04 **23. Februar 2021** 8,00 €

Organ der GMM VDE/VDI-GESELLSCHAFT MIKROELEKTRONIK, MIKROSYSTEM- UND FEINWERKTECHNIK

Elektronik

EMBEDDED SYSTEM TECHNOLOGY

SECURE ELEMENTS FÜR IOT-ANWENDUNGEN

SICHERHEIT EINFACH HANDHABEN

MICROCHIP

NEU

Jetzt 28 Seiten Elektronik automotive als Heft im Heft!

Qseven, SMARC oder COM? Entscheidungshilfen in Sachen Computermodul

Model-based System Engineering – von der Idee bis zum virtuellen Produkt

EMBEDDED WORLD – UND NIEMAND DARF HINFAHREN

Nächste Woche, am 1. März, öffnet die embedded world ihre Pforten. Dieses Jahr sind mit Pforten nicht die Tore an den Messehallen gemeint, eher die Ports an den Servern, auf denen die Messe als Softwarecode ausgeführt wird. Ab dem 1. März steht die embedded world als virtuelle Messe per Internetzugang Besuchern aus aller Welt offen – sogar für fünf Tage.

Parallel zur Messe finden auch in diesem Jahr die embedded world Conference und die electronic displays Conference statt. Beide Konferenzen haben ein auf ebenfalls fünf Tage, vom 1. bis zum 5. März, erweitertes Programm. Statt im Konferenzzentrum der Messe Nürnberg können sich die Teilnehmer und Sprecher beider Konferenzen in diesem Jahr nur am Computerbildschirm treffen und per Chat sowie per Bild- und Tonübertragung kommunizieren. Nach fast einem Jahr Pandemie-Erfahrung dürfte dieses Prozedere inzwischen geübte Praxis sein – nicht nur im beruflichen Alltag.

Ganz gleich ob im Homeoffice, per „mobiles Arbeiten" oder im echten Büro am Schreibtisch, Konferenzen und Messen am Computerbildschirm zu verfolgen, das erfordert Zeitmanagement, Disziplin und auch konsequentes Handeln. Anders als bei einer realen Konferenz, bei der Sprecher und Teilnehmer anreisen müssen und allein schon durch ihre Abwesenheit den Arbeitsalltag hinter sich lassen, verleiten virtuelle Messen und per Internet übertragene Konferenzen zu Multitasking. Der Messebesuch und die Teilnahme an einer Konferenz werden meist in den Arbeitsalltag eingebettet und finden parallel zu anderen Tätigkeiten statt. Ein kompletter Messe- oder Konferenztag wie früher ist eher die Ausnahme.

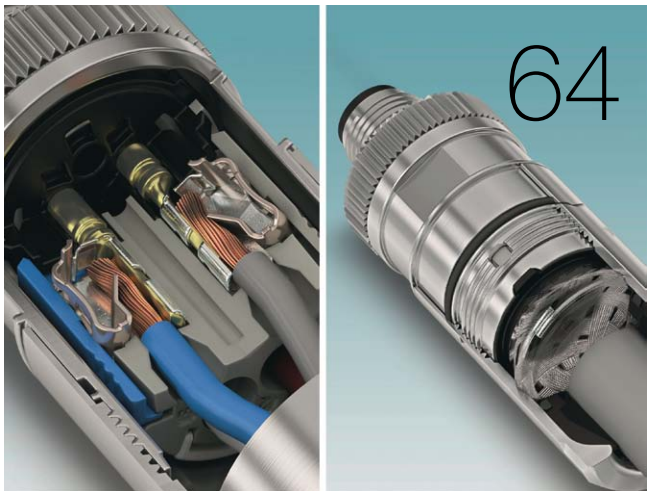
Deshalb starten beide Konferenzen später als sonst üblich, und die Vorträge werden aufgezeichnet, um sie zeitversetzt verfolgen zu können. So lassen sich auch Vorträge ansehen, die man bei einer normalen Konferenz verpassen würde, da sie parallel zu dem Vortrag laufen, für dessen Teilnahme man sich letztendlich entschlossen hat. Die Konferenzvideothek erleichtert es auch Teilnehmern aus anderen Zeitzonen. Sie können sich Vortragsvideos in ihrer Zeitzone zu den für sie üblichen Arbeitszeiten ansehen.

