen. Die Basis ist sofort verfügbar, inklusive zahlreicher Funktionen. Dies ist auf den ersten Blick sehr praktisch. Da Distributionen aber meist nicht auf das Endgerät des Kunden abgestimmt sind, muss das System angepasst werden. Unnötige Pakete müssen gestrichen, spezielle Treiber für CAN oder Wireless gesucht werden. Auch die Integration der Hardware, sowie die Tests für das System und die Stabilität müssen selbst durchgeführt werden. Nach erfolgter Implementierung der Funktionen und der Anbindung an die Hardware geht es weiter: Ist die Hardwareplattform fertig, beginnt die Wartung. Vor allem bei vernetzten Geräten spielen dann Themen wie Security eine wichtige Rolle, um z.B. Cyberattacken auf das Kundenprodukt zu verhindern. Ist das Gerät nach (idealerweise) etlichen Jahren am Ende seines Produktlebens angekommen, lautet der nächste Punkt auf der To-do-Liste Migration auf die nächste Gerätegeneration.

Einen Komplettanbieter für die ganze Plattform finden

Schließlich gibt es noch die Möglichkeit, externe Dienstleister als Komplettanbieter mit der Entwicklung und Betreuung der ganzen Hard- und Softwareplattform zu beauftragen. Diese kümmern sich (im Idealfall über den ganzen Produktlebenszyklus hinweg) um ein zuverlässiges Grundgerüst. Dies macht vor allem dann Sinn, wenn man sich als Gerätehersteller nicht in den umfangreichen Details der Hard- und Softwareintegration verlieren möchte. Man kann auf ein fertiges und funktionierendes Fundament aufbauen. Der größte Vorteil liegt auf der Hand: Die Konzentration auf die wichtigste Aufgabe, den Nutzen für den Kunden.

Die richtigen Fragen stellen

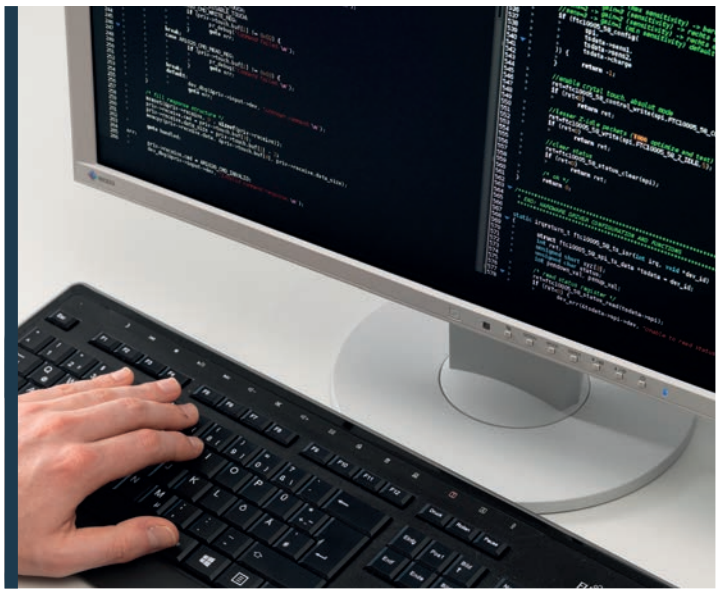
Egal, für welche Variante man sich als Entwickler am Ende entscheidet, die wichtigsten Fragen, die man sich vor dem Projektstart stellen muss, lauten:

1. Mit welchem Know-how stiften wir Nutzen für den Kunden und verdienen Geld?
2. Wie viel Ressourcen bleiben für die Entwicklung der Kernanwendung?
3. Welcher Weg ist der günstigste?
4. Wie minimiere ich das eigene Risiko?
5. Wie komme ich rasch zu einem marktfähigen Produkt?

Whitepaper als Wegweiser

Hilfestellung zu diesen Fragen bietet Ginzinger Electronic Systems mit seinem neuen Whitepaper zum Thema 'Ihr Weg zur robusten Embedded-Plattform'. Es bietet Unterstützung bei der Auswahl der richtigen Technologie im Spannungsfeld zwischen Gerätevernetzung, Usability, Gesetzgebung und Lizenzregelung. ■

www.ginzinger.com/ihrweg



Ginzinger setzt schon lange auf die Komplettintegration der Hard- und Software für die Produkte seiner Kunden. Ein bewährtes, skalierbares und logisches System vorintegrierter Hard- und Softwarebausteine ermöglicht den raschen Projektstart.

4 Missverständnisse im IIoT

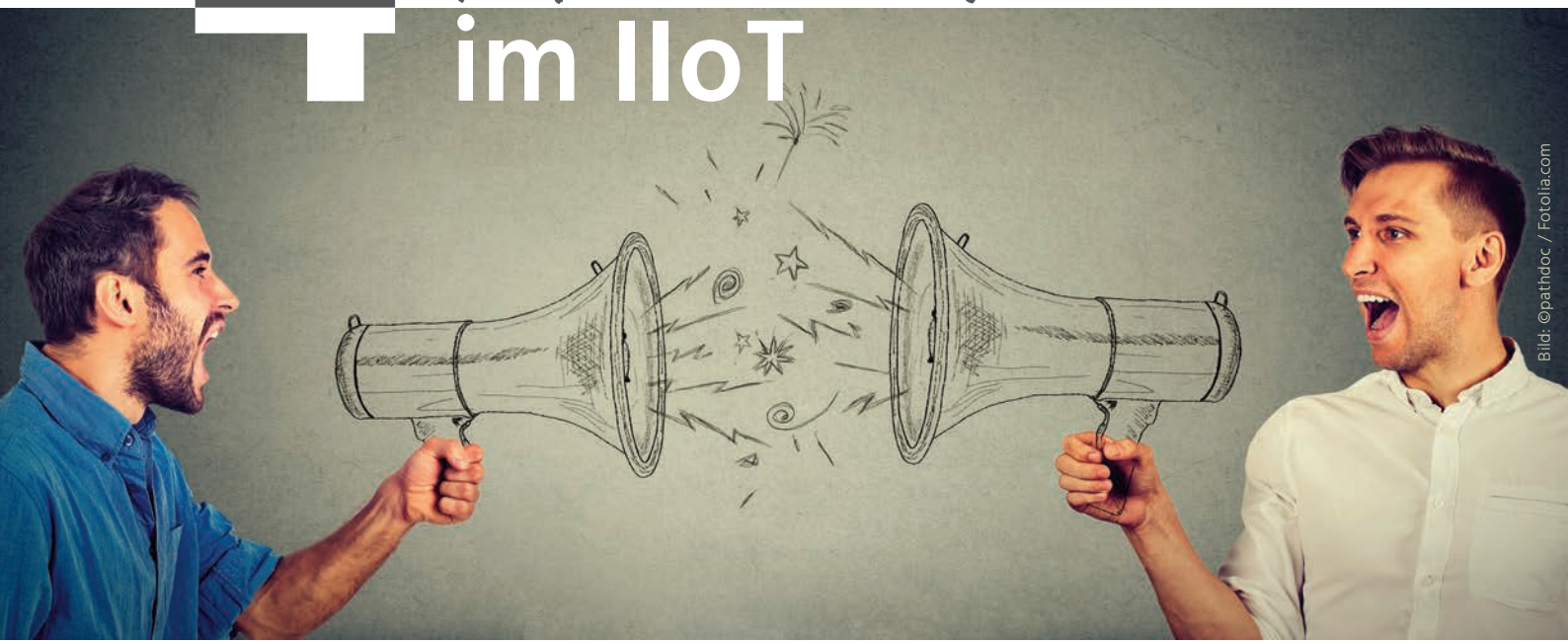


Bild: ©pathdoc / Fotolia.com

Die Digitalisierung der Industrie geht, abseits von kleineren Pilotprojekten, oftmals schleppend voran und wird von vielen als Mammutaufgabe wahrgenommen. Industrie 4.0 bedeutet tatsächlich gänzlich neue Anforderungen an die Datenhaltung und -analyse. In diesem Beitrag deckt Christian Lutz, CEO von Crate.io, die vier häufigsten Missverständnisse im IIoT auf, die Anwender und Entwickler von der Umsetzung abhalten.

TEXT: Christian Lutz, CEO & Co-founder, Crate.io GmbH **BILDER:** Crate.io GmbH

Analysten wie Gartner Research weisen darauf hin, dass IoT vollkommen neue Herausforderungen in Bezug auf Datenvolumen, Daten- und Abfragekomplexität sowie die Integration stellt. Tatsächlich ist es ein gewaltiger Unterschied, ob eine Maschine im Stand-Alone-Betrieb oder innerhalb einer vernetzten IIoT-Lösung mit Remote-Überwachung arbeitet.

Es gibt kein neues Datenproblem

Ein häufiger Fehler liegt darin zu versuchen, die IIoT-Infrastruktur auf Basis der bestehenden, traditionellen Datenbanken (z.B. Microsoft SQL Server, Oracle, et al.) zu implementieren. Diese sind meist technisch nicht in der Lage, die gestiegenen Anforderungen aufgrund der zu verarbeitenden Datenmengen zu erfüllen, aber auch zu teuer für solche Anwendungen. Traditionelle SQL-Datenbanken sind zwar einfach zu bedienen, aber nicht für die Abfrage von Maschinendatenströmen in Echtzeit konzipiert.

NoSQL-Datenbanken sind notwendig

Oft gehen Datenbank-Experten bei hohen Datenmengen und unstrukturierten Daten davon aus, dass hier zwangsläufig ein NoSQL-Anwendungsfall vorliegt. NoSQL-Datenbanken eignen sich tatsächlich insbesondere bei komplexen und flexiblen Abfragen, weil sie für eine effiziente Skalierung und verteilte Architekturen bestens geeignet sind. Allerdings sind die Infrastrukturen von NoSQL oft sehr kompliziert aufgebaut, was viel Zeit für Planung, Betrieb und Administration verschlingt. In der industriellen Praxis wird fast immer auch die Speicherung von relationalen Daten gefordert wie z.B. Topologien, Firmware Informationen, ERP- oder Artikel-Daten. Das bedeutet, dass zwei Systeme parallel gefahren und synchronisiert werden müssen. Ein weiteres Problem ist, dass es keine standardisierte Abfragesprache für NoSQL-Datenbanken gibt, weil diese jeweils ihre eigenen Abfragesprachen haben. Es werden also jeweils spezialisierte, erfahrene Programmierer für NoSQL-Datenbanken wie Cassandra, Elasticsearch oder MongoDB benötigt – und die sind teuer und rar. Die Alternative liegt hier darin, reine NoSQL-Datenbanken durch neuere und modernere SQL-basierte Lösungen wie die CrateDB zu ersetzen, die die Vertrautheit von ANSI SQL mit der Skalierbarkeit und Flexibilität von NoSQL kombinieren.

Die Lösung liegt in Time-Series

Spezialisierte Zeitreihendatenbanken kommen immer wieder in Mode. Seit es Historians gibt,

zeichnen sie Daten auf und können mithilfe integrierter Tools diese im Zeitverlauf grafisch darstellen bzw. abfragbar machen. Ein häufiger Fehler ist die Wahl einer Zeitreihendatenbank als Basis für eine IoT-Plattform. Denn wie die Praxis zeigt, sind Time-Series oft in ihrer Skalierbarkeit mit hoher paralleler Nutzung und auch Funktionalität eingeschränkt. Im IoT wird neben der Visualisierung von Datenströmen die Unterstützung bei einer Vielzahl von Analysen und Datenmodelländerungen gefordert, die beispielsweise zu verstehen ermöglichen, worin Ursachen für Auffälligkeiten liegen. Das interaktive Arbeiten mit Daten in Echtzeit ist also erforderlich – also auch unter hoher Last gleichzeitiges Lesen, Schreiben und Ausführen von adhoc Queries, wie z.B. für Machine Learning. Hinzu kommt die agile Anforderung Datenschemata zur Laufzeit anpassen zu können. Hierbei werden zu den nackten Sensordaten auch ERP-Daten, Qualitätsdaten oder Logistikdaten hinzugefügt, um anzuzeigen, ob Produktionsanomalien beispielsweise mit bestimmten Aufträgen verbunden sind oder auf Rohstoffe einzelner Lieferanten zurückzuführen sind. Datenmodelländerungen solcher Art erfordern häufig, dass Anwender ihre Zeitreihendatenbanken vollständig neu erstellen müssen, was zeit- und vor allem sehr kostenintensiv ist. Um das zu lösen, wird oft neben der Zeitreihendatenbank noch eine separate relationale Datenbank für Nicht-Zeitreihen-Daten eingesetzt. Das ist zwar eine schnell zu implementierende Lösung, allerdings wird es mit zunehmendem Wachstum der Datenbasis teuer und schwierig, die Daten in mehreren Datenbanken zu duplizieren und synchron zu halten.

KI ist erst mit bereinigten Daten möglich

Entwickler gehen manchmal davon aus, dass ihnen die Datenbasis oder Datenhygiene für das Aufsetzen einer KI fehlen. Unzureichende Daten könnten ja zu einer schlechten KI-gesteuerten Automatisierung führen. Die Befürchtung, unzulängliche Daten führten automatisch dazu, dass keine sinnnvollen Ergebnisse gewonnen werden können und Fehlentscheidungen getroffen werden, ist unbegründet. In der Praxis setzen die meisten Unternehmen eine Lösung wie CrateDB ein, um einen Echtzeit-Datenspeicher aufzubauen und mit KI-Technologien und maschinellem Lernen die menschliche Entscheidungsfindung zu optimieren, nicht um sie zu ersetzen. Eine praktische Herangehensweise ist es, die Daten im Prozess automatisch zu bereinigen, indem die Analyseergebnisse überwacht werden und so schrittweise ein sauberer Datenbestand entsteht. Der Versuch, zuerst alle historischen Daten als Voraussetzung für ein Projekt vollständig zu bereinigen, verzögert die Entwicklung und Implementierung von intelligenten IoT-Systemen und bietet oft zu wenige Daten oder Tiefe. Es ist in der Regel besser, einfach loszulegen und Rohdaten zu sammeln und auf dem Weg die Use-Cases zu entwickeln.

Resumée

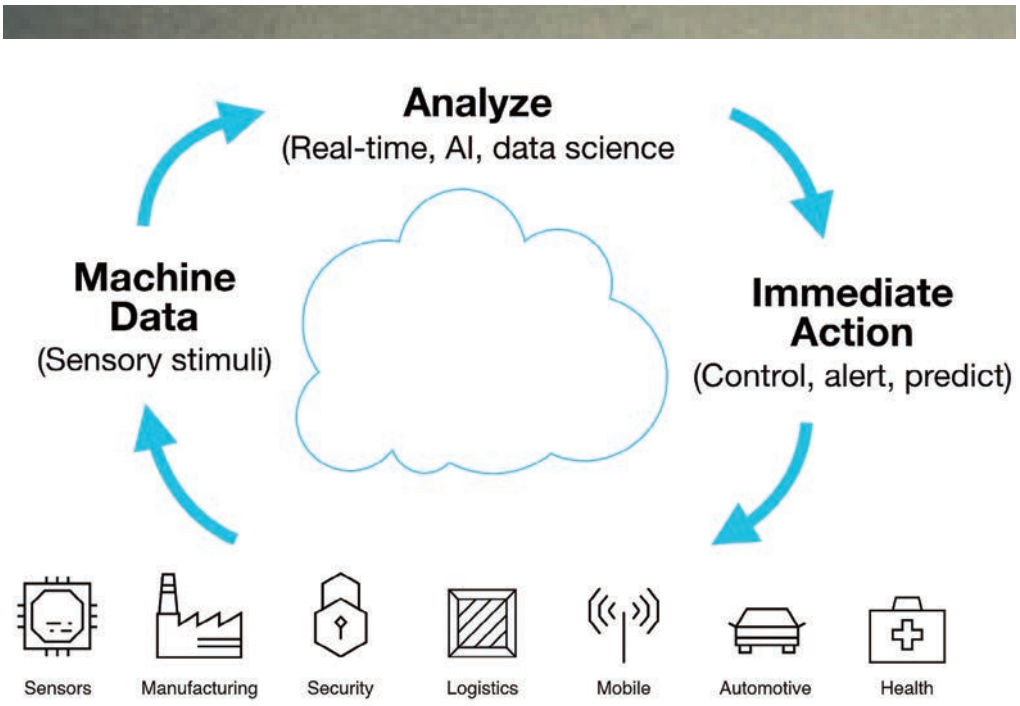
Tatsächlich schafft IoT in der Praxis gänzlich neue Anforderungen an die Datenhaltung und -analyse. Pipelines von Sensordaten – oft tausende oder hundertausende von Messwerten pro Minute und Dutzende von Nachrichtenformaten – müssen in Echtzeit integriert und analysiert werden, um das Verhalten von 'Dingen' zu überwachen, vorherzusagen oder zu kontrollieren. Eine schnelle Erfassung und Analyse von Maschinendaten sind die Voraussetzung, die datengesteuerte Automatisierung der Schlüssel zum Erfolg eines zukunftssicheren IoT-Projektes.

Ein Datenmanagementsystem in der Smart Factory muss:

- Schnelle Entwicklung und Time-to-Value garantieren,
- Echtzeit-Datenanalyse ermöglichen,
- konstante Betriebszeit sowie
- niedrige IT-Betriebskosten für Hosting, Integration und Administration gewährleisten.

Die oben genannten Missverständnisse hingegen, halten Entwickler und Anwender nur von der Umsetzung der Smart Factory ab. ■

www.crate.io



Viele Unternehmen halten sich zu lange an den Missverständnissen auf und vergessen einfach anzufangen.

Multiple Clouds vs. Multi-Cloud

TEXT: Richard Kunkel, AVI Networks
BILDER: AVI Networks Germany

Mehrere verschiedene Clouddienste zu nutzen ist für Unternehmen nichts ungewöhnliches. Einige sehen sich sogar dadurch bereits auf der technologischen Siegesstraße, denn Multi-Cloud-Strategien werden überall als Must-have propagiert. Tatsächlich befinden sie sich damit auf dem Holzweg: Die Nutzung Multipler Clouds ist eben nicht gleich Multi-Cloud.

Multi-Cloud ist derzeit einer der heißesten Trends für Unternehmen. Die Verwendung mehrerer Clouds gleichzeitig, kann viele Vorteile bieten. Richtig eingesetzt kann man mit der richtigen Kombination von Clouds unter anderem die Kosten für Infrastruktur senken, die Präsenz von Daten und Workloads in verschiedenen Regionen verbessern oder die Herstellerbindung an Cloudanbieter vermeiden. Unternehmen, die den Ansatz Multi-Cloud hingegen falsch verstanden haben, kann dieses Missverständnis viel Geld kosten. Denn eine fehlgeleitete Multi-Cloud-Strategie hat das Potenzial, Anwendungen, Teams und Budgets unnötig aufzusplitten. Eine fragmentierte Cloudstrategie zwingt die zuständigen Infrastrukturteams zu erheblichem Mehraufwand bei der Konfiguration, Bereitstellung und Skalierung von Anwendungen in der Cloud. All dies ist natürlich kostspielig, zeitaufwendig und steht im Widerspruch zum eigentlichen Versprechen der Multi-Cloud. Dabei ist dieser grundlegende Fehler eigentlich einfach zu vermeiden: IT-Verantwortliche müssen nur erkennen, dass die Multi-Cloud grundsätzlich eine Anwendungsstrategie und keine Infrastrukturstrategie ist.

Anwendungen von der Infrastruktur abstrahieren

Cloudressourcen von mehreren Anbietern zu erwerben ist der einfache Teil: Backup auf Azure, produktive Workloads in AWS und die kritischen Systeme laufen in der privaten Cloud im eigenen Rechenzentrum. Schwieriger ist es jedoch verschiedene Clouds nahtlos zu verbinden, damit man sich leicht über die einzelnen Cloud-Silos hinwegbewegen kann. Dieser Schritt ist jedoch zwingend notwendig, um den Mehrwert der Multi-Cloud nutzen zu können. Erreicht wird dies erst, wenn Anwendungen von der zugrunde liegenden

„Dienste, Geschäftsmodelle und die Einstellung zur Infrastruktur haben sich grundlegend verändert – diese Änderungen machen die Multi-Cloud realistisch und realisierbar."

Richard Kunkel

Infrastruktur und Anwendungsdiensten, wie z.B. Load Balancern, abstrahiert worden sind. So abstrahiert, wird eine heterogene Umgebung geschaffen, in der die Anwendung volle Flexibilität und Portabilität genießt und ihre benötigten Ressourcen erhält, ohne dass eine spezifische Konfiguration für die Cloudumgebung erforderlich ist. Ziel ist es, die Anwendung agnostisch für die Cloudinfrastruktur zu machen und Dienste direkt bei der Application anzuwenden, damit sie die gleiche Portabilität haben. Abstraktion ermöglicht es Unternehmen also, sich mit der Geschwindigkeit ihrer Anwendungen zu bewegen, nicht mit der Infrastruktur, die sie bereitstellt. Viele Plattformen, insbesondere containerbasierte Technologien, sind bereits agnostisch und überspannen problemlos mehrere Clouds. Die meisten Anwendungsdienste, wie Load Balancing und Web Application Firewalls, sind jedoch immer noch infrastrukturzentriert und passen nicht zu einer Anwendungsstrategie in der Multi-Cloud. Dies zeigt sich deutlich am Beispiel traditioneller Load Balancer, die sich aus mehreren Gründen nicht für Multi-Cloud-Konzepte eigenen.

