+++ KI in industriellen Applikationen S. 28 +++

1/2020
www.iot-design.de

TeDo Verlag GmbH
Februar
€ 7,80

Echtzeitbetriebssysteme
Die neue Rolle des RTOS in Embedded Systems
S. 44

IoT DESIGN
Smarte Systeme für das Internet of Things

Mit dem Cellular Twin per Plug&Play ins IoT
S. 6

grandcentrix
A Vodafone Company

Titelbild: ©NatalyaBurova/istockphoto.com

Code Coverage im IoT
Testabdeckung bei kleinen Targets
S. 32

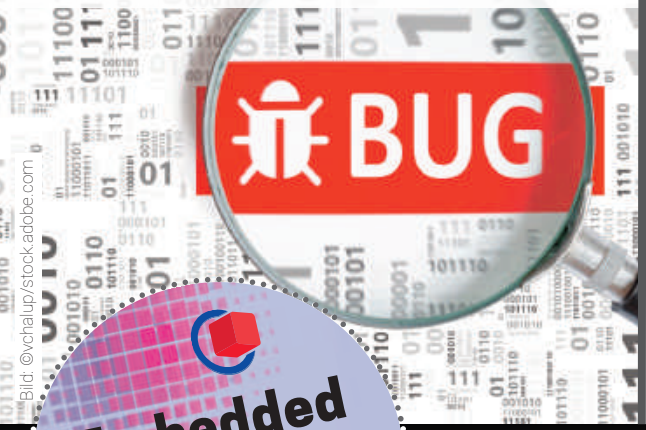
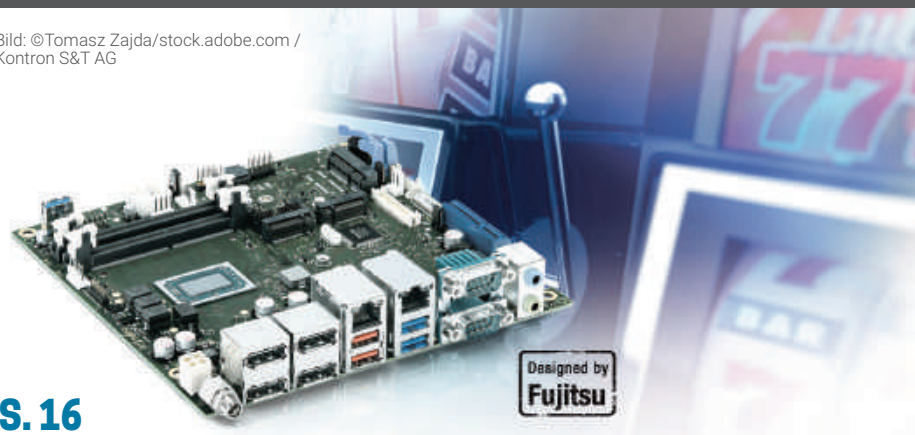


Bild: ©vchalup/stock.adobe.com

Bild: ©Tomasz Zajda/stock.adobe.com / Kontron S&T AG



S. 16

Anwendungsspezifische Motherboards
Angebot noch differenzierter

Embedded World
ab S. 9

» Embedded Security
IoT-Sicherheit eingebettet in Speicherkarten
S. 22

2ew20P
Ihr e-code für freien Eintritt
embedded-world.de/gutschein

Nürnberg, Germany
25.–27.2.2020

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

INNOVATIONEN ENTDECKEN

Über 1.000 Firmen und mehr als 30.000 Besucher aus 84 Ländern – hier trifft sich die Embedded-Community.

Seien Sie mit dabei! Jetzt kostenloses Ticket sichern!

Ihr e-code für freien Eintritt: 2ew20P

embedded-world.de/gutschein

@embedded_world #ew20 #futurestartshere

Medienpartner

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

Veranstalter Fachmesse

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

Veranstalter Konferenzen

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

NÜRNBERG MESSE

Editorial

Das Thema Embedded-Systeme bleibt heiß. Ein Indikator dafür: Die Embedded-World-Messe in Nürnberg überschreitet 2020 erneut die Ausstellungsfläche des Vorjahres und vergrößert sich um eine Halle. Es werden 1.150 Aussteller und rund 30.000 Besucher aus aller Welt erwartet. Fokusthemen der Veranstaltung sind unter anderem IoT und Embedded Systems sowie Software Engineering, Energieeffizienz und Functional Safety und Security – und damit so ziemlich alles, worum es sich auch immer in unserer IoT-Design dreht. Kein Wunder, denn die aktuellsten Fachinformationen über Hardware, Software und Methoden sind in unserer sich schnell ändernden Welt von zentraler Bedeutung, will man in umkämpften Märkten auf das richtige Pferd setzen.

Eins steht nämlich fest: Wer sich heute mit der Entwicklung von Embedded-Systemen für das Internet der Dinge beschäftigt, bei dem kommt so schnell keine Langeweile auf, denn die Welt ist im Umbruch: Neue Geschäftsmodelle können für ihre Anwendungen stets mehr Rechenleistung bei weniger Abwärme sehr gut gebrauchen. Gleichzeitig sind die Cyber-Security-Bedrohungen nicht nur häufiger, sondern auch differenzierter geworden, sodass die Themen Security by Design und das dazugehörige Testing immer aufwändiger werden. Und in Zeiten von Fachkräftemangel und Disruption soll man auch noch die Time-To-Market verbessern. Das funktioniert nur, wenn man nicht den Anspruch hat, alles selber zu machen, sondern an den richtigen Stellen auf Plug&Play-Lösungen setzt, die sich schnell und effizient auf einen konkreten Anwendungsfall anpassen und in die Marktreife überführen lassen. Eine solche Lösung stellen wir übrigens in unserer Coverstory vor (S. 6ff).

Wer die Nutzung von KI-Methoden direkt auf Embedded-Systemen plant, für den fängt die Sache gerade an interessant zu werden – auch das ein Thema dieser Ausgabe (S. 28ff). Die Rechenleistung, selbst für ‘normale’ wissensbasierte KI-Mechanismen, ist immer noch sehr hoch. Dennoch beginnt die dafür notwendige Rechenleistung auch auf Embedded-Systemen zur Verfügung zu stehen: Dafür sind die SoCs V1000 von AMD ein gutes Beispiel. Darin vereint das Unternehmen die Leistung der Zen CPU- und der Vega GPU-Architekturen in einem stromsparenden (12 bis 54W) Chip, der eine Rechenleistung bietet, die vor wenigen Jahren mehrere huntert Watt verbraucht hätte.

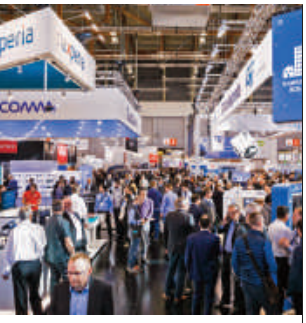
Die Möglichkeiten sind vielfältig, die Bedrohungen auch. Alles Wissenswerte rund um Embedded-Systeme und das Internet der Dinge gibt es wieder auf der Embedded World und mit jeder Ausgabe der IoT-Design.

In diesem Sinne wünsche ich Ihnen viel Spaß beim Lesen.

Ihr

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

Inhalt 1/2020



9

Embedded World
Messevorbericht

Marktspiegel
PC/104-Boards

Marktspiegel
Seite 24

34

News:
Beste Innovation bei der IoT-Sicherheit

SERVICE

NEUHEITEN

FACHWISSEN

IOT NEWS

Marktübersicht
Echtzeitbetriebssysteme (RTOS)

Marktübersicht Seite 35

Mit dem Cellular Twin

AUTOREN: Christian Pereira, SVP Sales & Operations und Fabian Kochem, Business Development Team Leader, Grandcentrix GmbH **BILDER:** Grandcentrix GmbH

Ein Blick in den Markt offenbart: **IoT-Produkte des deutschen Mittelstands sind nach wie vor rar gesät.** Nicht nur der notwendige Mut, es ist vor allem das Knowhow, das den mittelständischen Unternehmen für die Entwicklung und Umsetzung disruptiver Produkte und Services fehlt. **Helfen können echte Plug&Play-Lösungen** wie der Cellular Twin von grandcentrix. Denn sie bringt alles mit, was es braucht, um Anwendungen **schnell, effizient und zukunftsfähig** zu vernetzen.

per Plug&Play ins IoT

Bild: ©NatalyaBurova/istock.com

Viele mittelständische Unternehmen tun sich nach wie vor schwer, wenn es darum geht, die eigenen Produkte zu vernetzten und neue Geschäftsmodelle zu entwickeln. Das größte Manko ist zweifelsohne das fehlende Know-how und die Tatsache, dass sich dies in der aktuellen Situation auch weder zeitnah aufbauen noch einkaufen lässt. Hinzu kommt, dass der IoT-Markt mit prinzipiell guten Lösungsbausteinen zu stark fragmentiert und unübersichtlich ist. So stellt allein die Auswahl der einzelnen Komponenten sowie deren Orchestrierung für die meisten Unternehmen eine zu große Hürde dar, die überdies mit hohen Kosten und einem hohen zeitlichen Aufwand verbunden ist. Auch extern geführte Projekte sind – aus ähnlichen Gründen – für die meisten keine Option.

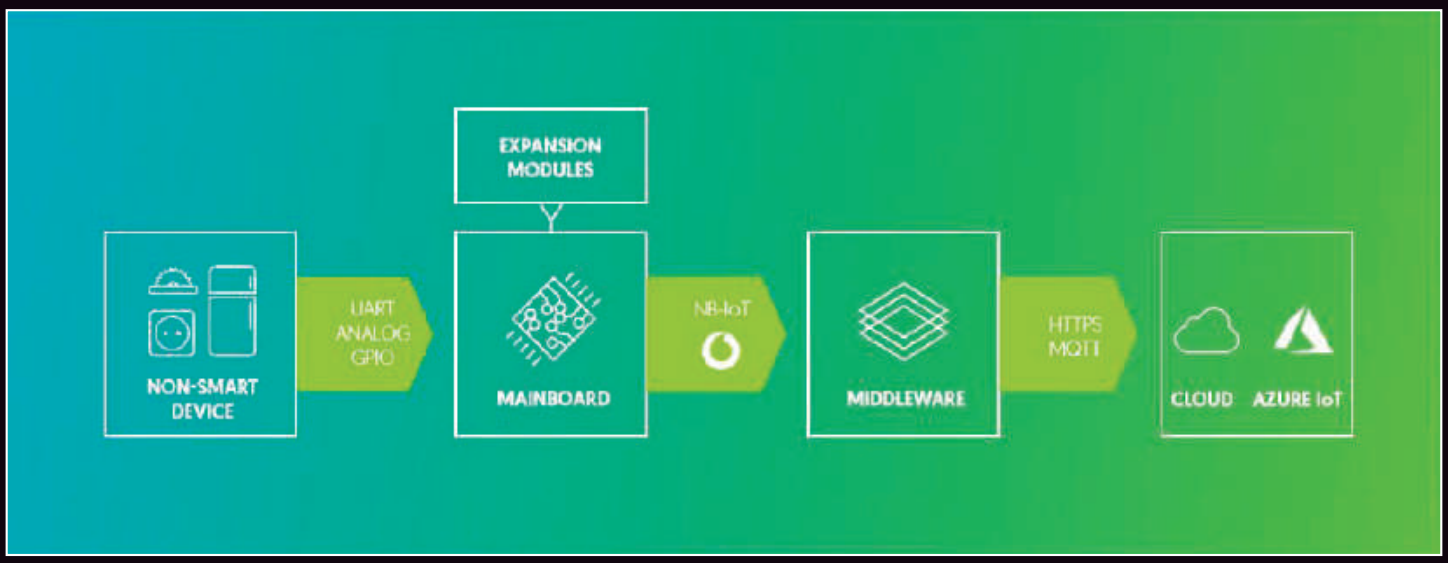
Wirklich helfen können ganzheitliche, integrierte Standard-IoT-Bausteine, die sich schnell und effizient auf einen konkreten Anwendungsfall anpassen und in die Marktreife überführen lassen. Eine solche Plug&Play-Lösung ist der Cellular Twin von grandcentrix. Er bringt das gesamte, notwendige Technologiespektrum vom Produkt bis zur Cloud mit: Hardware, Elektronikkomponenten, Software, Konnektivität.

Mittelstandstaugliches Mainboard

Geht es ausschließlich um die Hardware-Komponente, reiht sich das Mainboard – das Bindeglied zwischen Produkt und Internet – in die Riege klein dimensionierter Platinen ein, die daher auch in knapp bemessenen Bauraum integrierbar sind (Vgl. Bild 1). Doch der IoT-Baustein hebt sich von gängigen Angeboten ab, indem er als durchdachte IoT-Plattform konzipiert ist. Was gehört also zu diesem Gesamtpaket? Die Verbindung zur Produktsteuerung erfolgt über eine 15-polige Schnittstelle, die Verbindung zum Internet über ein integriertes Modem. Auf der Schnittstelle stehen jeweils vier digitale und analoge Eingänge (0-10V) sowie zwei digitale Ausgänge zur Verfügung. Hiermit deckt sie den Großteil der gängigen, industriellen Anwendungen ab. Zudem ist sowohl der Anschluss von simplen, analogen Sensoren und digitalen Tastern als auch von komplexeren Schnittstellen wie TTL-UART möglich. Gleiches gilt für externe LTE- oder GPS-Antennen. Nicht zuletzt erfolgt über die Schnittstelle die Stromversorgung des Mainboards – mit einem Spannungsbereich zwischen 3,3V und 17V.

Sind für den Einbau oder das Unterbringen von Sensoren weitere, physikalische Schnittstellen erforderlich, stehen sogenannte Daughterboards zur Verfügung, mit denen das Mainboard flexibel und für den konkreten Anwendungsfall erweiterbar ist. Dieser Architekturansatz (Vgl. Bild 2) unterscheidet den Cellular Twin von vielen, marktüblichen Angeboten und macht ihn vor allem auch für mittelständische Unternehmen attraktiv. Denn dieses Baukastensystem ermöglicht die einfache Integration spezieller Industrie-Standards wie RS485, RS232 oder 24V I/O und verhindert gleichzeitig das künstliche Aufblähen der Hauptplatine. Das spart Teile, minimiert die Produktionskosten und erhöht damit die eigene Marge.

Cellular Twin



Durch seine Architektur im Baukastensystem ermöglicht Cellular Twin die einfache Integration von Industriestandards.

OTA-Updates trotz NB-IoT

Die Verbindung zum Internet erfolgt auf Basis von Narrowband-IoT (NB-IoT) oder CAT-M1. Durch die Nutzung der lizensierten und weltweit flächendeckend ausgebauten Mobilfunkstandards garantiert grandcentrix eine hohe Quality-of-Service ihrer Anwendung – auch in entlegene Regionen oder bis in Kellergeschosse hinein. Doch im Kontext von Narrowband-IoT-Lösungen gilt es auch drei wesentliche, technische Herausforderungen zu lösen, die dem Fokus auf geringe Bandbreiten und kleine Datenvolumina geschuldet sind. So erschwert die geringe Datenübertragungsrate (0,2Mbps down, 0,02Mbps up) Over-the-Air (OTA) Firmware-Updates von mehreren Megabytes. OTA-Updates sind aber eines der wesentlichen Merkmale smarter Produkte. Auch die Verwendung von UDP als Datenübertragungsprotokoll ist nicht unproblematisch, da es in der Verwendung deutlich komplexer ist als das bekannte TCP Netzwerkprotokoll. Nicht zuletzt wird bei hohen Stückzahlen das Handling von SIM-Karten bzw. Preisverhandlungen mit den Carriern zum relevanten Faktor smarter Produkte. Der Cellular Twin löst die beschriebenen Herausforderungen wie folgt:

- Over-the-Air-Updates: Der relevante Teil der Firmware (kunden-individuelles Verhalten und Konfigurationsparameter) ist vom Betriebssystem entkoppelt und die isolierte Aktualisierung über NB-IoT – Over-the-Air möglich. Entscheidend ist das eingesparte Datenvolumen.

- Cloud-Einbindung: Die Transformation von UDP nach TCP löst das Verarbeitungsproblem der gesendeten Datenpakete und ermöglicht die Integration aller gängigen Cloud-Systeme.

- Carrier-Integration: Das Mainboard ist bereits mit einer SIM-Karte ausgestattet. Sie wird automatisch aktiviert, wenn das Gerät mit Strom versorgt wird.

Einen messbaren Mehrwert bieten die via Mobilfunk übermittelten Daten häufig erst durch die Analysen und Auswertungen angeschlossener Plattformen – bzw. durch die Verknüpfung mit anderen Prozessen wie APIs oder Message Broker. Hierfür ist das Mainboard mit einer Middleware ausgestattet, die MQTT-Server sowie beliebige HTTP(s) bedienen kann. Microsoft Azure IoT wird darüber hinaus nativ unterstützt. Sollte keines dieser Systeme zur Verfügung stehen, ermöglicht die Unterstützung von Azure IoT Central eine schnelle Visualisierung der übertragenen Daten.

Schnelle Marktreife

Es ist der umfassende Ende-zu-Ende-Ansatz, der den Cellular Twin zu einem Plug&Play-Angebot, das seinen Namen wirklich verdient. Letztlich hat das orchestrierte Gesamtangebot auch einen erheblichen Einfluss auf die Faktoren Zeit und Kosten: Entscheiden sich Unternehmen für den IoT-Baustein, ist schon nach wenigen Monaten der Start in die Serienproduktion möglich. Die Kosten liegen etwa 80 Prozent unter den gängigen Summen für Digitalisierungsvorhaben. Dem Mittelstand stehen hierdurch alle Optionen offen, wertvolle Marktanteile zu sichern bzw. zu erobern. ■

www.grandcentrix.net

Die Embedded World Exhibition & Conference 2020 auf Erfolgskurs

Die Embedded World ist die weltweit größte Fachmesse mit begleitenden Konferenzen rund um Embedded-Technologien und die internationale Leitmesse der Embedded-Community. Sie findet vom 25. bis 27. Februar 2020 in Nürnberg statt.

Besucher der Embedded World 2019

Jetzt Dein Ticket 2020 sichern!

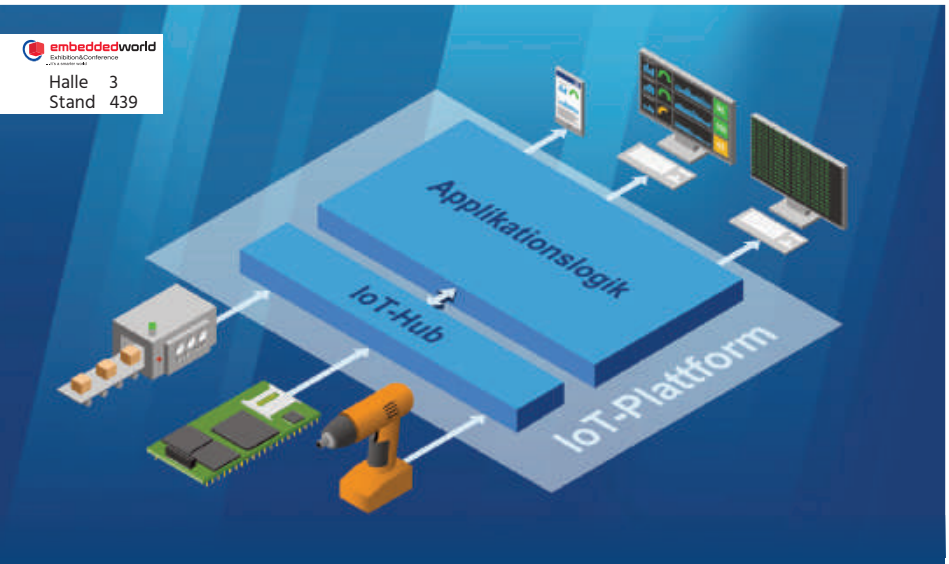
TEXT und BILD: NürnbergMesse GmbH

Die Embedded World überschreitet 2020 erneut die Ausstellungsfläche des Vorjahres und vergrößert sich um eine Halle. Es werden an die 1.150 Aussteller und rund 30.000 Besucher aus aller Welt erwartet. Fokusthemen sind unter anderem IoT und Intelligent Systems sowie Software Engineering, Energieeffizienz und Functional Safety und Security. Die beiden Konferenzen, Electronic Displays Conference und die Embedded World Conference, finden wieder zeitgleich zur Messe statt. Mit fast 180 Stunden intensiver Wissensvermittlung untermauert die Veranstaltung ihren Leitanspruch auch in Sachen Performance und Qualität.

Fachwissen von Experten für Experten

Expertpanels zu Embedded Vision, Safety & Security und Embedded Intelligence liefern den Fachbesuchern in den Foren dediziertes Expertenwissen und die Möglichkeit sich den Diskussionen zu beteiligen. Die Sonderpräsentationen machen das theoretische Fachwissen in den Hallen für die Besucher erlebbar. Eine kostenlose Eintrittskarte können Messebesucher schon jetzt mit dem **Gutscheincode ew20future** auf der Homepage der Embedded World erhalten. ■

www.embedded-world.de



embeddedworld Exhibition&Conference
Halle 3
Stand 439

IOT RETROFIT SDK

SSV hat ein System Development Kit entwickelt, um mit Hilfe von Sensoren, Gateways und KI-Diensten die IoT-Anwendungen der nächsten Generation schon heute als Retrofit zu realisieren. Die im SDK enthaltenen Treiber, Bibliotheken und **vollständig funktionsfähigen Codebeispiele** ermöglichen zusammen mit verschiedenen Sensoren und einem vorkonfigurierten Embedded Gateway den **schnellen Einstieg** in eigene Projekte. Eine mögliche Anwendung im Umfeld von Maschinen und Anlagen ist die **Kombination eines Machine-Learning-Algorithmus** zur automatischen 24/7-Zustandsüberwachung vor Ort mit einem Remote Collaboration Service zur Fehlerbehebung in der Cloud. Erkennt das Zustandsmonitoring einen Fehler, verständigt es über die Benachrichtigungsfunktionen einer IoT-Plattform den Service. Ein Mitarbeiter am Standort des Herstellers analysiert die in einer IoT-Datenbank gespeicherten Trenddaten der Anlage und unterstützt den Kunden bei der Fehlerbeseitigung. Das erste SDK ist ab Q1/2020 lieferbar. Eine weitere Variante ist zusammen mit einem NB-IoT-Modem und integrierter SIM-Karte ab Mitte 2020 erhältlich, um Machine-Learning-basierte Softsensor-Anwendungen für das Condition-based Monitoring über flächendeckende, zellulare IoT-Funknetze zu realisieren.

SSV SOFTWARE SYSTEMS GMBH ▪ WWW.SSV-EMBEDDED.DE

DK IoT Studio

Höchstmaß an *EINFACHHEIT*

Digi-Key stellt das DK IoT Studio vor. Die integrierte Entwicklungsumgebung soll Entwicklern und Anbietern die Erstellung von IoT-Lösungen erleichtern: *In wenigen Minuten von der Idee zum Prototyp, ganz ohne einen Code zu schreiben.* Indem sie Sensoren, Prozessoren und andere Bauteile aus der Bibliothek einfach auf die Entwicklungsoberfläche ziehen, können Benutzer Verbindungen herstellen und mit der Datenerfassung beginnen, die dann an ein Mobilgerät oder in die Cloud gesendet werden.

embeddedworld Exhibition&Conference
Halle 4A
Stand 633

Digi-Key Electronics • www.digikey.de

CODEANALYSE MIT ERWEITERTEN EINSATZMÖGLICHKEITEN

GrammaTech gibt die Verfügbarkeit von CodeSonar 5.2 bekannt. Durch die Software kann die statische

embeddedworld Exhibition&Conference
Halle 4
Stand 423

Codeanalyse mit einem einheitlichen Tool, sowohl bei Embedded-Systemen als auch bei Enterprise-Anwendungen durchgeführt werden. Die Unterstützung von Compilern und offenen Standards wurde verbessert. So arbeitet CodeSonar 5.2 mit den jeweils aktuellsten Versionen der Compiler JAR, GNU C und CLang zusammen.

GrammaTech Inc. • www.grammatec.com

Doppelpulstest in einer Minute

DAS SOFTWARE-PLUGIN FÜR DEN ARBITRÄR-/FUNKTIONSGENERATOR AFG31000 ERMÖGLICHT DIE DURCHFÜHRUNG VON DOPPELPULS-TESTS IN WENIGER ALS EINER MINUTE. ES ERLAUBT EINE IMPEDANZANPASSUNG ÜBER DIE PULSDAUER UND DEN ZEITABSTAND ZWISCHEN DEN PULSEN BEI BIS ZU 30 PULSEN. DIE PULSDAUER IST VON 20NS BIS 150MS EINSTELLBAR.

Tektronix GmbH, www.tektronix.de

embeddedworld Exhibition&Conference
Halle 4
Stand 104

» PCB-Design

embeddedworld Exhibition&Conference
Halle 4
Stand 371

Altium stellt die PCB-Design-Software Altium Designer 20 vor. Neuerungen sind z.B. der schnellere Schaltplaneditor, das High-Speed-Design oder die erweiterten interaktiven Router-Funktionen. Die neuen Features machen Board-Designs schneller und verbessern den Designvorgang. Neben dem Routing und Design wurde auch die Benutzerfreundlichkeit des Tools verbessert.

Altium Europe GmbH • www.altium.com

embeddedworld
Halle 3
Stand 235

Multi-Wireless-Modem

Gemeinsam mit Laird Connectivity präsentiert m2m Germany das neue Multi-Wireless-Modem Pinnacle 100. Der Pinnacle 100 kombiniert LTE CAT-M1, NB-IoT und Bluetooth. Das Modem ist eine voll integrierte Lösung und vereint die Vorteile der energiesparenden zellularen LTE-Konnektivität und die der Bluetooth 5-Technologie. Diese Kombination ermöglicht neue Anwendungsfälle mit kostengünstigen, Long-range Bluetooth-Sensoren, die alle an das LTE-Netzwerk der nächsten Generation angeschlossen werden können – bei einer viel einfacheren und kostengünstigeren Lösungsarchitektur. Der Pinnacle 100 beinhaltet einen leistungsstarken Cortex M4F-Controller mit einer hostlosen Zephyr RTOS-basierten Softwareimplementierung, vollständiger Bluetooth 5-Funktionalität und LTE CAT-M1/NB-IoT-Funktionen – allesamt vollständig zertifiziert. Dieses intelligente Modem bietet zusätzlich vollständige Antennenflexibilität, auf Grund von vorintegrierten und externen Optionen wie Laird's Revie Flex LTE und NB-IoT Antenne.

m2m Germany GmbH, www.m2mgermany.de

Energiesparendes Bluetooth-Modul

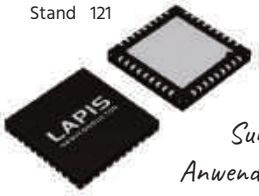
embeddedworld
Halle 4A
Stand 544

Das energiesparende PAN1740A Bluetooth 5.0-Modul zeichnet sich durch eine kompakte Größe aus. Es ist eine Weiterentwicklung, die eine SCHNELLERE BOOTZEIT bietet und BIS ZU ACHT VERBINDUNGEN unterstützt, um MEHR FLEXIBILITÄT bei der Erstellung anspruchsvollerer Anwendungen zu ermöglichen. Es kann als eigenständiger Anwendungsprozessor oder als Data Pump in gehosteten Systemen eingesetzt werden. Das Modul ist optimiert für Fernbedienungen (RCU) und die Unterstützung für Sprachbefehle. Es ist mit nur 9,0 x 9,5 x 1,8mm sehr kompakt und verfügt über ein Dialog-DA14585-Board und einen ARM Cortex-M0 Mikrocontroller. Der Betriebstemperaturbereich liegt zwischen -40 und 85°C.