Allein das Programm der embedded world Conference mit seinen 234 Vorträgen läuft in bis zu sechs parallelen Sessions. Zuzüglich der 19 Classes und der electronic displays Conference, die in ihrem Programm keine parallelen Vorträge vorsieht, wird an den ersten fünf Märztagen Know-how über bis zu elf Kanäle live in alle per Internet erreichbaren Regionen der Welt übertragen.

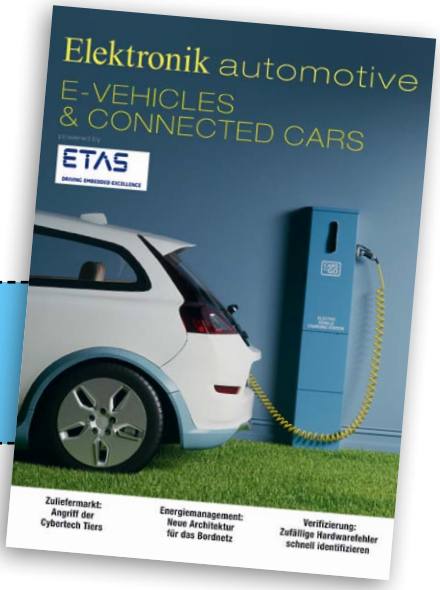
Das Internet und die digitale Übertragung und Speicherung der Audio- und Videosignale bietet Konferenzteilnehmern mehr Möglichkeiten als eine klassische Konferenz mit persönlicher Anwesenheit. Und doch wird jedem Stammgast der embedded world dieses Jahr etwas fehlen – mir auch.