Es ist an der Zeit, Load Balancing neu zu überdenken

Native Load Balancer der Cloudanbieter funktionieren fast selbstredend nur in ihrer jeweiligen Umgebung. So funktioniert AWS ELB beispielsweise nicht in Azure und Azures Application Gateway nicht in AWS. Und auch virtualisierte Load Balancer sind so konfiguriert, dass sie nur innerhalb eines Infrastruktursilos arbeiten. Diese an Hardware gebundenen Load Balancer funktionieren immer noch als Appliances, was bedeutet, dass sie fest mit ihrer Infrastruktur verbunden sind und nicht die gleiche Flexibilität und Portabilität bieten, wie die Anwendungen die sie unterstützen. Diese traditionellen Load Balancer sind auf die Infrastruktur ausgerichtet, nicht auf Anwendungen. Für IT-Teams besteht die Herausforderung darin, Anwendungen so in einer Multi-Cloud-Umgebung mit hoher Verfügbarkeit bereitzustellen, dass sie mit der Anwendungsstrategie übereinstimmen. Um dies zu erreichen ist an der Zeit, Load Balancing neu zu überdenken.

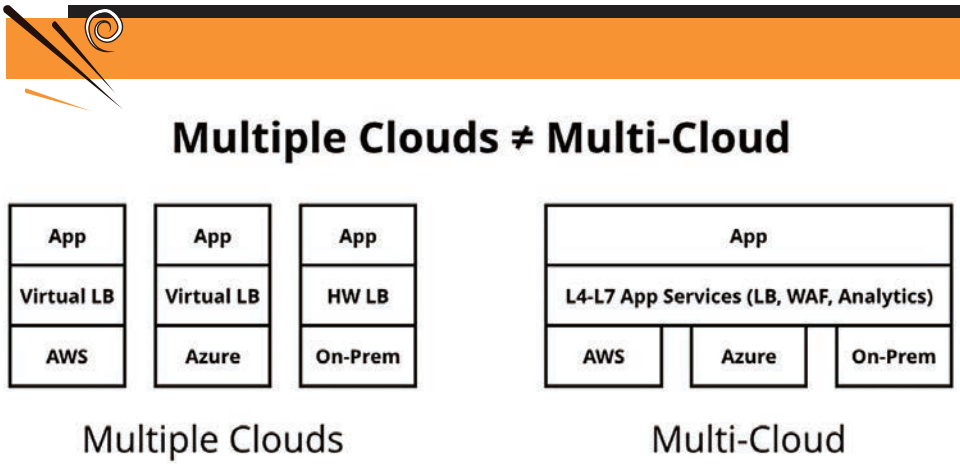
Rack and Stack gehört der Vergangenheit an

Die Infrastruktur von Rechenzentren hat sich in den letzten zehn Jahren grundlegend verändert. Zahllose Server und Appliances in Racks zu stapeln war früher üblich und die Verwaltung von Hardware galt früher als der schnellste Weg, um die benötigte Infrastruktur zu erhalten. Visionäre IT-Führungskräfte, Self-Service-Praktiker und CAPEX-bewusste Finanzteams spielten alle eine Rolle bei der Umstellung auf die Cloud. Investitionen in die Hardware-Infrastruktur sind heute seltener denn je. Anwendungsteams sind mehr daran interessiert, die benötigten Ressourcen zu erhalten, als darüber nachzudenken, woher sie diese geliefert bekommen. IT-Teams stehen somit vor der Herausforderung, die wachsende Nachfrage mit viel kleineren Budgets bewältigen zu müssen. Als Ergebnis all dieser Faktoren, haben sich die Dienste, das Geschäftsmodell und die Einstellung zur Infrastruktur grundlegend verändert – diese Änderungen machen die Multi-Cloud realistisch und realisierbar.

Für die Multi-Cloud ist ein anwendungsorientierter Lastausgleich erforderlich

Load Balancing hingegen, hat sich in den letzten zehn Jahren kaum verändert. Die wenigsten Innovationen, die wir von den etablierten Anbietern gesehen haben, waren die Neuverpackung ihrer Hardware Appliance in eine virtualisierte Edition, damit sie in der Cloud ausgeführt werden kann. Die Architektur ist die gleiche, ohne den Vorteil proprietärer Hardware, was bedeutet, dass sie nicht in der Lage sind, Dienste bereitzustellen, die Anwendungen benötigen, um in einer Multi-Cloud-Welt erfolgreich zu sein. Diese Appliances, ob Hardware oder virtuell, sind nicht anwendungszentriert und unterstützen in keiner Weise Multi-Cloud-Initiativen. Wie die meisten anderen Appliances müssen Load Balancer als Software-Services neu abgebildet werden – Dienste, die pro App bereitgestellt werden können und mit der Anwendung in die für die Anwendung am besten geeignete Umgebung verschoben werden. Multi-Cloud ist eine Anwendungsstrategie. Und der einzige Weg, diese Strategie zum Leben zu erwecken, besteht darin, Infrastruktur und Dienste zu nutzen, bei denen Anwendungen im Vordergrund stehen. ■

www.avinetworks.com



Sicherheit für Permissioned Blockchains

Das Herzstück jeder Blockchain ist ein Protokoll, das der Reihenfolge und Sicherheit einer Transaktion für den nächsten Block zustimmt. Der folgende Beitrag beschäftigt sich damit wie man die Integrität dieser Kette bewahrt.

TEXT: Duncan Jones, Thales eSecurity

Sogenannte permissioned Blockchains erfreuen sich wachsender Beliebtheit. Umso mehr, da Firmen den Blockchain-Trend für sich nutzen und gleichzeitig den 'Deckel darauf halten' wollen. Im Gegensatz zu den Vertretern der Non-Permissioned-Seite (wie Bitcoin oder Ethereum) sind bei permissioned Blockchains die Teilnehmer bekannt, und man kann ihnen gezielt besondere Rechte und Privilegien einräumen. Permissioned Blockchains werden von einer Genehmigungsinstanz kontrolliert, die jedem Einzelnen der teilnehmenden Knoten eine entsprechende Erlaubnis erteilt. Nur wer autorisiert ist kann auf das Transaktionsnetzwerk zugreifen. Sucht man bei einer gehypten Technologie wie der Blockchain nach konkreten Anwendungsbeispielen, handelt es sich meist um permissoned Blockchains. Die genehmigende Instanz kann ein Konsortium von Unternehmen sein, aber auch eine einzelne Organisation. Der folgende Beitrag beschäftigt sich insbesondere mit den Sicherheitsimplikationen, wenn man autorisierten Teilnehmern eine übersichtliche Blockchain bereitstellen will und gibt Empfehlungen für eine sichere Bereitstellung. Dazu ist es sinnvoll zunächst zu klären, was man unter permissioned Blockchains versteht und wie die Terminologie verwendet wird.

Bild: ©AndSus / Fotolia.com

Was macht eine Permissioned Blockchain aus?

Das Herzstück jeder Blockchain ist ein Protokoll, das der Reihenfolge neuer Transaktionen für den nächsten Block zustimmt, der sogenannte 'Konsensus'. Transaktionen können dabei jede Art von Informationen sein. Der Konsensus ist eine verbindliche Übereinkunft zwischen allen validierten Knoten. Jeden Computer, der sich mit einem Blockchain-Netzwerk verbindet, nennt man Node, also Knoten. Innerhalb der Blockchain sorgen die Konsensusmechanismen für die Integrität und Konsistenz der Daten. Es ist also ganz entscheidend, dass dieser Prozess sicher abläuft. In den sogenannten 'Non-Permissioned' Blockchains ist der Konsensus typischerweise der Versuch ein schwieriges mathematisches Problem im Austausch für einen vergleichsweise geringen finanziellen Lohn zu lösen. Die validierenden Knoten sammeln zunächst alle ihnen bekannten Transaktionen, wählen eine Reihenfolge und beginnen damit, die Aufgabenstellung des Blocks zu lösen. Ohne Zugangsbeschränkungen ist der Konsensusmechanismus entsprechend einfach, was unter anderem die Transaktionsgeschwindigkeit erhöht. Die Schattenseite: Im Grunde ist es reines Glücksspiel wer am Ende das Rennen macht. Auch wenn eine gewisse Wahrscheinlichkeit dafür spricht, dass es diejenigen sein werden, die über eine höhere Rechnerleistung verfügen. Das Konsensusprotokoll kann durchaus schwerwiegenden Angriffen auf die Kette standhalten (bis zu 50 Prozent aller Knoten können bösartig sein). Allerdings geht das auf Kosten der Transaktionsgeschwindigkeit und der Bestätigung. Bitcoin wickelt beispielsweise einzelne Transaktionen innerhalb einer Sekunde ab, die Bestätigung kann allerdings über eine Stunde dauern. In permissioned Blockchains läuft der Konsensus geordneter ab, und die Prüfer wechseln sich dabei ab, einen Block vorzuschlagen, den die anderen anschließend freigeben. Der Prozess läuft also viel schneller ab. Permissioned Blockchains erzielen deshalb eine hohe Durchsatzrate bei Transaktionen, die oftmals sofort bestätigt werden. Dieser Typ von Konsensus basiert im Allgemeinen darauf, dass mehr als zwei Drittel der Knoten vertrauenswürdig sind.

Wie sicher sind Permissioned Blockchains?

Der Terminus Blockchain beschwört sofort ein bestimmtes Bild herauf – das von dezentraler Kontrolle und Mehrwert durch Sicherheit. Große non-permissioned Blockchains wie etwa Bitcoin und Etherum haben in der Öffentlichkeit mittlerweile einen hohen Bekanntheitsgrad. Und zuweilen beeinflusst dieses Phänomen auch Unternehmen, die planen permissioned Blockchains zu nutzen. Eines sollte man verstehen: Senkt man die Zahl der Teilnehmer und verlässt sich auf vertrauenswürdige Prüfer, dann ähneln die Sicherheitsanforderungen und Herausforderungen eher denen in traditionellen IT-Systemen als denen großer Blockchains. Stellen wir uns eine permissioned Blockchain vor, die zwischen fünf führenden Bankhäusern aufgebaut wird. In einer Blockchain mit fünf Knoten bedeutet das, dass vier von ihnen (also zwei Drittel) vertrauenswürdig sein und sich korrekt verhalten müssen, damit der Konsensus erfolgreich abläuft. Im Wesentlichen gibt es zwei Gründe wenn Knoten sich nicht so verhalten wie sie sich verhalten sollten. Ihre legitimen Eigentümer haben unredliche Absichten oder die Knoten sind von einem Angreifer kompromittiert worden. Im ersten Fall geht es darum geheime Preisabsprachen und Verdunklung zu verhindern. Im zweiten Fall darum, die privaten Schlüssel der Knoten zu schützen, und sicherzustellen, dass sie nur dazu benutzt werden, die Nachrichten zu signieren, die sich im Einklang mit dem Konsensusprotokoll befinden. Genauso wichtig ist es die privaten Schlüssel der Blockchain-Konten zu schützen. Diese Schlüssel dienen dazu eine Transaktion zu signieren und so einen nicht autorisierten Geldfluss aus dem betreffenden Konto heraus zu verhindern. Der unberechtigte Zugriff auf diese Schlüssel würde dazu führen, dass Werte unrechtmäßig zwischen den beteiligten Banken übertragen werden. Es kann kostspielig werden, dieses Problem zu lösen und schlimmer noch, der unberechtigte Zugriff kann den Bestand des kompletten Projekts gefährden. Schließlich ist da noch der Dreh- und Angelpunkt des gesamten Systems, nämlich der Schüsselsatz, der die Teilnehmer überhaupt erst autorisiert. Hat ein Angreifer Zugriff auf diese Schlüssel ist er beispielsweise in der Lage neue validierende Knoten zu bevollmächtigen. Ein Angreifer kontrolliert dann beispielsweise ausrei-

Gymnasiastin entwickelt Zufallszahlengenerator

Zufallszahlen, die für eine sichere Verschlüsselung notwendig sind, generiert Gesa Dünnweber (17) vom Städtischen St.-Anna-Gymnasium in München jetzt selbst. Dazu hat sie ihre eigene Mikrochipanwendung konzipiert. Mit ihrem Projekt überzeugte die Gymnasiastin die Jury des Schülerwettbewerbs 'Invent a Chip'. Sie sicherte sich den mit 3.000 Euro dotierten ersten Platz im Entscheid. Den mit 2.000 Euro dotierten Platz zwei errang Niklas Dobberstein (16) vom Gymnasium Lindlar. Er entwarf einen intelligenten, ergonomischen Arbeitsplatz für mobile Büros. Die Preisträger erwartet neben den Geldpreisen jetzt die Aufnahme ins Auswahlverfahren für ein Stipendium der Studienstiftung des deutschen Volkes, Kontakte zu Industrie und Hochschulen sowie Einladungen zu Projektpräsentationen auf Messen.

VDE Verband der Elektrotechnik
www.vde.com

chende Stimmrechte, um potenziell die gesamte Kette zu beschädigen oder sogar zu zerstören.

Was tun gegen die Bedrohungen?

Während sich öffentliche Blockchains bei ihrer Sicherheit auf die schiere Zahl der Knoten verlassen, müssen permissioned Blockchains zu anderen Methoden greifen. Dazu gehören Verfahren die Blockchain zu härten beispielsweise durch geschützte Umgebungen für private Schlüssel sowie durch Prozesse und Verfahren für einen sicheren Betrieb der Blockchain als solcher. Private Schlüssel, die von validierenden Knoten verwendet werden, sollten auch physisch geschützt werden. Dazu dienen Technologien wie Hardware Security Modules (HSMs). HSMs sorgen dafür, dass die privaten Schlüssel nicht vom Serverspeicher ausgelesen werden können wenn der Knoten kompromittiert wurde. Es ist sogar möglich die eigentliche Logik des Konsensus mit HSMs zu schützen. Diese Methode stellt sicher, dass die betreffenden Daten tatsächlich dem Konsensusprotokoll entsprechen bevor sie mit dem Schlüssel signiert werden. Ein klassisches Anwendungsbeispiel ist, das doppelte Signieren zu verhindern wie etwa Forking. Unser Forschungsteam hat ein Open-Source Beispiel dieser Technik veröffentlicht, bei der eine beliebte permissioned Konsensus-Engine verwendet wurde. Will man die privaten Schlüssel der Blockchain-Konten schützen, sollte man einen auf dem potentiellen Risiko basierenden Ansatz wählen. Für Wallets (digitale Ordner), die nur geringfügige Werte repräsentieren, genügen in aller Regel einfache Methoden, wie ein HSM USB-Stick mit einem Schalter über den sich Überweisungen autorisieren lassen. Im Unternehmensumfeld mit entsprechenden Werten empfiehlt es sich kommerzielle HSMs einzusetzen und gegebenenfalls die Zeichnungspflichten auf unterschiedliche Zeichnungsberechtigte zu verteilen. Die privaten Schlüssel innerhalb einer Blockchain zu sichern ist deutlich einfacher als jede andere Art von Public Key Infrastructure (PKI) zu schützen. Trotz allem ist aber auch das eine Art von PKI. Anders als in der üblichen Wahrnehmung von Blockchains verlassen sich permissioned Blockchains auf eine PKI, die Anmeldeinformationen an ihre jeweiligen Teilnehmer ausgibt. Und jede einzelne Transaktion lässt sich unmittelbar mit Bezug auf den entsprechenden Vertrauensanker überprüfen und bestätigen. Es ist einleuchtend, dass die betreffenden Schlüssel wie jeder andere vergleichbare Vertrauensanker geschützt werden müssen – über HSMs, die Verteilung der Zeichnungsaufgaben, Auditing und so weiter.

Ein Blick in die Zukunft

Im Moment zeigt der Hype um das Thema Blockchain keinerlei Anzeichen sich abzuschwächen. Wir können vermutlich damit rechnen, dass Projekte, die permissioned Blockchains nutzen schon bald in den Branchennachrichten auftauchen werden. Wenn es daran geht solche Projekte zu entwickeln und umzusetzen, sollte Sicherheit vom ersten Tag an mit berücksichtigt werden. Wie immer, wenn sich eine neue Technologie anschickt die Märkte zu erobern, wird Sicherheit gerne zugunsten von Schnelligkeit zurückgestellt. Es ist also vermutlich nicht nur mit einem Anstieg entsprechender Projekte zu rechnen, sondern auch mit mehr Sicherheitslücken und Schwachstellen bei Consortium Blockchain-Implementierungen. Wenn der Hype sich ein wenig gelegt hat, werden vielleicht weniger Projekte in Auftrag gegeben. Aber zu diesem Zeitpunkt haben wir sicherlich bereits gute und praktikable Empfehlungen für Blockchain-Anwender von Körperschaften wie der Accredited Standards Committee X9 und der ISO/TC307 erhalten. ■

de.thalesesecurity.com

Connectivity-Lösungen für die IIoT-Welt

In der vierten industriellen Revolution verschmelzen die physische und die digitale Welt immer mehr miteinander. Um Mehrwerte aus den Daten der Maschine zu generieren, wächst die Zahl an Sensoren und Aktoren rasant. Damit nimmt die Vernetzung in Maschinen und Anlagen und damit auch die Anzahl an Verbindungen immens zu. Auf der diesjährigen Messe Electronica präsentierte Harting innovative, passende Connectivity-Lösungen für die IIoT Welt.

TEXT & BILD: HARTING Deutschland GmbH & Co. KG

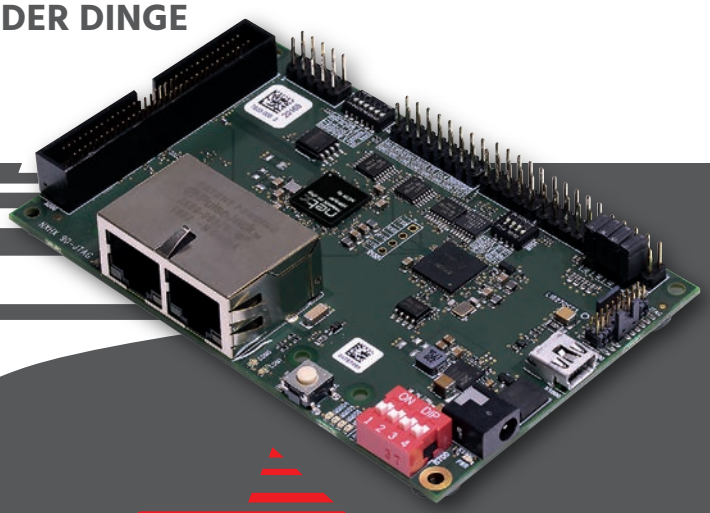
Zukünftig tauscht jede Maschine, jede Komponente in den Fabrikhallen große Mengen an Informationen und Daten aus. Auf der diesjährigen Messe Electronica präsentierte Harting innovative passende Connectivity-Lösungen für die IIoT Welt. Damit die Infrastruktur für das kommende IIoT noch kompatibel bleibt und auch der Anspruch an immer mehr intelligente Sensoren umsetzbar ist, passt sich diese Infrastruktur den neuen Ansprüchen an. Geräte werden immer kleiner und intelligenter, die notwendige Steckverbindung folgt diesem Trend.

Bereits 2016 hat Harting mit dem Helden der Industrial Ethernet Kommunikation ('Captain ix') einen Prozess zur Standardisierung neuer Schnittstellenstandards gestartet. Heute ist mit dem Harting ix Industrial ein Steckverbinder auf dem Markt, der es Geräteherstellern ermöglicht, bis zu 40 Prozent kleinere Geräte zu konzipieren. Um Geräte auch effizient herstellen zu können, muss die Connectivity einen optimalen Produktionsprozess unterstützen. SMT/SMD Bestückungstechnologie aller Schnittstellen sind notwendig für die effiziente Fertigung. Um die automatisierte Fertigung weiter zu unterstützen, sind Leiterplattenbuchsen auf Rollen lieferbar, in denen Gerätebuchsen Pick&Place-tauglich untergebracht sind. Auch die spätere Handhabung der Schnittstellen an den Geräten folgt der Performance. Die Einsparung von Montagezeit bei gleichzeitig einfacher und damit prozesssicherer Bedienung ist einer der unverzichtbaren Eckpunkte einer modernen Schnittstelle. Hier ist die PushPull-Verriegelungstechnik ein ganz wesentlicher Aspekt, da für immer kleinere Steckverbindungen bisher bekannte Verriegelungen wie z.B. die Schraubtechnik nicht mehr ausreichen werden.

Der Handling-Aspekt in der Connectivity wird daher immer wichtiger. Die PushPull-Technologie steigert die Bediensicherheit und Effizienz im Einsatz. Um auch die Komponente der Spannungsversorgung von Geräten kleiner und gleichzeitig leistungsfähiger zu gestalten, ergänzt Harting die M12 Power Baureihe zum Frühjahr 2019 um die genormte K-Kodierung für Powerversorgung. Mit 7,5kW bei 630V und 16A bietet die Geräteschnittstelle genügend Leistung für kompakte aber leistungsstarke Antriebe. Sie stellt damit eine zukünftige platzsparende Alternative zu 7/8" Lösungen dar und folgt ebenfalls dem Trend der Miniaturisierung. ■

www.harting.com

Der Harting ix Industrial ermöglicht es den Geräteherstellern bis zu 40 Prozent kleinere Geräte zu konzipieren.