Panasonic Industry Europe GmbH
www.panasonic.com

Drahtlose Kommunikation im Sub-GHz-Bereich

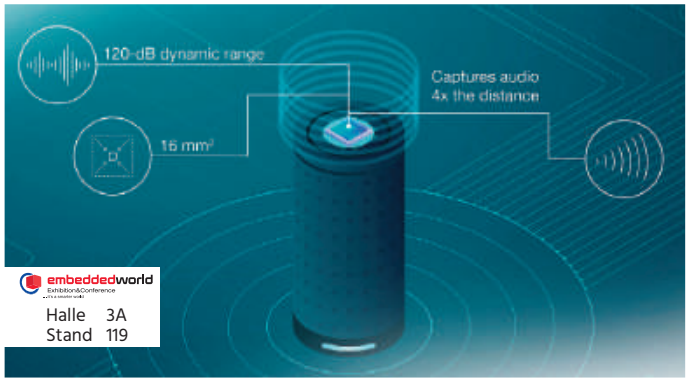
embeddedworld
Halle 3A
Stand 121



Der Multiband-LSI-Baustein ML7424 von Lapis Semiconductor ist für die drahtlose Kommunikation im Sub-GHz-Bereich entwickelt worden. Er eignet sich für Anwendungen, die über relativ große Übertragungsdistanzen eine geringe Leistungsaufnahme verlangen. Er deckt sowohl den Sub-1-GHz-Frequenzbereich als auch das 2,4-GHz-Frequenzband ab und bietet universelle Kompatibilität. Auch bei sich ändernden Umgebungsparametern verfügt er über stabile Eigenschaften für die drahtlose Übertragung.

Rohm Semiconductor GmbH, www.rohm.com

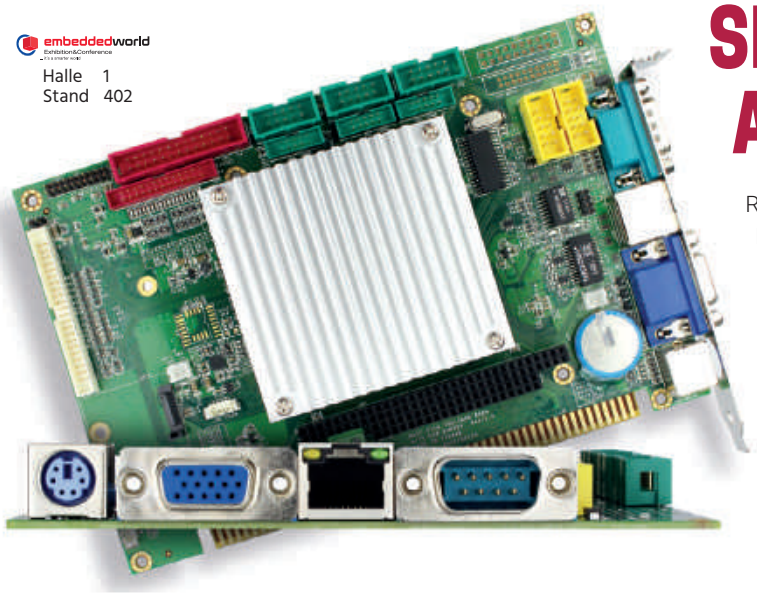
FERNFELD-SPRACHERFASSUNG



Texas Instruments stellt einen Audio-ADC vor, der die deutliche Erfassung von Audiosignalen über eine Entfernung ermöglicht, die **viermal größer** ist als bei anderen Bauelementen. Der TLV320ADC5140 gehört einer neuen Familie von Audio-ADCs an, mit denen eine verzerrungsarme Audioaufzeichnung in lauten Umgebungen möglich ist, ergänzt durch die Fähigkeit zu **Fernfeldaufzeichnungen in Hi-Fi-Qualität** in Umgebungen jeglicher Art. Er ermöglicht eine bessere Audioerfassung über die gesamte Größe eines Raums hinweg und erlaubt eine verbesserte **Erkennung leise gesprochener Befehle** in verschiedenen Anwendungen, zu denen Smart Speaker der High-End-Klasse, Soundbars, drahtlose Lautsprecher, IP-Netzwerkkameras, Telekonferenz-Systeme und intelligente Hausgeräte gehören.

Texas Instruments Deutschland GmbH, www.ti.com

embeddedworld
Halle 1
Stand 402



SLOT-CPU FÜR RETROFIT-ANWENDUNGEN

Retrofit spart Kosten, daher sind ISA und PC/104 gesuchte Standards im Industrie-PC-Bereich. Die ISA-Slot-CPU im halfsize-Format VDX3-6724 von Comp-Mall hat einen PC/104-Steckplatz und lässt sich über Backplane oder PC/104-Slot **anwendungsspezifisch** mit Mess- und Steuerkarten im ISA-Format ergänzen. Der Prozessor Vortex86DX3 mit 1GHz ist on-board, der DDR3-Arbeitsspeicher kann auf bis zu 2GB erweitert werden. Zum Datenausstauch stehen 1x LAN, 1x GbE LAN, 2x RS-232, 2x RS-232/485, 4x USB2.0, 16-Bit GPIO und 1x Parallel Port zur Verfügung. Ein programmierbarer Watchdog Timer **verbessert die Ausfallsicherheit** des Systems.

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

embeddedworld
Halle 1
Stand 478

IPC für leistungshungrige Systeme

Kontron präsentiert die dritte Generation seiner Industriecomputer im Box-PC Format - die KBox C-103-CFL Serie. Die Systeme basieren auf den aktuellsten Intel Core bzw. Intel Xeon E Prozessoren der neunten Generation mit bis zu sechs Prozessorkernen und sorgen für einen enormen *Performanceschub* bei gleichbleibender Verlustleistung. Durch m.2, mPCIe und PCI Express-Erweiterungsslots zeichnen sich die Systeme durch *hohe Flexibilität und Erweiterbarkeit* aus; kundenspezische Anpassungen können ohne Designrisiko umgesetzt werden.

Kontron Europe GmbH, www.kontron.de

Embedded-System mit Grafikerweiterung

Das industrielle Embedded-System TANK-870E9175 von ICP Deutschland bietet mit AMD Radeon E9175 Erweiterung eine **solide Performance.** Die AMD-Grafikeinheit bietet fünf Mini-Display-Port-Anschlüsse, bei einer maximalen Leistungsaufnahme der Grafikeinheit von 35W. Das System wird in zwei Varianten mit Intel Skylake Core i7 oder i5 Prozessor angeboten und unterstützt auf zwei DDR4 SO-DIMM Bänken maximal 64GB Arbeitsspeicher. Es bietet vier USB3.0, vier USB2.0 und vier RS232 mit Überspannungsschutz bis 2.5kV.

embeddedworld
Halle 1
Stand 201

ICP Deutschland GmbH
www.icp-deutschland.de

PoE-Embedded-Vision-System für AIoT-Anwendungen

Durch die Kombination von IoT und KI werden neue Anwendungsbereiche mit intelligenten Geräten entdeckt – genau dies setzt Axiomtek mit der eBox671-521-FL um. Das PoE-Vision-System ist hierzu mit einem 4-Ch PoE und MXM 3.1 Type A Slot ausgestattet – passend für die Anwendung im Bereich Machine Vision, Edge Computing, Verkehrsüberwachung, Deep Learning und AIoT. Der Box-PC überzeugt mit **HOHER RECHENLEISTUNG** *und wird von dem 8. Gen Intel Core i7/i5/i3 (Coffee Lake-S), Pentium oder Celeron mit Intel Q370 oder C246 Chipsatz angetrieben.* **ZAHLREICHE ERWEITERUNGSMÖGLICHKEITEN** *und I/O-Schnittstellen sowie eine* **HOHE GRAFIKLEISTUNG** *sorgen für* **EFFIZIENTE ARBEITSPROZESSE.**

Axiomtek Deutschland GmbH, www.axiomtek.de

embeddedworld
Halle 1
Stand 456

Bild: ©Romolo Tavani/Fotolia.de / Atlantik Elektronik GmbH

embeddedworld Halle 3 Stand 141

Atlantik Elektronik stellt das 5G IoT-Modul TurboX T55 SoM von Thundercomm vor. Es basiert auf der zweiten Generation des Qualcomm Snapdragon X55 5G Modem-RF-Systems. In beiden Designs, LGA und m.2, unterstützt es die 5G-NR-Bandbreiten des Sub-6GHz Spektrums sowie so gut wie alle erhältlichen Sub-6GHz-Spektrumbandbreiten, -modi oder eine Kombination derselben. Außerdem unterstützt es die LTE-FDD- und TDD-Konnektivität und verfügt über eine **INTEGRIERTE GNSS-KAPAZITÄT.** Mit dem 5G-Standalone und Non-Standalone Betriebsmodus des T55 können 5G-Anwendungen für eine Vielzahl neuer Branchen und Märkte realisiert werden. TurboX T55 SoM bedeutet eine enorme **VERBESSERUNG IN DEN BEREICHEN LEISTUNG, EFFIZIENZ UND GERINGE LATENZ.** Das optimierte T55 SoM verspricht hyperschnelle Verbindungen zwischen Geräten im Feld und dem 5G-Netzwerk, was eine beträchtliche Weiterentwicklung von IoT-Anwendungen und -Diensten ermöglicht.

ATLANTIK ELEKTRONIK GMBH ▪ WWW.ATLANTIKELEKTRONIK.DE

CAT-12 MODUL FÜR WELTWEITEN IOT-EINSATZ

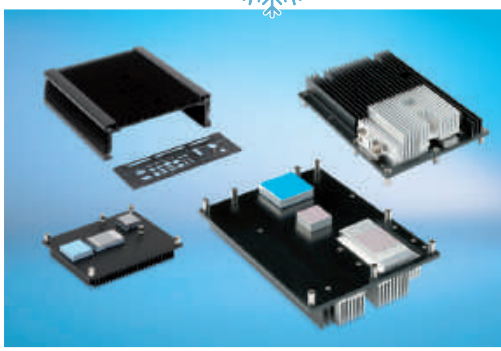
embeddedworld Halle 3 Stand 533

Das Quectel EM12-G LTE Advanced Category 12-Modul wurde für M2M- oder IoT-Applikation entwickelt. Durch die Übernahme der 3GPP Rel. 12 LTE-Technologie liefert es Geschwindigkeiten von bis zu 600Mbps im Downlink sowie 150Mbps im Uplink. Außerdem ermöglicht der m.2-Formfaktor des EM12-G die Kompatibilität mit dem Quectel Cat 6-Modul EM06 und dem zukünftigen Cat 16-Modul EM16. Somit können Nutzer einfacher zwischen den unterschiedlichen Kategorien wechseln. Das Modul unterstützt darüber hinaus die Qualcomm IZat Location Technology Gen9HT Lite (GPS, Glonass, BeiDou, Galileo). Dadurch liefert das integrierte GNSS schnellere, genauere und verlässlichere Positionsdaten.

Tekmodul GmbH
www.tekmodul.de

Integrierte Systeme effektiv kühlen

embeddedworld Halle 3 Stand 401



Kühllösungen für Embedded-Systeme erfüllen die gleichen Anforderungen wie die eingebetteten Systeme selbst: Sie müssen ebenfalls immer *kompakter und effizienter* werden. Naturgegeben erzeugen leistungsfähige integrierte Systeme und Industriecomputer hohe Verlustleistungen bzw. Wärme. Um die dauerhafte, fehlerfreie Funktionsfähigkeit des Systems zu erhalten, muss diese schnell und wirkungsvoll abgeführt werden. Dabei erfolgt die Kühlung idealerweise direkt am jeweiligen Hotspot. CTX führt in seinem Produktprogramm effiziente Kühllösungen, die speziell auf den Einbau in Embedded-Systeme und Industriecomputer ausgelegt sind. Die Kühlung mit den *CNC-gefertigten Kühlkörpern* von CTX funktioniert aktiv oder passiv. Die Produktpalette reicht von projektspezifisch kühlenden Gehäusen zum *Schutz von empfindlicher Elektronik* über wahlweise eloxierte, pulverbeschichtete oder bedruckte Frontplatten bis hin zu Heatspreader-Lösungen mit integrierten Heatpipes, die die Wärme der heißen Bodenplatte in kältere Lamellen ableiten. Auch Kühlkörper mit Kupfer-Inlay zur direkten Installation am Hotspot, ab Werk montierte Lüftereinheiten und komplette Sets aus Kühlkörper (mit/ohne Kupfer-Inlay), Isolierungen, Montagebolzen und Schrauben sind erhältlich. Zum Portfolio von CTX Thermal Solutions gehören außerdem Kühlkörper für die Automobil-, Haushalts- und Unterhaltungselektronik sowie spezielle Kühllösungen für den Bereich der *regenerativen Energien* und für die Haus- und LED-Technik.

CTX Thermal Solutions GmbH, www.ctx.eu

Sicher, leise und effizient

embeddedworld
Halle 2
Stand 351

FSP gibt die Erweiterung der FlexGuru-Serie bekannt. Die Serie **kompakter, modularer, leiser und effizienter Netzteile** wurde für IPC-, HTPC-, Edge-Computing, NAS und NAS-Server entwickelt. Die FlexGuru-Serie umfasst Modelle mit 250 und 300 Watt. Die **schlanken, aber leistungsstarken** Netzteile (150x40,5x81,5mm) bieten eine um **20 Prozent höhere Leistungsdichte** als andere Flex-ATX-Netzteile. Mit modularen Steckverbindern können Benutzer Kabel effizient umstecken und die Fehlerbehebungszeit reduzieren für eine insgesamt bessere, einfachere Nutzung. Dies gibt Benutzern auch die **Flexibilität,** das Netzteil auszutauschen, ohne jedes Kabel vom PC trennen zu müssen. Die Netzteile entsprechen den internationalen Sicherheitsstandards UL/EN/IEC62368-1 und 60950.

FSP Technology Inc. · www.fsp-group.com

Auf leisen Flügeln:

Lüfter mit unter 20 Phon

embeddedworld
Halle 4A
Stand 544

Mit der HA-Serie des Lüfterherstellers Sunon führt Schukat sehr leise Lüfter mit einer Lautstärke von unter 20 Phon im Programm. Damit besitzen die Lüfter eine so geringe Geräuschentwicklung, dass sie in einer normalen Arbeitsumgebung wie einem Büro oder Labor akustisch nicht mehr auffallen, wenn sie in einem Gerät mitlaufen. Um dies zu erreichen, hat der Hersteller die Komponenten angepasst, die für die aerodynamische Geräuschentwicklung zuständig sind – dazu gehören Verbesserungen und Neuentwicklungen an den großen Bauteilen wie Flügelrad und Lüftergehäuse ebenso wie eine wesentliche Optimierung der Details, unter anderem der Stege, die Motor und Gehäuse miteinander verbinden. Insbesondere für Applikationen in geräuschsensitiven Umgebungen ist dies entscheidend, darunter die Medizintechnik, IT-Telekommunikationsanlagen, Netzteile, Drucker und diverse Geräte wie Ticketautomaten, Spielautomaten oder Haushaltsgeräte. Die Lüfter der HA-Serie verfügen über ein geräuscharmes und wartungsfreies magnetisches Vapo-Lager und bieten eine Luftleistung zwischen 9,2 und 93,4m³/h. Verfügbar sind sie in den Gehäusemaßen in klassischer Bauform ab 40x40mm bis 120x120mm in der Basisvariante als 12VDC-Ausführung. Zusätzlich sind auch Ausführungen mit rundem Gehäuse ab Lager Schukat lieferbar.

Schukat Electronic Vertriebs GmbH • www.schukat.com

ERWEITERTER SUPPORT

Lynx hat eine Support-Erweiterung seines LynxSecure Separation Kernel Hypervisors für ARM-basierte Prozessorarchitekturen von NXP Semiconductors auf den Markt gebracht. Der Softwarehersteller portierte LynxSecure auf den NXP QorIQ Layerscape 1046A (LS1046A) Multicore-Kommunikationsprozessor, welcher 64-Bit-Quadcores des Typs ARM Cortex-A72 integriert. Der LynxSecure-Support für NXPs LS1046A folgt der existierenden Unterstützung des NXP S32V234 MPSoC. „Durch die Erweiterung ist es Systemarchitekten und Systemingenieuren, die strikte Anforderungen hinsichtlich Leistung, Safety und Security befolgen müssen, möglich, die Features und Fähigkeiten des NXP LS1046A in vollem Umfang innerhalb einer klaren, 'Secure-by-Design'-Softwaresystemarchitektur auszuschöpfen, wie sie Lynx Mosa.ic bietet", sagt David Beal, Porduktmarketingdirector bei Lynx.

LYNX SOFTWARE TECHNOLOGIES INC., WWW.LYNX.COM

embeddedworld
Halle 4
Stand 361

Bild: Lynx Software Technologies, Inc. / NXP Semiconductors

ERSTES FEC-FÄHIGES LAYER-1-TESTSYSTEM

Keysight hat die Funktionalität seines Layer-1-Multiport-Testsystems A400GE-QDD 400GE mit der des Bert-Systems M8040A kombiniert. Daraus entstand die FEC-fähige Empfänger-Testlösung N4891A 400GBase. Sie bietet die industrieweit erste FEC-fähige Compliance-Testlösung zur Messung des Frame Loss Ratio in 400G-Ethernet-Verbindungen mit FEC. In Kombination mit Keysight Compliance-Testlösungen bietet die 400GBase eine schnelle, genaue und wiederholbare optische und elektrische Stresssignalkalibrierung zur Prüfung der Interoperabilitätsanforderungen.

Keysight Technologies GmbH, www.keysight.com

embeddedworld
Halle 4
Stand 208

GEHÄUSE FÜR RASPBERRY PI

embeddedworld Exhibition&Conference
Halle 4A
Stand 516

Fischer Elektronik hat die Gehäuse für Raspberry-Pi-Einplatinencomputer angepasst. Für den Raspberry Pi 3 Model A+ steht Gehäuse RSP 2 , während für den Raspberry Pi 4 Model B das Gehäuse RSP 3 zu wählen ist. Die Gehäuse setzen sich aus Ober- und Unterschale zusammen, welche aus gestanztem und gebogenem Aluminiumblech, **Stärke 1,5mm,** bestehen. Die jeweilige Platine wird mit Hilfe von M2,5-Linsenkopfschrauben an vier Abstandsbuchsen aus Stahl in der Unterschale befestigt. Durch die **montagefreundliche Konstruktion** wird ein **einfacher Zugriff** auf die GPIO-Pins des Raspberry Pis gewährleistet.

FISCHER ELEKTRONIK GMBH & CO. KG ▪ WWW.FISCHERELEKTRONIK.DE

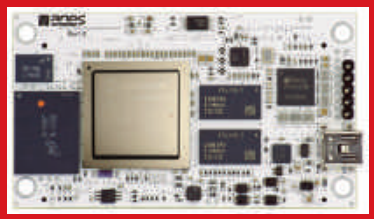
SICHERE MESSERGEBNISSE DURCH GALVANISCHE ISOLIERUNG

embeddedworld Exhibition&Conference
Halle 1
Stand 440

Die kompakten Oszilloskope von Plug-In Electronic können mittels Ethernet-Verbindung oder über USB2.0/3.0 verwendet werden. Sie verfügen über eine **INTEGRIERTE BATTERIE,** *die komplett kabellose Messungen ermöglicht, wodurch eine* **KONTINUIERLICHE DATENERFASSUNG** *gewährleistet ist. Aufgrund der* **PLUG&PLAY-FUNKTIONALITÄT** *können die WiFiScopes direkt mit dem Computer verbunden werden und sind ohne spezielle Netzwerkkenntnisse anwendbar und damit äußerst benutzerfreundlich.*

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

MULTI-CORE RISC-V SYSTEM-ON-CHIP FPGA FÜR DIE INDUSTRIE



ARIES EMBEDDED PÄSENTIERT SEIN SYSTEM ON MODULE 100PFZ. ES BASIERT AUF DER POLARFIRE-SOC-FPGA-FAMILIE VON MICROCHIP, DIE EIN *LEISTUNGSSTARKES* 64-BIT RISC-V MULTICORE-PROZESSOR-SUBSYSTEM MIT *STROMSPARENDER* FPGA-TECHNOLOGIE KOMBINIERT. DAS M100PFS EIGNET SICH FÜR APPLIKATIONEN, IN DENEN EINE LEISTUNGSFÄHIGE, SICHERE UND ENERGIEEFFIZIENTE RECHNERARCHITEKTUR MIT EINEM FPGA KOMBINIERT WERDEN SOLL.

ARIES EMBEDDED GMBH
WWW.ARIES-EMBEDDED.COM

embeddedworld Exhibition&Conference
Halle 3A
Stand 441

AIOT-LÖSUNGEN FÜR AI-EDGE-COMPUTING-ANWENDUNGEN

embeddedworld Exhibition&Conference
Halle 2
Stand 418

Asus stellt mit dem Mini-PC PN61T eine AIoT-Lösung für Edge-Computing-Anwendungen vor. Der Mini-PC ***mit geprüfter 24/7-Zuverlässigkeit*** arbeitet mit einem Intel Core i7-Prozessor und integrierter Google Edge TPU sowie mit einem Machine-Learning-Beschleuniger, der die ***Verarbeitungseffizienz erhöht,*** den ***Energiebedarf senkt*** und den Aufbau vernetzter Geräte und intelligenter Anwendungen erleichtert. Ein Dual-Array von Frontmikrofonen bietet Unterstützung bei der Audioeingabe, während ein Verbraucherinfrarotsensor eine Fernsteuerungsanwendung mit dem PN61T ermöglicht. Der Mini-PC bietet ***umfassende und schnelle Konnektivität*** mit mehreren Ports, einschließlich frontseitig angebrachter, leicht zugänglicher USB3.1 Gen2 Typ-C-Ports sowie Micro-SD-Kartenleser. Er besitzt außerdem ***zusätzliche USB-Ports,*** einschließlich eines USB Typ-C-Anschluss für schnelles Aufladen und eines HDMI-Ports auf der Rückseite. Der Mini-PC verfügt über konfigurierbare Portoptionen (einschließlich COM, VGA, DisplayPort, Intel LAN und Thunderbolt 3) für ältere Geräte, zusätzliche Displays und mehrere Netzwerkverbindungen.

ASUS COMPUTER GMBH
WWW.ASUS.COM

Nach Übernahme von Fujitsu Motherboards:

'Made in Germany'-Angebot von Kontron noch differenzierter

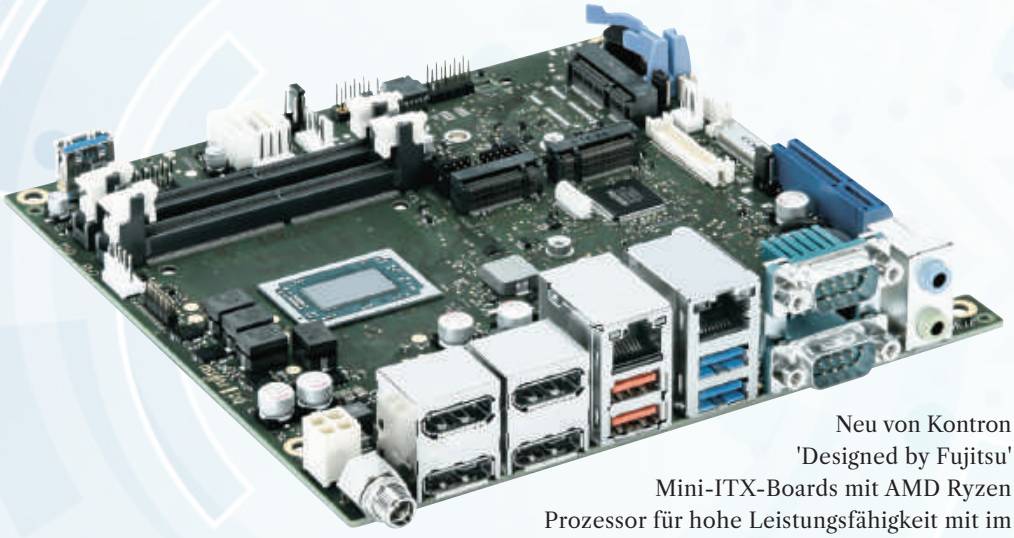


Bild: ©ftotti1984/stock.adobe.com

Neu von Kontron 'Designed by Fujitsu' Mini-ITX-Boards mit AMD Ryzen Prozessor für hohe Leistungsfähigkeit mit im System-on-Chip integrierter Grafik.

embeddedworld Exhibition&Conference
Halle 1
Stand 478

TEXT & BILDER: Kontron Europe GmbH

Für Insider kam es nicht wirklich überraschend, als Kontron ankündigte, das Mainboard-Geschäft von Fujitsu am Standort Augsburg zu übernehmen. Als Anbieter von IoT/Embedded Computer Technologie verfügt Kontron über umfassendes Knowhow bei Embedded Systemen und den entsprechenden Services. Die OEM Mainboards von Fujitsu in einer Vielzahl von Formfaktoren wie **Mini-ITX, Thin Mini-ITX, µATX, Mini-STX und ATX** bilden die passende Ergänzung zum bestehenden Embedded Motherboard Produktportfolio von Kontron aus pITX und Mini-ITX. Mit der Übernahme ist Kontron in der Lage, noch **mehr anwendungsspezifische Auswahlmöglichkeiten anzubieten** und neue Anwendungsfelder zu erschließen. Nur wenige Wochen nach der Übernahme des operativen Geschäfts wartete der Embedded-Spezialist bereits mit neuen Modellen auf.

Kontron brachte nach der Übernahme gleich ein knappes Dutzend neuer Motherboards 'Designed by Fujitsu' mit aktuellster Intel Technologie auf den Markt. Sie basieren auf der Intel Coffee-Lake-Plattform und ermöglichen durch ein umfangreiches BIOS-Update die Nutzung der neuen 9. Prozessorgeneration. Durch den Coffee-Lake-Refresh können Kunden, die die Boards bereits nutzen, auch ohne Tausch der Hardware die neuesten Prozessoren einsetzen. Die etablierten BIOS-Tools zur kundenspezifischen Anpassung von Board und Systemen wie beispielsweise die Verwendung des eigenen Logos und individueller BIOS-Defaults oder die Anpassung der Lüfterdrehzahl sind ebenfalls bereits verfügbar.