HARRY SCHUBERT

Redakteur
hschubert@weka-fachmedien.de



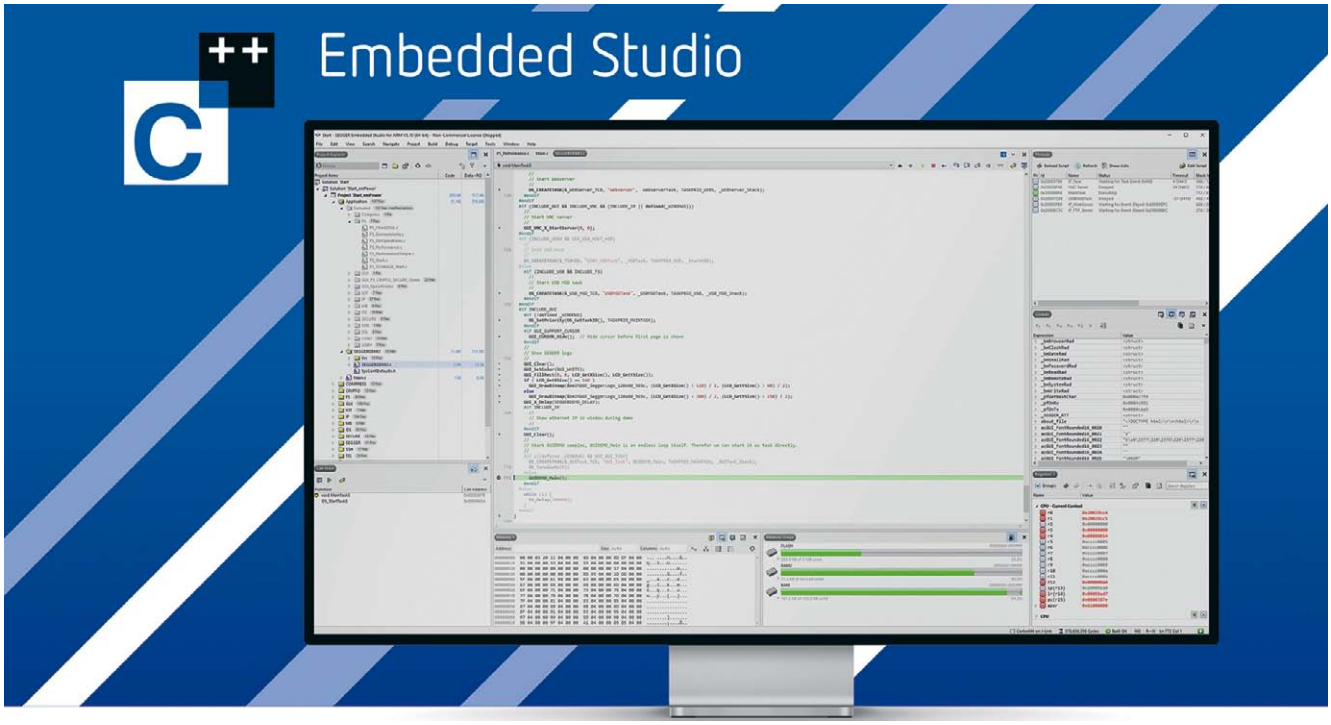
VORSCHAU



Ab Seite 27
Elektronik
automotive
als Heft im Heft!

ERGEBNISSE IN DER ZUSAMMENFASSUNG

„EMBEDDED STUDIO“ VON SEGGER MIT TOPBEWERTUNG



(Bild: Segger)

Zehn *Elektronik*-Leser haben die Entwicklungsumgebung „Embedded Studio“ von Segger einem umfangreichen Praxistest mit mehreren Experimenten unterzogen. Hier sind die Testergebnisse im Detail.

Von Gerhard Stelzer

In der *Elektronik*-Ausgabe 21-2020 haben wir Sie, liebe Leser, aufgefordert, sich bei uns als Tester für die Entwicklungsumgebung „Embedded Studio“ von Segger Microcontroller zu bewerben. Aus knapp einhundert Interessenten haben wir zehn Teilnehmer ermittelt. An jeden Tester wurde von der Redaktion ein Testbogen zur Bewertung und von Segger das Testobjekt – die „J-Link PLUS“-Debug-Hardware – versandt. Die Software selbst konnte jeder Tester direkt von der Homepage des Embedded-Spezialisten herunterladen. Jetzt liegen die Testergebnisse vor. Zunächst eine kurze Zusammenfassung der wichtigsten Eigenschaften des Testobjekts:

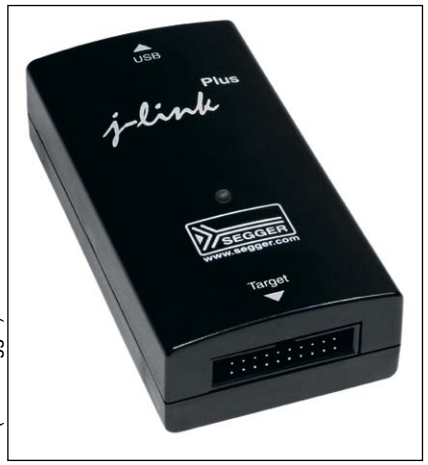
STECKBRIEF „EMBEDDED STUDIO“

Gegenstand dieser Testrunde ist die „Cross-Plattform IDE Embedded Studio“ von Segger. Mit Embedded Studio erhält der Entwickler eine Entwicklungsumgebung, die sich durch ihre Flexibilität im Einsatz und mit praxisgerecht optimiertem Code auszeichnet. Embedded Studio enthält die von Segger entwickelten eigenen Runtime- und Gleitkomma-Bibliotheken, Compiler und Linker. Primäres Entwicklungsziel bei Segger war dabei, einfach und problemlos auf das Zielsystem zugeschnittene, schnelle Programme mit geringstem

KOMPLEXES BUSINESS?
ES GEHT AUCH EINFACH.
YOUR SOURCING PLATFORM.