Universalchip auch für Spezialisten

Der netX 90 kommt mit vielen neuen Features und einer einfachen Integration in das Internet der Dinge. Das bedeutet aber nicht, dass Hilscher die Automatisierungsfunktionen vernachlässigt. Auch hier hat das Unternehmen viele Neuheiten an Board, erläutert Sebastian Hilscher: „Wir haben für Encoder z.B. das BiSS-Protokoll integriert und haben EnDat auf Hardwareebene implementiert. Zusätzlich haben wir mit dem netX 90 eine Motor Control Unit, d.h. wir haben diverse ADCs, die auch parallel samplen können, in den Chip eingebaut. Wir haben zudem eine Motion Unit, die auch PWM generieren kann. Wir haben also für die verschiedenen Automatisierungsbranchen Hardware mit eingebaut. Er hat auch wieder einen IO-Link-Master integriert, den wir bereits im netX 51 hatten, d.h. mit einem netX 90 kann man einen 8-Kanal-IO-Link-Master bauen. Das Besondere ist die Tatsache, dass wir diese Automatisierungstechnologien alle sehr gut unterstützen und Ihnen mit dem netX 90 nun den Weg in das IoT-Zeitalter ebnen."

Hilschers neuer Chip bringt viele Innovationen

Das Unternehmen Hilscher ist als ausgewiesener Experte für Kommunikation in industriellen Prozessen, Maschinen und Anlagen bekannt. In vielen Automatisierungsgeräten sorgen die Prozessoren der netX-Reihe seit vielen Jahren für den Echtzeit-Datenaustausch. Das besondere daran: Es handelt sich um Multiprotokoll-Chips, die viele industrielle Protokolle unterstützen. Mit dem erscheinenden netX 90 zündet das Unternehmen die nächste Stufe seiner Entwicklung. Was die neuen Chips können und was das für Anwender und Entwickler bringt, erläutern wir im vorliegenden Beitrag, für den uns Sebastian Hilscher Rede und Antwort stand.

TEXT: Kai Binder, TeDo Verlag GmbH **BILDER:** Hilscher Gesellschaft für Systemautomation mbH

Die Kernkompetenz von Hilscher ist die Technologie, Entwicklung und Produktion von industriellen Kommunikationslösungen für die moderne Fabrikautomation. Die Produkte von Hilscher reichen von PC-Karten, Gateways über OEM-Aufsteckmodule bis hin zu leistungsfähigen Asics mit den dazugehörigen Protokollstacks. Diese werden weltweit zur Kommunikation zwischen Automatisierungsgeräten und Steuerungen eingesetzt – bei PC-Karten ist Hilscher in diesem Bereich der Marktführer. Ein derart umfassendes Lösungsportfolio für Feldbusse und Real-Time-Ethernet ist das Alleinstellungsmerkmal von Hilscher.

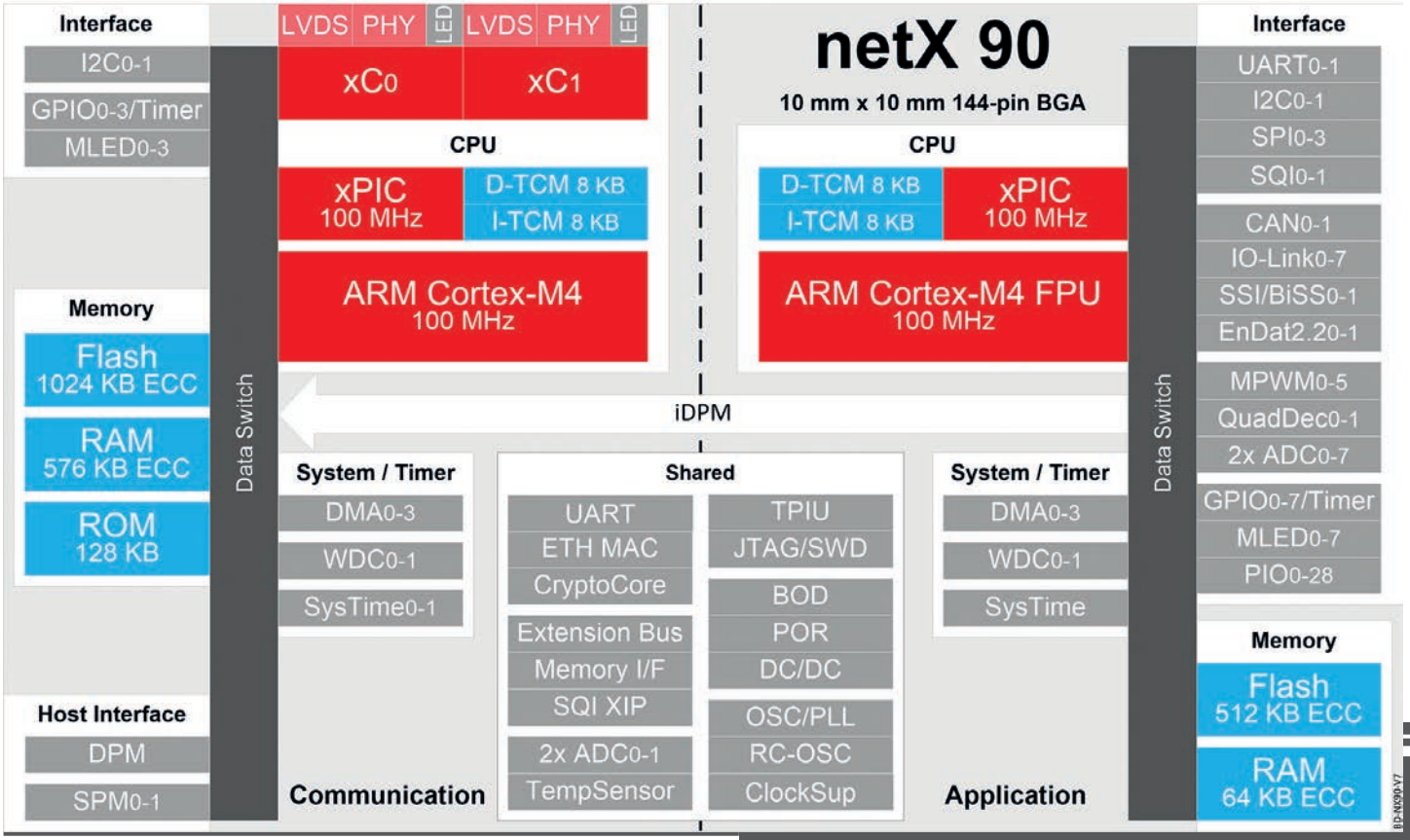
NEUES MULTIPROTOKOLL SOCS. Seit der Gründung des Unternehmens 1986 hat sich Hilscher auf die Unterstützung der Anwender bei ihren indus-

triellen Kommunikatinsprozessen verschrieben und gehört ohne Zweifel zu den weltweit führenden Experten auf diesem Gebiet. Heute gehört neben den bekannten PC-Einsteckkarten, Gateways und Asics auch leistungsfähige Multiprotokoll-Prozessoren – sogennante SoCs – die eine Vielzahl an Industrieprotokollen gleichzeitig verstehen zum Portfolio des Unternehmens. Sie heißen netX-Chips und werkeln nicht nur in vielen Hilscher-Geräten, sondern kommen auch bei Drittanbietern zum Einsatz, weil sie viele 'Fliegen mit einer Klappe schlagen'.

WAS IST NETX? Alle netX-Chips sind wahre Sprachtalente für die zahlreichen Ausprägungen der industriellen Kommunikation und deren diversen Dialekte. Dazu gehören Profibus und Profinet ebenso wie Ethernet/IP, Sercos, Ethercat, Modbus oder Powerlink. Zudem unterstützt netX immer schon Technologien wie UART, SPI, I2C, CAN, IO-Link und ein GPIO-Interface. All das, was die bisherigen netX-Chips können, kann netX 90 auch, aber er ist zudem mit echten IoT-Kommunikationstechnologien ausgestattet, die ihn für Geräte im Industrie-4.0-Zeitalter prädestinieren, aber erzählen wir der Reihe nach...

ZENTRALE EIGENSCHAFTEN VON NETX 90. Mittlerweile ist die nächste Hilscher-Generation in Person von Sebastian Hilscher im Unternehmen. Er ist als Manager netX Technology mit der Entwicklung der Technologie befasst: Er beschreibt die wichtigsten Talente des neuen Chips im folgenden so: "Der neue Chip bringt eine beachtliche Miniaturisierung mit sich, was sich positiv auf die Gerätegröße auswirkt. Das Gehäuse des netX 90 ist lediglich 10x10mm² klein. Gleichzeitig ermöglicht er höchste Performance, bringt eingebaute Security mit und ermöglicht eine deutlich verkürzte Entwicklungszeit für Gerätehersteller." Realität wird dies alles auch durch den Wechsel auf eine komplett neue Fertigungstechnologie bei TSMC (Taiwan Semiconductor Manufacturing Company), erläutert Hilscher. "Ein wesentlicher Punkt ist, dass wir keinen externen Speicher mehr benötigen, da er nun komplett integriert ist. Ein weiterer großer Vorteil ist die nun deutlich geringere Verlustleistung: Wir kommen mit den integrierten Ethernet PHYs auf eine Verlustleistung von unter einem Watt. Die geringere Abwärme und der geringere Verbrauch erschließen wieder neue Anwendungsfelder für Gerätebauer und Endanwender.

ZWEIKERN-TECHNOLOGIE TRENNT KOMMUNIKATION UND ANWENDUNG. Eine wesentliche Neuerung im netX 90 ist die Verwendung eines Zwei-Core-Systems, d.h. eine ARM-CPU arbeitet für die Kommunikationsseite und eine weitere ARM-CPU für die Applikationsseite. Sebastian Hilscher erläutert: "Für die Kommunikationsseite bieten wir von Hilscher auch die komplette Softwareinfrastruktur, das heißt die ganzen Protokollstacks, das Betriebssystem und vieles mehr als fertiges Binary. Der Kunde hat für seine Applikation einen kompletten ARM-Core für sich zur Verfügung und kann dort machen, was er möchte, ohne, dass sich die Prozesse gegenseitig auf der Hardware beeinflussen können. Das ist ein großer Vorteil im Vergleich zu den Vorgängern. Es



Blockschaltbild des Multiprotokoll-Chips netX 90

sind wirklich zwei getrennte Welten. Mit der verdoppelten Kernzahl ist natürlich auch eine erhebliche Leistungssteigerung des SoC verbunden. "In Bezug auf die generelle Geschwindigkeit der CPU", erklärt uns Sebastian Hilscher, "gehen wir von einer 2,8- bis 3-fachen Performance-Steigerung aus."

FIT FÜR INDUSTRIELLE IOT-ANWENDUNGEN. Doch netX 90 ist viel mehr als eine deutlich verbesserte Version der bisherigen netX-Serie. Vielmehr macht Sebastian Hilscher klar, dass der neue Chip die Plattform für völlig neue Geräteklassen ist, die das industrielle Internet der Dinge bedienen: "Der netX 90 kann, wie die bisherigen netX-Chips auch, als ganz normaler Companion-Multiprotokoll-Chip verwendet werden, falls man eine CPU zur Verfügung hat, auf der die Applikation bereits läuft. Er macht dann einfach nur die Kommunikation, aber er kann eben viel mehr als das: Er ist unsere Plattform für das IIoT, für das Automatisierungshersteller heute ihre Geräte konzipieren müssen. Dafür unterstützt der neue Chip sowohl OPC UA als auch MQTT und wir sind aktiv an der Open-Source-Variante von OPC UA beteiligt."

PARALLELE PFADE. netX 90 macht also die Feldkommunikation und die übergeordnete Kommunikation z.B. bis in die Cloud mit einem einzigen Gerätechip möglich. Doch ist das überhaupt sinnvoll? Hilscher dazu: "Was wir sehen, ist, dass gerade im Bereich IIoT nicht mehr nur die ganzen Prozessdaten per Steuerung übertragen werden, sondern eben parallele Pfade aufgebaut werden, d.h. man hat einmal den Pfad für die Steuerung vor Ort über Profinet, über Ethernet/IP, Ethercat usw. Daneben wird für übergeordnete Dinge noch ein paralleler Pfad über OPC UA betrieben, beispielsweise zu Cloud-Plattformen. Hier findet dann die Kommunikation für größere Diagnosen und weiteren Mechanismen und Funktionalitäten statt. Das sind heute häufig Ansätze, die helfen sollen, Prozesse oder die Performance zu optimieren.

SECURITY INTEGRATED. Gerade in industriellen Kommunikationsprozessen kommt es heute mehr denn je auf Security an, erläutert Hilscher und das wurde dementsprechend auch im netX 90 berücksichtigt: "Zum einen haben wir uns angeschaut, was für OPC UA als Security-Funktionalitäten definiert wurde. Für diese Security-Funktionalitäten haben wir im netX 90 heute bereits eine entsprechende Hardwarebeschleunigung eingebaut, damit die Verlustleistung auf dem geringen Niveau bleibt. Neben dieser Hardwarebeschleunigung haben wir im ROM-Code schon die Zertifikation der Firmware integriert. D.h. ich kann heute dem netX 90 vorgeben, dass das Gerät prüft, ob die Software, die auf dem netX läuft, signiert ist. Auf einem netX 90 kann dann wirklich nur vom Kunden signierte Software laufen und man hat nicht mehr die Möglichkeit, irgendeine andere Software aufzuspielen. Diese Funktion wurde in diversen Security-Levels integriert, beispielsweise sorgt Security Level 3 dafür, dass das komplette Debugging abgeschaltet wird." Aber auch die Entwicklungsprozesse im Hause Hilscher selber hätten sich im Hinblick auf die Security-Problematik in den vergangenen Jahren deutlich verändert: "Kunden möchten dort früh informiert werden, wenn es Probleme gibt", erklärt Hilscher. "Sie möchten auch selbst Probleme melden können und wir müssen dafür gewisse Reaktionszeiten einhalten. D.h., wenn ein Kunde ein Security Issue meldet, müssen wir in definierter Reaktionszeiten darauf reagieren.

STAND DER ENTWICKLUNG UND AUSLIEFERUNGSTERMIN. Der netX 90 steht kurz vor seiner Auslieferung, erläutert Sebastian Hilscher. "Genauer gesagt, haben wir den Chip heute schon bei uns im Hause, die ersten Bauteile sind gerade in Verifikation für den Final Chip. Der Plan ist die Entwicklungsboards und die ganzen Starterkits zum 1. November dieses Jahres verfügbar zu haben, auch für unseren Online-Shop. Also nochmal: Der 1. November ist zunächst das Datum für die Entwicklungsboards. Für die große Masse wird es dann allerdings noch bis nächstes Jahr Januar dauern, bis Stückzahlen verfügbar sind. Dann können wir den Chip wirklich in breiter Masse in den Markt streuen und unsere Kunden können mit der Serienfertigung beginnen. *(kbn)* ■

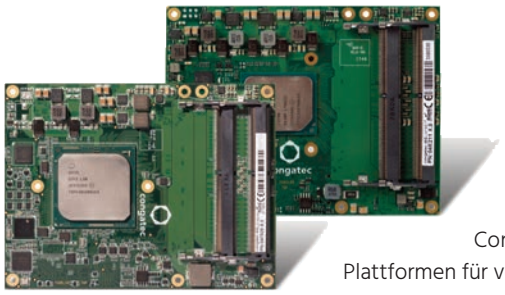
www.hilscher.com

hilscher
COMPETENCE IN COMMUNICATION

Über Hilscher

Die Kernkompetenz von Hilscher ist die Technologie, Entwicklung und Produktion von industriellen Kommunikationslösungen für die moderne Fabrikautomation. Die Produkte von Hilscher reichen von PC-Karten, Gateways über OEM-Aufsteckmodule bis hin zu leistungsfähigen Asics mit den dazugehörigen Protokollstacks. Diese werden weltweit zur Kommunikation zwischen Automatisierungsgeräten und Steuerungen eingesetzt – bei PC-Karten ist Hilscher in diesem Bereich der Marktführer. Ein derart umfassendes Lösungsportfolio für Feldbusse und Real-Time-Ethernet ist das Alleinstellungsmerkmal von Hilscher. Hilscher bietet auch die netX-Technologie für Gerätehersteller an, inklusive Entwicklungsdienstleistungen und kundenspezifischer Baugruppenfertigung. In diesem Bereich

ist Hilscher nicht nur anerkannter Systempartner der großen Hersteller, sondern zählt auch eine Vielzahl von Ingenieurbüros, Lösungsanbietern und Systemintegratoren zu seinen Kunden. Außerdem ist Hilscher in allen Feldbus- und Real-Time-Ethernet-Organisationen vertreten.



Mehr Rechenleistung für vernetzte Flugzeuge

Congatec präsentierte auf der Aeromart Toulouse 2018 seine neuen modularen Luftfahrt-Computing-Plattformen für vernetzte Flugzeuge, Passagier-Infotainment und Augmented-Reality-Applikationen. Die neuen COM Express Type 7 Server-on-Module wurden für konvergente Edge-Server in Flugzeugen entwickelt und sind ideal für Content-Delivery an Seatback-Displays und Mobilgeräte der Fluggäste, für Predictive Maintenance und andere Big-Data-Applikationen, sowie Videoüberwachung und cloudbasierte Flugschreiber. Die Plattformen eignen sich auch für Augmented-Reality-Applikationen in der Luftfahrt, um die Navigationsfähigkeiten bei schlechter Sicht zu optimieren. Sie lassen sich auch für KI-basierte, virtuelle Assistenten nutzen, um sowohl die Produktivität und Effizienz von Piloten, als auch das Flugerlebnis der Passagiere zu verbessern.

Congatec AG, www.congatec.com

Aris-Edge-Board mit NarrowBand-IoT-Technologie

Mit der Integration eines NB-IoT-Shields hat Arrow seine flexible Aris-Edge-Plattform (Arrow Renesas IoT Synergy) zur Entwicklung von IoT-Geräten um eine zusätzliche Komponente erweitert. Das von Shiratech entwickelte Shield verfügt über ein Quectel-BG96-Modul und wird auf das – auf dem energieeffizienten Renesas Synergy S3A3 Mikrocontroller basierenden – Aris-Edge-S3-Board gesteckt. Die Kombination dieser beiden Boards ermöglicht Anwendern eine einfache und schnelle Evaluierung von Sensordaten-Funkübertragungen (je nach Netzwerkverfügbarkeit via 2G/3G, NB-IoT oder CAT-M1) an die Azure-Cloud. Das Shield hat einen Arduino-Formfaktor, ein low-power Quectel BG96 LTE CAT-M1 & NB-IoT-Modem, integriertes GPS sowie eine Antenne. Unterstützt werden Downloads bis zu 300kBit/s und ein Upload von max. 375kBit/s. Darüber hinaus verfügt das Funkmodul über Bluetooth Low Energy (4.1/4.2), Thread und ZigBee-Stacks.

Arrow Central Europe GmbH, www.arrowce.com

Bild: ©Kzenon / Fotolia.com

Der Hersteller als Dienstleister

TEXT: Andreas Dangl, Business Unit Executive für Cloud-Services, Fabasoft Deutschland GmbH

Seit einigen Jahren ist zu beobachten, dass sich vor allem innovative produzierende Betriebe nach und nach vom klassischen Produktverkauf zum Lösungsanbieter weiterentwickeln. Der reine Fokus auf die Produktion schwindet, während der Servicegedanke und der Kundennutzen weiter in den Mittelpunkt rücken. Weltweit erfolgreiche B2C-Unternehmen wie Uber oder Airbnb zeigen, dass digitale und kundenorientierte Geschäftsmodelle hohes disruptives Potenzial bieten und dadurch ganze Branchen revolutionieren können. Wer erfolgreich sein möchte, der muss sein Geschäftsmodell an die sich ändernden Umweltbedingungen anpassen. Die Fähigkeit, innovative Geschäftsmodelle zu entwickeln, ist zu einer Grundvoraussetzung für die langfristige Wettbewerbsfähigkeit geworden.

Geschäftsmodell Servitization

Servitization beschreibt den Wandel eines Unternehmens vom reinen Produzenten hin zu einer Kombination aus Hersteller und Dienstleister. Ein Beispiel dafür ist der britische Flugzeugturbinenhersteller Rolls-Royce. Bei seinem ‘Power by the hour’-Angebot bezahlen Fluglinien für die Dienstleistung, die das Triebwerk erbringt. Das eigentliche Produkt bleibt Eigentum des Herstellers. Das Unternehmen ist somit über die gesamte Lebensdauer der Turbine für Überwachung, Wartung und Instandhaltung zuständig. Daraus ergeben sich große Vorteile für die Fluglinien: Kapitalausgaben werden zu Betriebsausgaben, finanzielle Risiken werden reduziert, sie erhalten Zugriff auf innovative Technologien und können sich vermehrt auf ihr Kerngeschäft konzentrieren. Rolls-Royce gelingt es

durch die Abrechnung der Flugstunden, konstante Umsatzströme zu generieren sowie die Kosten zu senken. Auch änderte sich die Haltung der eigenen Mitarbeiter: Während früher mit Wartung direkter Umsatz generiert wurde, entwickelten sich bei dem neuen Geschäftsmodell wartungsarmen Turbinen zum obersten Ziel. Der Zielkonflikt zwischen Hersteller und Kunde entfällt, da es nun im Interesse von Rolls-Royce liegt, dass die eigenen Geräte effizient und einwandfrei funktionieren.

Sensorik und Datenanalyse

Möglich wurde dies alles durch ein Überwachungssystem der Triebwerke. Cyberphysische Sensoren übermitteln in Echtzeit die Betriebsdaten an die Zentrale, wo sie überwacht und beurteilt werden können. Das Sammeln der Daten bildet somit die Basis für die Verrechnung mit der Fluglinie. Durch die Analyse des Verhaltens der Turbinen sammelte Rolls Royce zudem Informationen für die Weiterentwicklung der Turbinen.