Lifecycle-Zähler zurück auf Null

Dank des Refreshs besteht die Möglichkeit, bestehende Applikationen zu erneuern oder um neue Funktionen zu erweitern. Dieser Aufwand lohnt sich, da der Lebenszyklus damit von vorne startet: Mit dem ersten Acht-Kern-Prozessor im LGA1151-Sockel sorgt der Refresh für einen Leistungszuwachs bei voller Verfügbarkeit von sieben Jahren. Damit wird fast die 5GHz-Leistungsgrenze des neuen Spitzenmodells der Intel Core-9000-Serie, der i9-990-0K Prozessor, erreicht. Bislang setzte Kontron hauptsächlich auf gelötete Chips. Da diese kleinere Formfaktoren ermöglichen und sich durch eine geringere Leistungsaufnahme auszeichnen, sind sie besonders geeignet für Embedded Boards. Motherboards mit LGA-Sockel, wie bei den meisten bisherigen Fujitsu Boards der Fall, sind günstiger und freier skalierbar. Die Produkte von Kontron und Fujitsu ergänzen sich daher selbst bei gleichen Formfaktoren optimal. Kontron kann nun ein noch differenzierteres Portfolio anbieten und Kunden profitieren von einer breiteren Auswahlmöglichkeit gemäß ihrer spezifischen Anforderungen. So gibt es beispielsweise als Neuerung Modelle ohne Grafik wie den Intel Core i5-9400F – ein Vorteil bei Workstation- und Imaging-Anwendungen, wo dedizierte Grafikkarten via PCI-Express eingesetzt werden.

Boards in zwei Varianten

Bei den neuen Boards 'Made in Germany' bleibt Kontron dem Zwei-Varianten-Konzept von Fujitsu treu und bietet eine Extended-Lifecycle-Linie und eine Industrial-Linie an. Die Extended-

Extended Lifecycle Motherboards 'Designed by Fujitsu'

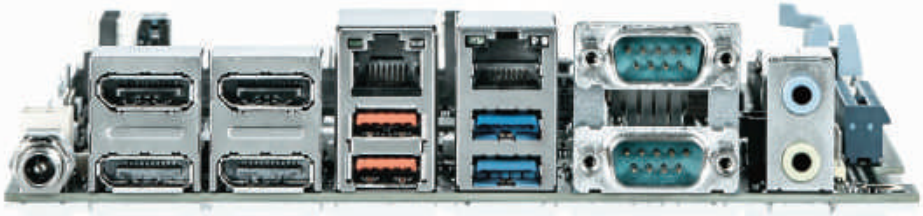
Die neuesten Extended Lifecycle Motherboards 'Designed by Fujitsu' unterstützen die 9. Generation Intel Core i Prozessoren und eignen sich für den langfristigen, kontinuierlichen Betrieb (24/7) in einem Temperaturbereich zwischen 0 und 50°C und bei hoher Systembelastung. Sie sind in den Formfaktoren Mini-STX, Mini-ITX und µATX erhältlich. Trotz des begrenzten Platzes bieten selbst die kleinsten Modelle – das D3654-B mSTX und das D3664-B mSTX - HDMI v1.4 und DisplayPort-Anschlüsse sowie m.2 Steckplätze. Das D3654-B mSTX basiert auf einem Intel H310 Chipsatz, das D3664-B mSTX auf einem Intel Q370. Das Motherboard D3664-B mSTX bietet zudem zwei USB3.1 Gen2 Anschlüsse sowie Intel Active-Management-Technik Support. Das D3674-B Thin-mITX hat umfangreiche Anschlüsse für HDMI v1.4, DP v1.2, Dual Channel LVDS, LAN und 9x USB (2.0 und 3.1 Gen1). Die drei µATX Motherboards sind in verschiedenen Preisklassen erhältlich. Die günstigste Variante ist das mit einem Intel B360 Chipsatz ausgestattete D3643-H µATX. Das D3644-B µATX mit einem Intel C246 Chipsatz ist die teurere Variante. Alle drei Boards bieten DDR4 mit einem Speicherplatz von 64GB sowie Anschlüsse für PCI Express, m.2, USB3.1 Gen2, DVI-D und DisplayPort. Das D3642-B µATX und das D3644-B µATX sind zudem mit 6x SATA sowie Intel Active-Management-Technik und vPRO bestückt.

Produktbezeichnungen: Extended Lifecycle D3654-B / D3664-B / D3674-B / D3642-B / D3643-H / D3644-B

BecomeCloud fusioniert mit EDNC

Der SAP Cloudhersteller BecomeCloud aus Karlsruhe und EDNC – Eugen Dojan Consulting aus Bünde fusionierten zum 01. Januar 2020. EDNC wird zukünftig ausschließlich unter dem Namen der BecomeCloud auftreten. Nach Angaben der Geschäftsführung sei das Ziel der Fusion eine deutlich verstärkte Beratungs- und Entwicklungsleistung im Bereich SAP Business ByDesign sowie SAP Cloud for Customer (C4/HANA). Durch diesen Schritt baut BecomeCloud sein Geschäft mit einem weiteren Standort in Bünde, nahe Osnabrück, im Nordwesten Deutschlands aus. Michael Kaupp, Geschäftsführer der BecomeCloud, fokussiert mit der Fusion insbesondere das erweiterte Skill-Set sowie zusätzliche Personalressourcen für Neu- und Bestandskunden.

www.becomecloud.com



Durch die Implementierung eines Intel I210 GbE-LAN-Controllers ist das Kontron D3713-V/R EtherCAT-fähig. Dadurch erweitert sich das Einsatzspektrum um Echtzeitapplikationen wie der Robotik, Signaltechnik oder der Prozessautomation.

Lifecycle-Linie garantiert eine Verfügbarkeit von 36 Monaten und ist auf semi-industrielle Einsatzbereiche wie etwa Kiosksysteme, Ticketautomaten oder interaktive Displays am Point of Sales ausgerichtet. Die Industrial-Linie ist für den Einsatz in rauen Umgebungen konzipiert, die eine Robustheit gegenüber Staub, Vibrationen und Temperaturschwankungen erfordern. Die Verfügbarkeit liegt bei sieben Jahren, die Geräte kommen damit für längere Zeit ohne Update aus.

Kundenspezifische Services ‘Made in Germany’

Für ausgewählte Modelle bietet Kontron sogenannte ‘Smartcases’ an. Dabei handelt es sich um eine Boxlösung mit einem nach Kundenspezifikationen fertig montierten Mini-PC inklusive Kühlung und Gehäuse. Ein weiterer Service ist das ‘Kitting’. Hier werden die Motherboards ab Werk mit den gewünschten Prozessoren und Speicherriegeln bestückt. Bei Bedarf wird auch das BIOS individuell konfiguriert, in ein Smartcase integriert und die komplette Einheit nach Kundenvorgaben getestet. Zum Lifecycle-Support und den Services von Kontron gehört auch das Merkmal ‘Made in Germany’. Das beinhaltet die Entwicklung und die Fertigung der Motherboards innerhalb einer zuverlässigen Lieferkette. Kontron stellt zudem weiterhin den bewährten technischen Support direkt aus Augsburg sicher, wovon vor allem Kunden aus Europa profitieren.

SUSiEtec

Mit dem IoT Software Framework SUSiEtec des Schwesterunternehmens Kontron Technologies bietet Kontron zusätzliche Services an, beispielsweise Software-Beratung und -Entwicklung für Anwendungen wie Edge- und Cloud-Computing und künstliche Intelligenz (Machine Learning und Deep Learning). SUSiEtec ist grundsätzlich offen für Drittthersteller, idealerweise wird es tief in die Kontron-Produkte vorintegriert, auch mit den neuen Motherboards im Portfolio.

Skalierbare, leistungsstarke Boards in Entwicklung

Die neuen Kontron Motherboards ‘Designed by Fujitsu’ sind nur ein Teil des über Kontron verfügbaren ehemaligen Fujitsu Portfolios. Eine Platine für ultrakompakte, stromsparende Systeme im Mini-STX- und Mini-ITX-Formfaktor mit der Gemini-Lake-Plattform ist schon erhältlich. Des Weiteren launchte Kontron Ende 2019 zwei Boards mit dem Cascade-Lake-Refresh. Zu den weiteren Neuerungen im Portfolio, deren Verfügbarkeit bereits absehbar ist, zählen Mini-ITX-Boards, die das AMD Embedded V1000/R1000 Series System on Chip unterstützen. Der AMD Ryzen Prozessor sorgt nicht nur für hohe Leistungsfähigkeit, die im SoC integrierte Grafik unterstützt darüber hinaus auch bis zu vier Bildschirme mit 4K Auflösung. ■

www.kontron.de

Elektromechanik für Embedded-Systeme

Embedded-Systeme sind nicht nur **Hidden Champions der elektrotechnischen Automation.** Sie sind ein **enormer Marktplatz für Investitionen und Innovationen.** Und die hören nicht bei der Prozessorarchitektur auf.

AUTOR: Marco Stapelmann, Manager Marketing Communications, Business Area Device Connectors, Phoenix Contact GmbH & Co. KG
BILDER: Phoenix Contact Deutschland GmbH

Ob Gebäudeautomatisierung, Personentransport, Industrie- oder Infrastrukturanwendungen – Embedded-Systeme sind in nahezu allen Branchen unverzichtbare Teilsysteme der elektrotechnischen Automation. Als solche erfassen und verarbeiten sie Signale und Daten, steuern Prozesse und bilden die Schnittstelle zwischen physikalischen Systemen, ihren Benutzern und der Umgebung. Wenngleich die eingebetteten Systeme stets dedizierte Aufgaben erfüllen und daher logisch ähnlich aufgebaut sind, orientiert sich die tatsächliche Hardware-Ausstattung an den Anforderungen der jeweiligen Anwendung. Platzbeschränkungen, Schutz vor physikalischen, elektromagnetischen oder mechanischen Störeinflüssen oder die (Echtzeit-)Kommunikation mit der Peripherie und dem Benutzer bilden mal scharfe und mal unscharfe Rahmenbedingungen für den Design-Raum. Und dessen Ausgestaltung endet nicht bei der Auswahl der eigentlichen Kontrolleinheit. Erst die Software, elektromechanische Schnittstellen sowie schützende Gehäuse machen aus Mikroprozessoren und Speichermodulen funktional eingebettete Systeme.

Hohe Anforderungen

Anders als handelsübliche PCs laufen Embedded-Systeme in der Regel im Dauerbetrieb – nicht selten in sicherheitskritischen Anwendungen. Beispiele sind die Car-to-X-Kommunikation, Industrie-PCs zur Maschinensteuerung und Prozessvisualisierungen sowie Smart Meter in der vernetzten technischen Gebäudeausstattung. An die Ausfallsicherheit der verwendeten Komponenten werden in derartigen (semi-)industriellen Anwendungen deutlich höhere Anforderungen gestellt als im Bereich der Heim- und Freizeit-Elektronik. Speziell für diese hohen Anforderungen bietet Phoenix Contact daher unterschiedliche elektromechanische Lösungen. Versteht man Embedded-Systeme als flexibel integrierbare Single-Board-Lösungen, kommt deren Anschlussfähigkeit eine besondere Bedeutung zu. Konventionelle PCI-Busse sind seit den 1990er Jahren als Standardschnittstelle für solche Erweiterungskarten etabliert und erfüllen als 32- oder 64-Bit-Datenbus auch hohe Anforderungen an die Echtzeitdatenübertragung. Häufig sind die Schnittstellen als Edge Connectors – also als Kontaktflächen an den Leiterplattenrändern - ausgelegt und daher auf die koplanare oder orthogonale Ausrichtung der zusätzlichen Leiterplatte beschränkt. Eine platzsparende mezzanine Ausrichtung ist mit dieser technischen Auslegung nicht möglich.

Flexibilität im Layout

Hier kommen nun Board-to-Board-Steckverbinder ins Spiel, die deutlich mehr Flexibilität in der Leiterplattenanordnung und im Geräte-Design mitbringen. Phoenix Contact bietet entsprechende Steckverbinder der Familie Finepitch in den Rastern 0,8 und 1,27mm an. Beide Produktserien eignen sich für die geräteinterne Verbindung mehrerer Leiterplatten. Dank horizontal und vertikal ausgeführter Varianten können Hersteller von Embedded Systemen je nach Anwendung mezzanine, orthogonale oder koplanare Leiterplattenanordnungen umsetzen. Die Steckverbinder für 12 bis 80 Pole lassen Stapelhöhen zwischen 6 und 13,8mm zu – und ermöglichen so flexible Elektronik-Layouts. Auf Wunsch gibt es sie auch mit fertig konfektionierten Steckverbindern und angeschlagenem Flachbandkabel. Für die Highspeed-Datenübertragung eignet sich vor allem die Serie Finepitch 0,8. Die kompakten Steckverbinder übertragen Daten mit bis zu 16Gbit/s und verfügen optional über seitliche Schirmmetalle für eine hohe Datenintegrität. Das neu entwickelte ScaleX-Kontaktsystem dieser Serie sorgt nicht nur für eine hohe mechanische Stabilität. Es erlaubt auch hohe Toleranzen bei produktions- oder montagebedingt abweichend positionierten Messer- und Federleisten. Ihr Fangbereich liegt bei ±0,7mm je Achse, die Winkeltoleranzen liegen beim Stecken bei bis zu ±2° in Längsrichtung und ±4° in Querrichtung.

Ideal für modulare Teilsysteme: Board-to-Board-Steckverbinder erlauben die flexible Anordnung von Leiterplatten.

Funktional verpackt

Mit der Gehäuseserie UCS hat Phoenix Contact auch eine passende ‘Verpackung’ für Embedded-Systeme im Programm. Die Gehäuse eignen sich hervorragend zur Aufnahme der Raspberry-Pi-Single-Board-Computer. Dank flexibler Leiterplattenbefestigungen können Gerätehersteller aber ebenso einfach Leiterplatten in Standardformfaktoren sowie individuelle Leiterplatten unterbringen. Diese Flexibilität ist für modulare Gerätekonzepte ideal, da sich je nach Anwendung ein oder mehrere Standard- und Erweiterungsboards einbauen lassen. Da in beiden Gehäuseschalen die volle Grundfläche zur Verfügung steht, begrenzt lediglich die Aufbauhöhe der elektronischen Bauteile die Gestaltungsoptionen. Speziell für Prototypen, Kleinserien oder einfache Heimanwendungen bietet Phoenix Contact die Gehäuseserie auch mit vorgefertigten Wandausschnitten für Schnittstellen und Displays der Raspberry-Pi-Varianten B2, B3 und B4. Die Polycarbonat-Gehäuse schützen die eingebauten Minicomputer zuverlässig vor mechanischen und physikalischen Einflüssen und eignen sich sowohl für den mobilen Tischeinsatz als auch für die Wandmontage.

Eckdaten – der Markt

Der globale Markt für eingebettete Elektronik wächst kontinuierlich. Analysten prognostizieren bis 2020 eine Marktgröße von mehr als 210 Milliarden Dollar[1]. Schrittmacher für dieses Wachstum sind die zunehmende Vernetzung und Kommunikation in Schlüsselbranchen wie der Gebäudeautomatisierung, der Automobilindustrie oder der Industrie- und Prozessautomation. Der Großteil des Marktvolumens und -wachstums entsteht durch technologische Fortschritte in der Prozessor- und Kommunikationstechnologie. Wenngleich Embedded-Systeme dem gleichen logischen Aufbau folgen, erlauben erst elektromechanische Schnittstellen und schützende Gehäuse die funktionale Ausgestaltung und Anpassung an unterschiedliche Anforderungen.

[1] www.grandviewresearch.com/industry-analysis/embedded-system-market
[1] vgl. https://www.transparencymarketresearch.com/pressrelease/embedded-system.htm

Elektromechanik als Maßanzug

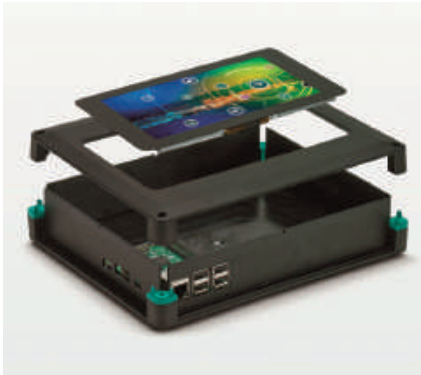
Embedded-Systeme sind so vielseitig und individuell, dass elektromechanische Standardlösungen häufig nicht alle Anforderungen abdecken können. Ein Beispiel sind explosionsgefährdete Bereiche in der Prozesstechnik. Dort eingesetzte Kommunikationsgeräte, HMI oder Kompaktsteuerungen müssen strenge Anforderungen an die elektrische Sicherheit erfüllen. Dies gilt im Speziellen auch für die Elektromechanik. Luft- und Kriechstrecken, Erwärmungsverhalten, Alterungsbeständigkeit und das Isolationsvermögen der Werkstoffe müssen auf die jeweilige Zündschutzart abgestimmt sein. Kunden, die Embedded Systems für spezielle Einsatzgebiete oder besondere Anforderungen entwickeln, unterstützt Phoenix Contact schon im Planungs- und Entwicklungsprozess mit Werkstoff-, Technologie- und System-Know-how. So entstehen bei Phoenix Contact in der Organisationseinheit Device Connector Solutions kundenspezifische Neuentwicklungen, die – je nach Anforderung – einzelne Komponenten umfassen, Technologien neu kombinieren, oder vollständig neue Lösungen ermöglichen. Neben applikationsspezifischen Gehäusesystemen gehören auch im Kundenauftrag individuell gefertigte Leiterplattenanschlüsse oder Steckverbinder für den Feldeinsatz zum Leistungsspektrum.

ScaleX-Kontaktsystem: Die doppelseitig ausgeführten Kontakte sorgen für eine hohe Stabilität und erlauben bis zu 500 Steck- und Ziehzyklen.

Fazit

Eingebettete Systeme sind so vielseitig wie die Branchen und Anwendungen, in denen sie zum Einsatz kommen. Erst die richtige Kombination aus Hardware, Software und Anschlusstechnik macht aber aus Single-Board-Computern oder Erweiterungskarten funktionale Einheiten. Da sich elektronische Bauteile rasant weiterentwickeln und so stets in neue Einsatzgebiete vordringen, sind Embedded Systems auch für die integrierte Elektromechanik ein Innovations- und Investitionstreiber. Phoenix Contact bietet daher vielfältige Lösungen für diesen Wachstumsmarkt. Kompakte Board-to-Board-Steckverbinder ermöglichen besonders flexible Anschlusslösungen. Elektronikgehäuse schützen die integrierte Elektronik. Und die fast 100-jährige Technologie- und Branchenerfahrung gibt Herstellern von Embedded Systems die Gewissheit, schon heute die Innovationen von morgen gestalten zu können. ■

www.phoenixcontact.de



Komplettgehäuse: Elektronikgehäuse der Serie UCS-RPI bieten eine funktionale Verpackung für Single-Board-Computer.

Kuda und Adlink planen gemeinsame Edge-IoT-Lösungen

Adlink Technology und der Münchener Systemintegrator Kuda geben bekannt, dass die Unternehmen eine Partnerschaft eingehen wollen. Ziel ist es, die Fertigungsunternehmen in Deutschland in die Lage zu versetzen, Möglichkeiten der sich schnell entwickelnden IoT-Technologie für ihre Projekte im Bereich Industrie 4.0 optimal zu nutzen.

Bild: ©ipopba/stock.adobe.com

Gemeinsam wollen beide Unternehmen Adlink-Digital-Experiment-IoT-Lösungen anbieten, mit denen Anwender operative Daten in kürzester Zeit vernetzen, übertragen und auswerten und so fundierte Entscheidungen fällen können – unabhängig davon welche Anlagen, Systeme und Cloudplattform sie bereits einsetzen.

www.adlinktech.com

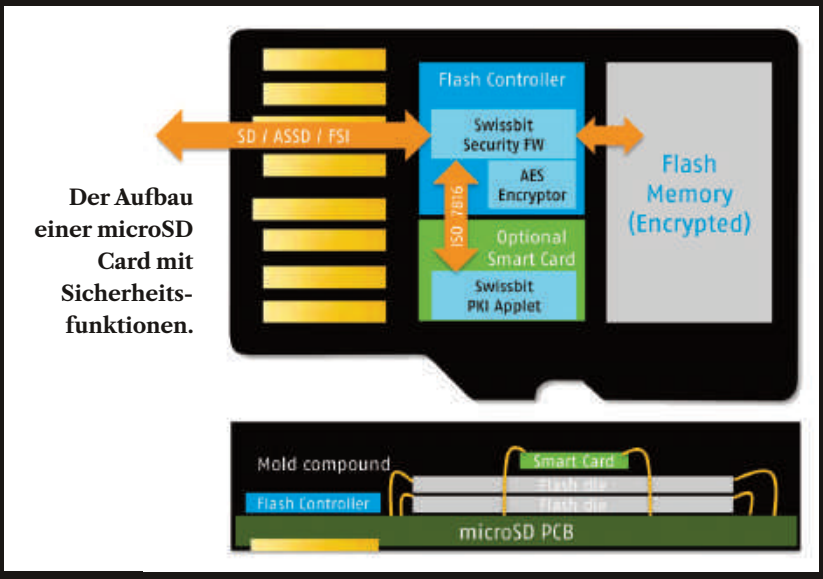
Geräte, Maschinen und Anlagen werden smart, aber auch angreifbar. Entwickler müssen beim Design vernetzter Geräte, Maschinen und Anlagen verstärkt Sicherheitsaspekte berücksichtigen. Ein flexibler, hardwarebasierter Lösungsansatz inklusive TPM und Datenverschlüsselung kommt jetzt von Swissbit.

FLEXIBLE SPEICHERKARTENLÖSUNG

IOT-SICHERHEIT EINGEBETTET IN SPEICHER-KARTEN

AUTOR: Hubertus Grobbel, Vice President Security Solutions, Swissbit AG BILDER: Swissbit AG

Über das Internet kommunizierende Systeme oder deren Gateways im IoT sollten aus der Perspektive der IT- und Datensicherheit eine eindeutige, nicht klonbare Identität aufweisen und zugleich in der Lage sein, Daten kryptografisch stark gesichert zu senden, zu speichern und zu empfangen. Reine Softwarelösungen bieten hier nur selten ausreichenden Schutz. Das stellt viele Entwickler und Hersteller vor große Herausforderungen. Ein Hardware basierter Lösungsansatz kommt jetzt vom Storage- und Security-Hersteller Swissbit AG. Die Grundidee dabei: Praktisch jedes Gerät braucht Speicher, etwa als Boot-Medium, für Logfiles und Datenzwischenspeicher bei Netzwerkunterbrechungen. Es bietet sich also an, die Speicherschnittstellen zu nutzen, um Sicherheitsfunktionen bereitzustellen.



Der Aufbau einer microSD Card mit Sicherheitsfunktionen.

Sicherheit im Memory-Card-Format

Die neuen Sicherheitsspeicherlösungen von Swissbit bestehen aus einem auf industrielle Anforderungen hin produzierten und getesteten Flash-Speicherchip und werden mit einer speziellen Version der durabit-Firmware mit integriertem AES-256-Bit-Enkryptor betrieben. In der Version DP (Data Protection) werden sämtliche Daten verschlüsselt und auf verschiedene Arten geschützt (CD-ROM-Modus, PIN-Schutz, versteckter Speicher, Worm-Modus). Für die hardwarebasierte Absicherung der Kommunikation im IoT ist dann ein weiterer Sicherheitsanker nötig. Die Sicherheitsmodule von Swissbit sind daher mit Lösungen wie einem Infineon/NXP Smart Card Chip CC EAL 5+/6+ ausgestattet. Für die Applikationsentwicklung stehen eine API, ein SDK und eine PKCS#11-Library zur Verfügung.

Den Dingen einen Ausweis geben

MicroSD Cards mit Secure Element haben sich in Sicherheitskreisen als Mittel zur Verschlüsselung von Mobiltelefonkommunikation bewährt. Analog zur sicheren Kommunikation zwischen Personen muss auch bei der Kommunikation der Dinge im Internet Identifikation, Authentisierung und Autorisierung stattfinden. Anders gesagt: Woher weiß ein 'Ding', dass die empfangenen Daten oder Datenabfragen von einem anderen 'Ding' korrekt sind und die Quelle einer Nachricht wirklich die Systemkomponente ist, die sie vorgibt zu sein? Swissbit-Security-Speichermedium mit Secure Element geben Anwendungen und Systemen eine eindeutige Identität. 'Dinge' bekommen einen fälschungssicheren Ausweis. Vernetzte Systeme können so vor Missbrauch und 'Identitätsdiebstahl' geschützt werden. Der Zugriff auf Daten kann eingeschränkt werden.

Speicherschnittstellen wie USB können genutzt werden um eine TPM-Funktion nachzurüsten.

Mit auf Memory Cards integrierten Smartcards erhalten Systeme nicht klonbare Identitäten und werden zu eindeutig identifizierbaren M2M-Kommunikationsteilnehmern, die in der Lage sind, sich zu authentisieren und Daten kryptografisch stark gesichert zu senden und zu empfangen. Eine weitere wichtige gerätebezogene Anwendung der Swissbit-Lösungen ist Trusted Boot. Dieses Konzept stellt sicher, dass Software nur auf bestimmter Hardware oder Hardwareklassen gestartet werden kann. Mit einer sicheren Flash-Karte lassen sich so Softwarelizenzierungen und Funktionsfreischaltungen regeln. Durch Zugangskontrolle, Code-Verschlüsselung oder digitale Signatur können Varianten in der Softwareausstattung von Produkten definiert und verwaltet werden.

Nachrüstbar und zukunftssicher

Im Vergleich zu einem fest verlöteten TPM ist die Idee eines steckbaren Sicherheitsmoduls zunächst ungewohnt. Der große Vorteil: Auch ältere Maschinen und Systeme verfügen in der Regel über eine USB-Schnittstelle oder Interfaces für Memory Cards. So können auch bestehende Geräte über Swissbit-Security-Speicher ohne großen Aufwand nachgerüstet und gesichert werden. Und die Nachrüstbarkeit hat noch einen anderen positiven Aspekt. Cyber Security ist bekanntlich ein ewiger Wettlauf. Die Entwicklung von Angriffs- und Verteidigungsmethoden verläuft in Zyklen, die nur schwer mit dem Produktlebenszyklus z.B. einer Industrieanlage in Einklang zu bringen sind. Es kann also nötig werden, den M2M-Kommunikationsteilnehmern einen neuen 'Ausweis' mit verbesserten Kryptografietechniken zu geben. Mit dem Lösungsansatz von Swissbit ist das möglich.