WILLKOMMEN BEI DER CONRAD SOURCING PLATFORM.
Die Plattform zur Beschaffung Ihres gesamten technischen Betriebsbedarfs. Noch einfacher mit unseren individuellen Einkaufsanbindungen – ob Webshop, eKatalog oder direkte eProcurement-Anbindung.
Mehr erfahren unter conrad.de/einfach

CONRAD | BESCHAFFUNG. EINFACH. SCHNELL. UMFASSEND.



(Bild: Segger)

Bild 1. Zur Durchführung des Tests des Embedded Studios stattete Segger alle Tester mit der „J-Link PLUS“-Debug-Hardware aus, die die Tester im Anschluss an den Test behalten durften.

Speicherbedarf entwickeln zu können. Daher wird Embedded Studio mit allen Komponenten auch für die Entwicklung der eigenen Produkte wie „J-Link“ Debug Probes, „J-Trace“ Trace Probes und der „Flasher“ Programmiergeräte eingesetzt. Das Zusammenspiel aus Entwicklung und interner Nutzung der eigenen Produkte ermöglicht es dem Tool-Hersteller aus eigener Erfahrung eine praxisnahe und zielgerichtete Weiterentwicklung zu betreiben.
In verschiedenen Phasen des „Build“-Prozesses werden Optimierungen vorgenommen, die der Reduzierung der Codegröße und der Verbesserung der Ausführungsgeschwindigkeit dienen. Der „Linker“ kann den in der Regel knappen Speicher von Mikrocontrollern optimal nutzen. Dabei können Codeblöcke über mehrere Speicherbereiche verteilt und nicht nutzbare Speicherstellen ausgelassen werden.
Embedded Studio unterstützt alle Funktionen, die J-Link und J-Trace auszeichnen, wie zum Beispiel unlimitierte „Breakpoints“ im Flash-Speicher oder RTT (Real Time Transfer). Auch Ozone, J-Link Debugger und Performance-Analysewerkzeug, sowie das Echtzeitanalyse- und Visualisierungswerkzeug SystemView lassen sich direkt aus einem Embedded-Studio-Projekt heraus ausführen. Genau wie SystemView und Ozone, funktioniert auch Seggers Embedded Studio, ganz im Sinne der Cross-Plattform-Philosophie, auf Windows, Linux sowie auf macOS. Für Ausbildungs- und nicht-kommerzielle Zwecke kann Embedded Studio lizenzkostenfrei und ohne Registrierung von der Segger Webseite heruntergeladen werden. Bei der Verwendung gibt es keine Einschränkungen in Hinblick auf Codegröße, Funktionsumfang oder Nutzungsdauer.
Im Praxistest wurde das Embedded Studio in drei Hauptkategorien nach Schulnoten von 1 bis 5 bewertet.

WAS WURDE GETESTET?

Der Praxistest gliederte sich in drei Teile:
➔ 1. Inbetriebnahme
➔ 2. Betrieb
➔ 3. Fazit
Die Tester konnten die Einzeldisziplinen des Testbogens mit Schulnoten von 1 bis 5 bewerten. Für Beurteilungen, die sich nicht in Noten ausdrücken lassen, gab es Kommentarfelder zur freien Beantwortung, die auch ausgiebig genutzt wurden.

1. INBETRIEBNAHME

Da es sich beim Testobjekt um eine Software handelt, haben wir die Testkriterien darauf angepasst. Die Inbetriebnahme umfasst die Aspekte Installation, Lizenzmanagement, Erstnutzung und Dokumentation.

1.1. INSTALLATION

- Download der Software 1,4
- Installation 1,4
- Umfang 1,3
- Verfügbarkeit für verschiedene Betriebssystem 1,0

➔ Ein Tester wünschte sich eine Installationsanleitung anstelle von „Release Notes“, ein anderer lobte den guten Einstieg im Vergleich zu Keil, Eclipse und Green Hills.