Bessere Produkte und Services

Die für die Analyse notwendigen cyber-physischen Systeme (CPS) sind vernetzte Systeme, die reale Objekte und Prozesse beobachten und ebenso beeinflussen können. Sie finden sich dort, wo hochkomplexe, physische Systeme durch die Kommunikation mit der digitalen Welt effektiver werden können. So werden unter anderem selbstständig arbeitende Produktionssysteme mit Fernüberwachung möglich. Durch das Sammeln und Auswerten einer großen Datenmenge erfahren Hersteller, wie ihre Kunden die Produkte bedienen und können sowohl Service als auch das Kundenerlebnis optimieren. CPS helfen also bei der Verbesserung von Produkten und Service. Die Eigenschaften von CPS stellen allerdings Anforderungen an die IT-Infrastruktur.

Hohe Ausfallsicherheit

Laut dem deutschen 'Competence Center for Cyber Physical Systems' können Public Clouds diese Anforderungen erfüllen und durch ihre Funktionalitäten quasi ein CPS-Rückgrat bilden. Sie bieten unterschiedliche IT-Ressourcen wie Rechenzeit, Speicher, Anwendungen, Dienste oder auch Daten dynamisch an und verwalten diese gleichzeitig. Darüber hinaus wird ihnen eine hohe Ausfallsicherheit zugeschrieben und sie bieten im Bedarfsfall zusätzliche Leistungen. Dabei fungiert die Cloud als zentrale Datensammelstelle für Business Analytics, Machine Learning und Prozesssteuerung. Somit wird der für Servitization notwendige Datenaustausch mit externen Partnern ermöglicht. Durch die Überwachung der kompletten Lieferkette von Dienstleistungen, kann dem Kunden individualisierter Service geboten werden.

Der passende Cloud Provider

Bei der Auswahl eines Anbieters können sich Unternehmen unter anderem an Zertifikaten orientieren. Dabei empfiehlt es sich, auf eine europäische Business-Cloud zu setzen, die regelmäßig von unabhängigen, externen Prüfstellen untersucht und zertifiziert wird. Wenn es um Datensicherheit und Datenschutz geht, ist insbesondere auf das C5-Testat des deutschen Bundesamts für Sicherheit in der Informationstechnik zu achten. Weltweit erfüllen nur neun Cloud Provider die Anforderungen des Testats, der österreichische Cloud-Anbieter Fabasoft war das erste europäische Unternehmen.

Fokus auf den Kundennutzen

Produzierende Betriebe, die sich ihre Wettbewerbsfähigkeit für die Zukunft erhalten wollen, sollten sich am Markt auch als Dienstleister positionieren. Der Umstand, dass ein Unternehmen selber produziert und somit über die Möglichkeit verfügt, wichtige Daten zu sammeln, die einem Reseller nicht zur Verfügung steht, lässt sich zur Differenzierung gegenüber Mitbewerbern einsetzen. Noch wichtiger als der Fokus auf das Geschäft ist der Fokus auf den Nutzen des Kunden - und auch den Kunden des Kunden. Dann stiftet das Sammeln von Produktionsdaten einen echten Mehrwert. Das zentrale Tool für den wirklich sicheren Austausch von Daten sind nach höchsten Standards zertifizierte europäische Cloud-Lösungen, da dort sensible Daten auch ausreichend geschützt sind. ■

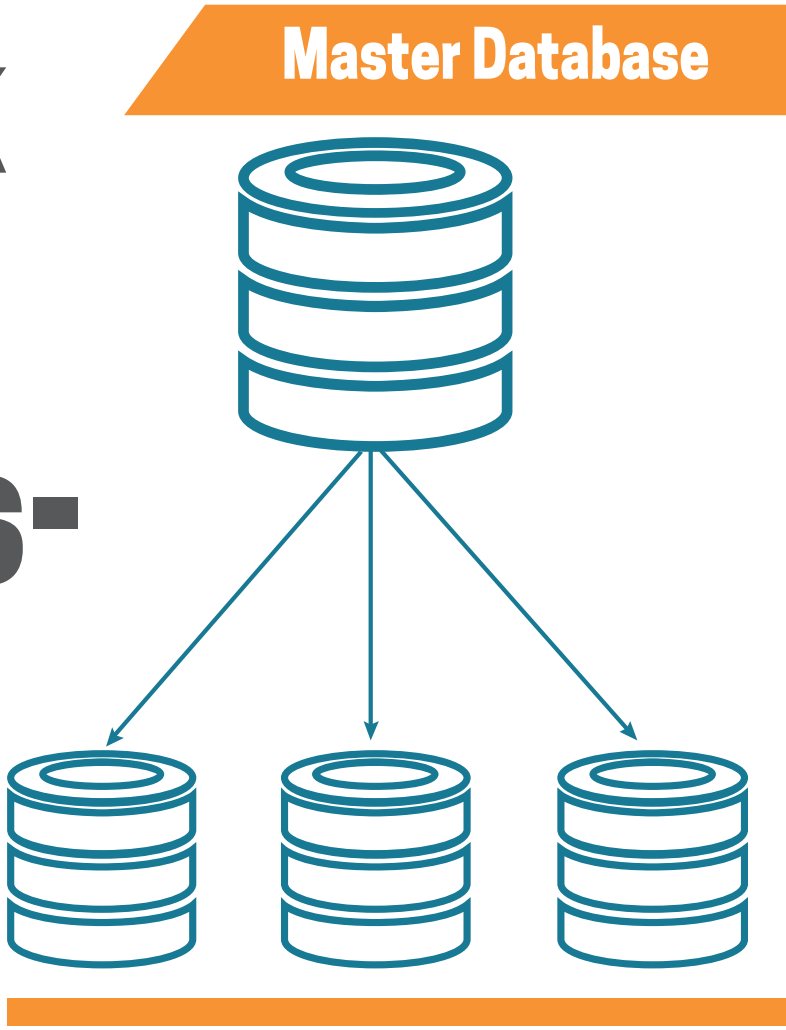
www.fabasoft.com/de

Bild: ©Kzenon / Fotolia.com

Der passende Service

Durch Überwachung der kompletten Lieferkette können dem Kunden individuelle Lösungen geboten werden.

Das Glück kurzer Reaktionszeiten



Relationale Datenbanksysteme und die meisten NoSQL-Datenbanksysteme basieren auf Master-Slave-Architekturen.

Unternehmen müssen heute kundenorientierter arbeiten und in der Lage sein, Innovationen schnell auf den Markt zu bringen. Dabei müssen Applikationen hohe Ansprüche an Verfügbarkeit und Performance erfüllen. Ausfallzeiten kann sich niemand leisten, denn die Kundenerwartungen sind hoch. All das erfordert eine flexible, skalierbare IT-Umgebung.

TEXT: Amit Chaudry, VP Product Marketing bei DataStax
BILDER: DataStax

Um den unterschiedlichen, wechselnden Anforderungen gerecht zu werden, geht der Trend dahin, mehrere Clouds zu kombinieren. Ob eine Hybrid Cloud aus Public Cloud und Private Cloud oder gar verschiedene Public Clouds – laut einer aktuellen Studie von 451 Research in 14 europäischen Ländern setzen bereits 84 Prozent der Unternehmen eine Kombination aus verschiedenen Cloudumgebungen ein. Mit Big Data Analytics und IoT setzen sich zudem Technologien durch, die ein exponentiell wachsendes Datenvolumen und viele verschiedene Datentypen mit sich bringen. Während es Unternehmen früher vorwiegend mit strukturierten Daten zu tun hatten, die man erst sammeln und dann an einer zentralen Stelle analysieren konnte, fließt heute ein kontinuierlicher Strom an unterschiedlichen Datentypen aus IoT-Systemen oder Smartphone-Applikationen herein, z.B. Maschinendaten, Videostreams, Social-Media-Beiträge oder Kundeninformationen. Diese treten an verschiedenen Stellen auf und müssen oft sofort ausgewertet werden.

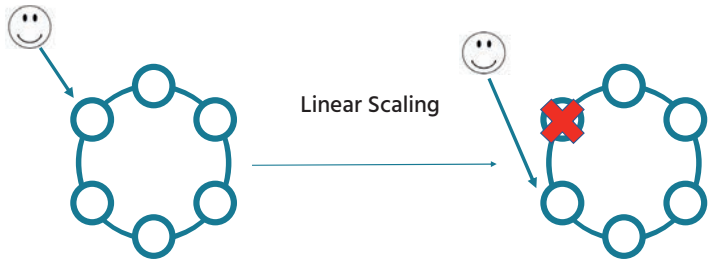
Relationale Datenbanken stoßen an ihre Grenzen

Sowohl die Hybrid- und Multi-Cloud-Umgebung als auch die veränderte Datenlandschaft stellen neue Anforderungen an das Datenmanagement. Mehr als ein halbes Jahrhundert waren relationale Datenbankmanagement-Systeme das führende Modell. Sie wurden für zentralisierte Workloads designt, eignen sich perfekt für strukturierte Daten und sind äußerst zuverlässig. Dieses Modell ist jedoch nicht mehr zeitgemäß, denn heute arbeiten Unternehmen mit verteilten Workloads und müssen riesige Mengen von teils unstrukturierten Daten speichern und analysieren. Zunehmend haben sich daher NoSQL-Datenbanken durchgesetzt, kurz für 'Not only SQL'. Sie wurden dafür konzipiert, große Volumen an verteilten und auch unstrukturierten Daten in Echtzeit zu verarbeiten, ohne dass man sich dabei Sorgen um Ausfallzeiten machen muss. NoSQLs versprechen horizontale Skalierbarkeit und eine

höhere Verfügbarkeit als relationale Datenbanken. Das reicht jedoch nicht aus, denn was Unternehmen heute brauchen, ist kompromisslose Performance und Hochverfügbarkeit. Hier stoßen auch die meisten NoSQL-Datenbanken an ihre Grenzen.

Das Master-Slave-Problem

Viele NoSQL-Datenbanken basieren ebenso wie SQL-Datenbanken auf einer Master-Slave-Architektur. Solche Systeme verfügen über einen Master, auf dem die Datenbank läuft, und Slaves, die mit dem Master verbunden sind. Auf den Slaves können Datenbankabfragen durchgeführt werden, aber nur der Master kann Daten schreiben. Er steuert zudem alle Datenbanktransaktionen und gibt den Slaves Anweisungen, was sie tun sollen. Eine Master-Slave-Architektur lässt sich skalieren, indem man weitere Slaves hinzufügt. Dadurch kann die Datenbank zwar mehr lesende Zugriffe gleichzeitig abarbeiten, alle schreibenden Aktionen und die Steuerung laufen jedoch weiterhin über den einen Master. Fällt er einmal aus, funktioniert das gesamte System nicht, bis ein neuer Master aufgesetzt ist. Um das zu vermeiden, setzen viele Datenbankkonzepte mehrere Master ein. Doch auch das kann das Problem nur bedingt lösen. Denn mit mehreren Mastern gibt es schlichtweg mehr Punkte, an denen die Datenbank ausfallen kann. Hochverfügbarkeit garantiert dies nicht. Gerade in verteilten Netzwerken wie der Hybrid Cloud sind Master-Slave-Architekturen außerdem äußerst komplex umzusetzen.



Fällt in einer Active Everywhere Database ein Knoten aus, wird der Datenverkehr automatisch an einen anderen geleitet. Das garantiert Hochverfügbarkeit in verteilten Netzwerken.

Die Lösung: NoSQL-Datenbank mit No-Master-Architektur

Ein neuer Ansatz für das Datenbankmanagement ist gefragt, der für Hochverfügbarkeit in verteilten Netzwerken sorgt. Dies gelingt mit einer Active Everywhere Database. Dabei handelt es sich um eine NoSQL-Datenbank, die ohne Master auf Basis von Apache Cassandra aufgebaut ist. Jeder Knoten im Cluster ist identisch, autonom und kann sowohl lesende als auch schreibende Transaktionen ausführen. Fällt ein Knoten aus, wird der Datenverkehr automatisch an einen anderen geleitet. Dieser übernimmt die Anfrage nahtlos, ohne dass dafür Code geändert werden muss. Es kommt zu keinerlei Performance-Einbußen. Sobald der ausgefallene Knoten wieder einsatzbereit ist, werden die Daten automatisch mit den anderen Knoten synchronisiert. Ein solches System ist ganz einfach skalierbar, indem man weitere Knoten hinzufügt. Außerdem lässt es sich problemlos auf verschiedene Clouds und Rechenzentren verteilen. Damit gewinnen Unternehmen einen weiteren Vorteil: Sie sind in der Lage, Datenbanken ganz nach Bedarf von einer Cloud in eine andere oder aus dem Rechenzentrum in die Cloud zu verschieben. Dadurch gewinnen sie mehr Flexibilität und machen sich nicht von einem Anbieter abhängig. Bietet ein anderer Provider ein günstigeres Angebot, können sie ohne großen Aufwand wechseln.

Fazit

Um wettbewerbsfähig zu bleiben, müssen Unternehmen heute in der Lage sein, riesige Mengen an Daten unterschiedlicher Typen zu verarbeiten. Dabei nutzen sie zunehmend Hybrid-Cloud- oder Multi-Cloud-Umgebungen. Das erfordert ein Datenbankmanagement, das sich für strukturierte und unstrukturierte Daten in verteilten Netzwerken eignet und dabei Hochverfügbarkeit garantiert. Mit einer Active Everywhere Database können Unternehmen Daten beliebig auf verschiedene Public Clouds und On-Premise-Infrastrukturen verteilen. So stehen die Daten jederzeit am richtigen Ort in der geforderten Geschwindigkeit zur Verfügung, um einen reibungslosen Betrieb von Anwendungen und ein positives Kundenerlebnis sicherzustellen. ■

www.datastax.com

Amit Chaudry, VP Product Marketing bei DataStax:

„Sowohl die Hybrid- und Multi-Cloud-Umgebung als auch die veränderte Datenlandschaft stellen neue Anforderungen an das Datenmanagement. Mehr als ein halbes Jahrhundert waren relationale Datenbankmanagement-Systeme das führende Modell. Dieses Modell ist jedoch nicht mehr zeitgemäß, denn heute arbeiten Unternehmen mit verteilten Workloads und müssen riesige Mengen von teils unstrukturierten Daten speichern und analysieren."

Bild: ©jamesteohart / istockphoto.com

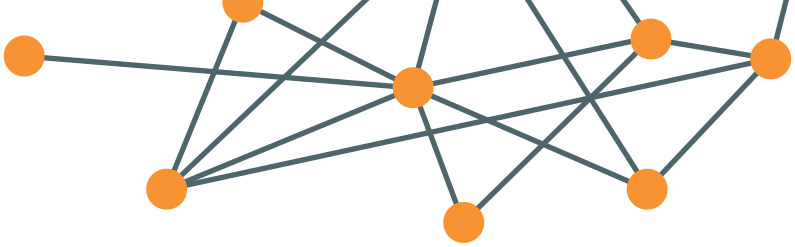
Traditionelle Netzwerksicherheit auf den 4day stellen

TEXT: Sascha Kremer, Director Carrier Development bei Cradlepoint Deutschland

Die nächste Mobilfunkgeneration 5G steht auf der Türschwelle. Aktuell rüsten die Carrier ihre LTE-Mobilfunknetze auf der ganzen Welt mit neuen Frequenzbändern und fortschrittlichen Funktechnologien auf. 5G wird enorme Veränderungen in den Mobilfunknetzen mit sich bringen, darunter größere Bandbreiten im Hochfrequenzbereich, das so genannte 'Millimeter Wave', geringere Latenzen, Network Slicing sowie eine wesentlich größere Verbindungsdichte. Insbesondere die Verbesserungen in den drei Bereichen Latenz, Übertragungsgeschwindigkeit und Verbindungsdichte werden einen signifikanten Einfluss auf bestehende Security-Architekturen haben. Müssen wir unsere Netzwerke besser absichern? Diese Frage allein reicht nicht, denn einen 'besseren' Job zu machen, ist nicht mehr gut genug. Es braucht neue Ansätze in puncto Netzwerksicherheit.

Veränderungen auf allen Ebenen des Netzwerks

5G wird sehr häufig mit einem höheren Datendurchsatz in Verbindung gebracht. Und in vielen Fällen ist das richtig. Tatsächlich haben einige 5G-Studien Datenraten von mehreren Gigabit pro Sekunde demonstriert, in einem Fall sogar 32GBit pro Sekunde. Das sind Größenordnungen, die aus heutiger Perspektive kaum vorstellbar sind. Und obwohl dies nicht der reale Durchsatz an jedem Endpunkt ist, stellt 5G doch enorme Anforderungen an die Netzwerkinfrastruktur, etwa an die Schaltkreise in Sicherheitsvorrichtungen im Rechenzentrum oder an die Konzentratoren, die mal eben das Zehnfache des Verkehrs bewältigen müssen. Latenzverbesserungen sind ebenfalls ein großer Fortschritt von 5G. Die meisten 4G-Verbindungen ermöglichen eine Latenzzeit von unter 100 Millisekunden pro Roundtrip, sehr oft sind auch Latenzzeiten von unter 50 Millisekunden möglich. Das Designziel des 5G-Standards ist eine Millisekunde. Hier beißt sich der



Hund in den Schwanz. Denn das typische Sicherheitsmodell einer VPN-Verbindung leitet den Datenverkehr vom Endpunkt zu einem zentralen Konzentrator, dann zum Zielserver (heutzutage oft im Internet), dann zurück zum Konzentrator und dann zurück zum Endpunkt. Je nachdem, wo sich diese drei Elemente (Endpunkt, Konzentrator, Zielserver) befinden, müssen zu jeder Transaktion Dutzende, wenn nicht gar Hunderte von Millisekunden hinzugefügt werden. Mit dem Datenhunger mobiler, verteilter oder weit entfernter Anwender und Applikationen geht das kaum überein. 5G ist auch für das Handling von vielen Geräten ausgelegt. Genauer gesagt: Sehr viele Endgeräte. Über IoT wird seit Jahren gesprochen. Aber in Wirklichkeit haben wir gerade erst begonnen. Gartner schätzt die aktuelle Zahl der IoT-Geräte auf rund 8,4 Milliarden, und prognostiziert 21 Milliarden bis 2020. Das ist das Zweieinhalbfache an Geräten im Vergleich zu heute – in nur zwei Jahren! Viele dieser IoT-Geräte sind keine üblichen IT-Endpunkte wie PC, Tablet oder Smartphone, für die herkömmliche Security- und VPN-Clients verfügbar sind. Manche dieser Geräte greifen auf Container oder IoT-Dienste in der Cloud zu. Spätestens jetzt stellen sich Security-Profis die Haare auf. Denn Sicherheit in IoT-Netzwerken nach aktuellem Anspruch kann mit den traditionellen IT-Sicherheitsmodellen nicht erreicht werden. Sicherheitsexperten warnen seit langem vor diesen kleinen, aber weit offenen Hintertürchen in Unternehmensnetze.

SD-Perimeter: Security upside down

Um gänzlich zu verstehen, warum wir die Netzwerksicherheit in der IoT-Ära überdenken müssen, führen wir uns die Entwicklung der traditionellen Netzwerksicherheit in den letzten zwei Jahrzehnten vor Augen. Wie das Internet wurden auch Unternehmensnetzwerke so konzipiert, dass sie sich zuerst verbinden und später Fragen stellen. Darüber hinaus wurden sie mit einem zusammenhängenden oder routingfähigen Adressraum erstellt, der es einem Endpunkt ermöglicht, jeden anderen Endpunkt im Netzwerk zu erreichen. Dieser Ansatz erforderte, dass Netzwerkadministratoren ein 'Filter-out'-Sicherheitsparadigma überlagern, um den Zugriff und den Datenfluss zwischen bestimmten Benutzern, Ressourcen und Geräten zu beschränken. Diese Konventionen haben sich recht gut bewährt, um relativ statische Netzwerke mit Tausenden von Endpunkten zu 'segmentieren'. In der Welt der IoT-Netzwerke, des Edge-Computing und der umfassenden Verfügbarkeit breitbandiger, drahtloser Pop-Up-Verbindungen nehmen das Volumen und die Vielfalt der Endpunkte massiv zu – daher auch der Begriff 'Massive IoT'. Und diese Endpunkte verändern sich ständig. Hunderttausende oder sogar Millionen von Geräten in einem Unternehmensnetzwerk sind keineswegs eine Illusion in weiter Ferne. Das Szenario ist sehr real, genauso wie die möglichen Bedrohungen. Als Antwort auf dieses ernste Security-Problem müssen wir das traditionelle Unternehmensnetzwerkmodell auf den Kopf stellen, Netzwerkfunktionen in die Cloud verlagern und Software nutzen, die das Internet überlagert. Dieser sogenannte 'Cloud Networking'-Ansatz, auch 'Software-Defined Perimeter' (SD-Perimeter) genannt, ermöglicht es Netzwerkverantwortlichen, ein Perimeter-gesichertes, virtuelles Netzwerk bereitzustellen, das sozusagen über dem Internet schwebt. Dieses Netzwerk ist für die Außenwelt vollständig 'getarnt'. Schließlich kann man nichts angreifen, was man nicht adressieren kann. Anstatt sich zuerst zu verbinden und sich zu authentifizieren, verhalten sich SD-Perimeter-basierte IoT-Netzwerke wie geschlossene Benutzergruppen. Bevor sich ein Gerät verbinden kann, benötigt es eine Einladung aus diesem Netzwerk. Aus Sicht der Gerätesegmentierung und -isolierung wird die langwierige und anfällige Filter-out-Methodik traditioneller Unternehmensnetzwerke durch die Möglichkeit ersetzt, verschiedene virtuelle Overlay-Netzwerke für jede Geräteklasse zu bilden, die voneinander getarnt sind. So sind etwa sauber und übersichtlich voneinander getrennte Netze für Überwachungskameras, Sensoren oder Stellglieder denkbar. Sollte beispielsweise ein Angriff auf eine Überwachungskamera stattfinden, können die Cyberkriminellen nicht in andere Teile des Netzwerkes und zu anderen Geräten vordringen.