Ausblick

Um der schnell wachsenden Nachfrage im Bereich Embedded IoT gerecht werden zu können, hat Swissbit erst im Oktober 2019 in Berlin ein neues Werk mit modernstem Advanced-3D-Chip-Scale-Packaging-Technologien eröffnet. Hier hat der Hersteller die Möglichkeit, für Kunden individuelle System-in-Package- und Multi-Chip-Module-Designs zu entwickeln und zu fertigen. Das erlaubt es, nicht nur Mikrocontroller, NAND-Chips und Krypto-Chips, sondern beispielsweise auch Sensoren, Wireless Chips und Antennen zu integrieren. Die Nutzung von Memory Interfaces mit TPM und Verschlüsselungsbausteinen für Sicherheitslösungen könnte daher erst der Anfang sein. Weitere Funktionalitäten lassen sich miniaturisieren und integrieren. ■

www.swissbit.com

Aktuelles Beispiel TSE für POS-Systeme

Der für Sicherheitsprodukte zuständige Swissbit-Geschäftsbereich Embedded IoT stellt auf der Embedded World aus. Als aktuelles Beispiel präsentiert das Unternehmen technische Sicherheitseinrichtungen (TSE) für die manipulationssichere Kassenaufzeichnung. Weitere Anwendungsbeispiele am Messestand sind eine Secure-Boot-Installation und der Schutz von Daten- und Videoaufzeichnungen beispielsweise bei Body-Cams oder Drohnenkameras.

Neuer Deputy Director bei EUTC

Andreas Thamm, Deputy Director European Technical Center (EUTC)

Das European Technical Center bietet Kundensupport durch spezialisierte FAEs, die die Kunden von der Produktauswahl, der Beantwortung technischer Fragestellungen bis hin zum Design-Support auf Systemebene unterstützen. „Es ist eine entscheidende Schnittstelle zwischen den Anforderungen der Kunden und der Produktentwicklung in Japan", kommentiert Toshimitsu Suzuki, Präsident Rohm Semiconductor Europe. „Mit der Einstellung von Andreas Thamm unterstreichen wir die Bedeutung des europäischen Marktes für Rohm. Seine Expertise im Bereich der Industrieautomatisierung und seine internationale Erfahrung im Segmentmarketing werden sicher helfen, die Produkte unserer lokalen Kunden in den Fokus zu stellen und die Bedürfnisse der Industrie an die Entwicklungsabteilungen weiterzugeben, um relevante Produkte für den europäischen Markt zu entwickeln."

www.rohm.de

PC/104-BOARDS

Im Hintergrund der PC/104-Entwicklung stand die Absicht verfügbare Desktop-Computertechnologie in die Welt der Embedded-Applikationen zu übertragen. Dabei waren einige Besonderheiten zu berücksichtigen wie die zumeist geringeren Platzverhältnisse beim Einbau. Dies führte zu einem Single Board Computer mit 90x96mm Platinenabmesssungen und der zusätzlichen Eigenschaft weitere Module ohne eine Backplane auf der Grundplatine zu stapeln. Dem technologischen Wandel begegnete man mit neuen Basisboards bzw. ergänzenden Modulen. Sobald sich z.B. schnellere Bussysteme auf dem Desktop-Markt etablierten, wurden sie in Form eines neuen Familienmitglieds übernommen und der neueste Stand für den Embedded-Bereich zur Verfügung gestellt. Der modulare Stapelaufbau ermöglichte dann auch das Retrofit bisheriger Applikationen. *(ghl)* ■

Anbieter	Internet-Adresse	Produktbezeichnung(en)	Formfaktorbezeichnung / Maße
ADL Embedded Solutions GmbH	www.adl-europe.com	ADLE3800PC	PCIe/104 Form Factor
ADL Embedded Solutions GmbH	www.adl-europe.com	ADLD25PC Pine View PCI/104-Express Single Board Computer	3,6x3,8" (90x96) PCI/104-Express v1.0a
ADL Embedded Solutions GmbH	www.adl-europe.com	ADLN2000PC Cedar View PCIe/104 Single Board Computer	PCIe/104 Form Factor
ADL Embedded Solutions GmbH	www.adl-europe.com	ADLQM87PC Haswell PCIe/104 Single Board Computer	4.5x3.8" (115x96) PCIe/104 Form Factor
ADL Embedded Solutions GmbH	www.adl-europe.com	ADLQM67PC Sandy Bridge PCIe/104 Single Board Computer	4.5x3.8" (115x96) PCI/104-Express v1.0a
ADL Embedded Solutions GmbH	www.adl-europe.com	ADL3GQM67PC Ivy Bridge PCIe/104 Single Board Computer	4,5x3,8" (115x96) PCI/104-Express v1.0a
Adlink Technology GmbH	www.adlinktech.com	AmITX-HL-G	
Adlink Technology GmbH	www.adlinktech.com	AmITX-BT-I	
Adlink Technology GmbH	www.adlinktech.com	CM2-BT2 Extreme Rugged PC/104-Plus	90x96 mm
Adlink Technology GmbH	www.adlinktech.com	CoreModule 920	116x96mm
ⓘ Advantech Europe BV	www.advantech.de	PCM-Serie	PC/104
AMC Analytik & Messtechnik GmbH	www.amc-systeme.de	PCM-33xx-Serie	PC/104, PC/104+, PCI/104
Bicker Elektronik GmbH	www.bicker.de	im erweiterdenden Temperaturbereich und Military	
Bihl+Wiedemann GmbH	www.bihl-wiedemann.de	AS-i PC/104 Master	96x90x16mm, PC/104+ (PCI u. ISA-Bus)
Delta Components GmbH	www.delta-components.de	CoreModule 920 PCI/104 Express 3rd Generation	PC/104 Express
Delta Components GmbH	www.delta-components.de	CoreModule 2-GF PC/104-Plus	PC/104-Plus
Delta Components GmbH	www.delta-components.de	CoreModule 1-86DX2 PC/104	PC/104
EMS Dr. Thomas Wünsche e.K.	www.ems-wuensche.com	CAN-Interface für PCI-104 basierende Systeme	PCI/104
Fortec Elektronik AG	www.fortecag.de	Advantech PCM-3365, PCM-3356, Diamond Systems Helix, Aries	PC/104, PC/104+, PCI/104
Glyn GmbH & Co. KG	www.glyn.de	PFM-CVS, PFM-LNP	PC/104+, PC/104
ICP Deutschland GmbH	www.icp-deutschland.de	PM	PC/104, PC/104+, PCI 104
ICP Deutschland GmbH	www.icp-deutschland.de	PC/104	
ICP Deutschland GmbH	www.icp-deutschland.de	PM-PV-D5251	PCI-104 Modul
IIE Ing.-Büro f. Industrie-Elektronik GmbH	www.iie.de	diverse	PC/104, PC/104+, PCI/104

Prozessor-Takt					Speicher		Embedded Betriebssysteme								Schnittstellen											
bis 500 MHz	501 bis 1.000 MHz	1 bis 2 GHz	über 2 GHz	Mehrproz. o. Multicore-CPU	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Linux (Varianten)	OS-9	QNX	RTOS	VxWorks	Windows CE.net	Windows XP embedded	andere Betriebssysteme	RS232 / RS422 / RS485	USB 2.0 / 3.0	PS/2 Keyboard + Mouse	IrDA	Grafik	Audio	Drahtlose Schnittstellen	Massenspeicherschnittstellen	Erweiterungssteckplätze	Digitale Ein-/Ausgänge	Ethernet 10 / 100 Mbit/s	Ethernet 1 Gbit/s	Feldbus-Schnittstellen
		•	•	•	2GB	8GB	•		•	•	•	•	•	•	•	8x 2.0, 1x 3.0			•	•	•	•	•	•	•	•	•
		•		•	1GB	4GB	•		•			•	•	•	•	8x 2.0	•		•	•	•	•	•	•	•	•	
		•		•	1GB	2GB	•		•				•	•	•	8x 2.0	•		•		•	•	•		•	•	
			•	•	2GB	8GB	•		•	•	•	•	•	•	•	8x 2.0, 2x 3.0			•	•	•	•	•	•	•	•	•
			•	•	1GB	8GB	•		•				•	•	•	8	•		•	•		•	•	•	•	•	
			•	•	1GB	8GB	•		•				•	•	•	8x 2.0	•		•	•		•	•	•	•	•	
				•																					•	•	
				•												4x 3.0, 2x 2.0									•	•	
		•				4GB	•		•		•			•		1x 3.0 + 2x 2.0						•		•	•	•	
		•				4GB	•		•		•			•		4x 2.0 …						•			•	•	
		•	•		2MB	16MB			•			•	•		•	4	•		•	•		•				•	
•	•	•	•	•	256MB	4GB	•		•				•	•	•	max. 4x	•		•	•		•	•	•	•	•	•
	•	•	•		512MB	16GB	•					•	•	•	•	•	•		•	•		•	•	•	•	•	•
							•					•	•														•
		•				2 o. 4GB	•		•		•			•	•	4x 2.0			•			•					•	
		•				4GB	•						•		•	6x 2.0			•	•		•				•	
	•					1GB	•						•		•	3x 2.0	•		•			•				•	•	
																											•
•	•	•	•			8GB	•							•	•	•			•	•		•	•	•	•	•	
•	•	•	•	•	1GB	16GB	•					•	•	•	•	8	•		•	•	•	•	•		•	•	•
		•	•	•	1GB	4GB	•					•	•	•	•	6	•	•	•	•	•	•	•	•	•	•	
•	•	•	•	•										•													
	•	•		•	1GB	4GB	•						•		•	4			•	•		•	•	•	•	•	
•		•			128MB	2GB	•	•	•	•	•	•	•	•	•	diverse	•	•	•	•	•	•		•	•	•	

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 23.01.2020

MARKTSPIEGEL PC/104-BOARDS

Bild: Peak-System Technik GmbH

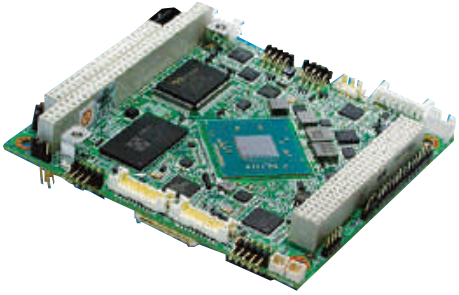


Bild: Fortec Elektronik AG

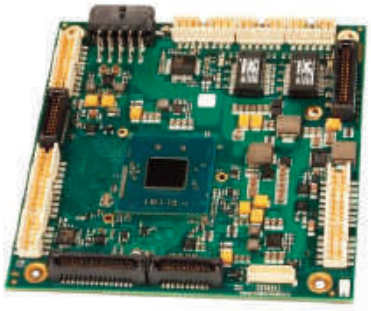


Bild: ADL Embedded Solutions GmbH

Anbieter	Internet-Adresse	Produktbezeichnung(en)	Formfaktorbezeichnung / Maße
Industrial Computer Source GmbH	www.ics-d.de	PFM-HDS	PC/104+
IPC2U GmbH	ipc2u.de	Vortex86DX 800MHz CPU, operating temperature: -40..85°C	PC/104+
IPC2U GmbH	ipc2u.de	Vortex86DX 800MHz CPU, operating temperature: -20..70°C	PC/104+
IPC2U GmbH	ipc2u.de	Vortex86SX 300MHz CPU, -40...+85°C	PC/104
IPC2U GmbH	ipc2u.de	Vortex86DX2 800MHz CPU, operating temperature: -20..70°C	PC/104
IPC2U GmbH	ipc2u.de	Vortex86DX CPU Module 512MB	PC/104
IPC2U GmbH	ipc2u.de	Vortex86DX 800MHz CPU Module with 256MB	PC/104
IPC2U GmbH	ipc2u.de	Vortex86SX 300MHz CPU Module with 128MB DDR2	PC/104
IPC2U GmbH	ipc2u.de	Vortex86MX+ 800MHz CPU Module with 1GB RAM	PC/104
IPC2U GmbH	ipc2u.de	Vortex86SX- 300MHz 128MB	PC/104
IPC2U GmbH	ipc2u.de	Vortex86DX2 800MHz CPU, operating temperature: -20..70°C	PC/104
IPC2U GmbH	ipc2u.de	SBC with AMD LX800 500Mhz	PC/104
IPC2U GmbH	ipc2u.de	Vortex86SX 300MHz CPU Module with 128MB DDR2	PC/104
IPC2U GmbH	ipc2u.de	Vortex86SX 300MHz CPU, operating temperature: -40.. +85°C	PC/104
Moxa Europe GmbH	www.moxa.com/de	C1xxH/PCI Serie, CP-1xx/J Serie, C2xx/3xxTurbo/PCI Serie, usw.	PC104, PC104+, PCI, PCI-Express, Univ. PCI
Peak-System Technik GmbH	www.peak-system.com	PCAN-PCI/104-Express - CAN-Interface für PCI/104-Express	PCI/104 Express (PCI Express, PCI-Durchleitung)
Peak-System Technik GmbH	www.peak-system.com	PCAN-PC/104 - CAN-Interface für PC/104	
Peak-System Technik GmbH	www.peak-system.com	PCAN-PC/104-Plus - CAN-Interface für PC/104-Plus	PC/104 (ISA) PCAN-PC/104-Plus (PCI, ISA-Durchleitung)
Peak-System Technik GmbH	www.peak-system.com	PCAN-PCI/104-Express FD	
Peak-System Technik GmbH	www.peak-system.com	PCAN-PC/104-Plus Quad - Vierkanal-CAN-Interface für PC/104-Plus	90,2x95,9mm PCIe/104 PC/104-Plus (PCI, ISA-Durchleitung)
Plug-In Electronic GmbH	www.plug-in.de		PC/104, PC/104+, PC/104+ (nur mit PCI-Bus)
Rutronik Elektronische Bauelem. GmbH	www.rutronik.com	PCM-33xx, MOPS	PC/104, PC/104+, PCI/104
Sorcus Computer GmbH	www.sorcus.com	MAX3pc104	PC/104
Syslogic Datentechnik AG	www.syslogic.de	IPC/NETIPC-4	PC/104

Prozessor-Takt					Speicher		Embedded Betriebssysteme								Schnittstellen											
bis 500 MHz	501 bis 1.000 MHz	1 bis 2 GHz	über 2 GHz	Mehrproz. o. Multicore-CPU	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Linux (Varianten)	OS-9	QNX	RTOS	VxWorks	Windows CE.net	Windows XP embedded	andere Betriebssysteme	RS232 / RS422 / RS485	USB 2.0 / 3.0	PS/2 Keyboard + Mouse	IrDA	Grafik	Audio	Drahtlose Schnittstellen	Massenspeicherschnittstellen	Erweiterungssteckplätze	Digitale Ein-/Ausgänge	Ethernet 10 / 100 Mbit/s	Ethernet 1 Gbit/s	Feldbus-Schnittstellen
				•		4GB									•	4x 2.0	•		•	•		•	•	•			
	•					512MB										•									•		
	•					256MB										2									•		
•						128MB										2									•		
	•						•		•		•		•			2				•					•		
	•															2											
	•															2											
•						128MB																			•		
	•															4				•					•		
•						128MB										2									•		
	•						•		•		•		•			2									•		
•						1GB									•	2									•		
•						128MB										4									•		
•						128MB																			•		
																									•	•	•
							•		•				•	•													•
							•		•				•	•													•
							•		•				•	•													•
							•							•													•
							•		•		•		•	•													•
			•			8GB	•								•	2x3.0,12x2.0	•		•	•		•				•		
•	•	•					•					•	•												•	•	
•	•			•	8MB	64MB	•				•	•		•	•	X-Bus-Module	•	•	•		•	•	•	•	•		•
	•						•	•			•	•	•		•	2						•	•		•		•

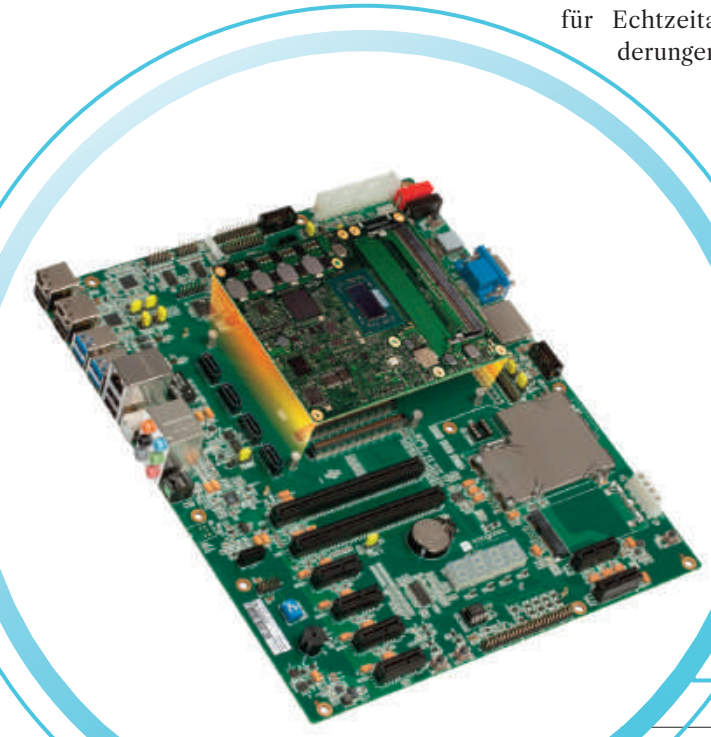
Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 23.01.2020

KÜNSTLICHE INTELLIGENZ IN ECHTZEIT

AUTOR: Zeljko Loncaric, Marketing Engineer, Congatec AG BILDER: Congatec AG

Soll künstliche Intelligenz in industriellen Applikationen zum Einsatz kommen, sind vielfach parallele Rechenprozesse bei kürzesten Reaktionszeiten in Echtzeit von Nöten. Das stellt an Embedded Computer Technologien wie Computer-on-Modules mit AMD Ryzen Embedded V1000 Prozessoren ganz neue Anforderungen.

An den Einsatz von KI im industriellen Umfeld werden hohe Anforderungen an die zu integrierende Logik gestellt, denn bei schnellen Prozessen – wie bei Inspektionssystemen – gibt es oft keine weitere Kontrollinstanz. Deshalb muss bei industriellen KI-Systemen stets sichergestellt werden, dass die Entscheidungsfindungsprozesse der KI-Systeme nachvollziehbar und auch immer korrekt sind. Das Training der KIs ist im industriellen Umfeld deshalb komplex. Auch gibt es kaum Negativbeispiele. In der Industrie müssen Fehler von Anfang an vermieden werden. Daher werden hier häufig digitale Twins eingesetzt, um Negativbefunde zu simulieren und dadurch beispielsweise gewisse Bewegungsabläufe von Robotern von vorneherein auszuschließen. Wie entwickelt und betreibt man also fehlerfreie industrielle KI für Echtzeitanforderungen?



Die Migration hin zur KI ist mit AMD basierten COM Express Computer-on-Modules von Congatec eine einfache Aufgabe, da sie bestehende COM Express Designs mit anderer Prozessortechnologie problemlos ersetzen können.

GPGPU: eine wichtige Technologie für KI

Bei den meisten Systemen erfolgt die Hauptarbeit der Mustererkennung in der GPGPU-gestützten Cloud mit ihrer immensen parallelen Rechenleistung. In der produzierenden Industrie ist das jedoch – zumindest derzeit noch – ein Ausschlusskriterium, da es oft um schnelle Prozesse geht. Hier muss man also dafür sorgen, dass sich die Intelligenz am Edge befindet, weshalb in den Geräten, Maschinen und Anlagen der Industrie auch zumeist KI Systeme im Einsatz sind, die für Echtzeit-Applikationen wissensbasierte Intelligenz anwenden und Daten für Deep Learning an zentrale Clouds weiterleiten, die aktuell noch nicht in Echtzeit angeschlossen werden können. Möglich ist es also schon heute, ein übergeordnetes System mit allen neuen Daten weiter zu trainieren und die lokalen Devices über regelmäßige Softwareupdates auf den aktuellen Stand des Wissens zu bringen, sodass man solche Systeme schon heute als selbstlernende Systeme einstufen kann. Das Lernen findet hier nur weniger als Lernkurve sondern in zyklischen Update-Stufen statt. Dies ist auch ein Grund, weshalb Themen wie die digitalen Zwillinge oder industrielle Edge-Server so wichtig sind: Kann man beides bereitstellen, kann selbst Deep Learning zunehmend echtzeitfähig werden.

Die passenden Embedded-Prozessoren

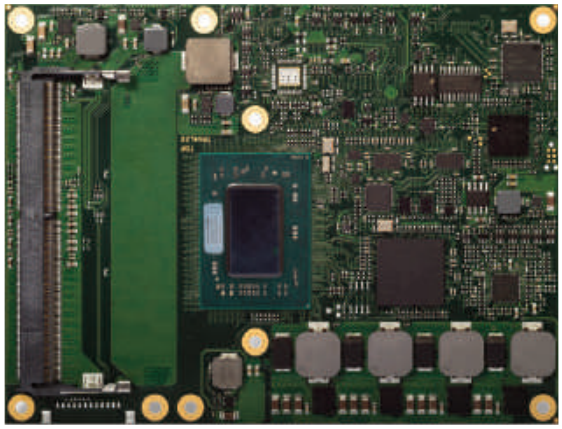
Ganz gleich, welches Setup OEM für ihre KI wählen: Bezogen auf die einzelne echtzeitfähige Maschine oder Anlage sind die Anforderungen an die benötigte Verarbeitungsleistung auch bei ‚normaler', rein wissensbasierter KI immer noch sehr hoch. Neueste Embedded Accelerated Processing Units (APUs) von AMD unterstützen diesen

Bedarf, da sie neben dem klassischem x86er Prozessor eine leistungsfähige GPU bieten, die über ihre General Purpose Funktionen auch parallele KI-Rechenprozesse unterstützt, wie sie in den Rechenzentren zur Anwendung kommen. Diese lässt sich zudem über diskrete Embedded GPUs des gleichen Herstellers weiter skalieren, sodass man die offene parallele Rechenperformance genau an den Bedarf der industriellen KI-Applikation anpassen kann.

Standard-Modul auf Standard-Board: Das Mini-ITX Motherboard conga-IT6 kann mit dem neuen Modul bestückt und damit in jedes Industriesystem montiert werden, das den ATX-Standard nutzt.

AMD Ryzen Embedded V1000

Mit ihrer gestiegenen Rechen- und Grafikleistung empfiehlt sich dabei die energiesparende und industriell-robuste AMD Ryzen Embedded V1000-Series. Sie bietet mit einer Gesamtleistung von bis zu 3,6 TFLOPs aus der Multi-Purpose CPU und der leistungsstarken General Purpose Grafikeinheit eine flexible Rechenleistung, die vor wenigen Jahren nur mit Systemen erreichbar war, die mehrere hundert Watt verbrauchten. Heute ist diese Rechenleistung schon ab 15 Watt verfügbar. Damit kann sie selbst in lüfterlose und komplett geschlossene und damit höchst robuste Geräte für den Fabrikeinsatz integriert werden. Als echtzeitfähige Prozessoren unterstützen sie zudem auch Speicher mit Error Correction Code (ECC), was für die meisten industriellen Maschinen und Anlagen essenziell ist.



Das COM Express Type 6 Benchmark-Modul für lokale Industrie-KIs: Das conga-TR4 mit AMD Embedded Ryzen Prozessor.

Umfassender Softwaresupport

Auch in Bezug auf das nötige Software-Environment für eine schnelle und flächendeckende Einführung von KI und Deep Learning bieten diese AMD Embedded Prozessoren umfassenden Support an Tools und Frameworks wie TensorFlow, Caffe und Keras. Besonders wichtig ist dabei der Open Source Gedanke, damit OEMs nicht von einer proprietären Lösung abhängig sind. So steht hier auch das Tool HIPfy zur Verfügung, mit dem sich proprietäre Applikationen in portable HIP C++ Applikationen portieren lassen, so dass die gefährliche Abhängigkeit von einzelnen GPU-Herstellern wirkungsvoll vermieden werden kann. KI zu entwickeln ist zudem auch mit der Verfüfgbarkeit von OpenCL 2.2 deutlich einfacher geworden, denn seitdem ist die OpenCL C++ Kernel Sprache in OpenCL integriert, was das Schreiben parallel arbeitender Programme deutlich erleichtert. Mit einem solchen Ökosystem sind sowohl wissensbasierte KIs als auch Deep Learning vergleichsweise einfach umzusetzen und nicht nur den milliardenschweren IT-Giganten wie Google, Apple, Microsoft und Facebook vorbehalten.

Schnelles Design-in mit Computer-on-Modules

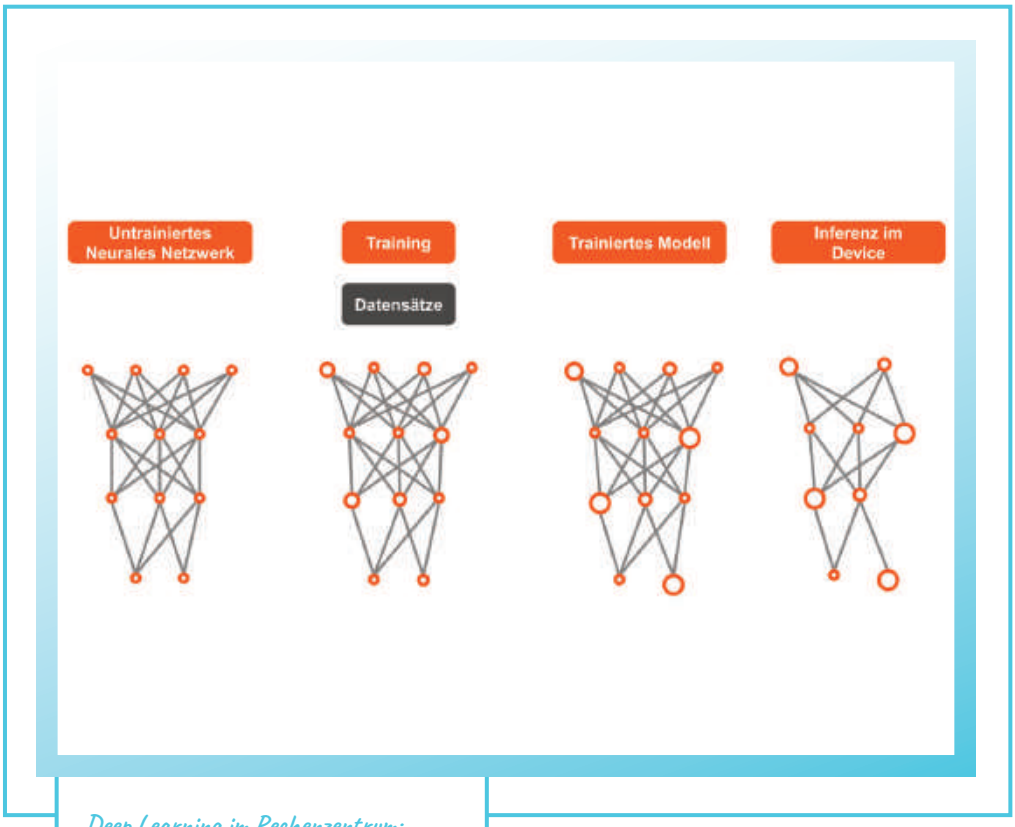
Jetzt bleibt nur noch die Frage, wie OEMs diese hardwareseitigen KI-Enabler möglichst schnell und effizient in ihre Applikationen eindesignen können. Einer der effizientesten Wege führt über standardisierte Computer-on-Modules, die mit umfassendem Support für das GPGPU-Processing ausgestattet wurden. Man davon ausgehen, dass OEM beim Einsatz von Computer-on-Modules rund 50 bis 90 Prozent Ihrer NRE-Kosten sparen. Durch den modularen Ansatz der Module wird die Applikation zudem auch bedarfsgerecht skalierbar: Durch einen einfachen Tausch lassen sich ohne weiteren Designaufwand auch neue Leistungsklassen auf vorhandene Carrierboard-Designs integrieren, sodass OEMs die Funktionalität ihrer Designs leicht um diese innovativen Features erweitern können.