1.2. LIZENZMANAGEMENT

- Verständlichkeit der Lizenzbedingungen 1,4
- Benutzung mit „non-commercial“ Lizenz 1,2
- Lizenzmanagement 1,7

➔ Das Gros der Tester kam gut zurecht. Ein Tester meinte: „Die Non-Commercial-Lizenz halte ich für eine gute Idee, um z.B. Studenten oder privat engagierte Ingenieure an das Produkt zu binden. Meiner Meinung nach zahlt sich das aus.“

1.3. ERSTNUTZUNG

- Startzeit 1,1
- Erster Eindruck 1,4
- Einstieg in die Entwicklung 1,4

➔ Ein Tester lobt das Dashboard: Es sei sehr informativ, man sehe u.a. ob es Updates gibt und zuletzt verwendete Projekte. Mehrere Tester erwähnten den schnellen Start der Software. Lob gab es auch für die gute Übersichtlichkeit.

1.4. DOKUMENTATION

- Benutzerhandbuch 2,0
- Zusätzliche Dokumentation 1,7
- Support 1,3

➔ Das Benutzerhandbuch halten manche Tester für etwas unübersichtlich. Die integrierte Hilfefunktion dagegen kommt sehr gut an. Ein Tester: „Super Online-Handbuch.“
Insgesamt sind die Tester mit der Inbetriebnahme sehr zufrieden, was sich in einer Durchschnittsbenotung von 1,4 widerspiegelt.

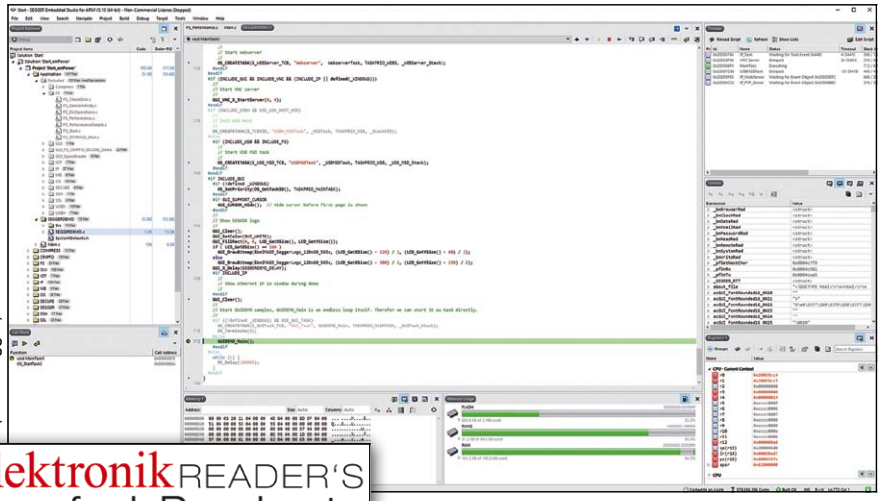
2. BETRIEB

Das umfangreichste Testfeld ist die praktische Arbeit mit der integrierten Entwicklungsumgebung (IDE) im täglichen Betrieb. Dabei wurden die drei Tätigkeitsfelder Projekt-Management, Applikationsanalyse und Debugging auf den Prüfstand gestellt.

2.1. PROJEKTMANAGEMENT

- Projekterstellung 1,3
- Erweiterung eines Projekts 1,8
- Konfiguration 1,8
- Eigentliche Entwicklung 1,8

➔ Ein Tester fand die Projektoptionen anfangs etwas undurchsichtig und gewöhnungsbedürftig. Ein anderer Tester lobt den sehr leichten Einstieg in ein komplexes Tool. Weitere Stimmen: Erweiterung per Drag-and-Drop wäre praktisch; Bessere Erklärung der unterschiedlichen Konfigurationsebenen wünschenswert.



(Bild: Segger)

Elektronik READER'S Proofed Products 2021 ★★★★½

Bild 2. Die Entwicklungsumgebung Embedded Studio von Segger wurde im Betrieb mit der Durchschnittsnote 1,5 bewertet und für ihre Übersichtlichkeit gelobt.

2.2. APPLIKATIONSANALYSE

- Speicherbedarf 1,4
- Analysemöglichkeiten 1,3
- Map File 1,6
- Linker 1,9
- Post-Build 1,7

→ Den Speicherbedarf schätzen mehrere Tester als sehr gering ein. Ein Tester wünscht sich eine strukturierte Aufbereitung des Map-Files, ein anderer einen direkten Export zu .pdf.