Moderne CIOs schneiden alte Zöpfe ab

IT-Trends wie 5G, Edge Computing, IoT und Software-Defined Networking krempeln die Netzwerkinfrastruktur von Unternehmen sprichwörtlich um. Traditionelle Security-Modelle müssen daher ebenso auf den Kopf gestellt werden, im wahrsten Sinne des Wortes. Moderne CIOs erkennen, dass die Sicherheit in der aufstrebenden vernetzten Wirtschaft einen neuen Ansatz zur Verbindung und zum Schutz von Menschen, Orten und Dingen erfordert. ■

www.cradlepoint.com

Das Vertrauen wiederherstellen

Bild: © artinspiring / Fotolia.com

Privilegierte Zugriffskonten sind für Hacker ein beliebtes, weil leichtes Angriffsziel. Als häufigsten Grund dafür nennen Sicherheitsexperten **leichtfertiges und überholtes Passwortmanagement administrativer Konten.** Dies schürt nicht nur beim Kunden mangelndes Vertrauen. Dabei lässt sich dieses mit Software leicht wieder aufbauen.

TEXT: Martin Grauel, EMEA Technical Sales Manager, One Identity

Cybersicherheit als solche und insbesondere der Schutz von vertraulichen Daten waren vielleicht nie wichtiger als gerade jetzt. Die allgemeine Aufmerksamkeit richtet sich inzwischen sehr viel stärker auf das Thema. Die Risiken sind höher denn je. Kein Unternehmen, keine Organisation kann sich mehr hinter einer magischen 'BlackBox' verschanzen, die im Hintergrund sämtliche Sicherheitsvorkehrungen übernimmt. Ohne konzertierte Aktion wird es nicht gehen, und die betrifft Menschen, Prozesse und Technologien zu gleichen Teilen. Tatsächlich haben Identity und Access Management sowie das Privileged Access Management (abgekürzt IAM und PAM) einen großen Anteil an den Sicherheitsbemühungen eines Unternehmens. Das hat einen Grund. Privilegierte Konten betreffen die wichtigsten Daten einer Firma, Benutzer dieser Konten können auf höchst vertrauliche Informationen zugreifen. Es ist also entscheidend, dass wirklich nur die Nutzer auf genau die Daten zugreifen, die sie brauchen, um die mit ihrem Job verbundenen Aufgaben zu erledigen. Und nur auf diese Daten und nicht etwa auf sämtliche sensible Informationen eines Unternehmens. Erst das Zusammenspiel von übergreifender Governance, dementsprechenden Praktiken und Richtlinien, gewährleistet überhaupt mit Cyberangriffen Schritt halten zu können. Eine erst kürzlich durchgeführte Befragung von über 1.000 mittelständischen und großen Unternehmen liefert allerdings eher alarmierende Befunde. Beinahe ein Drittel der befragten Organisationen verlässt sich beispielsweise bei der Passwortverwaltung auf inzwischen völlig überholte manuelle Ansätze wie etwa Excel-Tabellen. Weitere 75 Prozent der IT-Sicherheitsexperten räumen ein, Passwörter zumindest ab und zu mit Kollegen zu teilen, und ein Viertel der Befragten tut dies üblicherweise oder sogar immer. Und auch was das Vergeben und Entziehen von Zugriffberechtigungen angeht, stimmen die Studienergebnisse nicht gerade optimistisch. Firmen brauchen für die komplette Provisionierung bzw. Deprovisionierung eines Benutzers Zeiträume von mehreren Tagen (44 Prozent) bis in einigen Fällen hin zu mehreren Wochen (32 Prozent). Die erschreckende Zahl von 77 Prozent von IT-Sicherheitsexperten gab zu, dass es für sie vergleichsweise einfach wäre sensible Daten zu stehlen, sollten sie die Firma verlassen. Vor dem Hintergrund dieser Ergebnisse betrachtet überrascht es dann schon weit weniger, dass stolze 87 Prozent der im Rahmen der Studie Befragten den PAM-Programmen ihres eigenen Unternehmens nicht vollständig vertrauen. Schlechtes Identity und Access Management kann in Kombination mit mangelhaften Sicherheitspraktiken zu schwerwiegenden Unterbrechungen der Geschäftsabläufe und Datenschutzvorfällen führen. Kein Un-

ternehmen kann sich heutzutage Sicherheitsschwachstellen leisten. Ebenso wenig wie einen Serviceausfall. Effektive IAM- und PAM-Programme sind eine wichtige Komponente um Cyberrisiken zu minimieren. Genauso tragen IAM und PAM dazu bei, die Sicherheitsbelange anderer Unternehmen zu verbessern. Die Studienergebnisse enthüllen, dass etliche Unternehmen weltweit aber genau daran scheitern. Selbst wenn es um grundlegende Best Practices und Sicherheitsmaßnahmen sowohl beim Identity und Access Management als auch bei der Verwaltung privilegierter Konten geht.

Bessere Methoden für IAM und PAM

Anmeldeinformationen zu stehlen ist für böswillige Akteure einer der simpelsten Wege sich Zugang zu einem Unternehmensnetzwerk zu verschaffen. Am begehrtesten ist der Zugriff auf privilegierte (administrative) Konten. Diese Konten verschaffen einem Eindringling nahezu unbegrenzten Zugriff auf die Infrastruktur eines Unternehmens, eingeschlossen die wichtigsten und vertraulichsten Systeme und Daten. Je mehr Konten für einen Angreifer verfügbar sind, desto größer der potenzielle Schaden. Dazu gehören Datenschutzverletzungen und das Offenlegen von Daten, der Verstoß gegen Compliance-Richtlinien, Strafen sowie Vertrauensverlust des Unternehmens bei seinen Kunden und Rufschädigung.

Das empfehlen die Experten

1 PASSWÖRTER FÜR PRIVILEGIERTE KONTEN NACH JEDEM KONTOZUGRIFF ZURÜCKSETZEN: Damit begrenzen Sie das gemeinschaftliche Nutzen von administrativen Anmeldeinformationen. So sind vertrauliche Unternehmensdaten um ein Vielfaches besser geschützt als über statische und wieder verwendbare Passwörter.

2 NICHT MEHR AKTIVE BENUTZERKONTEN SOFORT DEPROVISIONIEREN: Mitarbeiter wechseln die Firma, werden entlassen oder Stellen anderweitig besetzt – als ganz natürlicher Teil unternehmerischer Lebenszyklen. Es sollte ein ebenso natürlicher Bestandteil dieser Lebenszyklen sein, nicht mehr gültige Zugriffsberechtigungen auf das Firmennetzwerk unverzüglich zurückzurufen. Selbst, wenn Mitarbeitende sich im Guten von ihrer Firma getrennt haben, ist es das Risiko nicht wert schlummernde Konten über einen langen Zeitraum hinweg beizubehalten. Nicht zuletzt können sich auch Hacker solcher nicht mehr aktiv genutzter Konten bemächtigen.

3 BENUTZERPASSWÖRTER SCHNELL ZURÜCKSETZEN. Sicherheitsmaßnahmen, die für die Benutzer sperrig und komplex in der Anwendung sind, führen schnell zu Frustration. Der unerwünschte Nebeneffekt: Sicherheitsmaßnahmen werden als Zeitverschwendung betrachtet. Probleme mit dem Vergeben und Verwalten von Passwörtern zu lösen ist ein unternehmerischer Imperativ. Einerseits, um zu gewährleisten, dass Mitarbeitende produktiv arbeiten, andererseits, um zu verhindern, dass sie selbst Mittel und Wege finden, Sicherheitsmaßnahmen zu umgehen (etwa in dem sie Passwörter teilen).

4 SÄMTLICHE AKTIVITÄTEN RUND UM EINE IDENTITÄT ÜBERWACHEN UND PROTOKOLLIEREN. Bei vertraulichen Informationen ist es wichtig zu wissen, wer auf welche Dateien zugreifen kann. Insbesondere dann, wenn die Daten gefährdet sind. Für Auditoren sind die diesbezüglichen Protokolldaten wichtig. Sie helfen bei der Ursachenforschung und Analyse sollte es bereits zum Schlimmsten gekommen sein. Sie fungieren aber auch als Frühwarnsystem und weisen auf potenziell schädliche Aktivitäten eines Benutzers hin.

Fazit

Dies sind neben vielen weiteren mehr grundlegende Best Practices, die dazu beitragen, das Risiko von Datenschutzverletzungen zu senken. Aber auch Risiken, die mit nicht erlaubten Aktivitäten eines Benutzers zusammenhängen, einzugrenzen. Natürlich haben Technologien einen nicht ganz unerheblichen Anteil daran, hier Hilfestellung zu leisten. Etwa indem sie Prozesse automatisieren sowie Lücken bei der Verwaltung privilegierter Konten aufdecken und zu schließen. Je größer die Zahl schlecht verwalteter Benutzerkonten und privilegierter Konten ist, desto größer der potenzielle Schaden. Er reicht von Datenschutzverletzungen und Datendiebstahl, über mangelnde Compliance und Strafen bis zum Vertrauensverlust bei Kunden und schwerwiegenden Schäden an Marke und Ruf. Es bleibt also zu hoffen, dass Unternehmen in den kommenden Jahren etwas mehr Vertrauen in ihre Prozesse zum Identity und Access Management und das Management privilegierter Konten haben. ■

www.oneidentity.com

CIOS BEFÜRCHTEN UMSATZEINBUßEN

Dynatrace hat im Rahmen einer weltweiten Umfrage unter 800 CIOs ermittelt: Fast drei Viertel (74%) der IT-Führungskräfte befürchten, dass Performanceprobleme im Internet der Dinge ihren Geschäftsbetrieb und Umsatz erheblich beeinträchtigen. Als Hauptgrund gaben 78% an, ihr Unternehmen führe möglicherweise planlos IoT-Strategien ein. So glauben 69% der Befragten: IoT wird zu einer großen Belastung für das Performance Management, das die zunehmende Komplexität der modernen Enterprise-Cloud-Umgebungen bewältigen soll. Die vollständige Studie 'Overcoming the Complexity of Web-Scale IoT Applications: The Top 5 Challenges' von Dynatrace kann hier heruntergeladen werden. Die CIO-Umfrage befasst sich mit den Herausforderungen für Unternehmen bei der optimalen Bereitstellung von Angeboten, wenn sie weitere IoT-Lösungen einführen.

www.dynatrace.de

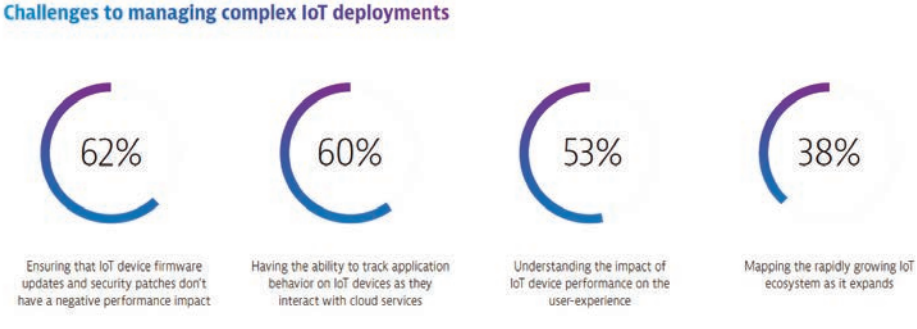


Bild: © denisismagilov/Fotolia

Security und Leistung in der Cloud vereinen

TEXT: Klaus Gheri, Vice President and General Manager Network Security, Barracuda Networks AG

Moderne Anwendungen müssen skalieren und performant sein. Dazu werden viele Implementierungen auf Public-Cloud-Plattformen wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) gehostet, was für Elastizität und Geschwindigkeit sorgt. Die Cloudnutzung boomt und die Vorteile liegen auf der Hand.

Die Herausforderung besteht jedoch in der Sicherung von Anwendungen in der Cloud – das Problem: Traditionelle On-Premises-Sicherheitskonzepte lassen sich nicht effektiv auf Public-Cloud-Applikationen übertragen. Deshalb sollten Unternehmen auch nicht versuchen, ihre alten lokalen Security-Tools einfach in eine Cloudumgebung zu verlagern. Die Sicherung von Cloudapplikationen erfordert neue Ansätze, Richtlinien, Konfigurationen und Strategien, die es Unternehmen ermöglichen, Geschäftsanforderungen wie Leistung und Skalierbarkeit mit den nötigen Sicherheitsvorkehrungen in Einklang zu bringen.

Balance von Leistung und Sicherheit

Die Akzeptanz der Public Cloud bei Unternehmen nimmt rapide zu, doch Sicherheitsbedenken sind immer noch eine Hürde beim Wechsel in die Cloud. Vielen Unternehmen ist oft nicht klar, wie die Sicherheitsverantwortung in der Cloud verteilt ist. Nach dem Shared-Responsibility-Modell ist es Aufgabe des Cloud Providers, die Infrastruktur zu schützen, das bedeutet, er sorgt für die physische Sicherheit, die globale und regionale Konnektivität sowie die Stromversorgung und Kühlung seiner Rechenzentren. Doch es ist Sache der Unternehmen, ihre Daten und Anwendungen in der Cloud zu schützen. Bedrohungsvektoren wie Cyberangriffe, Softwarefehler und menschliches Versagen gelten daher in gleicher Weise in der Cloud wie On-Premises und erfordern entsprechende Sicherheitsvorkehrungen. Dennoch stellen viele Unternehmen die Anwendungsleistung und -geschwindigkeit über die Sicherheit. Angesichts der Risiken sollte diese Faktoren jedoch in einem ausgewogenen Verhältnis zueinander stehen. So ist der Einsatz von Layer 7-Schutzmaßnahmen für die Sicherung von Applikationen äußerst wichtig, doch jede Technologie muss hierbei tief in bestehende Cloud-Plattformen und Lizenzmodelle integriert werden. So sollte sie eng mit der dynamischen Skalierbarkeit von Public

Cloud-Anbietern wie AWS, Azure und GCP verbunden sein, um sicherzustellen, dass die Anforderungen an das Performance-Management ohne manuelle Eingriffe in Echtzeit erfüllt werden. Außerdem sollten Unternehmen direkten Zugriff auf die nativen Protokollierungs- und Berichtsfunktionen der Cloudplattformen haben.

Anwendungsschwachstellen in der Cloud managen

Viele Anwendungsschwachstellen bleiben oft so lange unbemerkt, bis es zu spät ist. Leider sind Fixes oder Patches ein reaktiver Prozess, der Schwachstellen viel zu lange offen lässt – Monate sind keine Seltenheit. Die automatische und kontinuierliche Behebung von Schwachstellen ist für die Gewährleistung der Anwendungssicherheit sowohl On-Premises als auch in der Cloud von größter Bedeutung. Daher ist es unerlässlich, eine Reihe von Richtlinien zu implementieren, die kontinuierlichen Schutz durch ein regelmäßiges Schwachstellenmanagement und -behebungsverfahren bieten. Dies kann auch automatisiert werden, um sicherzustellen, dass Anwendungsänderungen keine Schwachstellen öffnen.

Vier Punkte zur Auswahl einer effektiven Cloudsicherheitslösung

Im Folgenden einige Best Practices für effektive Anwendungssicherheit in der Cloud:

1. Auf die Cloud spezialisiert: Die Sicherheitslösung sollte anspruchsvollste Anwendungsfälle erfüllen können, wie sie für Cloud gehostete Anwendungen spezifisch sind. Außerdem ist es zwingend erforderlich, dass sie sich direkt in native Public Cloud Services wie Elastic Load Balancing, AWS CloudWatch, Azure OMS und andere sowie Cloud-Access-Technologien wie Azure ExpressRoute oder AWS Direct Connect integriert.

2. API: Die Lösung sollte eine möglichst umfassende API bereitstellen, die eine für Cloud Einsatzszenarien angemessene Kontrolle durch bereits verwendete Orchestrierungswerkzeuge von DevOps-Teams wie z.B. Puppet ermöglicht.

3. Skalierbarkeit und zentrale Verwaltung: Sicherheitsanwendungen müssen in Hochverfügbarkeits-Clustern implementiert und mit Hilfe von Cloud-Templates automatisch skaliert werden können. Außerdem sollten sie eine Verwaltung und Überwachung von einer einzigen Konsole aus bieten.

4. Flexible Lizensierung: Wichtig ist darüber hinaus, dass die Lösungen vollständige Lizenzflexibilität bieten, einschließlich einer rein verbrauchsabhängigen Abrechnung. Auf diese Weise können Unternehmen so viele Instanzen wie nötig bereitstellen und bezahlen nur den Datenverkehr, der durch diese Anwendungen gesichert ist. Grundsätzlich erfordert die Sicherung von Anwendungen in der Cloud neue Security-Strategien. Unternehmen sollten daher ihre eingesetzten Lösungen unter die Lupe nehmen und prüfen, wo es der Nachbesserung bedarf, um eine kontinuierliche Überwachung und Schwachstellenbehebung von Anwendungen in der Cloud zu gewährleisten. Dabei ist es wichtig, jede Anwendung auf entsprechendem Sicherheitsniveau zu schützen. So sollten die Security-Maßnahmen auf den aktuellen Cloudverbrauch abgestimmt sein und entsprechende Tools genutzt werden, die speziell für Cloudumgebungen entwickelt wurden. ■

www.barracuda.com

Partnerschaftlich das IIoT schützen

Trend Micro und Moxa arbeiten zukünftig im Rahmen des Technology Alliance Partner Programs bei der Entwicklung von Sicherheitslösungen für das Industrial Internet of Things (IIoT) zusammen. Die Lösungen werden zunächst in den Bereichen Endpoint-Lockdown, Firewalls für Operational-Technology-Netzwerke und Embedded Security zu finden sein.

www.trendmicro.de

Das IoT erobert den Himmel

In unserer **digitalen Welt** kommt auch die **Luftfahrtindustrie** längst nicht mehr ohne die entsprechenden Technologien aus. Und es ist an der Zeit das **Potenzial des Internet of Things** für den digitalen Wandel **voll auszuschöpfen**. Dieser Beitrag zeigt, welche Technologien welche Vorteile bieten.

TEXT: Dwayne Charrington, technischer Autor, ProProfs Help Desk

Bessere Dienstleistungen zu erbringen ist seit langem ein treibender Faktor für die Luftfahrtindustrie. Kombiniert man IoT und künstliche Intelligenz (KI) führt das zu deutlich mehr Verbesserungen. Der 'Connected World' Report des World Economic Forums schätzt, dass verspätete Flüge an amerikanischen Großflughäfen die kommerzielle Luftfahrt bis 2020 alleine mehr als 20 Milliarden US-Dollar kosten werden. Smarte Flughäfen nutzen bereits aktuelle IoT-Technologien. Zum einen, um die Kundenerfahrung zu verbessern, zum anderen um Verluste wie diese auszugleichen. Ein Bericht von Deloitte bestätigt das. Mobil- und Beacon-Technologien verbessern Reise- und Einkaufsqualität an Flughäfen. IoT-Tools, wie die Gesichtserkennung beschleunigen und optimieren das Boarding der Reisenden oder beschleunigen den Weg zum Terminal. Offensichtlich hat das IoT viele Prozesse bereits grundlegend verändert. Im Folgenden beschäftigen wir uns mit konkreten IoT-Anwendungen in der Luftfahrtbranche.

Stressfreier Sicherheitscheck mit Gesichtserkennung

Die größte Herausforderung für Flughafenbehörden und Kunden gleichermaßen ist die Sicherheitskontrolle. Und die kann man mithilfe des IoT deutlich effizienter gestalten. An den Checkpunkten verwendet man Software zur Gesichtserkennung. Mit dieser Technologie ordnen die Flughafenbehörden Gesichtsmerkmale eines Kunden den Daten in Blockchain-Systemen zu. Diese Informationen zur Identität eines Kunden liegen jedem Checkpunkt vor. Das senkt automatisch den Zeitaufwand zwischen Check-In und Boarding am Gate. Warteschlangen verkürzt man mit automatischen Sensoren. Wenn Identität und Bordkarte des Reisenden auf dem Handy gespeichert sind, werden sie von Sensoren erfasst. Auch die Sicherheitsteams können sowohl auf diese Informationen zugreifen als auch auf Analysen der Gepäckstücke. Reisende profitieren dank der Sensortechnologie von kürzeren Wartezeiten, was den gesamten Ablauf im Flughafenterminal benutzerfreundlicher gestaltet. Die Sicherheitskontrolle ist für Reisende erwiesenermaßen der größte Stressfaktor. Laut 'The Future is Connected' Report von SITA aus dem Jahr 2016 verbinden 36 Prozent damit negative Emotionen auf ihrer Reise. Biometrie trägt also durchaus mit dazu bei, dass eine Flugreise beim Kunden in positiver Erinnerung bleibt. Stephen Challis, Head of Product Development bei der Société Internationale de Télécommunications Aéronautiques (SITA) dazu im The Independent: „In Brisbane wird ein sechsmonatiger biometrischer Testlauf durchgeführt. Passagiere melden sich mit ihren Pässen, Bordkarten und Fotos beim Check-In-Schalter an. Passagiere sehen dann am Boarding Gate in die Kamera, und schon sind sie bereit für den Abflug. Flughafenpassagiere werden dadurch erheblich schneller und bequemer abgefertigt." Auch der San Jose International Airport in Kalifornien nutzt Gesichtserkennung um die langen Schlangen an der Passkontrolle zu verkürzen. Alle ankommenden und abfliegenden internationalen Passagiere werden dazu einem Screening unterzogen und bei der Passkontrolle fotografiert. Die Software vergleicht das Bild mit dem im Visum oder Pass, das vom US Federal Government vorliegt.