Künstliche Intelligenz in der Industrie

Die Embedded-Hersteller Syslogic und Nvidia gehen eine Zusammenarbeit ein. Nvidia bringt sein Know-how bezüglich KI-fähiger Prozessortechnologie ein, Syslogic ihre langjährige Erfahrung in der Entwicklung und Fertigung von ultrarobusten Embedded-Systemen. Nvidia als KI-Vorreiter bietet mit seiner Jetson Plattform aktuell drei unterschiedlich performante Prozessorfamilien – Jetson Nano, Jetson TX2 und Jetson AGX Xavier. Diese lassen sich ideal für KI-Anwendungen am Netzwerkrand einsetzen. Das Ziel der beiden Unternehmen ist es, den Weg für KI-Anwendungen im Embedded-Markt zu ebnen. Konkret bietet Syslogic Embedded-Systeme mit Nvidia Technologie, welche für den Einsatz in Bau- und Landmaschinen, in Zügen, in Minenfahrzeugen sowie für Verkehrstechnik- oder Smart-City-Anwendungen entwickelt wurden.

www.syslogic.de

Bild: Syslogic GmbH



Deep Learning im Rechenzentrum: Intelligenz im lokalen Industrie-Device.

COM Express – der Standard für High-End Module

Der Formfaktor unter den Modulen für diese Leistungsklasse ist der Standard COM Express, der von der PICMG herstellerunabhängig seit vielen Jahren weiterentwickelt wurde und der von allen führenden Embedded Computing Lieferanten unterstützt wird. Unternehmen wie congatec bieten AMD Ryzen Embedded V1000 Prozessor basierte Module beispielsweise im COM Express Basic Type 6 Formfaktor an, der hinreichend Kapazität bietet, die gesamte Performancerange von 15 bis 54 Watt TDP abzudecken. Dank RTS-Hypervisor Support kann das echtzeitfähige conga-TR4 Modul zudem KI Plattformen unterstützen, bei denen die Anbindung von Deep Learning Systemen und Digitalen Twins über Virtuelle Maschinen umgesetzt werden soll, sodass die harte Real-Time Processing stets sichergestellt werden kann. Und auch für den UIC-Standard der SGET für den Datenaustausch über IoT-Gateways ist das Modul dank seiner standardisierten APIs vorbereitet, sodass sich OEM Kunden voll und ganz auf die Entwicklung der Applikation konzentrieren können. Fehlende ‚Glue Logic' kann auf Kundenanforderung jederzeit auch bedarfsgerecht entwickelt und bereitgestellt werden.

Embedded High-End Edge-Server Design Optionen

Wollen OEM ihre Digitalen Zwillinge und Deep Learning Intelligenz zudem in das industrielle Edge bringen, stellt congatec hierfür ebenfalls Optionen bereit: Embedded Designs auf Basis der neuen, bis zu zehn Jahren langzeitverfügbaren AMD EPYC Embedded 3000 Prozessoren. Die Prozessoren der Embedded Server Klasse ermöglichen mit ihren bis zu 16 Cores, 10 Gigabit Ethernet Performance und bis zu 64 PCIe Lanes selbst Deep Learning Applikationen am Edge des IIoTs, sodass Entwicklern damit alles zur Verfügung gestellt wird, was sie von Seiten der Hardwareplattformen für Deep Learning basierte KI Plattformen im industriellen Echtzeit-Einsatz benötigen. ■

www.congatec.com

AUTOMATISIERTE CODE-PRÜFUNG

TEXT: Perforce Software UK Ltd. BILD: ©Eisenhans/fotolia.com

Durch die Digitalisierung steigt der Software-Anteil in Geräten und Maschinen aller Art. Während Sicherheit und Effizienz zu den zentralen Faktoren gehören, die nahezu jede Software-Entwicklung heute erfüllen muss, stellen viele Branchen individuelle Anforderungen an das jeweilige Projekt. Um diese umfassend abzudecken, hat Perforce Software 2019 die US-Firma Rogue Wave Software übernommen. Mit deren Lösung Klocwork hat der Spezialist für Versionskontrolle und Enterprise-DevOps nun zwei Lösungen zur statischen Code-Analyse im Portfolio – neben Klocwork auch seine Lösung Helix QAC. Beide Lösungen sind für unterschiedliche Szenarien optimiert, wodurch sie sich für den Einsatz in verschiedensten Kontexten eignen.

Ein geeignetes Tool zur statischen Codeanalyse muss in der Lage sein, sich leicht an die jeweiligen Projektanforderungen anzupassen und die bestehenden Herausforderungen zu bewältigen. Aus diesem Grund hat Perforce nun zwei separate Produkte in seinem Portfolio für die statische Codeanalyse: Helix QAC und Klocwork. Die Kernfunktionalitäten der statischen Code-Analyse sind beiden Lösungen gemein: Sowohl Helix QAC als auch Klocwork prüfen Software-Code bereits während der Eingabe und identifizieren so Fehler oder riskante Code-Abschnitte. Dazu erzeugen sie ein akkurates Verhaltensmodell der entsprechenden Software und verfolgen jede der Variablen mit den Werten nach, die sie zur Laufzeit erhalten würden. Da kritische Stellen so bereits frühzeitig im Entwicklungsprozess entdeckt werden, lassen sich Aufwand und Kosten für die Fehlerbehebung deutlich reduzieren. Gleichzeitig unterscheiden sich beide Lösungen durch ihren Fokus und spezialisierte Funktionen:

1 Helix QAC unterstützt die Programmiersprachen C und C++ und eignet sich besonders dann, wenn eine strikte Compliance mit Sicherheitsstandards erreicht werden muss. Entsprechend empfiehlt sich Helix QAC für sicherheitskritische Anwendungen, in denen eine höchstmögliche funktionale bzw. softwarebezogene Sicherheit unerlässlich ist.

2 Klocwork unterstützt C, C++, Java und C# und lässt sich vor allem dazu nutzen, die Qualität großer Codebasen im Enterprise-Maßstab sicherzustellen. So eignet sich Klocwork für Software-Entwicklungsteams, die umfangreiche Code-Mengen z.B. in einer Continuous-Integration-Pipeline effizient und automatisiert prüfen müssen.

Entsprechend sind beide Lösungen in unterschiedlichen Marktsegmenten verbreitet: Während Helix QAC zu den führenden Tools zur statischen Code-Analyse in der Automobilindustrie zählt, kommt Klocwork vorrangig in Embedded-Branchen wie z.B. der Medizintechnik zum Einsatz. Durch die Kombination beider Tools in seinem Portfolio bietet Perforce nun umfassende Erfahrung bei der Realisierung dynamischer, qualitativ hochwertiger statischer Code-Analyse für unterschiedlichste Szenarien, unabhängig davon, in welcher Branche das jeweilige Entwicklungsteam tätig ist und mit welchen Entwicklungsprozessen dieses arbeitet. ■

www.perforce.com

Bild ©vchalup/stock.adobe.com

embeddedworld
Exhibition&Conference
Halle 4
Stand 423

Testabdeckung bei kleinen Targets

Sicherheit bei IoT-Anwendungen **beginnt bei den Sensoren und Aktoren**. Hier werden Daten erzeugt, die das IoT so wichtig machen. Und hier werden Aktionen ausgeführt, die auf den gesammelten, aggregierten und analysierten Daten basieren. Um diese **Embedded-Geräte sicher** zu machen, müssen sie intensiv getestet werden. Die **Überwachung**, ob alle notwendigen Tests erfolgt sind, ist gerade bei den kleinen Targets **nicht trivial**. Hier sind teilweise andere Vorgehensweisen nötig als bei Server-Anwendungen.

AUTOR: Klaus Lambertz, Geschäftsführer der Verifysoft Technology GmbH BILDER: Verifysoft Technology GmbH

Wer sich mit der Sicherheit im IoT befasst, hat aktuell kaum Langeweile. Hier sind noch viele Fragen offen, wie die Daten und Anwendungen gegen Missbrauch hinreichend geschützt werden können. Denn klar ist, dass die in der IT bewährten Ansätze mit Firewalls und Malware-Scannern bei kleinen Embedded-Geräten nicht funktionieren. Gleichzeitig werden die IoT-Geräte für viele Unternehmen immer kritischer, sie bilden zunehmend die Basis der Geschäftsmodelle. Die Hersteller sind also gefordert, ihre Embedded-Systeme von Anfang an möglichst sicher zu entwickeln, so wenig Angriffsfläche wie möglich und ein Maximum an Zuverlässigkeit zu bieten.

SICHER DURCH TESTING. Für sichere Embedded-Geräte ist das Testing ein wichtiger Baustein innerhalb des Entwicklungsprozesses, um Fehler möglichst frühzeitig zu erkennen. Zahlreiche Normen für die Entwicklung sicherheitskritischer Software stellen deswegen klare Anforderungen, welche Testmethoden anzuwenden und welche Testabdeckungen zu erzielen sind. Hierbei gibt es unterschiedliche Komplexitätsstufen, die je nach Kritikalität des Systems genutzt werden. Die wichtigsten sind:

- Statement Coverage (Anweisungsüberdeckung): Es wird ermittelt, welche Anweisungen durch die Tests ausgeführt wurden. Toter Code kann dabei ebenso erkannt werden wie Anweisungen, für die noch kein geeigneter Test erstellt wurde.

- Branch Coverage (Zweigüberdeckung): Sie erfasst, ob alle Programmzweige durchlaufen wurden. Dieses ist die Mindestanforderung, die an das Testing gestellt werden sollte. Branch Coverage ist zudem mit einem vertretbaren Aufwand realisierbar.

- MC/DC (Modified Condition/Decision Coverage): MC/DC ist die höchste in den Normen geforderte Testabdeckungsstufe und sehr kom-

plex. Um den Testaufwand zu minimieren, werden alle atomaren Bedingungen einer zusammengesetzten Bedingung herangezogen. Für jede der atomaren Bedingungen wird ein Testfallpaar getestet, das zur Veränderung des Gesamtergebnisses der zusammengesetzten Bedingung führt, wobei sich jedoch nur der Wahrheitswert der betrachteten atomaren Bedingung ändert. Hierbei muss der Wahrheitswert der anderen atomaren Bedingungen konstant bleiben.

CODE WÄCHST DURCH INSTRUMENTIERUNG. Zur Ermittlung der Testabdeckung dienen Code Coverage Analyser. Diese arbeiten in der Regel nach dem gleichen Prinzip: Sie instrumentieren den Code vor der Übergabe an den Compiler, ergänzen Ihn also mit Zählern für die gewünschten Testebenen. Die Zähler werden meist als globale Arrays abgelegt. Wann und wie diese Zähler dann verändert werden, hängt von der geforderten Code-Coverage-Stufe ab. Der vor allem bei kleinen Targets unangenehme Nebeneffekt der Instrumentierung ist, dass der Code umfangreicher wird. Dadurch werden sowohl RAM als auch ROM zusätzlich belastet. Bereits eine kleine in C geschriebene While-Bedingung kann so deutlich wachsen. Aus der Ausgangsstruktur

```
while (! b == 0 )
{
  r = a % b;
  a = b;
  b = r;
}
result = a;
```

wird durch die Instrumentierung – in diesem Fall mit dem Code-Coverage-Werkzeug Testwell CTC++ - folgende Struktur:

```
while ( (( ! b == 0 ) ?
(ctc_t[23]++, 1) : (ctc_f[23]++,
0)) )
{
  r = a % b ;
  a = b ;
  b = r ;
}
result = a ;
```

Bei Server- oder PC-Anwendungen kann dieser Effekt vernachlässigt werden. Bei Embedded-Geräten hingegen oft nicht, da die Hardware-Ressourcen aus Kostengründen oft sehr knapp kalkuliert sind. Hier ist darauf zu achten, einen Code Coverage Analyser mit einem vergleichsweise geringen Instrumen-

ROM Usage	
Without Instrumentation	60Bytes
Coverage Level Function Coverage	67Bytes
Coverage Level Branch Coverage	118Bytes
Coverage Condition Coverage	285Bytes
Additional RAM Usage Without Bit Coverage (32 Bit Counter)	
Coverage Level Function Coverage	4Bytes
Coverage Level Branch Coverage	16Bytes
Coverage Condition Coverage	28Bytes
Additional RAM Usage With Bit Coverage	
Coverage Level Function Coverage	1Bit
Coverage Level Branch Coverage	4Bit
Coverage Condition Coverage	7Bit

```
Hits/True False Line Source
                    1 /* File io.c ----------------------------------------
                    2 #include <stdio.h>
                    3 #include "io.h"
                    4 /* Prompt for an unsigend int value and return it */
Top
          10        5 unsigned io_ask()
                    6 {
                    7     unsigned    val;
                    8     int         amount;
                    9
                   10     printf("Enter a number (0 for stop program): ");
           0   10  11     if ((amount = scanf("%u", &val)) <= 0) {
                   12         val = 0;     /* on 'non sense' input force 0 */
                   13     }
          10       14     return val;
                   15 }
```

Testwell CTC++ Report mit Coverage-Informationen im Quellcode.

tierungs- Overhead zu nutzen, da die Zähler sonst schnell die Grenzen des verfügbaren Speichers sprengen. Das gilt insbesondere, wenn sehr anspruchsvolle Testabdeckungsstufen wie MC/DC erforderlich sind. Spezielle, auf Embedded-Systeme optimierte Analyser wie Testwell CTC++ von Verifysoft Technology sind hierfür die richtige Wahl.

PARTIELLE INSTRUMENTIERUNG. Sollte das Code-Coverage-Tool einen zu hohen Instrumentations-Overhead haben, kann diese Hürde beim RAM mit der partiellen Instrumentierung umgangen werden. Dabei werden nur kleine Ausschnitte des zu testenden Programms instrumentiert und getestet. Der Test wird nacheinander mit allen Programmteilen wiederholt, die daraus gewonnenen Daten werden zu einem Gesamtbild zusammengefügt. Dadurch kann die Testabdeckung für das vollständige Programm ermittelt werden. Ein anderer Ansatz auf kleinen Targets ist, die Größe der Zähler zu beschränken. Normalerweise arbeiten Code-Coverage-Werkzeuge mit 32-Bit-Zählern. Diese können zumindest theoretisch auf 16 oder 8Bit reduziert werden. Hierbei sollte man aber Vorsicht walten lassen, denn unter Umständen können die Zähler dann überlaufen. Die gewonnenen Daten müssen also mit großer Sorgfalt interpretiert werden. In extremen Fällen können die Zähler zudem auf einzelne Bits gesenkt werden. Diese Bit-Coverage kann z.B. dann sinnvoll sein, wenn es nicht relevant ist, wie oft ein Programmabschnitt durchlaufen wurde.

Auch die gewählte Coverage-Stufe beeinflusst die Anforderungen an den verfügbaren RAM. Der zusätzlich benötigte Platz im ROM hingegen lässt sich kaum begrenzen. Zur Erfassung der Code Coverage ist eine kleine Bibliothek erforderlich, die u.a. für die Übertragung der Zählerstände an einen Host zuständig ist. Nicht zu vergessen: Neben dem Speicher belastet die Instrumentierung auch den Prozessor im Target. Hierdurch kann es vorkommen, dass ein definiertes Timing nicht mehr eingehalten wird. Besonders wenn die CPU bereits eng am Limit arbeitet, können fehlerhafte Abläufe auftreten. Die Buskommunikation ist dafür besonders anfällig. Hier sollte der Tester aufmerksam den Ablauf überwachen und die Ergebnisse sorgfältig prüfen. Leistungsfähige Code-Coverage-Tools sind jedoch in der Lage, den Speicherbedarf für die Instrumentierung sowie die Änderungen des Laufzeitverhaltens relativ gering zu halten.

FAZIT. Für den langfristigen Erfolg von IoT-Initiativen wird die Sicherheit eine wichtige Rolle spielen. Neben den Anwendungen für die Industrie müssen auch IoT-Programme für den privaten Bereich so entwickelt und getestet werden, dass die Risiken für Anwender und Hersteller beherrschbar sind. Während die MC/DC-Coverage für sicherheitskritische Anwendungen in Autos und Flugzeugen zwingend vorgeschrieben ist, sollte in allen anderen Bereichen zumindest Branch-Coverage Standard sein. Aktuell fordern zwar nur wenige Normen einen Nachweis der Testabdeckung für Software, die nicht sicherheitskritisch ist, allerdings ist es nur eine Frage der Zeit und der Markdurchdringung bis die Standardisierungsgremien und Branchenverbände die Anforderungen auch abseits der sicherheitskritischen Anwendungen erhöhen. Bessere Tests sind nicht zuletzt im Interesse der Hersteller selbst, da fehlerhafte Produkte hohe Folgekosten verursachen und den Ruf des Unternehmens erheblich schädigen können. Die vom PC bekannte Bananen-Software, die erst beim Nutzer reift, werden die Kunden im Embedded-Bereich kaum akzeptieren wollen. ■

www.verifysoft.com

Beste Innovation bei der IoT-Sicherheit

Juniper Research hat die diesjährigen Gewinner der Future Digital Awards for Technology and Innovation bekannt gegeben. In der Kategorie IoT-Innovation hat der britische Marktanalyst die eSIM-Managementplattform AirOn von G+D Mobile Security als 'Best IoT Security Innovation of the Year' prämiert. Mit der Plattform bietet das Unternehmen eine Lösung für das sichere Lifecycle-Management von eSIMs auf mobilen Geräten, und zwar vollständig kompatibel mit allen Geräten und dem gesamten eSIM Ecosystem.

www.gi-de.com

ECHTZEIT-BETRIEBSSYSTEME

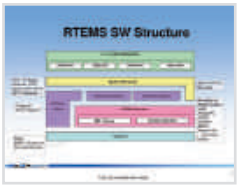
Der Funktionsumfang von Geräten wird heute vor allem durch die Software definiert. Doch ein großer Funktionsumfang bedeutet viel Programmieraufwand. Ein gutes Betriebssystem mit dem passenden Entwicklungskit kann hier erhebliche Zeitersparnisse bringen.

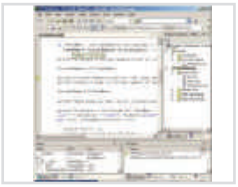
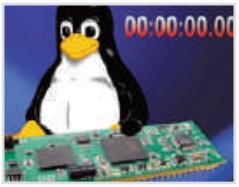
Embedded-Echtzeitbetriebssysteme ermöglichen deterministische Reaktionen in Situationen, in denen es darauf ankommt. Doch die Rolle der RTOS ist im Wandel, auch wenn die grundlegenden Anforderungen an Zuverlässigkeit, Determinismus und Sicherheit bestehen bleiben. Entwickler suchen heute komfortable Tools, die denen der IT in nichts nachstehen und eine möglichst häufig wiederverwendbare Plattform, die skalierbar mit den Herausforderungen wachsen oder auch schrumpfen kann. Unsere Marktübersicht zeigt 20 Systeme als Basis für moderne IoT- bzw. Embedded-Entwicklungen. *(kbn)* ■

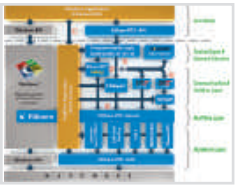
	JamaicaVM	
Anbieter Produkt-ID Ort Telefon Internet-Adresse	Aicas GmbH **10315** Karlsruhe 0721/ 663968-77 www.aicas.com	B&R Industrie-Elektronik GmbH **10323** Bad Homburg 06172/ 4019-0 www.br-automation.com
Produktname	JamaicaVM	Automation Runtime
Einsatzgebiet	Bildverarbeitung, Steuerung, Bewegungs-Steuerung, CNC-Steuerung, Robotik, Fahrzeuge, Steuerung, Robotik, Fahrzeuge	Industrial Automation, Steuerung, Bewegungs-Steuerung, CNC-Steuerung, Robotik, Netzwerkknoten
Beschreibung des Echtzeitbetriebssystems	kompakte, echtzeitfähige Java Virtual Machine für Embedded Systems	Garantiert höchste Leistung für eingesetzte Hardware, läuft hardwareunabhängig auf allen B&R Zielsyst., IEC61131-3 ANSI-C C++
x86, 68xxx, ARM StrongARM, Geode, MIPS, Pentium M, PowerPC, Xscale Weitere Hardwareplattformen	alle, alle, alle, alle, alle, alle, alle, alle, Blackfin, SH-4, ERC-32, Sparc	✓,✓,✓,✓, ,✓,,
Erreichbare Verfügbarkeit (Ausfallsicherheit)	hochverfügbar	hochverfügbar durch CPU Redundanz
Speicherbedarf für das Betriebssystem	1MB	je nach Anwendung
Speicherverwaltung für die Applikation	-	✓
CPU-Typ	32Bit	16, 32Bit
Maximale Anzahl von Prioritätsebenen	65.535	256
Bedienoberfläche	grafisch (Eclipse) oder Kommandozeile	grafisch
Remote Debugging	verfügbar	✓
Entwicklungs-Tools	Eclipse	Automation Studio
Verfügbare Programmiersprachen	Java	IEC61131-3, C, C++
Tools zur Systemanalyse	Thread Monitor, Datenflussanalyse	Automation Studio, Webbasierende Diagnose
Dynamisches Hinzuladen von Komponenten	verfügbar	✓, stoßfreier Download
Unterstützte Feldbusse	verfügbar	Powerlink, CANopen, CAN, Profibus, ASi, Ethernet/IP, Devicenet, Modbus TCP, Profinet, usw.

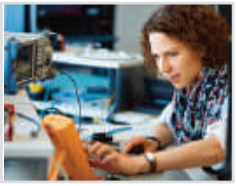
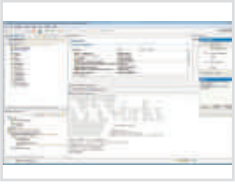
Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 28.01.2020

MARKTÜBERSICHT ECHTZEITBETRIEBSSYSTEME

					
Anbieter Produkt-ID Ort Telefon Internet-Adresse	embedded brains GmbH **13928** Puchheim 0049/89/ 1894741-00 www.embedded-brains.de	Embedded Office GmbH & Co. KG **22285** Wangen 07522/ 99983-0 www.embedded-office.com	Embedded Tools GmbH **14473** Münster 0251/ 98729-0 www.embedded-tools.de	Hitex GmbH **10309** Karlsruhe 0721/ 9628-0 www.hitex.de	IEP GmbH Ing.-Büro f. Echtzeitprogrammierung **10304** Langenhagen 0511/ 70832-0 www.iep.de
Produktname	RTEMS	Flexible Safety RTOS	smx 4.2	CMX-RTX	RTOS-UH
Einsatzgebiet	Medizin, Raumfahrt, Wissenschaft, Roboter, Musik, Militär, Industrie, Kommunikation	Steuerung, Robotik, Fahrzeuge	Embedded Systems	Steuerung, Bewegungs-Steuerung, CNC-Steuerung, Robotik, Fahrzeuge, Netzwerkknoten	Steuerung, Bewegungs-Steuerung, Robotik, Fahrzeuge, Netzwerkknoten, CNC-Steuerung
Beschreibung des Echtzeitbetriebssystems	Open-Source-Echtzeitbetriebssystem für überwiegend displaylose, echtzeitfähige eingebettete Systeme	Das Flexible Safety RTOS ist ein vor-zertifizierter Echtzeitkern. Der Kernel zeichnet sich durch einzigartige Flexibilität aus.	hard-real-time RTOS für ARM/Cortex, ColdFire u. PowerPC Prozessoren. Ohne Royalties im Sourcecode. System Lev. Debugging Tools usw.	Preemtives Multitasking-Echtzeit-Betriebssystem für eine Vielzahl von 8, 16, 32, 64Bit Mikrocontrollern und DSPs. Royalty-free, usw.	Modulares Echtzeitbetriebssystem mit Bedienschnittstelle, Dateisystem, Ethernetanbindung, Unterstützung div. Feldbusse, usw.
x86, 68xxx, ARM StrongARM, Geode, MIPS, Pentium M, PowerPC, Xscale, Weitere Hardwareplattformen	i386, 68K, ARM, , MIPS, , PowerPC, , SPARC, NOIS II, Microblaze, Coldfire	alle Cortex-M/ -R/ -A Mikrocontroller, alle Mikrocontroller ab e200-z4, alle Infineon TriCore Mikrocontroller	alle ColdFire V1/ V2/ V3/ V4, ARM7/9/11, Cortex-M3 -M4, -A8, -A9, 4xx, 5xx, 8xx, 5200, usw.	alle, alle, alle, , MIPS32 und MIPS64, , alle, alle, MSP430, H8, M16C, M32C, ST7, ST10, C167, XC166	, 683xx, 680x0 alle Taktfrequenzen, , , , , MPC8xx, MPC5xx, MPC5xxx, MPC8xxx, MPC7xxx alle Taktfrequenzen
Erreichbare Verfügbarkeit (Ausfallsicherheit)					
Speicherbedarf für das Betriebssystem	-	-	5 - 20kB	512Bytes (CMX-Tiny+) - 20 kB (je n. Prozessor)	2 - 256KB
Speicherverwaltung für die Applikation	-	-	-	anwenderdefiniert - anwenderdefiniert	8KB - 4GB
CPU-Typ		32Bit	32Bit	8, 16, 32, 64Bit CPUs	32Bit CPU
Maximale Anzahl von Prioritätsebenen			127	254	32.000
Bedienoberfläche		nicht vorhanden	grafisch	nicht vorhanden	befehlsorientiert
Remote Debugging			ja, smxAware live	über Third Party Tools	Debugger
Entwicklungs-Tools	GNU, msys2, Cygwin	alle auf dem Markt verfügbaren Cross-Entwicklungsumgebungen	IAR Workbench ARM, Rowley CrossWorks, CodeWarrior	CMX-BUG, Compiler architekturabhängig	Compiler, Debugger
Verfügbare Programmiersprachen	C	C	C, C++	C	ANSI-C, Pearl90, Codesys, Assembler
Tools zur Systemanalyse			✓, smxAware, smxAware live	Third Party Tools	Laufzeitanalyse
Dynamisches Hinzuladen von Komponenten		CAN (optional)	optional	✓	✓
Unterstützte Feldbusse			optional	optional CAN open	CAN, CANOpen, Devienet, Interbus, Profibus, Arcnet, Ethernet, ModBus

					
Anbieter Produkt-ID Ort Telefon Internet-Adresse	Miray Software AG **10327** München 089/ 72013-643 www.miray-software.com	On Time Informatik GmbH **10303** Hamburg 040/ 2279-405 www.on-time.com	Sigmatek GmbH & Co KG **10325** Lamprechtshausen +43 6274/ 4321-0 www.sigmatek-automation.com	SSV Software Systems GmbH **10305** Hannover 0511/ 40000-13 www.ssv-embedded.de	Synertronixx GmbH **10311** Hannover 0511/ 262 999 0 www.synertronixx.de
Produktname	Symobi, Sphere SP/MP	On Time RTOS-32 6.0	Lasal OS	RT-Preemption-Patch	Linux / RTAI
Einsatzgebiet	Steuerung, Digital Signage, Kiosk-Systeme, Micro-Server, Messknoten	Steuerung, Robotik, Bewegungs-Steuerung, Bildverarbeitung, CNC-Steuerung, Echtzeit Datenerfassung	Steuerung, Bewegungs-Steuerung, Robotik	Steuerung, Netzwerkknoten, Robotik	Automatisierung, Messtechnik, Steuerungstechnik, Netzwerkknoten
Beschreibung des Echtzeitbetriebssystems	Generisches, portables embedded RTOS, Microkernel, Client-Server-Architektur, modular & skalierbar, GUI, usw.	Win32 API kompatibles Echtzeitbetriebssystem für 32/64-bit x86 CPUs, unterstützt Microsoft Visual Studio u. Borland Compiler, usw.	Preämptives Multitasking, Dateisystem, Speicherverwaltung, Netzwerk, Grafik	Herstellerunabhängige Echtzeiterweiterung	Echtzeitbetriebssystem mit Dateisystem, Speicherverwaltung, TCP/IP-Stack, Administrationstools
x86, 68xxx, ARM StrongARM, Geode, MIPS , Pentium M , PowerPC , Xscale Weitere Hardwareplattformen	✓, , ✓, , MIPS32, ✓, ✓, ✓	alle x86 CPUs ab 386, 32-bit und 64-bit, auch Intel Atom und Vortex86, alle x86 kompatiblen Geode-Modelle, alle Pentium M und Core Duo Modelle	✓, , ✓, ✓, , ✓, , Atom	, , ARM 9, , , , ,	, , ARM 9 200 MHz, , , , ,
Erreichbare Verfügbarkeit (Ausfallsicherheit)		99,999%	99,9999%	99,8%	99,9%
Speicherbedarf für das Betriebssystem	256KB - 16MB	16k RAM/ROM - ca. 512k	256kB - 64 MByte (Linux)	2 - 4MB - 4MB	16MB
Speicherverwaltung für die Applikation	bis 1GB	1k - 1TB	bis 4GB	1MB - 16MB	-
CPU-Typ	32Bit, MMU	32, 64Bit (im 32Bit Modus)	32Bit	32Bit	32Bit
Maximale Anzahl von Prioritätsebenen	32	256	256	8	
Bedienoberfläche	grafisch	grafisch	befehlsorientiert		befehlsorientiert
Remote Debugging		Remote Debugging ü. Ethernet, RS232, LPT	✓	✓	
Entwicklungs-Tools	MS Visual Studio, Eclipse	Microsoft Visual Studio, Borland C++, Borland Delphi	Lasal	GNU-basiert	
Verfügbare Programmiersprachen	C, C++	C, C++, Pascal, Ada, Assembler	IEC61131-3, C, C++, AWL, KOP, EasyCase	C	C
Tools zur Systemanalyse	Diagnoseausgabe auf dem Target	Visual Studio Debugger, Kernel Tracer, Profiler, Tracealyzer, usw.	Lasal, Varan Analyzer, Varan Service Tool		
Dynamisches Hinzuladen von Komponenten	DLLs, Treiber, Dienste	Win32 DLLs	✓, on-the-fly	✓	
Unterstützte Feldbusse		CAN	Varan, CAN, CANopen, Seriell	CAN, Modbus, weitere a.A.	