2.3. DEBUGGING

- Hardware-Set-up 1,3
- Downloadzeit 1,1
- Performance/Reaktionszeit 1,2
- Analysefenster 1,7
- Debug-Ausgaben 1,4
- Ausführungskontrolle 1,3

→ Ein Tester hob die sehr schnelle Ausführung hervor. Ein anderer lobte die Debug-Funktionen als intuitiv und übersichtlich. Ein weiterer Tester monierte eine etwas umständliche Bedienung der Analysefenster.
Das heißt, auch im Betrieb kann das Embedded Studio mit einer Durchschnittsnote von 1,5 durchaus überzeugen.

3. FAZIT

Zur abschließenden Beurteilung sollten die Tester einerseits verschiedene übergreifende Aspekte bewerten und auch ihre Gewichtung dieser Aspekte im Hinblick auf eine Kaufentscheidung für ein Produkt angeben. Bei den folgenden Benotungen wurde keine Gewichtung berücksichtigt.

- Preis-Leistungsverhältnis 1,8
- Lieferumfang/Dokumentation 1,8
- Praktischer Betrieb 1,3
- Gesamteindruck 1,6

→ Ein Tester kommentierte: „Insgesamt finde ich das Embedded Studio eine sehr gelungene und brauchbare Entwicklungsumgebung." Ein anderer: „Insgesamt ein gut strukturiertes Tool, mit dem der Einstieg erstaunlich leichtfällt." Ein weiterer Tester: „Der J-Link Debugger und das Embedded Studio sind tolle Werkzeuge für die professionelle Entwicklung von Embedded-Produkten. Das Kompilieren und Laden von Sourcecode auf das Target erfolgen extrem schnell, Debugging reagiert zuverlässig und schnell. Doku und Wiki/Videos könnten meiner Meinung nach etwas aufpoliert/aktualisiert werden." Als Gesamtnote des Fazits steht nun eine 1,6 im Zeugnis.

Bei den Gewichtungen fällt auf, dass es im Wesentlichen zwei Gruppen gab. Einer Gruppe ist das Preis-Leistungsverhältnis am wichtigsten, der anderen Gruppe Betrieb und Gesamteindruck. Hier gibt es also eine Aufteilung nach preisbewusst und premium. Interessanterweise zeigten sich am Ende aber beide Gruppen sehr zufrieden mit dem Embedded Studio von Segger. GS

66. INTERNATIONAL ELECTRON DEVICES MEETING

DIE HIGHLIGHTS DER HALBLEITERFORSCHUNG

TEIL 2

Die traditionsreiche Halbleiterkonferenz IEDM war wegen der Corona-Pandemie in den virtuellen Raum verlagert, was dem Feuerwerk an Highlights aber keinen Abbruch tat. Nach den Trends bei den CMOS-Technologien in Teil 1 folgt die Fortsetzung zu Speichern und Quanten-Computing. Von Gerhard Stelzer

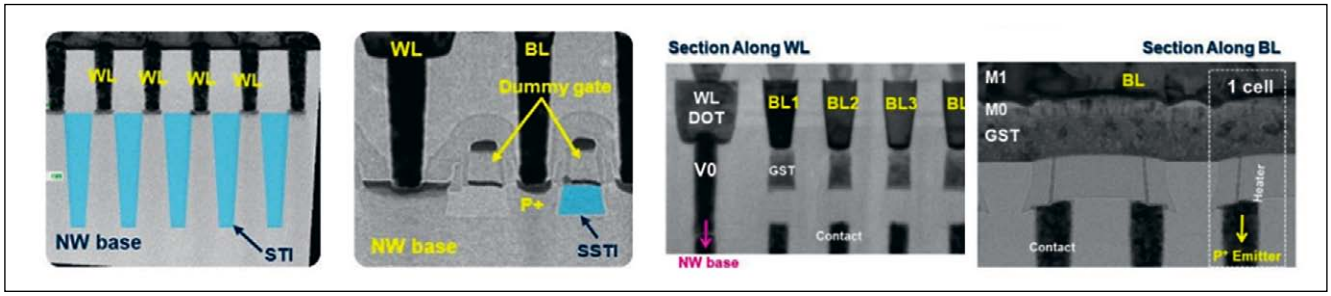
Drei Speichertechnologien schicken sich an, besonders anspruchsvolle Anwendungen zu revolutionieren.