Schnelle Navigation am Flughafen

Müde und frustrierte Kunden, die Flughafenmitarbeiter mit langen Schlangen und dem üblichen Ansturm auf die Check-In Schalter in letzter Minute nerven? Das sind Szenarien die im Zeitalter smarter Flughäfen der Vergangenheit angehören. Digitale Beacons lassen sich strategisch im Flughafengebäude platzieren. Sie geben per SMS-Nachricht Updates in Echtzeit an die Reisende weiter. Die Updates informieren beispielsweise über verfügbare Parkplätze, An- und Abfahrtszeiten des Airport-Shuttle, mit ihnen kann man Tische im Restaurant reservieren und vieles mehr. Mehr als 95 Prozent aller Reisenden führen bei Flugreisen ein Mobilgerät mit. Solche Services sind also sowohl für Flughäfen als auch für Kunden attraktiv und praktikabel. Auch das sogenannte Passenger Flow Management, also das Management von Passagierströmen, lässt sich über Beacons realisieren. Meldet ein Beacon z.B. hohes Passagieraufkommen an Sicherheitscheckpunkt 1 kann der Betreiber entsprechend reagieren indem er etwa Passagiere an einen weniger ausgelasteten Check Point weiterleitet oder indem er zusätzliches Abfertigungspersonal bereitstellt. Smarte Flughäfen führen Passagiere über Beacon-verlinkte Karten nahtlos vom Check-In bis zum Abflug. Dank einer einfachen Navigation haben Flughafenpassagiere mehr Zeit, die sie für sich nutzen können. Zufriedene

Bild: ©Jag_cz / Fotolia.com

Kunden wiederum steigern den Umsatz am Flughafen. Beacons helfen außerdem dabei, Flughafenpersonal zu orten, und auf diese Weise die Flughafensicherheit durchgehend zu garantieren. Verbesserte operative Effizienz ist ein weiterer Hauptvorteil dieser Technologie. Wie Beacons funktionieren zeigt der Côte d'Azur Airport. Für die Strecke Nizza - Paris sind hier unterschiedliche Beacons im Terminal installiert, um kontextbezogene Ladeninformationen und -werbung an Reisende im Terminal weiterzugeben. Die Beacon-gesteuerte Flughafen-App sammelt automatisch Punkte, wenn Premium-Mitglieder den Flughafen passieren. Premier Gold Mitglieder nutzen automatisch ihre Vielfliegerkarte mit Zugang zur Fast Track Sicherheitskontrolle.

Sicheres Gepäckmanagement

IoT Beacons und RFID Tags sind für eine sichere Ortung und das Management von Gepäck unabdingbar. Beacons verbinden sich zu einem mobilen Netzwerk eines Flughafens. Der größte Vorteil verglichen mit Barcodes ist, dass mit RFID Informationen auch außerhalb des Gepäcksystems ausgelesen werden können. Live-Informationen über den genauen Standpunkt eines Gepäckstücks, von der Gepäckabgabe bis zum Frachtraum sind möglich. Passagiere erhalten SMS-Benachrichtigungen in Echtzeit wo sich ihr Gepäck befindet. Das Bodenpersonal erhält Benachrichtigungen, welches Gepäck auf welchen Flug muss. Das ist vor allem von Vorteil, wenn Gepäckstücke von einem Flugzeug zum anderen umgeladen werden müssen. Zusätzlich vereinfacht die Methode den Frachtprozess, denn Technologien helfen auch dabei verlorene Stücke aufzuspüren. Und wenn weniger Gepäckstücke verloren gehen, sinken die Erstattungskosten. Jedes Jahr gehen 25 Millionen eingecheckte Taschen und Koffer verloren. Beacon und RFID-basierte IoT-Lösungen können diese Zahl nicht nur drastisch senken, sondern auch die operative Effizienz steigern und Sicherheitsbedenken der Kunden entkräften. Der Hong Kong International Airport zeigt wie es funktionieren kann: Mehr als 50 installierte Beacons im Terminal 1 senden relevante Informationen an Reisende. Über eine App werden sogar Fotos vom Gepäckband verschickt. Zusätzlich leitet der Flughafen Reisende mit benutzerfreundlichen und interaktiven Karten durch wichtige Bereiche.

Weniger Verspätungen

Bluetooth Beacon Sensoren geben Sensordaten ab. Sie sind mit Sensorfähigkeiten ausgestattet, die Bewegung (Beschleunigungsmesser), Luftdruck, Temperatur, Feuchtigkeit, Magnetismus (Hall Effekt), Licht, Nähe, Herzschlag, Nahfeldkommunikation (NFC) und Sturzerkennung melden. Dank BLE sind die Sensoren am besten für IoT-Anwendungen einsetzbar. Flughäfen überwachen damit Starts und Landungen. Es ist inzwischen möglich einfache Wetter-Beacons an jeder Start- und Landebahn mit einem umfangreicheren Netzwerk zu kombinieren. Passagier-Apps bieten dank Netzwerküberwachung zeitgenaue und akkurate Informationen. So erfahren Passagiere, warum ein Flug noch nicht starten kann oder verspätet ist. Die separate Überwachung der einzelnen Start- und Landebahnen ist insbesondere wichtig bei potenziell unberechenbaren Wetterbedingungen wie Sturm, Hagel oder Eis. Flughäfen sind besser ausgestattet Entscheidungen im Interesse der Passagiersicherheit zu treffen. Zwischen Juni 2015 und Juni 2016 waren mehr als eine Million Flüge verspätet. Dies entsprach annähernd 64 Millionen Minuten Wartezeit für Reisende. Verspätungen und die damit verbundenen Kosten für die Luftfahrtindustrie kann man u.a. über vernetzte IoT-Wetter-Überwachung reduzieren.

Passagierströme und -verhalten erfassen

Näherungssensoren verbinden Airline-Technologien und Flughäfen mit den Smartphones der Reisenden. Laut dem Unacast Proxbook Report Q3 2016 betreiben fast 90 Prozent aller Flughäfen weltweit entweder eine kommerzielle Anwendung oder ein Testprojekt mit Näherungssensoren. Der Report schätzt, dass der Wert dieser Branche bis 2022 auf 52.46 Milliarden US-Dollar steigt. Näherungssensoren verbessern beides: Flughafensicherheit und das Shopping-Erlebnis von Passagieren. Sicherheitsteams sind in der Lage zusätzliches Personal an belebtere Stellen zu schicken. Geschäfte profitieren von Werbebotschaften und Angeboten, die direkt an potenzielle Kunden gesendet werden, die sich in räumlicher Nähe befinden oder mittels

Jedes Jahr gehen 25 Millionen eingecheckte Taschen und Koffer verloren. Beacon und RFID-basierte IoT-Lösungen können diese Zahl nicht nur drastisch senken, sondern auch die operative Effizienz steigern und Sicherheitsbedenken der Kunden entkräften.

Augmented Reality direkt zum Shop geführt werden. So nutzt bspw. der Gatwick Airport in Großbritannien Beacons und Näherungssensoren für die Navigation durchs Flughafengebäude. Allgemeine Informationen über die 'Personendichte' in verschiedenen Beacon-Zonen unterstützen die Flughafenabläufe.

IoT und Cybersicherheit

Flughäfen sind offensichtlich vernetzter als je zuvor. Sie nutzen die Cloud, integrierte Systeme und das IoT für ihre operative Effizienz. Die Vernetzung öffnet allerdings gleichzeitig Türen für Spear Phishing-Angriffe, Sicherheitsvorfälle, Identitätsdiebstahl, Malware und Social Engineering. Ein Angriff auf ein Flughafensystem legt vielleicht persönliche Daten von Passagieren offen, beeinflusst Back-Office-Systeme und Sicherheitschecks, manipuliert Ankunft- und Abflugdaten und so weiter. Das würde einen geregelten Flughafenablauf nicht nur negativ beeinflussen, sondern auch dem Ruf schaden und damit dem Umsatz. Leider gibt es keine 'Einheitslösung' für die Cybersicherheit an Flughäfen. Es hilft, nicht nur die aktuellste Software zur Malware-Erkennung oder die neueste Firewall zu installieren. Eine proaktive Risikoanalyse ist der beste Weg, um Schwachstellen zu erkennen und ein ganzheitliches Informationstechnologie- (IT) Sicherheitsprogramm zu erstellen. Ein umfassender Computersicherheitsplan vereint Penetration-Tests und Schwachstellenanalyse-Tools, Risikomanagement-Programme und die richtigen Quellcode-Methoden. Zusätzlich müssen Flughäfen Maßnahmen zur physikalischen Sicherheit ergreifen und Netzwerksicherheitslösungen implementieren. Schließt man die Lücke zwischen Computersicherheit und IT, stärkt das die wirksame Abwehr von Angriffen. Flughäfen sind gehalten, kontinuierlich interne Schulungen zu Sicherheitsregeln und deren Umsetzung durchzuführen. 'Best Practices' in Sachen Sicherheit sollten nicht nur für die eigene Umgebung gelten, sondern auch für Händler und Partner. Am besten sucht man sich einen IoT-Anbieter, der bereits Funktionen wie Verschlüsselung und starke Authentifizierung in seine Lösungen integriert.

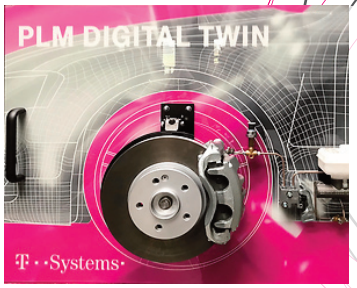
Leider gibt es keine 'Einheitslösung' für die Cybersicherheit an Flughäfen. Es ist an der Zeit, neue Technologien mehr als bisher zu nutzen.

Ein weiter Weg: IoT am Himmel

Wenn es um die ideale Umsetzungsstrategie für das IoT geht, müsste die Luftfahrtindustrie sich an die bekannte 'starten, lernen, beweisen, verbessern'-Methodik halten. Es ist an der Zeit, neue Technologien mehr als bisher zu nutzen. Durch die Integration des IoT mit anderen Technologien wie Cloud Computing, Big Data, Robotik und Künstliche Intelligenz entstehen neuartige Möglichkeiten die Servicequalität von Airlines deutlich zu verbessern. Während sich die Luftfahrtindustrie auf die IoT-Revolution vorbereitet, hat der Wandel im Kopf bereits begonnen. Digitale Technologien und Fähigkeiten, die Airlines heute schon nutzen, werden eine wichtige Rolle in deren Evolution zum intellektuellen Unternehmen von morgen spielen.

www.globalsign.com

T-Systems und PTC erweitern Partnerschaft



T-Systems baut die Kooperation mit PTC, einem Spezialisten für Produktentwicklung und IoT, aus. Die Geschäftskundentochter der Deutschen Telekom bietet nunmehr das gesamte Produkt- und Lösungsportfolio von PTC für Kunden der Automobil-, Luftfahrt- und herstellenden Industrie an – und das weltweit. Das von T-Systems unterstützte PTC-Portfolio umfasst Creo (CAD), Windchill (PLM), Integrity (ALM), Vuforia (AR) und ThingWorx (IoT).

www.t-systems.de

Kompakter Router für IoT und M2M

Hy-Line Communication Products bietet mit dem AirLink LX40 von Sierra Wireless einen **kompakten Router mit LTE-Cat.M1 und NB-IoT** an. Dieser ermöglicht **'out-of-the-box' sichere und managebare LTE-Netzwerke für IoT-, Unternehmens- und Security-Anwendungen wie IP-Kameras, Point-of-Sale-Terminals und Smart Lockers.** Des Weiteren eignet sich der Router auch für den Anschluss von industriellen Datenerfassungsgeräten und unterstützt die Verarbeitung von IoT-Daten On-the-Edge mit dem Aleos Application Framework (AAF). Eine Version mit Wi-Fi ist ebenfalls verfügbar, um als lokaler Hotspot zu fungieren oder eine Verbindung zu Wi-Fi-Infrastrukturen herzustellen. Die Stromversorgung kann einfach per PoE erfolgen.

HY-Line Communication Products Vertriebs GmbH, www.hy-line.de/communication

Erweiterbare kompakte Box-PC-Serie

Comp-Mall stellt die robuste Embedded-Computer-Serie DS-1200 vor. Das System ist mit dem Intel Q370-Chipsatz ausgestattet und unterstützt die 8. Generation (Coffee Lake) der Intel-LGA-1151-Prozessoren. Mit einer Grundfläche von 227x261mm (kleiner DIN A4) und Höhen von 88, 108 und 128mm ist der Platzbedarf sehr gering. Die Serie ist in drei verschiedenen Ausführungen erhältlich, die ohne oder mit bis zu zwei PCI/PCIe-Erweiterungssteckplätzen kommen.

Comp-Mall GmbH, www.comp-mall.de

Kompaktes Board mit AMD SoC

Das Embedded Board Nano-GLX von ICP im Formfaktor Epic ist kompakt, hochauflösend und verfügt über eine integrierte Dual Core GX-210KL CPU von AMD. Die geringe Abwärme von 4,5W bietet ausreichende Voraussetzungen für die Entwicklung thermisch anspruchsvoller Embedded Systeme in der industriellen Automation. Die bis zu 8GB DDR3 oder DDR3L SDRAM sorgen für ausreichend Arbeitsspeicher. Eine kombinierte Kühl- und Montageschale ermöglicht dabei lüfterlosen Betrieb und gleichzeitig flexiblen Einbau. Der Anschluss zweier unabhängiger Displays ist mittels VGA, LVDS oder HDMI-Schnittstelle möglich, wobei letztere eine 4K-UHD-Auflösung bietet.

ICP Deutschland GmbH, www.icp-deutschland.de

Transflektives Industrie-Display

SE Spezial-Electronic präsentiert für den In- und Outdoor-Einsatz in hellen Umgebungen das 2,83"-Industrie-TFT WF0283ATDAJDNN0 von Winstar. Die Anzeige mit einer Auflösung von 240x320 Bildpunkten basiert auf einer transflektiven Displaytechnik, bei der das Umgebungslicht zur Darstellung mit beiträgt. Für den Betrieb bei geringer Helligkeit steht eine Hintergrundbeleuchtung mit einer Leuchtdichte von bis zu 500cd/m^2 zur Verfügung. Angesteuert wird das mit einem TFT-Driver HX8367-A mit internem Framebuffer ausgestattete Display über ein paralleles 8-/16Bit-Mikrocontroller-, ein serielles 3-/4-Draht- oder ein 9-/18Bit-RGB-Interface.

SE Spezial-Electronic GmbH, www.spezial.com/de

Neue Version von Connext

Real-Time Innovations präsentiert die neueste Version seiner Konnektivitäts-Software Connext 6. Sie wurde speziell für komplexe autonome Systeme mit großen Datenmengen entwickelt, z.B. bei autonomen Fahrzeugen und klinischer Medizintechnik. Connext 6 bietet Systemarchitekten die Möglichkeit, unter anderem Sensordaten mit hoher Bandbreite effektiv zu verwalten und standardisierte Schnittstellen einfach zu integrieren.

Real-Time Innovations, www.rti.com

Welche IoT-Lösungen nutzt der Mittelstand?

Wie eine **Studie des Digitalverbandes Bitkom** aus dem Jahr 2018 zeigt, **nutzen vier von zehn Industrieunternehmen eine IoT-Plattform**. Die Bedeutung der Vernetzung von Produkten, Anlagen und Maschinen wird für die eigenen Unternehmensziele also hoch eingeschätzt. Folgende **Praxisbeispiele** veranschaulichen, wie vielfältig der Mittelstand das Potenzial der IoT-Technologie heute nutzt.

TEXT: Bernd Groß, SVP IoT & Cloud Business, Software AG BILDER: Cumulocity GmbH

Mit Hauptsitz im bayrischen Kaufbeuren bietet der Telemetrie-Spezialist Sensor-Technik Wiedemann (STW) anspruchsvolle Lösungen in den Bereichen Elektrotechnik, Automatisierung und Vernetzung. Benannte Lösungen sind oft spezifisch auf bestimmte Branchen oder gar Teilsegmente zugeschnitten, um Kundenvorstellungen möglichst präzise zu realisieren. Für die Londoner Verwaltungsbehörde Greater London Authority hat das Unternehmen ein IoT-Projekt umgesetzt, mit dessen Hilfe der Emissionsausstoß von Bussen des öffentlichen Personennahverkehrs überwacht wird. Das Ziel: Bis zum Jahr 2021 sollen im Zuge der Initiative Ultra Low Emission Zone mehr als 5.000 Busse mit der Technologie ausgestattet werden, um die Luftqualität innerhalb der Stadt zu verbessern. Die Fernüberwachung der Busse realisiert STW auf Grundlage der Plattform Cumulocity IoT, die in diesem Fall als White-Label-Lösung im Einsatz ist. Sie ermöglicht es, technische Daten, Störungen, Routen, Standorte und Kraftstoffverbrauch zu überwachen und in Echtzeit zu visualisieren.

OFFSHORE-ENERGIEANLAGEN

Sensor-Technik Wiedemann ist hier gleich mit zwei Projekten vertreten, das zweite auf dem Feld der Offshore-Energiegewinnung: Bei der Wartung von Offshore-Energieanlagen wie Windrädern oder Gezeitenkraftwerken organisieren eigenständige Dienstleister den Transport von Fachpersonal zu den jeweiligen Anlagen auf See. STW stattet die Transportboote hier mit speziellen Sensoren aus, mit deren Hilfe Daten beispielsweise zum Wellengang gemessen werden. Auf Grundlage dieser Daten lassen sich nützliche Schlüsse ziehen. Beispielsweise kann die Wahrscheinlichkeit von Seekrankheit auf dem Boot durch Erschütterungen nach einer verpflichtenden ISO-Norm berechnet, wonach auch die Kosten einer Fahrt eingeschätzt werden - die Fahrt ist bei starken Wellen z.B. deutlich teurer. Alle Sensordaten werden in einer Anwendung zentral gebündelt und lassen sich in Echtzeit beobachten und steuern.

Internet der Dinge 2019: Zahl der IoT-Projekte wächst

Zusammen mit dem Umfrageinstitut IDG Research Services hat der IoT-Dienstleister Tresmo die aktuelle Studie 'Internet der Dinge 2019' herausgegeben. Für die Studie wurden mehr als 500 Unternehmen aller Größen und Branchen in Deutschland befragt. Demnach bewerten 51% der Unternehmen die Relevanz des IoT für sich als hoch oder sehr hoch. 2017 waren es 47%. Besonders hoch sind die Relevanzwerte bei Großunternehmen mit mehr als 1.000 Mitarbeitern (56%) und Unternehmen mit einem IT-Etat ab 10Mio.€ aufwärts (61%). Die Zahl der Firmen mit IoT-Projekten hat sich seit dem letzten Jahr mehr als verdoppelt – von 21 auf 44%. Die Einsatzgebiete sind breit gestreut: Vernetzte Produktion, Logistik, Qualitätskontrolle und die Einführung smarter, vernetzter Produkte liegen mit nur geringem Abstand vorne. 31% der Unternehmen haben Probleme, für ihre IoT-Initiativen entsprechend qualifizierte IT-Fachkräfte zu gewinnen.

www.tresmo.de

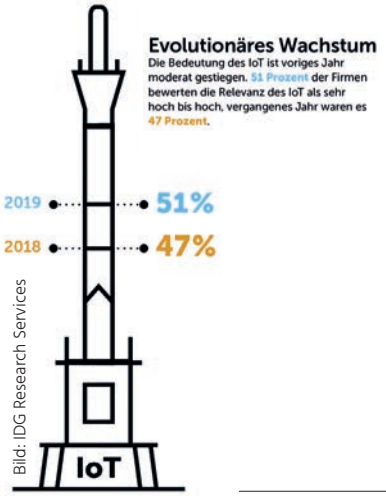
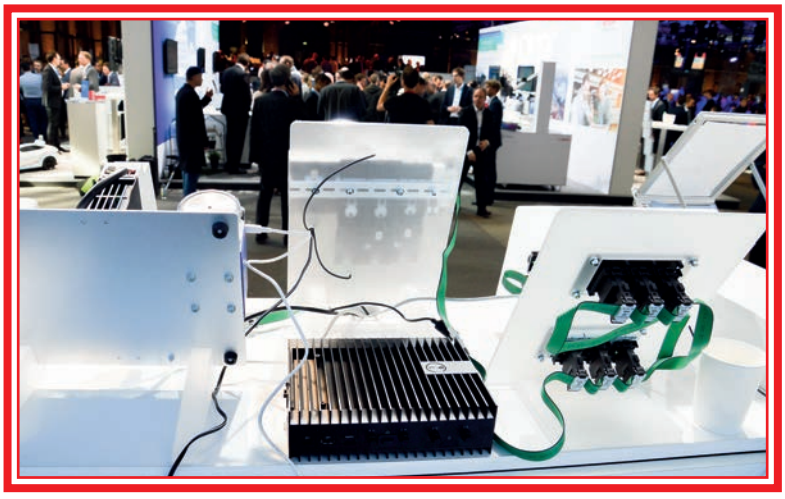


Bild: IDG Research Services

DIE VERNETZTEN KAFFEEMASCHINEN

Das Unternehmen Lyreco ist ein großer Anbieter für Büro- sowie Arbeitsplatzlösungen und unter anderem Lieferant hochwertiger Kaffeemaschinen und dazu passender Kaffeekapseln. Um den Bestand der Kapseln und die Funktionstüchtigkeit der Maschinen bei Firmenkunden stets im Blick zu haben, setzt das Unternehmen eine IoT-Lösung um, die zum einen die Menge der vorhandenen Kapseln, zum anderen relevante Funktionsparameter der Kaffeemaschinen in Echtzeit analysiert. Dabei werden die Maschinendaten in das SAP-ERP-System von Lyreco integriert und das Bestandsmanagement komplett automatisiert, was wiederum zu Kosteneinsparungen führt. So ist es möglich, rechtzeitig Nachschub an Firmenkunden zu liefern oder im Falle eines technischen Ausfalls einen Techniker zu schicken. Durch den Einsatz der IoT-Lösung konnte das Unternehmen Situationen, in denen der Bestand bei Kunden gänzlich zur Neige ging oder Kaffeemaschinen komplett ausfielen, um ein Vielfaches reduzieren.