			
IntervalZero **14164** München 089/ 207040-235 www.intervalzero.com	IntervalZero **14174** München 089/ 207040-235 www.intervalzero.com	Kithara Software GmbH **10322** Berlin 030/ 2789673-0 www.kithara.de	Lynx Software Technologies / Embedded Office **10313** Wangen im Allgäu 07522/ 970008-0 www.embedded-office.com
RTX64	RTX2016	Kithara 'RealTime Suite' (RTS)	LynxOS 7.0 (neueste Version seit 2013)
Bildverarbeitung, Steuerung, Bewegungs-Steuerung, CNC-Steuerung, Robotik, Fahrzeuge	Bildverarbeitung, Steuerung, Bewegungs-Steuerung, CNC-Steuerung, Robotik, Fahrzeuge	Automatisierung, Prüfsysteme, Steuerungen, Fahrzeugtechnik, Bewegungs-Steuerung, CNC-Steuerung, Robotik, Bildverarbeitung	Mil-Aero, Industrie, IoT, Medizintechnik, Büroautomatisierung
SMP (Symmetric Multi Processing) fähige Echt-zeiterweiterung f. Standard Win. mit allen Eigen-schaften wie Win. u. eigener Speicherverwaltung	SMP (Symmetric Multi Processing) fähige Echt-zeiterweiterung f. Standard Win. mit allen Eigen-schaften wie Win. u. eigener Speicherverwaltung	Echtzeitsystem (preemptive, multitasking, priority based)	Deterministisches hart-echtzeitfähiges RTOS mit POSIX-konformen APIs in einem 'small footprint' Embedded Kern, usw.
x86-Prozessoren (mind Dual-Core) von Intel, AMD, speziell Multicore-PCs und Boards, clusterfähig	alle aktuellen Prozessoren von Intel und AMD, speziell Multicore-PCs	alle aktuellen x86/x64 ab Dual-Core	Pentium, Pentium II/III, Intel 386/486..., , , , MIPS32 RISC, MIPS64..., Advantech PCM-9582, Dynatem C3PM..., Freescale MPC821, MPC74xx...,XScale 80200
99,99%	99,99%		Hochverfügbarkeit
1 MB, da nur eine Instanz	MB, da nur eine Instanz	Windows + 50MB - Windows + 200MB	-
begrenzt auf max. 64Bit bzw 128GB	begrenzt auf max. 32Bit	5MByte - mehr. 100MB	-
Multicore-CPUs auf x86-Basis mit 64-bit Win.	Multicore-CPUs auf x86-Basis	x86/x64, 32/64Bit CPUs ab Dual-Core	32 und 64Bit
128 reichen vollkommen aus	128 reichen vollkommen aus	255	256
grafisch	grafisch		befehlsorientiert
wird unterstützt via Ethernet	wird unterstützt via Ethernet	✓, Kithara Kernel Tracer	SpyKer
Microsoft Visual Studio	Microsoft Visual Studio 2013 und 2015	vorhandene Entwicklungsumgebung, z.B. Microsoft Visual Studio	Luminosity Eclipse IDE
C, C++, C# (via Library)	C, C++, C# (via Library)	C, C++, Delphi, C# (mit DLL)	C, C++
Tracealyzer, Object Viewer, RTSS Task Manager	Platform Evaluator, Object Viewer, RTSS Task Manager, RTX Analyzer, Performance View, usw	✓, Kithara Kernel Tracer	
unterstützt	unterstützt	✓, als DLL	✓
CAN, Ethercat, Profinet, EthernetIP, Power-link, Sercos, CC-Link via Partnerkarten	Ethercat, CANopen, CAN, Profinet, Ethernet, Sercos etc via Partnerkarten	Ethercat, CANopen	

			
Sysgo AG **10317** Klein-Winternheim 06136/ 9948-0 www.sysgo.com	Texas Instruments **14191** Freising 08161/ 800 www.ti.com	Vector Informatik GmbH **10306** Stuttgart 0711/ 80670-400 www.vector.com	Wind River GmbH **12319** Ismaning 089/ 962445-0 www.windriver.com
PikeOS	SYS/BIOS Real-Time Kernel	Microsar OS	Wind River VxWorks
sicherheitskritische Anwendungen: Avionik, Steuerung, Fahrzeuge	Steuerung	Steuergeräte, automotive und non-automotive	Steuerung, Luft-/ Raumfahrt, Militär, Netzwerke, Consumer Electronic, Robotik, Industrieaw., Me-dizin, Fahrzeugnavig., -sicherheit, Telem.
Echtzeitbetriebssystem mit Erweiterungen wie Dateisystem, Virtualisierungsplattform auf Basis eines Mikrokernels	Echtzeitbetriebssystem für DSP, MPU und MCU Bausteine. Multi-Tasking Support, Hardwareabstraktion u. Speicherverwaltung	Multitasking-Echtzeit-Betriebssystem speziell für Embedded-Anwendungen, entwickelt nach ISO 26262 / ASIL-D mit Partition, usw.	Skalierbarkeit, Zuverlässigkeit, stabile Echtzeit-Performance, Multi-Core-Beschleunigungs-fähigk. mit Betriebssystemkonfig. für AMP, SMP
x86-64, Nein, ARM, , ✓, , ✓, Nein SPARC V8, LEON, SH4	, , AM335x, , , , , MSP430, C6000 DSP, C2000 DSP, Stellaris	, , alle, , , , , Renesas RH850, Infineon Tricore, MPC57xxx	x86, Freescale ColdFire, ARM, , MIPS, Pentium M, Freescale, AMCC PowerPC, Xscale, SPARC, Fujitsu FR-V, SH-4, ATOM
hochverfügbar		99,99%	Extrem hohe Verfügbarkeit (SIL 2/3,DO 17,lev.A)
512MB RAM -	32kB -	20 - 70k	keine feste Grenze, architekturabhängig
-	-	plattformabhängig	keine Beschränkung durch das OS
32Bit CPU	16 + 32Bit	32, 64Bit CPUs	32, 64Bit
253	32	32.768	256
grafisch	nicht vorhanden	nicht vorhanden	grafisch
✓	Über Code Composer Studio	Über ORTI Standard oder XCP	über Netzwerk, serielle Leitung o. USB, usw.
CODEO (Eclipse-basierend)	Code Composer Studio C, Assembler	Grafischer Konfigurator	Wind River Workbench, Eclipse basierend
C, C++, Java, Ada, SoftSPS	System Analyzer	C, C++	C, C++, Ada
✓ (Tracing)	Nein	CANoe, Timing-Architects Tool Suite, GLIWA T1	On-Chip Debug JTAG, System Viewer, Per-form. Profiler, Memory An., Data Mon., usw.
möglich		Nein	Treiber, Kernelapplikationen, Echtzeitprozesse
CAN		CAN, LIN, FlexRay, Automotive Ethernet	CAN; andere über Partnerlösungen, z.B. Profibus

Alle Einträge basieren auf Angaben der jeweiligen Firmen. Stand: 28.01.2020

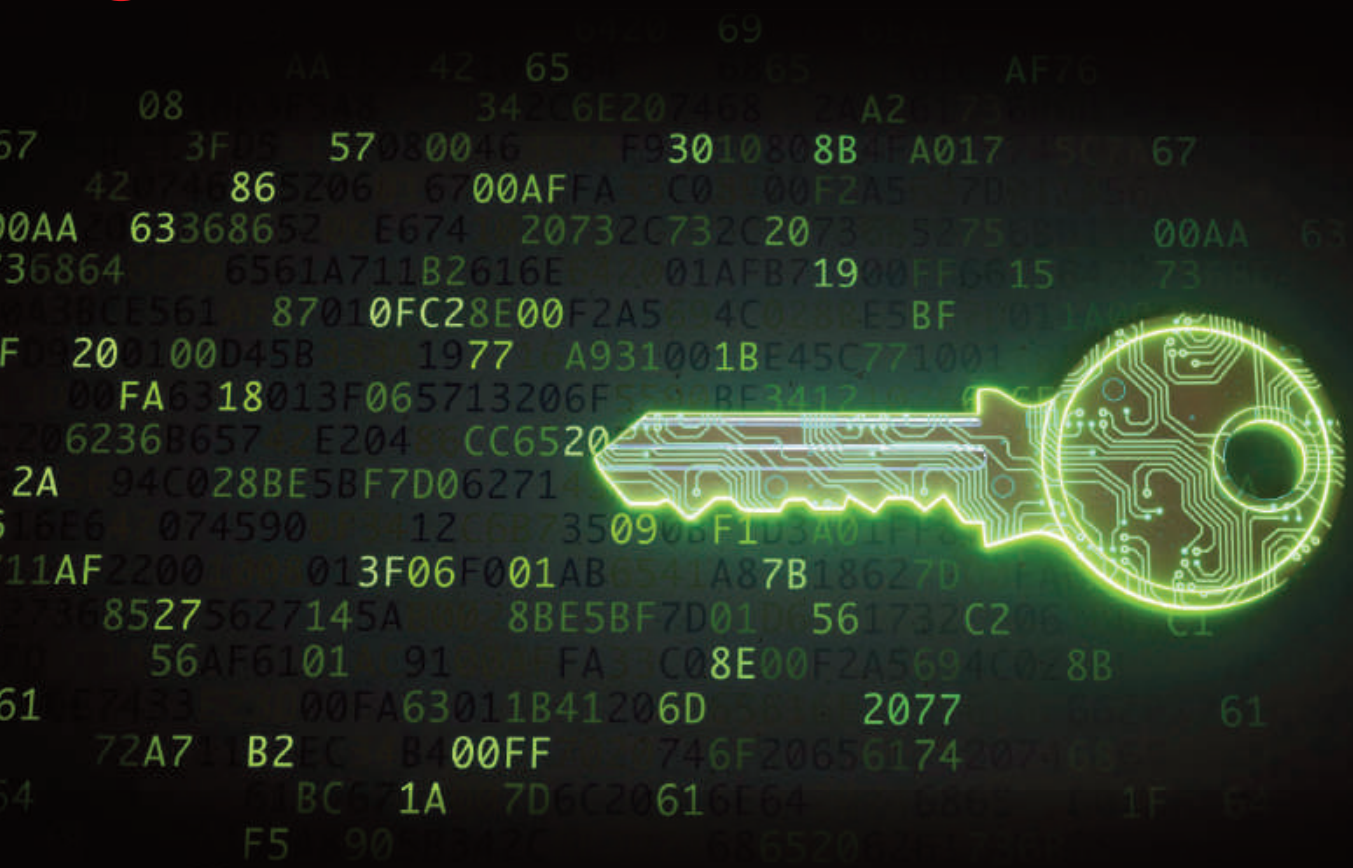


Bild: ©matejmo/istock.com

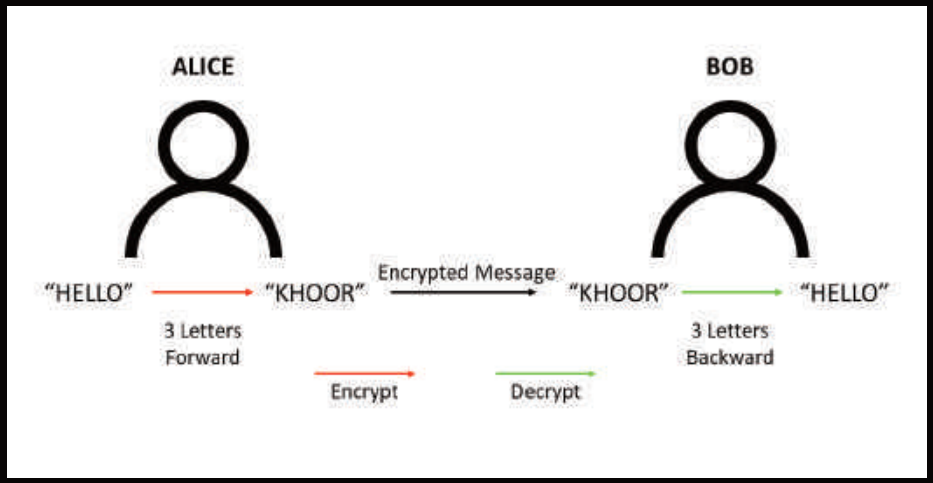
INFORMATIONSSICHERHEIT

So einfach wie P-K-I

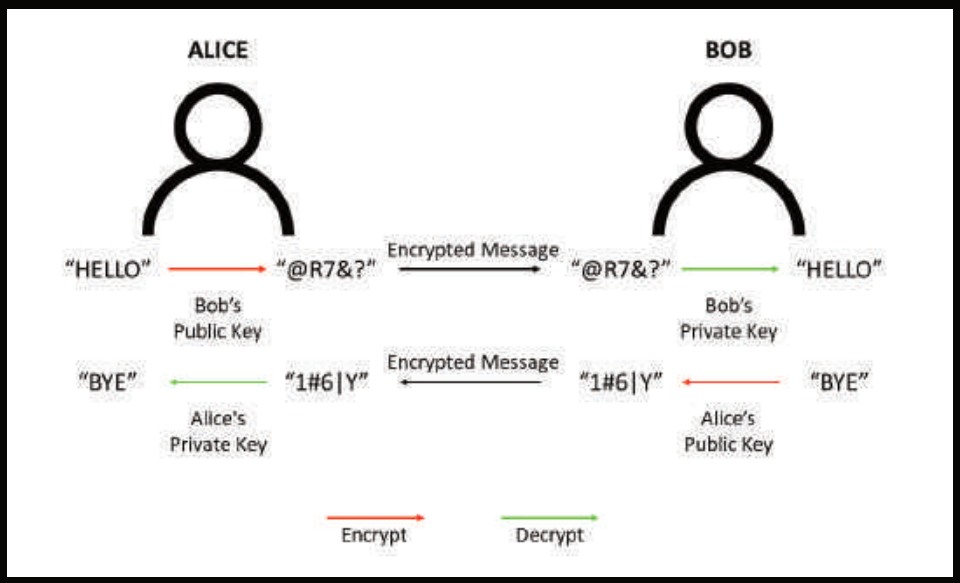
AUTOR: Sebastian Schulz , Regional Product Manager (EMEA) bei GlobalSign Ltd. **BILDER:** GMO GlobalSign Ltd.

Wer nicht in der IT-Branche tätig ist, der ist wahrscheinlich noch nicht auf die Abkürzung 'PKI' gestoßen, nicht mit dem Konzept vertraut oder - wahrscheinlicher - hat noch nie davon gehört. Kein Wunder, denn PKI soll als Akteur im Hintergrund arbeiten. Das Grundkonzept ist recht einfach, und der Hype darum hat sich längst gelegt. Trotzdem ist das Schlüsselmanagement weiterhin eine grundlegende Komponente der Informationssicherheit.

PKI steht für Public-Key-Infrastruktur. Jeder Buchstabe in der Abkürzung verrät ein wenig mehr darüber, womit wir es zu tun haben. Zum besseren Verständnis und einen didaktisch sorgfältigen Ansatz zur Erklärung der PKI müssen wir mit dem „K" beginnen, das für „Key (Schlüssel)" steht. Auf dem Gebiet der Kryptographie, also der Wissenschaft vom Versenden von Geheimnachrichten (das Wort selbst leitet sich vom Griechischen kryptós für "versteckt, geheim" und graphein für „schreiben" ab), wird der Begriff mit einer etwas anderen Bedeutung verwendet als erwartet. Haben Sie schon einmal Kryptogra-



phie verwendet? Haben Sie eine geheime Nachricht auf einem Zettel, unlesbar für die Augen Ihrer neugierigen Klassenkameraden, an Ihren Schwarm in der Schule geschickt? Möglicherweise haben Sie etwas ganz Ähnliches getan wie in der nebenstehenden Abbildung illustriert. Der Vorgang des Vorverlegens um drei Buchstaben im Alphabet wird in mathematischen Begriffen als ein Algorithmus bezeichnet. In der Kryptographie wird das Verschieben von Buchstaben als Kryptosystem bezeichnet. Die Zahl 3 wird in diesem Fall als Schlüssel bezeichnet.



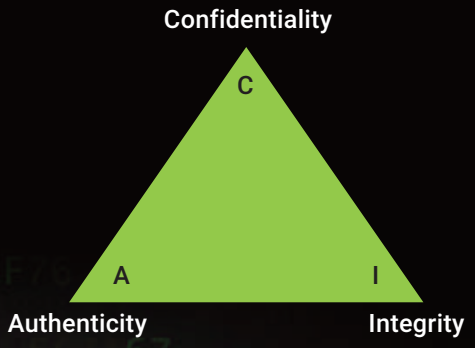
Stellen Sie sich nun vor, Sie haben versucht, das oben abgebildete System bei einem Brieffreund anzuwenden, der Tausende von Kilometern entfernt wohnt. Es könnte funktioniert haben – aber nur, wenn Sie es geschafft haben, das Kryptosystem und den Schlüssel an ihn weiterzugeben. Und das ist das Problem – die 'Zwickmühle', wenn Sie so wollen – dessen, was wir jetzt symmetrische Kryptographie nennen: Sie benötigen einen sicheren Kanal, um den Schlüssel weiterzugeben, aber Sie können keinen sicheren Kanal einrichten, bis ein Schlüssel weitergegeben wurde. Der niederländische Kryptograph Auguste Kerckhoff machte im 19. Jahrhundert diese sehr wichtige Beobachtung an Kryptosystemen: "Es [das Kryptosystem] sollte keine Geheimhaltung erfordern, und es sollte kein Problem sein, wenn es in die Hände des Feindes fällt." Heutzutage kennen wir dies als Kerckhoffs'sches Prinzip, und es ist in der Praxis der Kryptographie unverzichtbar. Dies macht jedoch die Geheimhaltung des Schlüssels elementar wichtig. Ohne dieses Vorgehen würde ein Lauscher genau wissen, wie er Ihre Nachricht entschlüsseln kann.

'Öffentliche' Schlüssel – aber nicht unbedingt öffentlicher Zugang

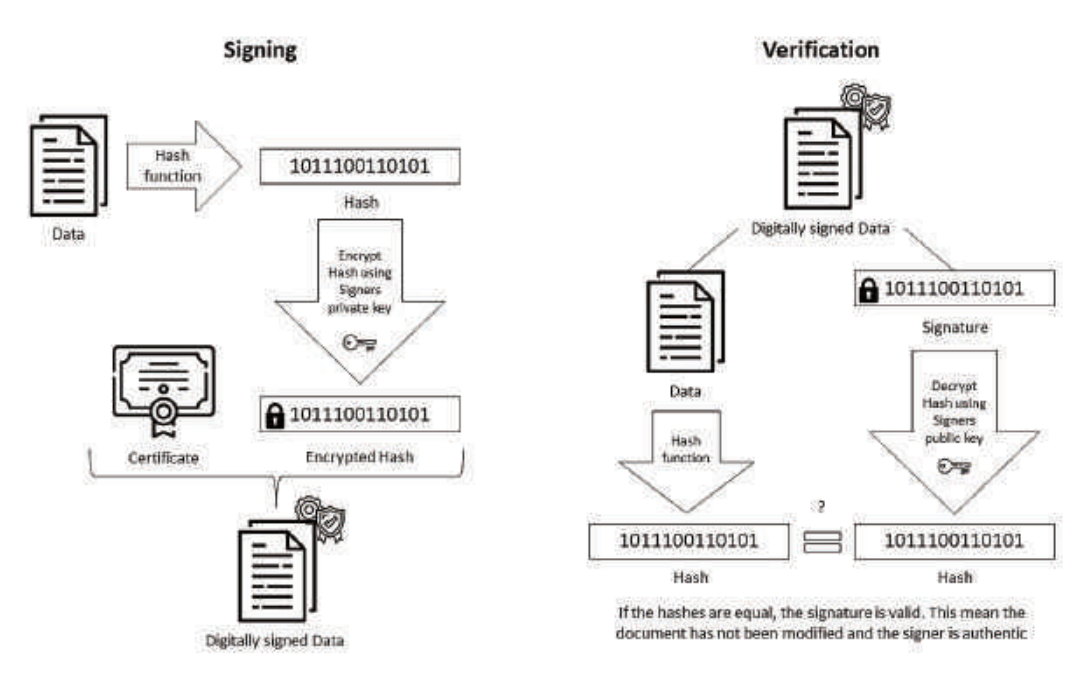
Glücklicherweise haben die Kryptographen Whitfield Diffie, Martin Hellman und Ralph Merkle ein Konzept entwickelt, das dieses zentrale Problem der Weitergabe eines Schlüssels über einen unsicheren Kanal löst. Stellen Sie sich Folgendes vor: Alice möchte Bob einen Gegenstand schicken. Sie packt ihn in eine kleine Metallschachtel und sichert diese mit einem Vorhängeschloss. Alice müsste ihre Schachtel packen, mit ihrem Vorhängeschloss verschließen und sie dann an Bob senden. Zum Entsperren müsste Alice ihren Schlüssel an Bob senden. Aber stellen Sie sich Folgendes vor: Statt, dass Alice die von ihr verschickte Schachtel mit ihrem eigenen Vorhängeschloss verschließt, benutzt sie das Vorhängeschloss von Bob, zu dem nur Bob den passenden Schlüssel besitzt. Bob muss sich keine Sorgen machen, sein Vorhängeschloss weiterzugeben, da es nur zum Verschließen einer Schachtel verwendet wird, nicht zum Öffnen. Das ist toll, da Bob ein Paket erhalten und öffnen kann, ohne dass Alice oder Bob jemals einen Schlüssel weitergeben müssen. Der Vergleich ist nicht perfekt, aber er ist für unsere Zwecke so nahe wie möglich an einem realen Beispiel. Technisch gesehen wird dieser Prozess der Datensicherung als Kryptographie mit öffentlichem Schlüssel bezeichnet. Anstelle des Vorhängeschlosses und seines Schlüssels aus unserem Beispiel sprechen wir in der Kryptographie mit öffentlichen Schlüsseln von privaten Schlüsseln und öffentlichen Schlüsseln. Und im Gegensatz zu den Vorhängeschlössern funktioniert die Kryptographie mit öffentlichen Schlüsseln in beide Richtungen: Öffentliche Schlüssel können die Verschlüsselung von privaten Schlüsseln entschlüsseln und umgekehrt. Darüber hinaus ist es praktisch unmöglich, einen privaten Schlüssel aus dem entsprechenden öffentlichen Schlüssel abzuleiten. Dies basiert auf einem Konzept namens 'Trapdoor-Einwegfunktionen', das viel tiefer in mathematische Gleichungen eintaucht, als wir es hier behandeln können. Der Kernpunkt: Da sie jeweils einen öffentlichen und einen privaten Schlüssel besitzen, können Alice und Bob absolut geheim kommunizieren. Es steht ihnen frei, den öffentlichen Schlüssel (daher der Name) öffentlich zu machen und haben dennoch die Garantie, dass die Kommunikation vertraulich bleibt - solange sie die Sicherheit ihres privaten Schlüssels beachten.

Was ist mit dem 'I'? Identität? Integrität? Infrastruktur?