Hochdichte 28-nm-FDSOI-Embedded-PCM-Speicher (Fully Depleted Silicon-on-Insulator) für den Automotive-Einsatz:

In heutigen Fahrzeugen werden zahlreiche Mikrocontroller zur Überwachung und Steuerung von Fahrerassistenzsystemen (ADAS), des Antriebsstrangs, von Infotainment- und Komfortsystemen sowie weiteren Funktionen eingesetzt. Diese SoCs (System on Chips) müssen eine hohe Leistung, eine geringe Stromaufnahme und ein hohes Maß an Zuverlässigkeit bieten. Da der Softwarecode, mit dem automobile Systeme betrieben werden, immer größer wird, wächst auch der Bedarf an mehr Codespeicher in hochdichten nichtflüchtigen Embedded-Speichern (eNVM). Auf der IEDM stellte ein Team von STMicroelectronics/CEA-Leti eine ultra-dichte (Zellgröße = 0,019 µm²) eingebettete Phase-Change-Memory-Technologie (PCM) für Automotive-SoCs vor, die den strengen AEC-Q100-Grade-0-Standard für Zuverlässigkeit im Automobilbereich erfüllt. Sie nutzt ein 28-nm-FDSOI-Substrat, eine neuartige SSTI-Isolierung (Super-Shallow Trench Isolation) für die Bit-Leitung (die kein Ätzen und Füllen des Grabens erfordert), Triple-Gate-Oxide-Transistoren für hohe Spannungen (5 V) und einen kompakten BJT-Selektor (Bipolar Junction Transistor) (Paper 24.2).

3D Embedded DRAM mit gestapelten antiferroelektrischen HZO-Kondensatoren:

Intel-Forscher stellten ihre Arbeit vor, bei der sie das antiferroelektrische (AFE) Material Hafnium-Zirkonium-Oxid (HfZrO2) verwenden, um einen 3D-Kondensator mit tiefem Graben für



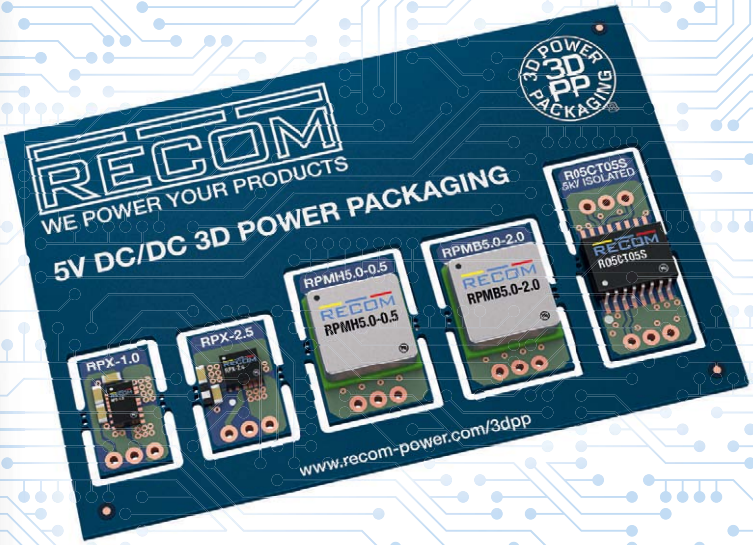
Auf der IEDM stellte ein STMicroelectronics/CEA-Leti-Team eine ultra-dichte eingebettete Phase-Change-Memory-Technologie für Automotive-SoCs vor, die den strengen AEC-Q100-Grade-0-Standard erfüllt. Sie nutzt ein 28-nm-FDSOI-Substrat. (Bild: IEDM | STMicroelectronics | CEA-Leti)