IoT-Hardwarelösung für den Mittelstand ...



DIE ROLLE VON IOT-PLATTFORMEN

Die beschriebenen Anwendungsbeispiele, die alle derzeit in dieser Form im Einsatz sind, veranschaulichen die verschiedenen Möglichkeiten, wie Unternehmen das Internet der Dinge für ihre Zwecke nutzen können. Die Rolle, die eine IoT-Plattform als Herzstück der meisten IoT-Projekte einnimmt, ist hier nicht zu unterschätzen. Sie hat das Potenzial, die technischen Herausforderungen, die sich Unternehmen bei der Umsetzung von eigenen IoT-Projekten stellen, maßgeblich zu vereinfachen. Kriterien, die eine State-of-the-Art-Plattform ausmachen, sind beispielsweise ihre Plattformarchitektur, Skalierbarkeit, Protokolldiagnostizität, die schnelle Integrierbarkeit in unternehmenseigene Prozesse und Systeme, eine 'codefreie' Handhabung sowie vorkonfigurierte Services für typische Anwendungsfälle - beispielsweise Predictive Maintenance, Echtzeitanalyse oder Track and Trace.

MOTOR FÜR GESCHÄFTSMODELLE

Die genannten Use Cases zeigen ferner, welches strategische Potenzial die Erhebung von Daten in IoT-Lösungen bietet. Durch die umfassende Sammlung und Analyse zahlreicher Datensätze bildet das Internet of Things den Nährboden für neue Geschäftsmodelle. Unternehmen aus der Fertigung oder Hersteller von Werkzeugmaschinen profitieren beispielsweise von der genauen Auswertung ihrer eigenen Daten, da sie erstmals in Echtzeit Informationen über die Nutzung ihrer Maschinen beim Anwender, über Bestände, Auffälligkeiten oder sonstige Sensordaten erhalten. Insbesondere angesichts aufkommender technischer Entwicklungen, wie beispielsweise 5G, bleibt abzuwarten, wie sich der gegenwärtige Status Quo verändern wird. ■

www.cumulocity.com

VIELSEITIGER DANK IOT

IHS Markit geht davon aus, dass es bis 2025 weltweit an die **75,4 Milliarden IoT-Geräte** geben wird. In ein paar Jahren wird es gang und gäbe sein, dass Geräte in den meisten Industrie- und Verbrauchersektoren **mit dem Internet verbunden** sind. In diesem Beitrag erklärt **Jonathan Wilkins**, Marketingleiter von EU Automation, dem Zulieferer für obsolete Industriebauteile, welche **Auswirkungen** das IoT **auf kundenseitige Unternehmen** hat und **was Hersteller daraus lernen können**.

TEXT: JONATHAN WILKINS, Marketing Director, EU Automation Ltd. **BILD:** EU Automation Ltd.

IoT-Geräte sind allgegenwärtig. Manche sind nützlich, wie z.B. Fitness-Tracker, die den Puls, zurückgelegte Schritte und die Nahrungsaufnahme dokumentieren. Manche sind weniger nützlich, wie z.B. der Quirky Egg Minder, der die Anzahl der Eier im Kühlschrank und deren Verfallsdatum dokumentiert. Von sorgfältig ausgewählten IoT-Geräten können verschiedene Branchen profitieren, wie z.B. die Fertigungsindustrie, das Gesundheitswesen und die Stadtplanung.

» Die richtige Zielgruppe

Man geht davon aus, dass es bald mehr Millennials als Babyboomer geben wird, und dass diese die größte Verbrauchergruppe mit verfügbarem Einkommen darstellen werden. Da sie bis 2020 jährlich 4 Billiarden US-Dollar ausgeben werden, sollten sich Unternehmer Gedanken darüber machen, wie sie diese Bevölkerungsgruppe am besten ansprechen. Millennials wachsen im digitalen Zeitalter auf und können sich somit mühelos an innovative Technologien anpassen. Bei der Aktualisierung ihrer Dienstleistungen sollten Unternehmer darüber nachdenken, wie IoT-Geräte sie dabei unterstützen können, ihre Zielgruppe zu erreichen und wettbewerbsfähig zu bleiben.

» Zielgerichtete Werbung

Sie brauchen einfach nur Ihren Social-Media-Feed durchscrollen, um zu sehen, wie Werbetreibende bereits Technologien einsetzen, um Aufmerksamkeit für sich zu erzeugen. KI-Algorithmen erkennen Muster im Surfverhalten und zeigen dementsprechend darauf abgestimmte, zielgerichtete Werbung an. Je mehr IoT-Geräte genutzt werden, desto mehr Möglichkeiten haben Werbetreibende, mit Verbrauchern in Kontakt zu treten. Wenn Fitness-Tracker beispielsweise erkennen, dass Sie nach dem Laufen einen Supermarkt betreten, um sich einen Snack zu kaufen, können Werbetreibende Ihnen sofort für dieses Geschäft einen Gutschein zusenden. Hersteller können ähnliche Technologien nutzen, um den Zustand von Maschinen zu überwachen und die Produktivität der Fertigungsanlagen zu optimieren. KI erkennt Veränderungen des Maschinenzustandes und benachrichtigt Ingenieure über Probleme, die zu Ausfallzeiten führen könnten.

» Das smarte Hotel

Herausragender Kundendienst ist im Gastgewerbe der Schlüssel zum Erfolg. Hoteleigentümer können mithilfe intelligenter Sensoren den Aufenthalt ihrer Gäste personalisieren und den Energieverbrauch reduzieren. Sensoren können Licht und Temperatur erkennen, sich die Vorlieben der Gäste merken und so dafür sorgen, dass die Anpassungen, die Gäste im Zimmer vornehmen, beibehalten werden. Darüber hinaus können Sensoren auch das Tageslicht und die Zimmertemperatur messen und künstliches Licht und die Temperaturregelung entsprechend anpassen. Hersteller sollten darüber nachdenken, wie sich mithilfe von Sensoren sowohl ihre Fertigungsanlage als auch ihre Produktion optimieren lässt. Sie können mithilfe der Daten, die Sensoren erfassen, die Maschineneffizienz erhöhen und den Strom- und Wasserverbrauch der Fertigungsanlage anpassen, um die Energieeffizienz zu erhöhen und die Strom- und Wasserrechnung zu reduzieren.

» Wandel im Einzelhandel

Da immer mehr Menschen online einkaufen, sollten sich Einzelhändler überlegen, wie sich das Einkaufen vor Ort im Geschäft mithilfe von Technologie einfacher gestalten lässt. Der Zebra-Einzelhandelsstudie 2017 zufolge haben weltweit 70 Prozent der Einzelhändler Interesse daran, das Kundenerlebnis in ihren Geschäften mithilfe von IoT-Technologie zu verbessern. Intelligente Sensoren können Verbrauchern das Einkaufen erleichtern. Einzelhändler können damit das Navigieren ihrer Kunden durch das Geschäft verfolgen und Regale neu anordnen, um deren Einkaufserlebnis zu optimieren. 87 Prozent der Einzelhändler wollen mithilfe von MPOS-Systemen, also mobilen Point-of-Sale-Punkten im Geschäft, den Kunden an jeder beliebigen Stelle des Geschäfts zahlen lassen können. Erstausrüster können mithilfe ähnlicher IoT-Technologien ihre Produktivität optimieren und dafür sorgen, dass Verbraucher das beste Produkt erhalten. Sie können mithilfe dieser Technologie Dinge wie Lagerbestände, Qualitätssicherung und wichtige Dokumente verwalten, um die Produktqualität zu erhöhen und Lieferzeiten zu reduzieren.

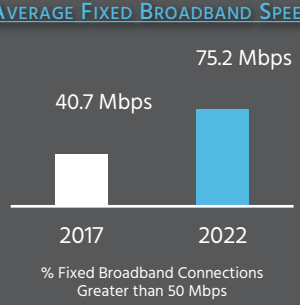
» Immer aktuell

In diesen Anwendungsbereichen Technologien einzusetzen, kann für zufriedenere Kunden sorgen. Da die Technologie jedoch so nah am Verbraucher ist, muss sie immer effizient funktionieren, um etwaige Unannehmlichkeiten zu vermeiden. Sowohl kundenseitige als auch Industrieunternehmen sollten Maßnahmen ergreifen, um Ausfallzeiten zu vermeiden, da diese kostspielig sein können. Sie sollten ein prädiktives Instandhaltungsprogramm einrichten, das den Maschinenzustand überwacht und Maschinenausfälle im Voraus erkennt. Vor einem Ausfall können Ingenieure mit Zulieferern für Ersatzteile wie z.B. EU Automation Kontakt aufnehmen und obsolete, neue oder wiederaufbereitete Ersatzteile bestellen, um ihre Anlagen instand zu halten. Wir nutzen intelligente Technologie, die uns zum richtigen Zeitpunkt die richtigen Informationen bereitstellt, wie z.B. eine Smartwatch, die unsere Fitness misst, oder ein intelligentes Eierfach, das das Verfallsdatum von Eiern überwacht. Handelsunternehmen sollten in IoT-Technologie investieren, um die Informationen zu erhalten, die sie brauchen, um den Bedürfnissen ihrer Kunden gerecht zu werden und sich im digitalen Zeitalter einen Wettbewerbsvorteil zu verschaffen. ■

www.euautomation.com

Deutschland auf gutem Weg zur Industrienation 4.0

In Deutschland steigen sowohl der Datenverkehr als auch die Anzahl der vernetzten Geräte weiterhin stark an. Das zeigt der jährliche Cisco Visual Networking Index (VNI). Gleichzeitig wird deutlich, dass Deutschland noch mehr in den Breitbandausbau investieren muss. Hochgerechnet auf den Status Quo wächst die Durchschnittsgeschwindigkeit zwar



von 44 auf 75,2MBit/s. Doch im Vergleich mit den USA (100,5MBit/s) und China (98,9MBit/s) zeigt sich, dass weiter daran gearbeitet werden muss, den Anschluss noch zu schaffen. Der mobile Datenverkehr wuchs hierzulande 2017 um 34 Prozent. Bis 2022 wird er um das Vierfache steigen. Neben Mobilität wird auch das Internet der Dinge eine immer größere Rolle spielen.

www.cisco.com

KI für die Produktion nutzbar machen

Auf ihrer Herbsttagung in Berlin hat die Wissenschaftliche Gesellschaft für Produktionstechnik (WGP) einstimmig beschlossen, praktische Wege aufzuzeigen, wie künstliche Intelligenz in die Produktion integriert werden kann. Ein WGP-Standpunktpapier soll Chancen und Risiken der KI für das produzierende Gewerbe erstmals umfassend beleuchten.

TEXT & BILDER: Wissenschaftliche Gesellschaft für Produktionstechnik

Prof. Berend Denkena: „Künstliche Intelligenz birgt enorme Chancen, auch für die Produktionstechnik.

„Künstliche Intelligenz birgt enorme Chancen, auch für die Produktionstechnik", erläutert Prof. Berend Denkena, Präsident der WGP und Leiter des Instituts für Fertigungstechnik und Werkzeugmaschinen (IFW) der Leibniz-Universität Hannover. „Wir können und wollen als Forschungsgemeinschaft diesen Megatrend vorantreiben und werden zügig die für die Produktionstechnik bedeutenden Fragen ausarbeiten, um die neue Technologie künftig auch in der Produktion vermehrt nutzen zu können." Das Standpunktpapier soll ein Weckruf an Unternehmen sein, sich mit Fragen der KI praktisch auseinanderzusetzen und wird praktische Handlungsempfehlungen für die Einführung der Technologien enthalten. Bis zur WGP-Frühjahrstagung im Frühsommer 2019 soll es fertiggestellt sein. Zwar habe es schon vor rund 30 Jahren Arbeiten zur Produktionsplanung oder der Maschinendiagnose mit künstlichen neuronalen Netzen gegeben. „Allerdings sind die zur Verfügung stehenden Datenmengen und auch die Möglichkeiten der Verarbeitung und Speicherung mittlerweile groß genug, um KI praktisch umzusetzen", so Denkena. „Und diese Datenverfügbarkeit wird in Zukunft weiter steigen." Zwar gebe es an unterschiedlichen Instituten bereits Forschungsprojekte zur KI in der Produktion. „Wir wollen nun aber eine Grundlage schaffen, auf der die bereits existierenden Erfahrungen strategisch so weiterentwickelt werden, dass die bislang nur punktuell genutzten neuen Wertschöpfungspotentiale durch KI in der Produktion auch systematisch gehoben werden können", berichtet Prof. Jörg Krüger, Initiator des Standpunktpapiers und Leiter des Fachgebiets Industrielle Automatisierungstechnik im Institut für Werkzeugmaschinen und Fabrikbetrieb (IWF) der TU Berlin sowie Leiter des Geschäftsfeldes Automatisierungstechnik des Fraunhofer Instituts für Produktionsanlagen und Konstruktionstechnik IPK in Berlin. „Als WGP verfügen wir mit unseren rund 40 Forschungsinstituten über ein einmaliges Domainwissen der Produktion. Dieses wollen wir auch zum Nutzen der deutschen Industrie einsetzen."

Hohes Wertschöpfungspotential für die Produktion

Die WGP hat sich zu diesem Schritt entschieden, auch wenn Kritiker befürchten, dass der Hype um Künstliche Intelligenz zu überzogenen Erwartungen bezüglich der Geschwindigkeit ihres breiten Einsatzes in der Produktion führen könnte. „Mag sein, dass Technologien wie das so genannte Deep Learning – eine Teildisziplin des Machine Learning, die derzeit den Hype der KI ausmacht – den Höhepunkt der Hype-Welle überschritten haben", gibt Krüger zu. „Trotzdem wird es technologisch weiterhin stark bergauf gehen, das Tempo der Innovationen womöglich sogar noch zunehmen. Deswegen investieren Forschungsinstitutionen in der Produktionstechnik derzeit kräftig in KI-Technologien und in Personal mit entsprechender Expertise." Dass dies die richtige Strategie ist, belegen Untersuchungen, die hohe Wertschöpfungspotentiale der KI für das produzierende Gewerbe aufzeigen. Das Institut für Innovation und Technik (IIT) in Berlin berechnete in seiner im Juli 2018 erschienenen Studie PAiCE, dass das KI-induzierte zusätzliche Wachstum im produzierenden Gewerbe von 2019 bis 2023 bei 31,8 Milliarden Euro liegen wird. Das entspricht in etwa einem Drittel des gesamten Wachstums der Branche in diesem Zeitraum. KI-Anwendungen könnten dabei die Überwachung und Wartung von Produktionsanlagen, optimiertes Ressourcen- und Wissensmanagement, Qualitätskontrolle, Robotik und nicht zuletzt intelligente Assistenzsysteme sowie Sensorik sein. Um die internationale Wettbewerbsfähigkeit des deutschen Innovationssystems auch weiterhin zu gewährleisten, empfehlen die Berliner daher weitere Forschungsaktivitäten. Dabei seien KI-Technologien mit Querschnittscharakter, wie etwa das maschinelle Lernen und Computer Vision, gezielt zu fördern.

Die richtigen Fragen finden und formulieren

„Wir müssen aber auch den Transfer der KI in das produzierende Gewerbe fördern", mahnt Krüger. „Noch ist der Wissenstransfer von der rasant fortschreitenden Forschung in die Wirtschaft ein Nadelöhr. Und auch die Ausbildung von Fachkräften hierzu wird noch nicht systematisch genug verfolgt. Das alles behindert den Transfer in die unternehmerische Praxis und damit die Wertschöpfung." Um diesen Transfer auf breiter Ebene in Gang zu bekommen und die vorhergesagten Potentiale schnell und effizient zu erschließen, sind produktionstechnische Kompetenzen gefragt. „Ein KI-System weiß nicht, was wir wie produzieren wollen", erklärt Krüger. „Wir müssen also zuerst einmal die für die Produktion notwendigen Fragen an KI-Systeme definieren und formulieren." Natürlich dürfe dabei auch nicht der Blick über den Tellerrand vergessen werden. „Ohne Expertise aus den Informations- und Kommunikationstechnologien beispielsweise lassen sich unsere gesteckten Ziele nicht erreichen." Eine höhere Wertschöpfung sehen die WGP-Experten übrigens nicht nur in vollautomatisierten Systemen, die meist nur in größeren Konzernen zu finden sind. Auch in teilautomatisierten Systemen und Assistenzsystemen für den Werker ließe sich die Wertschöpfung dank KI deutlich erhöhen. „Schaffen wir es, KI systematisch in Produktionsprozesse zu integrieren, ergeben sich klare Wettbewerbsvorteile für die gesamte deutsche Industrie", ist sich Krüger sicher. ■

www.wgp.de

Computer on Module

i-need.de PRODUCT FINDER

Direkt zur Marktübersicht: **www.i-need.de/75**

Sie versprechen eine **schnelle Anwendungsentwicklung** und die **Sicherheit eines erprobten Systems:** Computer on Module. Die **Anzahl an verfügbaren Systemen ist schier unübersehbar.** Unser Marktspiegel kann daher nur einen **kleinen Ausschnitt** daraus zeigen.

Die Beliebtheit der Boards ist kein Wunder, denn sie übertragen das Bild eines Computers auf eine Platine. Dementsprechend vollständig sind sie, was die üblichen Erwartungen angeht: CPU, Speicher, Grafik, Bussysteme und Erweiterungsmöglichkeiten. Und das auf einem Formfaktor, der uns immer wieder in Erstaunen versetzt, darüber welche hohe Leistung heute von so einer vergleichsweise kleinen Platine zur Verfügung gestellt wird. Insbesondere die Möglichkeit der Ergänzung um Expansion Boards spielt für Entwickler eine zentrale Rolle, denn sie sind häufig die Verbindung zum Prozess. *(kbn)* ■

Anbieter	Internet-Adresse	Produktbezeichnung(en)	Formfaktorbezeichnung
Adlink Technology	www.adlinktech.com	nanoX-BT COM Express Mini Size Type 10 Module	84 x 55 mm
Adlink Technology	www.adlinktech.com	cExpress-BW COM Express Compact Size Type 6	95 x 95 mm
Adlink Technology	www.adlinktech.com	cExpress-BL COM Express Compact Size Type 6	95 x 95 mm
Adlink Technology	www.adlinktech.com	cExpress-SL COM Express Compact Size Type 6	95 x 95 mm
Adlink Technology	www.adlinktech.com	Express-BL	125 x 95 mm
Adlink Technology	www.adlinktech.com	Express-BE COM Express Basic Size Type 6	125 x 95 mm
Adlink Technology	www.adlinktech.com	Express-SL COM Express Basic Size Type6	125 x 95 mm
Adlink Technology	www.adlinktech.com	ETX-BT	114 x 95 mm
Adlink Technology	www.adlinktech.com	Q7-BT Qseven Module with 4th Gen. Intel Atom	12 x 10 cm
Adlink Technology	www.adlinktech.com	LEC-BW SMARC Short Size Module	82 x 50 mm
Adlink Technology	www.adlinktech.com	LEC-Q1000 SMARC Short Size Module	
Adlink Technology	www.adlinktech.com	LEC-iMX6 SMARC Short Size Module	
Adlink Technology	www.adlinktech.com	LEC-BTS SMARC Short Size Module	
Axiomtek Deutschland	www.axiomtek.com	5th/4th Generation Intel Core COM Express Type	CEM881
Axiomtek Deutschland	www.axiomtek.com	4th Generation Intel Core i7/ i5/ i3 and Celeron	CEM880
Axiomtek Deutschland	www.axiomtek.com	Intel Atom Processor E3845 COM Express Type 6	CEM843
Axiomtek Deutschland	www.axiomtek.com	Intel Celeron Proc. J1900/N2807 COM Expr. T. 6	CEM842
Axiomtek Deutschland	www.axiomtek.com	CEM100	COM Express
Axiomtek Deutschland	www.axiomtek.com	CEM850	
Axiomtek Deutschland	www.axiomtek.com	CEM860	COM Express
Beck IPC	www.beck-ipc.com	IPC@CHIP SC145, IoT@chip	22,5 x 22,5 mm - 88pin Castellations
Bicker Elektronik	www.bicker.de	Com Express	
Bicker Elektronik	www.bicker.de	Com Express, Q7, ETX, SMARC	
Bicker Elektronik	www.bicker.de	Com Express, Q7, ETX	
congatec	www.congatec.com	COM Express Typ 7 conga-B7AC	95 x 125 mm (3.74" x 4.92") Basic
congatec	www.congatec.com	SMARC conga-SA5	82 x 50 mm (3,23" x 1,97")
congatec	www.congatec.com	Qseven conga-QA5	70 x 70 mm (2,75" x 2,75")
congatec	www.congatec.com	µQseven conga-UMX6	40 x 70 mm sub-credit-card
congatec	www.congatec.com	COM Express Typ 10 conga-MA4	55 x 84 mm (2.17" x 3.31")
congatec	www.congatec.com	COM Express Typ 6 conga-TCA5	95 x 95 mm (3,74" x 3,74")
Delta Components	www.delta-components.de	COM Express Module 620X	95 x 95 mm (W x L)
DH electronics	www.dh-electronics.de	DHCOM AM335x	
Emtrion	www.emtrion.de	emCON-RZ/G1M	82 x 50 x 10 mm
Emtrion	www.emtrion.de	emCON-RZ/G1E	82 x 50 x 10 mm
Emtrion	www.emtrion.de	emCON-RZ/G1H	
Emtrion	www.emtrion.de	DIMM-RZ/A1H	67.6 x 45 x 10 mm
Emtrion	www.emtrion.de	DIMM-AM335x	67,6 x 45 x 10 mm
Emtrion	www.emtrion.de	DIMM-MX537	DIMM-PC, 67,6 x 50 mm
Emtrion	www.emtrion.de	DIMM-MX6S/DL	SODIMM Modul
Emtrion	www.emtrion.de	DIMM-MX257	DIMM-PC