Die Kryptographie mit öffentlichen Schlüsseln wurde in der Welt der Informationssicherheit weithin als revolutionär gefeiert. In erster Linie, weil durch geschickte Anwendung der Kryptographie mit öffentlichen Schlüsseln einige Garantien für die entscheidenden Aspekte von Datenschutz und Sicherheit gegeben werden können. Die drei Fundamente von Datenschutz und Sicherheit werden oft als "CIA-Dreieck" bezeichnet. (Dies ist ziemlich ironisch, da die Kryptographie mit öffentlichen Schlüsseln zu einem der schlimmsten Albträume für die US-amerikanische Central Intelligence Agency (auch als CIA bekannt) wurde.



CIA ist in diesem Kontext die Abkürzung für Confidentiality, Integrity, and Authenticity (Vertraulichkeit, Integrität und Authentizität). Mit anderen Worten: Verhindern von Lauschangriffen, Sicherstellen, dass eine Nachricht nicht verändert werden kann, und Überprüfen des Absenders einer Nachricht. Wir haben erklärt, wie Alice und Bob ihre Unterhaltung vertraulich halten. Lassen Sie uns jetzt einen Blick auf die beiden Komponenten Integrität und Authentizität werfen. Um Integrität und Authentizität behandeln zu können, müssen wir zwei weitere Begriffe einführen: Hashing und digitale Zertifikate. Hashing lässt sich leicht als 'Fingerabdruck einer Datei nehmen' erklären. Ein Fingerabdruck ist eine eindeutige Kennung einer Person. Doch unabhängig von der Person ist jeder Fingerabdruck (in etwa) gleich groß und gibt keine Auskunft über das Aussehen oder den Charakter der Person. Ein Dokumenten-Hash hat die gleichen Eigenschaften wie ein Fingerabdruck: einzigartig, einheitlich groß und anonym. Digitale Zertifikate sind Identitätsnachweise für den Besitzer eines bestimmten öffentlichen Schlüssels (und damit des entsprechenden privaten Schlüssels), ähnlich wie Ausweise Identitätsnachweise für eine Person sind. Alice kann ein digitales Zertifikat von einer so genannten Zertifizierungsstelle (CA) erhalten, genau wie bei einem Ausweis vom Passamt. Sie müsste ihre Identität gegenüber einem Teil der CA, der als Registrierungsstelle (RA) bezeichnet wird, nachweisen, genau wie sie bei der ersten Beantragung eines Ausweises eine Geburtsurkunde vorlegen müsste. Nachdem die RA die Identität von Alice überprüft hat, stellt sie ihr öffentliches und privates Schlüsselpaar aus. Da öffentliche Schlüssel weitergegeben werden müssen, aber zu groß sind, um sie sich einfach zu merken, werden sie zum sicheren Transport und für die Weitergabe auf digitalen Zertifikaten gespeichert. Da private Schlüssel nicht weitergegeben werden, werden sie in der Software oder im Betriebssystem gespeichert, die Sie verwenden, oder auf kryptographischer Hardware (z.B. einem USB-Token oder Hardware-Sicherheitsmodul (HSM)) gespeichert, die Treiber enthält, mit der Sie sie mit Ihrer Software oder Ihrem Betriebssystem verwenden können. Da private Schlüssel (im Idealfall) privat bleiben, können wir sicher sein, dass alle Aktionen, die von Alices privatem Schlüssel ausgeführt werden (wie das Entschlüsseln einer Nachricht oder das digitale Signieren eines Dokuments – mehr dazu weiter unten), tatsächlich von Alice ausgeführt wurden. Durch die Kombination von Hashing, digitalen Zertifikaten und Kryptographie mit öffentlichen Schlüsseln können wir eine digitale Signatur erstellen, die die Integrität und Authentizität von Nachrichten garantiert. Der Prozess des Signierens und Validierens von Signaturen vereint die drei Elemente. Wenn der Hash aus dem Klartext und das Ergebnis der Entschlüsselung übereinstimmen, wissen wir, dass die Nachricht nicht verändert wurde, wodurch die Integrität gewährleistet ist. Wenn wir den öffentlichen Schlüssel von Alice erfolgreich zur Entschlüsselung verwenden, wissen wir auch, dass es ihr privater Schlüssel gewesen sein muss, der zur Verschlüsselung verwendet wurde, wodurch die Authentizität gewährleistet ist. Aus diesem Grund kann die Public-Key-Infrastruktur auf der Kryptographie mit öffentlichen Schlüsseln aufbauen. Erinnern Sie sich wie Alice ein Zertifikat von einer CA bekommt?



Das Schöne an PKI ist, dass eine CA das Zertifikat von Alice mit ihrem privaten Schlüssel digital signiert und damit garantiert, dass die RA vor der Ausstellung des Zertifikats ihre Identität tatsächlich verifiziert hat. Jeder kann dann die Integrität und Authentizität von Alices Zertifikat überprüfen, indem er den öffentlichen Schlüssel der CA zur Validierung verwendet. Das Zertifikat, das dem öffentlichen Schlüssel der CA zugeordnet ist, wird als Root Zertifikat bezeichnet, wodurch die CA zu einer Root CA wird. Technisch gesehen kann eine CA von jedem kreiert werden, der einen PC hat. Andererseits ist es ein kompliziertes Unterfangen, seine CA öffentlich vertrauenswürdig zu machen, da dazu strenge Audits der Authentifizierung, Sicherheit und andere von WebTrust.org festgelegte Überprüfungsmethoden gehören. Infolgedessen werden nur wenige CAs von Browsern, Betriebssystemen und anderen Softwareprogrammen als öffentlich vertrauenswürdig anerkannt. Aber eine externe CA bietet weit mehr als nur öffentliches Vertrauen: Widerrufsdienste, Zeitstempelberechtigung, ein tiefes Verständnis für die Kosten, das Wissen und die Arbeitskräfte, die zur Sicherung der Infrastruktur und zur Einhaltung der Best Practices erforderlich sind und in einigen Fällen die Fähigkeit, das alles für Sie zu managen. ■

www.globalsign.de

Bild: ©momius/stock.adobe.com

Vertrauen im IIoT

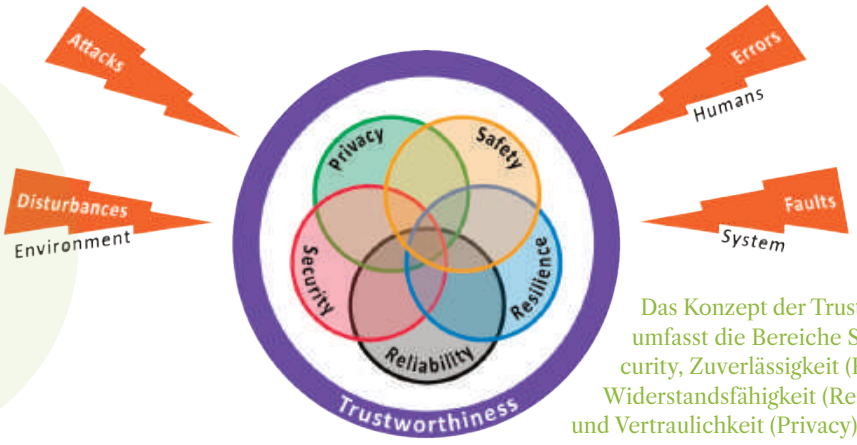
Das IIoT benötigt eine robuste und zuverlässige Architektur, denn das sichere Funktionieren aller beteiligten Komponenten ist die Grundlage der darauf aufbauenden Geschäftsmodelle. Ungeplante Ausfälle, potenzielle Angriffsflächen oder kompromittierbare Daten sind dabei nicht akzeptabel. Das Industrial Internet Consortium (IIC) hat sich dieses Themas angenommen und eine Referenzarchitektur mit Security-Framework veröffentlicht. Diese fordert nicht zuletzt die Entwickler auf, Sicherheitsaspekte frühzeitig zu berücksichtigen – angefangen bei der Software-Qualität.

AUTOR: Mark Hermeling, Senior Director Product Marketing bei GrammaTech, Inc. BILDER: GrammaTech, Inc.

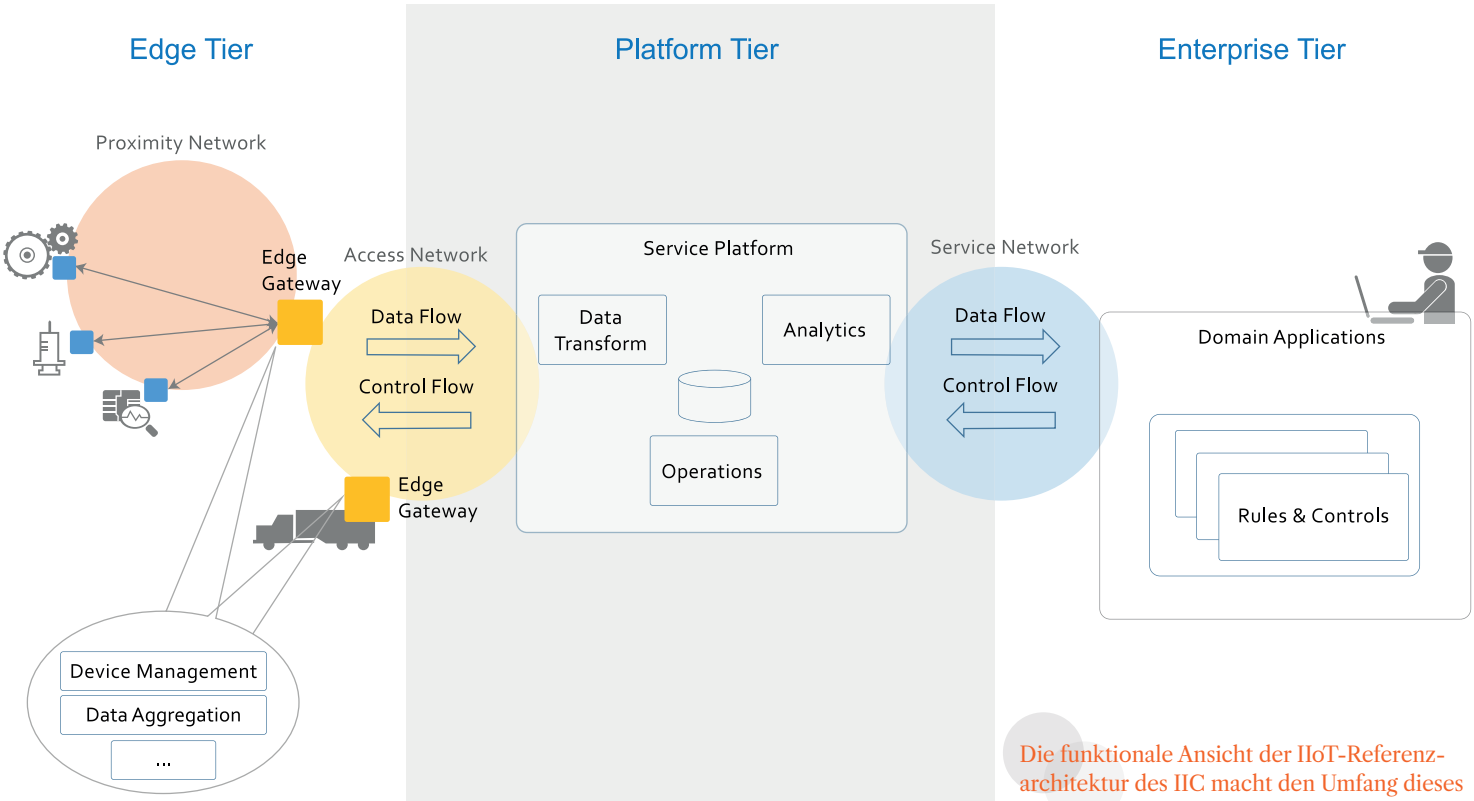
Das Industrial Internet of Things (IIoT) nimmt in den Digitalisierungsinitiativen vieler Branchen eine zentrale Position ein. Vor allem die Fertigung benötigt ein zuverlässiges, robustes und sicheres IIoT. Denn die Steuerung von Maschinen und anderen Anwendungen sind für den Geschäftsbetrieb kritisch. Während Ausfälle in einigen Nischen sicher zu verschmerzen sind, dürfen unter keinen Umständen kompromittierte Daten in das Netz gelangen oder Angreifer Zugriff auf diese Infrastruktur erlangen. Angriffe wie z.B. 2019 gegen einen norwegischen Aluminiumhersteller zeigen, dass der Schutz des IIoT höchste Priorität haben muss. Allerdings: Viele Unternehmen haben die IIoT-Sicherheit noch nicht priorisiert auf der Agenda. Laut einer Studie des TÜV Rheinland vom vergangenen Jahr hat nur jedes fünfte Unternehmen bereits Sicherheitsmaßnahmen für smarte Fertigungsanlagen implementiert. Das Industrial Internet Consortium (IIC) befasst sich deswegen damit, wie das IIoT sicherer, zuverlässiger und nutzbarer werden kann. Die Mitglieder des IIC sind Unternehmen der IT-Branche und Forschungseinrichtungen aus der ganzen Welt.

Eine Grundüberlegung dabei ist: Die Basis eines langfristig funktionalen IIoT, das auch die Vernetzung der Marktteilnehmer untereinander und branchenübergreifend ermöglicht, ist Vertrauenswürdigkeit oder 'Trustworthiness'. Daten, Systeme und Protokolle müssen dazu fünf grundlegende Eigenschaften aufweisen:

1. Safety
2. Security
3. Zuverlässigkeit
4. Widerstandsfähigkeit
5. Vertraulichkeit



Das Konzept der Trustworthiness umfasst die Bereiche Safety, Security, Zuverlässigkeit (Reliability), Widerstandsfähigkeit (Resilience) und Vertraulichkeit (Privacy).



Die funktionale Ansicht der IIoT-Referenzarchitektur des IIC macht den Umfang dieses Ansatzes End to End deutlich.

Robuste IIoT-Architektur

Um die Entwicklung einer entsprechend robusten Architektur voranzutreiben, hat das IIC eine Referenzarchitektur vorgestellt. Diese soll Entwicklern und Software-Architekten dabei helfen, stärkere und zuverlässigere IIoT-Systeme zu erzeugen. Zudem ist es das Ziel, einen allgemein akzeptierten IIoT-Ansatz zu finden, um die Interoperabilität und Vertrauenswürdigkeit über das gesamte IIoT-Ökosystem hinweg zu gewährleisten. Die Arbeit an dieser Referenzarchitektur, die fortlaufend optimiert wird, ist auf mehrere Arbeitsgruppen aufgeteilt. Damit wird gewährleistet, dass sowohl technologische also auch organisatorische und unternehmerische Aspekte berücksichtigt werden. Eine der IIC-Arbeitsgruppen, der auch GrammaTech angehört, befasst sich dabei speziell mit Fragen der Sicherheit. Die Ergebnisse wurden in einem Security-Framework zusammengefasst. Dieses deckt die unterschiedlichen sicherheitsrelevanten Bereiche wie Identifikation, Zugriffskontrolle, Root of Trust oder Schutz der Integrität ab. Das Ziel dabei ist es, einen allgemeinen Konsens zu erarbeiten, wie IIoT-Strukturen und -Systeme so abgesichert werden können, dass sie auch für kritische und sicherheitsrelevante Anwendungen vertrauenswürdig sind. Ein Aspekt dabei ist der Entwicklungsprozess. Das Framework selbst spezifiziert keine technologischen Details. So heißt es in Sektion 3.3 des Security-Frameworks recht unspezifisch: „Gründliche Vorgehensweisen in der Softwareentwicklung können den Entwicklern dabei helfen, mögliche Sicherheitsrisiken und Schwachstellen zu erkennen und zu beseitigen." Es bleibt den verschiedenen Anhängen zum Framework überlassen, konkretere Handlungsempfehlungen zu skizzieren. Ein wichtiger Baustein dabei ist, bereits in frühen Phasen des Software Development Lifecycles sicherzustellen, dass die Embedded-Systeme so fehlerarm wie möglich sind, um Sicherheitslücken zu vermeiden. Anhang C befasst sich u.a. mit Methoden, die eine gründliche Vorgehensweise charakterisieren. Um die Integrität der Software sicherzustellen, wird hier explizit die statische Code-Analyse empfohlen. Ganz zurecht, denn dieses Verfahren hat sich in unterschiedlichen, sicherheitsrelevanten

Harting und Expleo Group kooperieren

Harting und Expleo haben eine Kooperationsvereinbarung geschlossen. Vorstandsvorsitzender Philip Harting und Peter Seidenschwang, Head of Industry bei Expleo Germany, unterzeichneten die Vereinbarung, mit der beide Parteien die langfristige Zusammenarbeit im Bereich datengesteuerter Dienste und IoT-Lösungen für Industriekunden bekräftigen. Harting bietet den modularen, nach Industriestandards ausgelegten Edge-Computer Mica für zahlreiche Industrieanwendungen an, die Expleo mit ihren Experten für Konnektivität, Visualisierung, Datenanalyse und künstliche Intelligenz realisiert. Die gemeinsame Absichtserklärung durch die Geschäftsführung beider Unternehmen vertieft die langjährige Zusammenarbeit im Rahmen des Mica.network, der Nutzerorganisation rund um Hartings Edge Computing System Mica.

www.harting.com

Branchen wie Luftfahrt oder Automotive bewährt und wird in zahlreichen Normen ausdrücklich gefordert. Bei der statischen Code-Analyse wird der Code nicht ausgeführt. Ähnlich wie ein Compiler erzeugen Analyse-Tools wie CodeSonar von GrammaTech aus dem Quellcode eine 'Intermediate Representation' (IR). Anhand der IR untersucht das Tool alle möglichen Daten- und Kontrollflüsse.

Früh mit der Qualitätssicherung beginnen

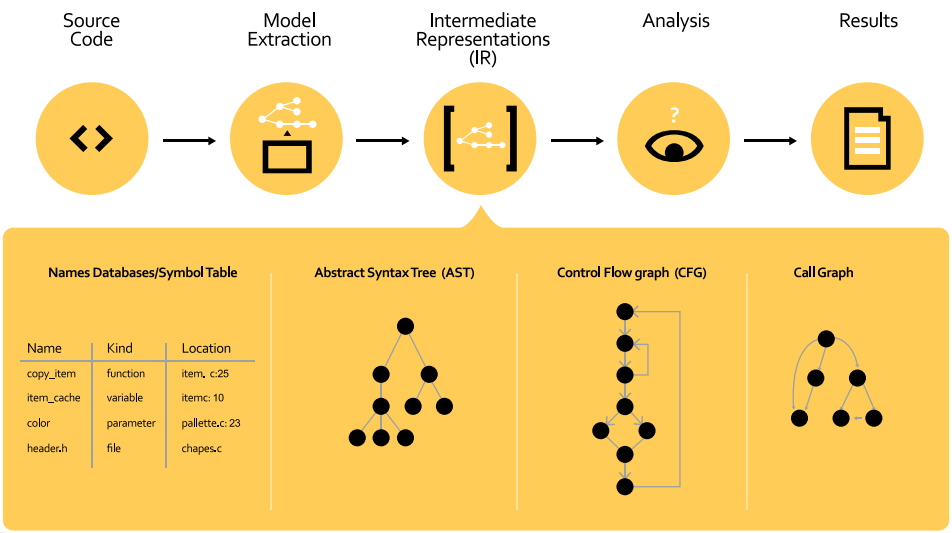
Da kein ausführbarer Code vorliegen muss, kann die statische Analyse bereits sehr früh im Entwicklungsprozess implementiert werden. Im Rahmen agiler Methoden wie Continuous Integration etwa ist eine erste Analyse direkt am Arbeitsplatz des Entwicklers möglich, eine weitere Überprüfung kann in der Mainline die täglichen Integrations erfassen, zudem ist eine tiefgreifende und ausführliche Analyse am Build-System sinnvoll. Typische Fehler, die durch die statische Analyse erkannt werden, sind z.B. Buffer Overflows, Null-Pointer Dereferenzierungen oder einfach Verstöße gegen Programmierrichtlinien. Die statische Code-Analyse schließt damit eine Lücke des herkömmlichen Testings. Damit im Testing ein Programmierfehler erkannt werden kann, müssen drei Bedingungen gleichzeitig erfüllt sein:

1. Der Testfall muss den fehlerhaften Code durchlaufen,
2. der Fehler muss zu einer Error Condition führen und
3. die Error Condition muss zu einer Abweichung des Ergebnisses von dem erwarteten Ergebnis führen.

Zudem muss ein lauffähiger Code vorhanden sein, das Testing kann also erst in einer recht späten Phase des Entwicklungsprozesses greifen. Hier gilt: Je später ein Problem im Code entdeckt wird, desto aufwändiger und teurer wird die Beseitigung.

Fazit

Die IIoT-Referenzarchitektur des IIC ist ein wichtiger Schritt hin zu einem universellen, sicheren und vertrauenswürdigen Industrial Internet of Things. Es gilt vor allem, dieses IIoT so auf- und umzusetzen, dass die Integrität von Daten und Software jederzeit gewährleistet ist. Der Sicherheitsgedanke muss bereits bei der Entwicklung der Systeme eine hohe Priorität genießen. Denn die nachträgliche Absicherung der Struktur, wie es bei der herkömmlichen IT in Form von Firewalls, Malware-Scanner, IDS/IPS und dergleichen mehr üblich ist, kann zwar Fehler in der Software kaschieren. Doch bieten auch sie keinen absoluten Schutz, was die IT tagtäglich schmerzhaft erfahren muss. Software, die nach hohen Standards entwickelt, überprüft und getestet wird, macht Angreifern das Leben schwer. Und ermöglicht eine vertrauensvolle Kommunikation im IIoT. ■



Die von Compilern bekannte Intermediate Representation dient Analyse-Tools wie CodeSonar von GrammaTech als Modell zur Untersuchung.

www.grammatec.com

DIE NEUE ROLLE DES RTOS IN EMBEDDED SYSTEMS

Die Welt der eingebetteten Systeme durchläuft eine bedeutende Entwicklung, die sich auf die Rolle des Echtzeitbetriebssystems und den Entwurf von Anwendungen auswirkt, die auf Determinismus, höchste Zuverlässigkeit und Leistung angewiesen sind. Gleichzeitig haben sich die grundlegenden Anforderungen an ein RTOS nicht geändert.

AUTOR: Michel Genard, Vice President Products, Wind River GmbH BILD: Wind River GmbH

Eingebettete Systeme und die auf ihnen laufenden Echtzeitbetriebssysteme sind in der Regel für Prozesse und Maschinen von entscheidender Bedeutung. Das kann etwas so Alltägliches wie ein Aufzug oder so exotisch wie ein Mars Rover sein. In vielen Fällen stellt die einwandfreie Funktion des RTOS den Schutz von Menschenleben und der Umwelt sicher. Es gibt vier nicht verhandelbare Säulen, die ein RTOS leisten muss:

› **SICHERHEIT:** Ein RTOS muss sicher sein und Gegenmaßnahmen zur Cybersicherheit unterstützen.

› **SAFETY:** Ein RTOS und sein Determinismus bieten die Vorhersehbarkeit und Zuverlässigkeit der Leistung, um negative Auswirkungen auf seine Umgebung zu verhindern.

› **ZUVERLÄSSIGKEIT:** Ein RTOS muss immer die erwar-

Bild: ©popba/gettyimages.com

tete Leistung erbringen und auf deterministische Weise dasselbe Ergebnis erzielen.

› **ZERTIFIZIERBARKEIT:** Eingebettete Systeme müssen häufig vor ihrem Einsatz von Fachgruppen oder Regierungsbehörden zertifiziert werden, z.B. die DO-178C der FAA für die Avionik, die IEC61508 SIL 3 für industrielle Systeme, ISO26262 ASLID für Automobilanwendungen und IEC62304 für die medizinische Sicherheit.

Neue Methoden

Die Welt der eingebetteten Systeme verändert sich schnell. Das Innovationstempo gewinnt durch den technologischen Fortschritt und den verstärkten Wettbewerb an Dynamik. Niedrigere Technologiekosten und Veränderungen in den Geschäftsmodellen beschleunigen diese Entwicklung noch weiter, da die Systeme der Informationstechnologie (IT) und der Betriebstechnik (OT) zusammenwachsen. Infolgedessen gehen die Entwickler von Software für eingebettete Systeme auf der Suche nach mehr Effizienz, Produktivität und Portabilität zu modernen Methoden über. Sowohl die Hardware- als auch die Software-Entwicklung schreitet schneller als je zuvor voran. Neue Software-Ingenieure kommen in den Embedded Bereich mit einem hohen Komfortniveau mit Abstraktion und konzentrieren sich lieber auf die Anwendung als auf die zugrunde liegende Infrastruktur. Daher wollen sie eingebettete Systeme mit IT-ähnlichen Methoden, Programmiersprachen und Frameworks erstellen. Gleichzeitig nutzen die Ingenieure kostengünstige Hardware wie Raspberry Pi, um kostengünstige Prototypen zu bauen und schnell vom Konzept zum funktionierenden Gerät zu gelangen.

Neue Hardware und Virtualisierung

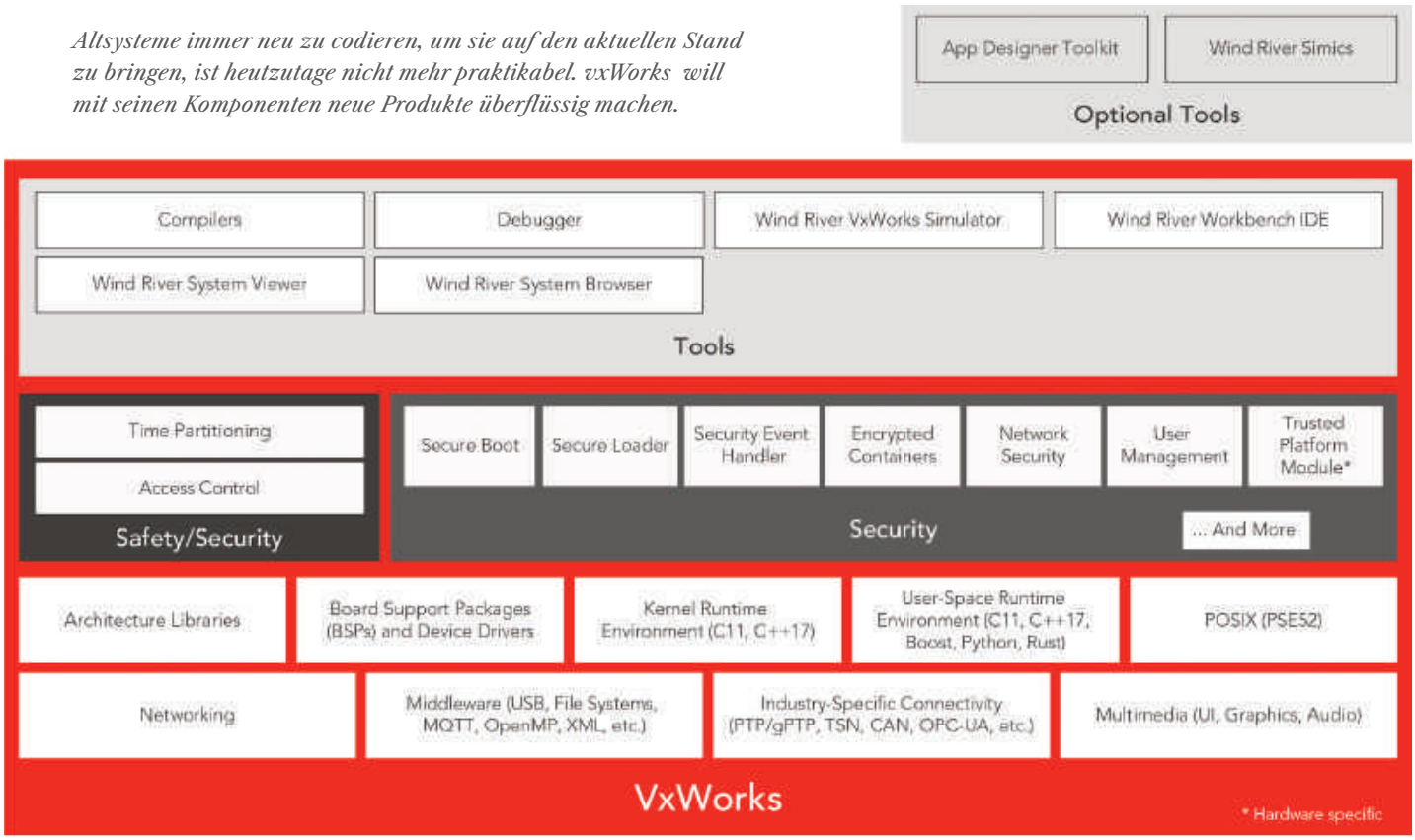
Die rasante Entwicklung von Multi-Core-basierten Hardware-Plattformen ermöglicht die Konsolidierung von Systemen und Anwendungen. Mit 2 bis 64 CPUs auf einem einzigen Chip lassen sich beispielsweise Kosten, Größe und Gewicht des Endprodukts reduzieren.