Bild: congatec AG

Bild: epis Automation GmbH & Co. KG

CPU Takt					Speicher		Em.-Betriebssysteme					Schnittstellen									
51 bis 500 MHz	501 bis 1.000 MHz	1 bis 2 GHz	über 2 GHz	Mehrproz. oder Multicore-CPU	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Linux (Varianten)	OS-9 / QNX / RTOS	VxWorks	Windows CE.net	Windows XP embedded	RS232 / RS422 / RS485	USB 2.0 / 3.0	Grafik	Audio	Drahtlose Schnittstellen	Massenspeicherschnittstellen	Digitale Ein-/Ausgänge	Ethernet 10 / 100 Mbit/s	Ethernet 1 Gbit/s	Feldbusschnittstellen	Starterkit, Applikationsboard
		•				to 4 GB (2 GB / 4 GB)	•		•				4x und 1x client		•		•	•	•	•		
		•				up to 8 GB	•						4x 3.0, 8x 2.0				•	•	•	•		
			•			up to 32 GB	•		•				2x 3.0, 6x 2.0		•		•	•	•	•		
			•			up to 32 GB	•						4x 3.0 + 4x 2.0				•	•	•	•		
	•					up to 32 GB	•		•				4x 1.1/2.0/3.0		•		•		•	•		
			•				•						4x 3.0 ,4x 2.0				•	•	•	•		
	•					up to 32 GB	•		•				4x v. 3.0 und 4x		•			•	•	•	•	
				•			•		•				4x 2.0		•		•		•			
		•					•	•	•				1x 3.0, 5x 2.0		•	•		•	•	•		
				•			•	•	•				1x 3.0 host, 2x	•	•		•	•	•	•		
•							•						1x 2.0 device; 2x host					•	•			
	•						•	•	•				2x 2.0 host, 1x OTG		•				•	•	•	
		•		•			•	•	•				1x 3.0 + 3x 2.0	•	•			•	•	•		
																			•	•		
		•			512 MB	8 GB	•			•	•		8	•	•		•	•	•	•		
		•			512 MB	8 GB							8	•	•		•	•		•		
				•	1 GB	16 GB	•			•	•		8x 2.0 / 2x 3.0	•	•		•	•				
	•	•		•	128 MB	128 MB	•	•				•	2 2.0	•	•	•	•		•		•	•
		•	•		2 GB	16 GB	•			•		•	2.0, 3.0	•	•		•	•	•	•		
	•	•	•		2 GB	16 GB	•			•	•	•	•	•	•		•	•	•	•	•	•
	•	•	•		512 MB	16 GB	•			•	•	•	•	•	•		•	•	•	•	•	
		•	•	•		48 GB	•		•				2x 3.0, 4x 2.0	•	•		•				•	
		•	•	•		8 GB	•						2x 3.0, 4x 2.0	•	•		•			•		
		•		•		8 GB	•						1x 3.0, 5x 2.0	•	•		•			•		
		•		•		1 GB	•						4x 2.0	•	•		•			•	•	
		•		•		4 GB	•						8x 2.0, 2x 3.0	•	•		•					
		•		•		8 GB	•							•	•		•				•	
		•				8 GB							11x (7x 2.0 und 4x 3.0)	•								
•	•	•			128 MB	512 MB	•	•				•	•	•	•	•	•	•	•	•	•	•
		•				1024 MB, 32 GB Fl.	•	•					1*host, 1*device	•	•			•		•		•
		•				2048 MB, 32 GB Fl.	•	•					1*host, 1*device	•	•		•	•	•			•
					1 GB	2 GB	•					•	1x host / 1x device		•			•	•	•	•	
•						10 MB,16 MB NOR F.	•					•	1*host, 1*device	•	•			•	•			•
	•				256 MB	1 GB	•					•	1*host, 1*device				•	•	•		•	•
	•				256 MB	1 GB	•	•		•		•	2	•	•		•	•	•		•	•
			•	•	512 MB	4 GB	•	•		•		•	1*host, 1*device	•	•		•	•	•		•	•
•					64 MB, 256 MB		•			•		•	2	•	•		•				•	•

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand 7.12.2018

MARKTSPIEGEL

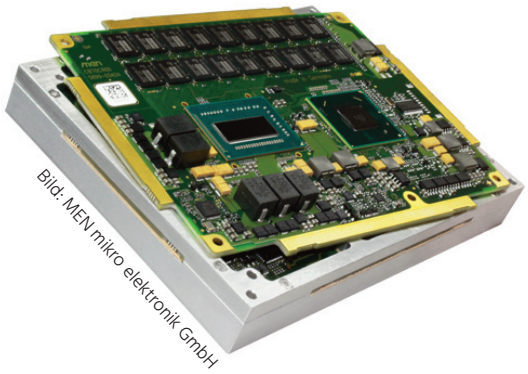


Bild: MEN mikro elektronik GmbH

Bild: Kontron Europe GmbH

Anbieter	Internet-Adresse	Produktbezeichnung(en)	Formfaktorbezeichnung
epis Automation	www.epis-automation.com	SOM-6894 und weitere SOM- Module	COM_Express 95 x 95 mm (95 x 125 mm)
esd electronics	www.esd.eu	CAN-CBX-CPU 5201	
F&S Elektronik Systeme	www.fs-net.de	COM QBlissA9	70 x 70 x 11 mm Qseven
F&S Elektronik Systeme	www.fs-net.de	COM PicoMODA5	80 x 50 x 10 mm PicoMOD
F&S Elektronik Systeme	www.fs-net.de	COM PicoMODA9	80 x 50 x 10 mm PicoMOD
F&S Elektronik Systeme	www.fs-net.de	SOM	100 x 80 x 11 mm NetDCUA5
F&S Elektronik Systeme	www.fs-net.de	COM efusA9	47 x 62.1 x 11 mm efus
F&S Elektronik Systeme	www.fs-net.de	COM efusA9X	47 x 62.1 x 11 mm efus
frenzel + berg electronic	www.frenzel-berg.de	hipecs CORE10	
GE Automation & Controls	www.geautomation.com/	bCOM6-L1400	Type 6 COM Express module, 95 x 125 mm
GE Automation & Controls	www.geautomation.com/	bCOM6-P1100 - Rugged COM Express	Type 6 COM Express module, 95 x 125 mm
GE Automation & Controls	www.geautomation.com/	bCOM6-L1200	Type 6 COM Express module, 95 x 125 mm
ICP Deutschland	www.icp-deutschland.de	IEM, ICE, iQ7	ETX, SOM Express, Q7
IEP Ing.-Büro f. Echtzeitprogra.	www.iep.de	Core-563	72 x 57 mm
IIE Ing.-Büro f. Industrie-Elek.	www.iie.de	ICE-QM871	COM Express Basic Type 6
INCOstartec	www.incostartec.com	LILLY-A837 ARM Cortex-A8, AM/DM37xx	
INCOstartec	www.incostartec.com	µLILLY-1135 ARM 1136JF-S, i.MX35x	51 x 51 x 11 mm
INCOstartec	www.incostartec.com	System On Module - picoLILLY1135 mit ARM1135	51 x 40 x 6 mm
Industrial Computer Source (D.)	www.ics-d.de	HM920-QM87	COM Express Basic, Type 2
Kontron	www.kontron.de	SMARC-sXBTi	SMARC
Kontron	www.kontron.de	COMe-mBT10	COMExpress Mini
Kontron	www.kontron.de	COMe-cPV2	COM Express compact;COM.0;Type 2; 95x95mm
Kontron	www.kontron.de	COMe-bHL6	125 x 95 mm COM Express Basic
Kontron	www.kontron.de	COMe-cHL6	
Kontron	www.kontron.de	COMe-bIP6RXT	
Mass	www.mass.de	Raspberry Pi 3B	
MEN Mikro Elektronik	www.men.de	CB70C Rugged COM Express Basic module	95 x 125 mm (3.74" x 4.92") Basic
MKC Michels & Kleberhoff Co.	www.mkc-gmbh.de	eNetMaxi	47 x 60 mm
MKC Michels & Kleberhoff Co.	www.mkc-gmbh.de	eNetMini	32 x 41.1 mm
MKC Michels & Kleberhoff Co.	www.mkc-gmbh.de	eWebSrv	60 x 47 x 8 mm (BxTxH)
SSV Software Systems	www.ssv-embedded.de	eSOM/3517	eSOM-200, 80 x 50 mm
SSV Software Systems	www.ssv-embedded.de	eSOM/2586	eSOM-200, 80 x 50 mm
SSV Software Systems	www.ssv-embedded.de	DNP/9263	DIL-64
SSV Software Systems	www.ssv-embedded.de	eSOM/9263	eSOM-200, 50 x 80 mm
SYS TEC electronic	www.systec-electronic.com	ECUcore-1021	55 x 84 mm
Syslogic	www.syslogic.de	Syslogic CoreExpress Serie	Core Express, 65 x 9 x 58 mm
taskit	www.taskit.de	Stamp9G45	53,6 x 38 x 6 mm
taskit	www.taskit.de	Stamp9G20	53 x 38 x 6 mm
TES Electronic Solutions	tes-dst.com	i. MX 6 basiert, alle Prozessorvarianten	SMARC Formfaktor
Toradex AG	www.toradex.com	Familie der Apalis ARM Computermodule (CoMs)	45 x 82 mm
TQ-Systems	www.tq-group.com	COM Express Mini, Type 10	84 x 55 mm
TQ-Systems	www.tq-group.com	COM Express Compact Module, Type 6	
TQ-Systems	www.tq-group.com	TQMLS102xA - mit Layerscape LS102xA	55 x 44 mm
TQ-Systems	www.tq-group.com	TQMa6x (ARM9)	70 x 46 mm
TQ-Systems	www.tq-group.com	TQMa53 (ARM Cortex-A8)	55 x 44 mm (TQMa53)
TQ-Systems	www.tq-group.com	TQMa335x (ARM8)	54 x 38 mm
TQ-Systems	www.tq-group.com	TQMa28 (ARM9)	26 x 40 mm
X-SPEX	diris.eu	Video-Rekorder-Board (für Aufnahme, Verarb. usw.)	100 x 80 mm

CPU Takt					Speicher		Em.-Betriebssysteme					Schnittstellen									
51 bis 500 MHz	501 bis 1.000 MHz	1 bis 2 GHz	über 2 GHz	Mehrproz. oder Multicore-CPU	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Linux (Varianten)	OS-9 / QNX / RTOS	VxWorks	Windows CE.net	Windows XP embedded	RS232 / RS422 / RS485	USB	Grafik	Audio	Drahtlose Schnittstellen	Massenspeicherschnittstellen	Digitale Ein-/Ausgänge	Ethernet 10 / 100 Mbit/s	Ethernet 1 Gbit/s	Feldbusschnittstellen	Starterkit, Applikationsboard
		•				16 GB	•						10x							•		
•				•	500 MB SD		•	•	•			•	1						•		•	
		•			1 GB	4 GB	•	•					5x		•	•	•		•	•		•
•				•	512 MB	512 MB	•						2x		•		•	•	•			•
		•			512 MB	4 GB	•						3x		•	•	•	•	•			•
•				•	256 MB	512 MB	•						2x		•		•	•	•			•
		•			512 MB	1 GB	•						2x		•		•		•	•		•
•	•			•	512 MB	1 GB	•						2x	•	•	•	•		•	•		•
•												•	1				•	•	•		•	
		•			2 GB	8 GB	•		•		•		8 2.0, 4 3.0	•	•		•			•		
		•			2 GB	8 GB	•	•	•				7 2.0 host, 1 2.0 device	•	•		•			•	•	
	•	•			2 GB	8 GB	•		•		•	•	8	•	•		•			•	•	
		•	•	•	1 GB	4 GB	•			•	•	•	6	•	•	•	•	•	•	•		
•					8 MB/8,5 MB F.	8 MB/ 8,5 MB F.		•				•					•	•	•		•	
			•		1 GB	16 GB						•	8x 2.0, 4x 3.0	•	•		•		•			•
•	•	•	•	•	128 MB	32 GB	•			•	•	•	3	•	•		•	•	•	•	•	•
•					128 MB	256 MB	•			•		•	3	•	•	•	•	•	•			
	•				128 MB	256 MB	•			•		•	2x 2.0			•	•	•	•		•	
				•	1 GB	16 GB							8 2.0	•				•				
				•		bis zu 8 GB	•		•			•	1x 3.0 und 2x 2.0	•			•	•		•		
				•		bis zu 8 GB	•		•			•	2x 3.0 bis zu 8x 2.0	•	•		•		•	•		
		•				4 GB	•	•	•	•	•		8x 2.0	•	•		•		•	•	•	
				•		16 GB	•		•				4x 3.0, 4x 2.0	•	•		•		•	•		
				•		bis zu 16 GB	•		•				2x 3.0, 8x 2.0	•			•		•	•		
				•		bis zu 16 GB	•		•				4x 3.0, 4x 2.0	•	•		•		•	•		
				•	1 GB		•	•				•	4x 2.0	•	•	•	•	•	•		•	
			•	•		16 GB	•						4 3.0, 4 2.0	•	•		•			•		
	•			•	512 MB		•					•	2x				•	•	•			•
•					256, 512KB F.,...			•				•	bis zu 24 GPIOs und/oder					•	•			•
•					16 MB,32 MB Fl.		•					•						•	•		•	•
	•				256 MB		•						2	•		•			•		•	•
	•				128 MB	a.A.	•	•	•	•	•								•	•	•	
•					32 MB	32 MB	•						1				•		•		•	•
•					128 MB	128 MB	•						2	•			•		•		•	•
			•	•	1 GB		•			•	•		2x host 1x de. 2.0 1x host		•				•		•	•
		•			512 MB	2 GB	•			•	•											
•					128 MB	512 MB	•			•		•	2x host, 1x device	•				•	•			•
•					64 MB	128 MB	•			•		•	2x host, 1x device					•	•			•
	•				512 MB	4 GB	•				•	•	1x 2.0 OTG, 2x 2.0 host	•	•	•	•	•		•	•	
	•	•		•	512 MB, 4 GB	4 GB, 16 GB eMMC	•	•					3.0, 2.0	•	•	•	•			•	•	
		•			2 GB	8 GB	•				•	•	4x (3.0, 2.0)	•	•	•	•			•		
					4 GB	16 GB	•				•	•	8x	•	•	•	•			•		
	•				bis 2 GB	bis 16 GB/512 MB	•	•	•			•	•	•				•	•	•		
	•				bis 2 GB	bis zu 16 GB	•	•	•			•	•	•			•		•	•	•	•
	•				bis 1 GB	16 GB e-MMC	•	•		•		•	•	•	•		•	•	•		•	•
	•				bis 512 MB	bis 16 GB	•	•				•	•	•	•				•	•	•	
•					bis 256 MB	bis 16 GB	•	•	•	•		•	•	•	•		•	•	•		•	•
	•					4 GB	•					•	•	•	•	•	•	•	•		•	•

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand 7.12.2018

embeddedworld2019
Exhibition&Conference
... it´s a smarter world

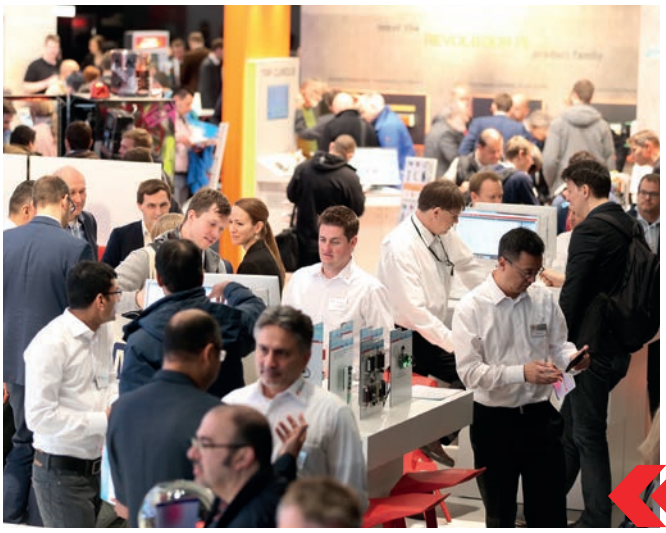
Embedded World 2019

Innovationen leben vom Wissensaustausch und Fachmessen spielen bei diesem Wissensaustausch eine wichtige Rolle. Vom 26. bis 28. Februar 2019 ist wieder Embedded World in Nürnberg.

Die Embedded World hat sich einen festen Platz im Terminkalender vieler Entwickler und Hersteller erarbeitet – das beweisen die stetig wachsenden Besucher- und Ausstellerzahlen aus dem In- und Ausland. Das dürfte sie auch ihrem klaren Fokus auf Embedded-Technologien verdanken. Reisen bildet, so heißt es. Und was im allgemeinen gilt, das gilt für die Reise zu einer Fachmesse erst recht: Allzu oft stecken wir so sehr in unserem Tagesgeschäft, dass man den Freiraum für neue Ideen verliert. Die Embedded World präsentiert Innovationen und Besucher können sich auf Sonderschauen über neueste Trends und Produktentwicklungen informieren. Das schafft Raum für Kreativität und neue Ideen.

Arbeitsmesse

Die Embedded World ist eine typische Arbeitsmesse: Hier wird über konkrete Lösungen geredet, über Technologien diskutiert und gelernt, hier treffen sich Gegenwart und Zukunft der Embedded-Branche. Zu einer festen Institution wurde mittlerweile der Student Day. Mit Unterstützung von Sponsoren erhalten 1.000 Hochschüler aus Deutschland und Österreich die Gelegenheit, ihr Fachwissen zu vertiefen und Kontakte zu möglichen Arbeitgebern zu knüpfen. Am 'Gemeinschaftsstand Junge Unternehmen' zeigen innovative Unternehmen ihre produkt- und verfahrensmäßigen Neuentwicklungen.



Bilder: ©Frank Boxler / NürnbergMesse GmbH

Inserentenverzeichnis

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,
E-Mail: kbinder@tedo-verlag.de)
Georg Hildebrand (ghl),

WEITERE MITARBEITER
Bastian Fitz, Tamara Gerlach, Frauke Itzerott, Pascal Jenke, Susan Jünger, Theresa Klingelhöfer, Kristine Meier, Melanie Novak, Christina Jilg, Sarah-Lena Schmitt, Florian Streitenberger, Natalie Weigel, Sabrina Werking

ANZEIGEN
Markus Lehnert, Tel.: +49 6421 3086-0,
E-Mail: mlehnert@tedo-verlag.de
Es gilt die Preisliste der Mediadaten 2018

GRAFIK & SATZ
Julia Marie Dietrich, Tobias Götze, Fabienne Heßler, Kathrin Hoß, Melissa Hoffmann, Ronja Kaledat, Patrick Kraicker, Moritz Klös, Timo Lange, Ann-Christin Lölkes, Nadin Rühl

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

ERSCHEINUNGSWEISE
4 Hefte für das Jahr 2019

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

Titelbilder:
Kontron S&T AG (1);
©jamesteohart / istockphoto.com (1)

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

2ew19P
E-Code für freien Eintritt
embedded-world.de/gutschein

Nürnberg, Germany
26.–28.2.2019

embedded world
Exhibition&Conference
... it´s a smarter world

INNOVATIONEN ENTDECKEN

Tauchen Sie ein in die Welt der Embedded-Systeme und entdecken Sie Innovationen für Ihren Erfolg.

embedded-world.de

Medienpartner

Markt&Technik – Die unabhängige Wochenzeitung für Elektronik
Computer & Automation – Fachmedium der Automatisierungstechnik
DESIGN&ELEKTRONIK – Know-how für Entwickler
SmarterWorld – Solutions for a Smarter World
Elektronik – Fachmedium für industrielle Anwender und Entwickler
MEDIZIN elektronik – Fachmedium für Elektronik in der Medizintechnik
Elektronik automotive – Fachmedium für professionelle Automobilelektronik
elektroniknet.de

Veranstalter Fachmesse
NürnbergMesse GmbH
T +49 9 11 86 06-49 12
F +49 9 11 86 06-49 13
besucherservice@nuernbergmesse.de

Conference organizer
WEKA FACHMEDIEN GmbH
T +49 89 2 55 56-13 49
F +49 89 2 55 56-03 49
info@embedded-world.eu

NÜRNBERG MESSE