Erweiterte RFID-Lösungen in Kooperation

Denso Wave mit Sitz in Japan und RFKeeper, ein in Israel ansässiger Hersteller von RFID-Software, sind eine Kooperation eingegangen, um ihre Lösungen für den Retailbereich mithilfe von RFID-Technologie zu erweitern. „Durch unsere Partnerschaft können wir Unternehmen im Bereich Einzelhandel sowie auch entlang der Lieferkette weltweit RFID-Lösungen anbieten", erklärt Haim Bar-On, CEO bei RFKeeper. Das israelische Unternehmen hat eine IoT-Lösung entwickelt, mit der Nutzer Waren in Echtzeit steuern können, indem sie Filialen und Online-Shops miteinander verknüpfen. „Unser Ziel ist es, mit der Kombination von Densos und unseren RFID-Lösungen die Effizienz und den Komfort der Prozesse zu optimieren", fasst Bar-On zusammen.

www.denso-wave.eu

Altsysteme immer neu zu codieren, um sie auf den aktuellen Stand zu bringen, ist heutzutage nicht mehr praktikabel. vxWorks will mit seinen Komponenten neue Produkte überflüssig machen.



Virtualisierung wird bei eingebetteten Systemen immer häufiger eingesetzt. Mehrere eingebettete Systeme können jetzt in virtualisierter Form auf einem Hypervisor auf einer einzigen Hardware ausgeführt werden.

Legacy-Systeme

Diese Kombination aus erhöhter Leistung, mehr Konnektivität, schnelleren Designzyklen und schnellerer Innovation bei den Komponenten macht selbst relativ neue Produkte überflüssig. Dies wirft die Frage auf, was man mit Altsystemen machen kann. Es ist finanziell nicht tragbar, Embedded-System-Anwendungen immer wieder neu zu codieren, da sich die Plattformen schnell weiterentwickeln und die Systemanforderungen ändern. Die Systemhersteller wollen natürlich den vorhandenen Code so weit wie möglich wiederverwenden. Diese Legacy-Systeme funktionieren zwar noch, müssen aber mit neuen Funktionen modernisiert werden. Und die erheblichen Investitionen, die für Zertifizierung von Software getätigt wurden, sollen erhalten bleiben, wenn Code auf neue Hardwaresysteme migriert wird.

Druck auf das RTOS

Veränderte Erwartungshaltungen gegenüber eingebetteten Systemen gehen kaskadenförmig bis hinunter zu den Betriebssystemen, die sie antreiben. Heutige RTOS müssen mit der Innovation Schritt halten und moderne Entwicklungspraktiken übernehmen. Sie müssen in der Lage sein, mit neuen, komplexeren Prozessoren zu arbeiten. Ihr Design sollte die neuen, schnelleren Entwicklungszyklen in der Industrie ermöglichen. Dies bedeutet, dass sie mit den Frameworks, Sprachen und Methoden kompatibel sein müssen, die von der neuen Generation von Entwicklern eingebetteter Systeme eingesetzt werden. Heutige RTOS müssen mit Virtualisierung arbeiten und trotzdem alle diese neuen Kriterien erfüllen, ohne dass dabei Kompromisse bei Safety, Security, Leistung und Zuverlässigkeit eingegangen werden müssen. ■

www.windriver.com

VxWorks führend

Der aktuelle Generationswechsel im Bereich der Embedded-Systeme und des RTOS ist nur der letzte in der erfolgreichen Karriere von VxWorks. VxWorks gehört seit mehr als 30 Jahren zu den führenden RTOS in den Bereichen Luft- und Raumfahrt & Verteidigung, Automotive, Industrie, Medizin und anderen kritischen Infrastrukturbereichen. Es ist das Betriebssystem hinter neun verschiedenen Marsmissionen, darunter der Mars Reconnaissance Orbiter sowie die Mars Exploration Rover Spirit und Opportunity. Es wird auch in Milliarden anderer kritischer Geräte eingesetzt, die sich auf der Erde befinden, von der Automobilindustrie bis hin zur Fertigung, ob es sich um ein deterministisches, ultra-zuverlässiges oder Multi-Core Embedded-System handelt.

Bild: ©metamorworks/Shutterstock.com

Sicherheit von Industrial Applikationen mit OWASP

Immer wieder hört man von umfangreichen Datensicherheits-Verletzungen bei Unternehmen jeglicher Größe. Die Häufigkeit und Schwere von Cybersecurity-Problemen nimmt kontinuierlich zu. Es stellt sich die Frage: Wer ist als nächstes betroffen und was kann man dagegen tun? Genau hier setzt OWASP an.

AUTOR: Arthur Hicken, Evangelist, Parasoft Deutschland GmbH
BILDER: Parasoft Deutschland GmbH

Die offene Community mit kostenlosen Informationen und Schulungen zum Thema Applikationssicherheit ist für seine OWASP Top 10 bekannt, eine Liste mit aktuellen gefährlichen Sicherheitsrisiken für Web-Applikationen. Wer in Sachen Applikationssicherheit bisher noch nicht viel unternommen oder sich auf Ad-hoc-Maßnahmen beschränkt hat, für den sind die OWASP Top 10 ein ausgezeichneter Ansatzpunkt.

OWASP hat ausreichende Dokumentation für die Top 10 vorgelegt und eine Website für jede Schwachstelle von A1 bis A10 eingerichtet. Diese erläutert, worum es sich bei jeder Schwachstelle handelt, und gibt einen Risikowert an, der bei der Priorisierung und Selektierung möglicher Schwachstellen hilft.

In den OWASP Top 10 findet sich eine Unmenge an kostenlos verfügbarer und laufend aktualisierten Informationen, Schulungsmaterial und Ratschlägen. Man erfährt etwas über gängige Sicherheitsprobleme

sowie über Strategien, um diese Probleme zu detektieren und teils komplett zu umgehen.

Konformität bedeutet auch, dass man genau wissen muss, welches spezielle Element des Toolkits welchen Teil des Standards unterstützt. Im Fall der statischen Analyse weiß man also, welche(r) Checker welche Elemente des Standards unterstützen, und ob es Elemente im Standard gibt, die mehr als die statische Analyse erfordern (z.B. Peer Code Review oder Software Composition Analysis).

Am Ende beginnen

Am einfachsten geht man an das Thema Security heran, indem man am Ende anfängt und externe, in einer späten Phase des Zyklus ansetzende und das gesamte System erfassende Tests einsetzt, wie etwa Penetration-Tests: Diese sind ideal für den Nachweis, dass die Applikation bzw. das System keine der vom OWASP aufgezählten Schwachstellen enthält. Allerdings ist dieses Testen nach dem Blackbox-Prinzip keineswegs die effizienteste Methode zum Produzieren eines Codes, der sicherer ist. Besser ist es also, sich nicht auf Blackbox-Tests zu verlassen, um die Software abzusichern, Bugs aufzudecken oder den Nachweis zu erbringen, dass die Software sicher ist.

Findet man mit Penetration-Tests eine Sicherheitslücke, sollte man sich fragen, warum das so ist, um anschließend der Ursache des Problems auf den Grund zu gehen. Anstatt durch Testen für Sicherheit zu sorgen, sollten Sicherheitskomponenten beim Design gleich mit eingebaut werden.

Hierfür gibt es SAST-Tools mit Support für OWASP, wie zum Beispiel die statische Codeanalyse.

Aber ist SAST nicht ein Ärgernis?

Die Eleganz der statischen Analyse liegt darin, dass man in einer sehr frühen Phase des Zyklus mit der Überprüfung auf Sicherheitsprobleme beginnen kann, etwa durch eine zeitliche Vorverlegung der Sicherheitstests. Befasst man sich mit dem Thema Security erst spät oder ganz am Ende der Entwicklung (DevOpsSec), lässt sich die statische Analyse dafür nutzen, das Thema Security früher zu behandeln, noch bevor die Tests beginnen und während der Code gerade erst geschrieben wird (DevSecOps).

Nachteilig an der statischen Analyse ist ihr Ruf, sehr viel ‚Noise' zu produzieren, beispielsweise Hunderte oder gar Tausende Regelverletzungen, obwohl man gerade dachte, man wäre fertig für die Freigabe. Zum Glück gibt es einige gute Strategien, um hiermit umzugehen:

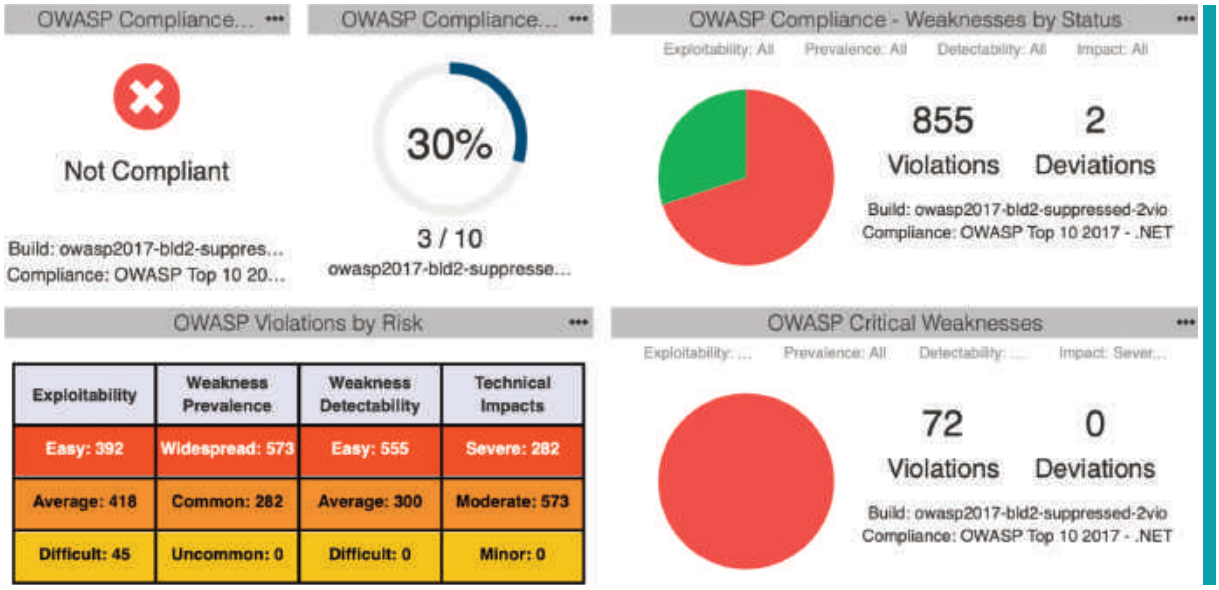
1. Sicherheitstests nicht bis zum Schluss aufsparen. Es empfiehlt sich, mit den statischen Analysen zu starten sobald man mit dem Coding anfängt. Wartet man dagegen ab und führt die statischen Analysen nur im Rahmen der CI/CD-Pipeline aus, so summieren sich zu viele Meldungen und überfordern das Entwicklungsteam. Man sollte also die Analyse am Desktop laufen lassen, um Probleme zu finden, und sie im CI/CD-Kontext ausführen, um einfach zu verifizieren, dass der Code korrekt erstellt wurde.
2. Feinabstimmung an der Konfiguration. Einige statische Analyse-Checker sind im Kontext des Codes vielleicht gar nicht erforderlich. Man sollte die Applikation prüfen und entscheiden, welche Sicherheitsrisiken relevant sind. Es macht Sinn, sich nur mit diesen zu befassen und niemals Ausschau nach Problemen zu halten, deren Beseitigung ohnehin nicht geplant ist.
3. Das Alter des Codes. Der mittlerweile uralte Grundsatz 'If it ain't broken, don't fix it' sollte auch auf Bestandscode angewandt werden. Das heißt: Ältere Codes nur mit den wichtigsten Security-Scannern prüfen. Kleinere Probleme bedeuten nur Zeitverschwendung, und die damit einhergehenden Änderungen bergen ihrerseits Risiken. Ein Code, den man nicht zu reparieren beabsichtigt, sollte auch nicht geprüft werden.

Es geht um die Risiken. SAST-Tools decken sowohl reale als auch potenzielle Schwachstellen auf, allerdings ist nicht mit allen Resultaten das gleiche potenzielle Risiko verbunden. OWASP hat hier geholfen, indem für jeden Eintrag in der Top-10-Liste das Risiko im Hinblick darauf definiert wurde, wie einfach sich eine Schwachstelle ausnutzen lässt, wie leicht die Schwachstelle zu entdecken ist und welche tatsächlichen Folgewirkungen ein Exploit haben kann.

Vermeidung ist wirkungsvoll

Möchte man seine Applikation wirklich abhärten, kommt hier ein wichtiger Hinweis: Auf Sicherheit zu testen, ist wesentlich einfacher als Sicherheit

Mit dem übersichtlichen OWASP Dashboard können Entwickler und Manager das Projekt und dessen Fortschritt kontinuierlich begleiten und einsehen.



Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
Application Specific	Easy: 3	Widespread: 3	Easy: 3	Severe: 3	Business Specific
	Average: 2	Common: 2	Average: 2	Moderate: 2	
	Difficult: 1	Uncommon: 1	Difficult: 1	Minor: 1	

SAST-Tools liefern hilfreiche Angaben, um SAST-Resultate zu priorisieren und zu selektieren.

mit einzubauen. Zum Glück werden statische Analyse-Checker in den verschiedensten Varianten angeboten. Einige halten Ausschau nach typischen Problemen wie etwa 'tainted data' und versuchen herauszufinden, ob die Applikation einen Ablauf enthält, bei dem dieses Problem vorkommen kann. Dies sind die gängigsten Checker vieler SAST-Tools. Der größere Nutzen von statischen Codeanalysen liegt jedoch in Checkern, die zwei ganz besondere Dinge durchsetzen:

① Ein Muster, mit dem es in der Vergangenheit wiederholt Probleme gab. Dies mag zwar nicht so interessant aussehen wie ein bestimmter, zu einem Exploit hinführender Stack-Trace. Aber es kann wesentlich gründlicher sein, einfach alles zu reparieren, das schwächer ist als es sein sollte, anstatt sich bei der Reparatur auf solche Probleme zu beschränken, für die es einen erwiesenen Angriffsvektor gibt.

② Anforderungen bestimmter Codierungsweisen, um eine einwandfreie Funktion zu gewährleisten. Automobil- und Luftfahrt-Normen wie MISRA oder JSF bedienen sich dieser Technik, um die funktionale Sicherheit zu gewährleisten. Die gleiche Technik, nicht nur einen schlechten Code zu melden, sondern einen guten Code zu verlangen, ist beim Erstellen sichererer Applikationen hilfreich.

Hat man sich nie mit dem Thema Security auseinandergesetzt, wird die Umsetzung der OWASP Top 10 nicht einfach, aber möglich ist sie. DAST ist eine einfache Möglichkeit, mit den Top 10 anzufangen, und SAST hilft anschließend bei der zeitlichen Vorverlegung der Security-Tests. Richtig implementiert, kann SAST sogar Probleme vermeiden und nicht nur detektieren. Es ist also sinnvoll nach Tools Ausschau zu halten, die den Standard mit Detektierung und präventiven Checkern vollständig abdecken. Es lohnt sich, die richtige Nutzung der OWASP-Risikobewertung zu lernen, denn sie liefert wertvolle Hilfestellung bei der Priorisierung der Ergebnisse und um sicherzustellen, dass die Tools diese Risikoinformationen zusammen mit den Resultaten ausgeben. Dies hilft, um sich auf das Wesentliche zu konzentrieren, und ist entscheidend für eine erfolgreiche OWASP-Implementierung. Mit diesen Tipps sollte man in der Lage sein, sofort mit der Beseitigung der verbreitetsten und gefährlichsten Sicherheitsrisiken für Web-/Industrial-Applikationen zu beginnen. ■

www.parasoft.com

Qualitätsoffensive auf dem Weg zum Hersteller

Das Mess- und Prüflabor wurde unter ESD-Schutzmaßnahmen eingerichtet.

Hy-Line Computer Components hat im Rahmen seiner Qualitätsoffensive, hin zum Hersteller, einen wichtigen Schritt gemacht und einen gesonderten Raum unter ESD-Schutzmaßnahmen in das neue Mess- und Prüflabor eingerichtet. Durch ein DMS1000 Digitalmikroskop ist es mit 300-facher Vergrößerung möglich auch kleinste Bauteile, Leiterbahnen, Einschlüsse und optische Merkmale zu betrachten. Gleichzeitig ist eine kontaktlose Bemaßung im µm-Bereich, Tiefenschärfenbetrachtung und Bilddokumentation möglich. Durch den Einsatz gesonderter Polfilter, anpassbarer Beleuchtung und wechselbarer Objektive sind auch optisch anspruchsvolle Auffälligkeiten dokumentierbar. Gerade die Überprüfung von Glas und Sensorprodukten unterliegt starken äußeren Einflüssen, die Test- und Messergebnisse beeinträchtigen können.

www.hy-line.de

Die Softwareentwicklerkonferenz zu IoT und Industrie 4.0

Das Internet der Dinge ist vom Hype in der Realität angekommen. IoT-Projekte bringen zahlreiche Herausforderungen mit sich. Die Building IoT ist die Fachkonferenz für IT-Profis, die Anwendungen und Produkte im Internet der Dinge entwickeln. Teilnehmer erhalten einen aktuellen Überblick über die wesentlichen Aspekte der IoT-Entwicklung und das stetig wachsende technische Ökosystem mit seinen Chancen und Risiken. Schließlich bietet die Building IoT die Möglichkeit, sich mit Entwicklern auszutauschen, die sich mit denselben Themen wie die Teilnehmer beschäftigen. Die Konfernz richtet sich an IT-Fachleute, die in ihren Unternehmen mit der technischen Umsetzung von IoT-Produkten und -Projekten befasst sind – unabhängig von einer speziellen Branche. Sie stehen vor der Aufgabe, bestehende IT-Systeme mit Konzepten des IoT zu erweitern oder völlig neue Produkte und Systeme für das Internet der Dinge zu entwickeln. Die Konferenz behandelt in Grundlagenbeiträgen unterschiedliche Teilbereiche wie die Auswahl passender Hardware, Protokolle und Cloud-Plattformen. Tiefgreifende Vorträge sorgen dafür, dass auch Experten auf ihre Kosten kommen. Projektberichte aus verschiedenen Industriezweigen veranschaulichen die mit IoT-Systemen gemachten Erfahrungen und helfen dabei, Potenziale aufzudecken. Die zentralen Schlagwörter der Konferenz werden dabei auch auf ihre Praxistauglichkeit hin untersucht.

www.buildingiot.de

Bosch Connected-World 2020

Bild: ©rcfotostock/stock.adobe.com

Bosch ConnectedWorld 2020 ist Treffpunkt für Experten, die vernetzte Produkte und Lösungen schaffen, die für das Leben erfunden wurden. Die Konferenz über IoT und digitale Transformation findet vom 19. bis 20. Februar in Berlin statt. Sie richtet sich an Führungskräfte, Entscheidungsträger, digitale Transformatoren, Innovatoren, Entwickler, Unternehmer und IoT-Enthusiasten aus verschiedenen Branchen weltweit. Teilnehmer können ihre eigene, auf ihre Bedürfnisse zugeschnittene Agenda erstellen, indem sie zwischen Keynotes und Breakout-Sitzungen wählen, die ihnen helfen, das IoT und die damit verbundene Welt bis in den Kern zu verstehen. Auf 10.000m² Fläche und mit mehr als 150 Präsentation und zusätzlich zwölf Keynotes können Teilnehmer die neueste IoT-Software und -Hardware, Anwendungsfälle und wertvolle Best Practices kennen lernen.

www.bosch-connected-world.com

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, Christina Jilg, Susan Jünger, Lena Krieger, Kristine Meier, Melanie Novak, 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 2020

GRAFIK & SATZ
Julia Marie Dietrich, Tobias Götze, Fabienne Heßler, Kathrin Hoß, Ronja Kaledat, Patrick Kraicker, Ann-Christin Lölkes, Cara Richter, Nadin Rühl

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

ERSCHEINUNGSWEISE
4 Hefte für das Jahr 2020

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

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

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

EINZELBEZUG:
Einzelheft: €7,80 (inkl. MwSt.)

ISSN 1869-8832
Vertriebskennzeichen (ZKZ) 18427

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

DIE APP FÜR DAS INTERNET OF THINGS

Alle IoT-News zu Embedded Systems und Cloud & Co. sofort erfahren!

JETZT KOSTENLOS DOWNLOADEN!

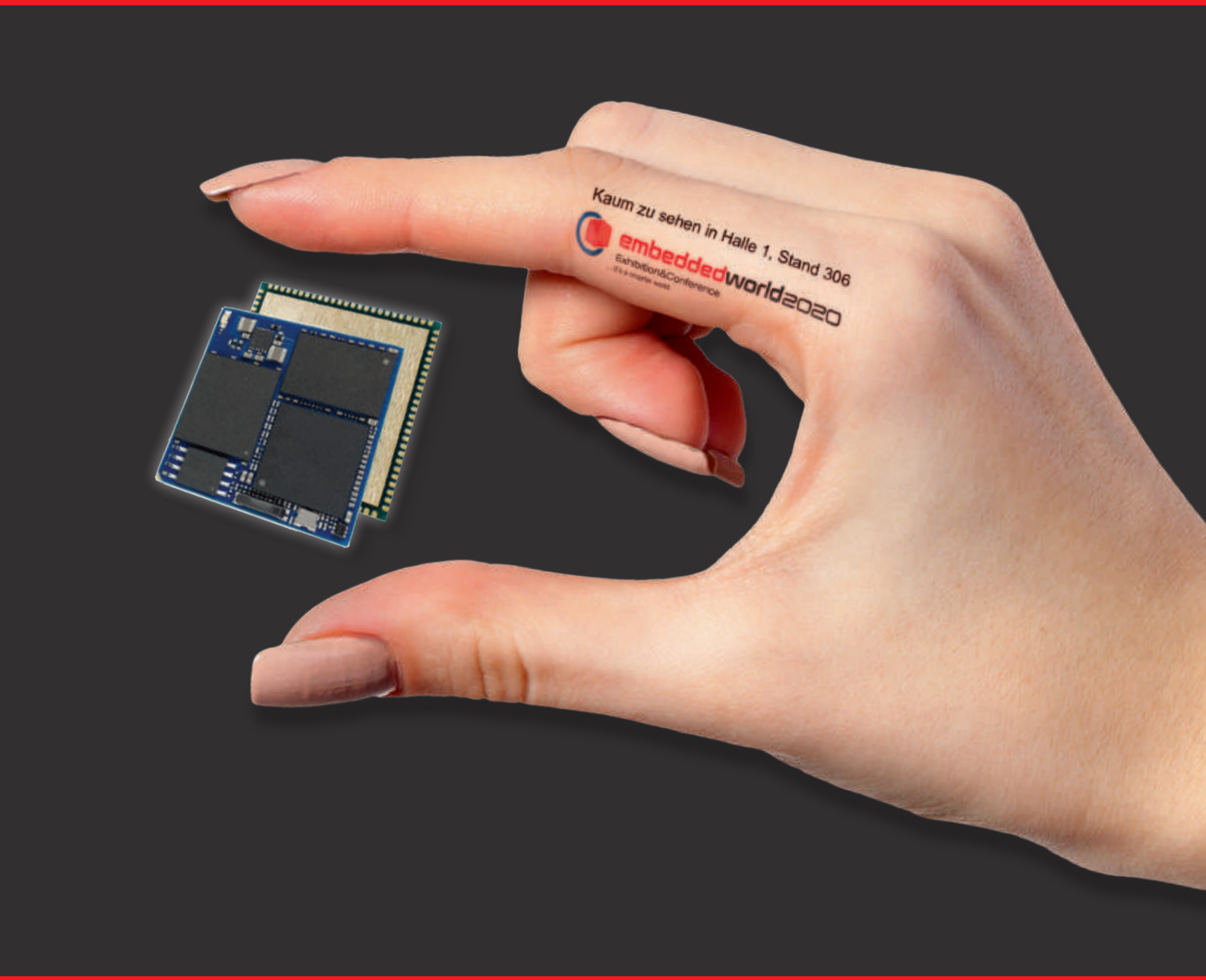
Laden im App Store

JETZT BEI Google Play

NEWS ARENA

powered by: IoT DESIGN

Quadcore Power auf 27 x 27 mm



Einfach auf die Platine löten!

Mit der neuen CoM QS-Familie von Ka-Ro geht die Integration auf der Platine kinderleicht – **Dank Single-Sided Design!**

Extreme Rugged approved!
Die Lötmodule setzen auf leistungsstarke **Prozessoren von NXP (i.MX8) und ST (STM32MP1).**

Pin-Kompatibel bei skalierbarer Rechenleistung, riesiger Speicher bis zu 1GByte DRAM und **4 GByte eMMC.**

Setzen Sie auf **Zuverlässigkeit mit dem ROTEN SUPPORT.** Fordern Sie jetzt Ihr Infopaket an!

FIRST CLASS PREMIUM SUPPORT

GLYN
High-Tech Distribution

www.glyn.de/dss | dss@glyn.de