HÖHERE LEISTUNGSDICHTE DURCH 3D POWER PACKAGING®

RECOM

RPM, RPMB, RPMH
NICHT ISOLIERTE LGA POWER MODULE

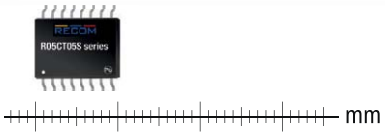
- 0.5A, 1A, 1.5A, 2A, 3A, & 6A Ausgangsstrom
- 4-65VDC Eingangsspannung
- Variable Ausgangsspannung bis zu 28VDC
- Wirkungsgrad bis zu 99%, ohne Kühlkörper
- 6-seitige Abschirmung für niedrige EMI
- Weiter Betriebstemperaturbereich (-40°C bis +107°C)
- Für batteriebetriebenes Equipment, Telecom, FPGA, oder POL Applikationen
- Vollständig geschützte Ausgänge (SCP, OCP, OTP, UVLO)
- Hergestellt in Europa



RPX
NICHT ISOLIERTE QFN POWER MODULE

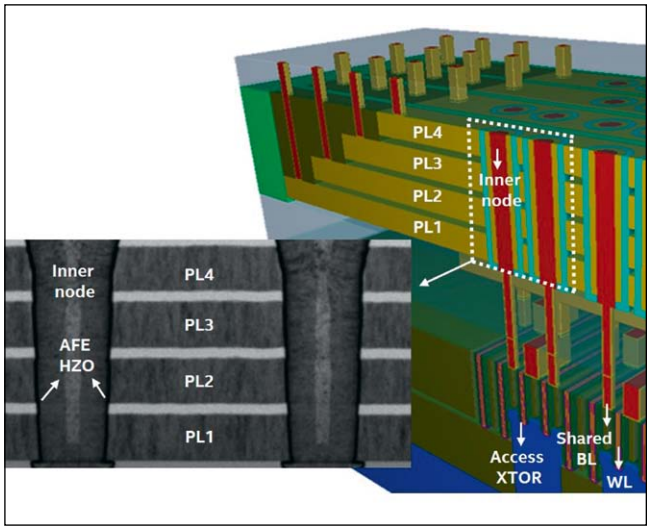
- 1A, 1.5A, & 2.5A Ausgangsstrom
- Eingangsspannung bis zu 36VDC
- Variable Ausgangsspannung bis zu 30VDC
- Übergossene Leadframe-Technologie für kostengünstiges, leistungsstarkes Design
- Integrierte FETs, Induktivitäten und Passive für einfaches Design
- Hervorragende Wärmeleistung für die härtesten Anwendungsanforderungen
- Vollständig geschützte Ausgänge (SCP, OCP, OTP, UVLO)
- Hohe Leistungsdichte

R05CT05S
ISOLIERTER SOIC-16 DC/DC WANDLER



- Sekundärregelung 0.5W
- Ultra-flaches Design (2.65mm)
- Ausgangsspannung 3.3 oder 5VDC
- Weiter Betriebstemperaturbereich (-40°C to 125°C)
- 5kVAC verstärkte Isolation
- Für die Peripherie medizinischer Geräte, COM-Port-Isolation, Transceiver-Isolation, Strommessung
- Entspricht CISPR32 Klasse B EMC Limits
- 62368-1 und 60601-1 mit 2MOPP zertifiziert
- Vollständig geschützte Ausgänge (SCP, OCP, OTP, UVLO)

Mehr Informationen zu RECOM 3D POWER PACKAGING®: Tel. +49 (0) 7231 801-1283 | axel.stangl@rutronik.com



3D Embedded DRAM mit gestapelten antiferroelektrischen HZO-Kondensatoren stellten Forscher von Intel vor. (Bild: IEDM | Intel)

den möglichen Einsatz in eingebetteten DRAM-Speichern herzustellen. Er zeigte eine Lebensdauer von zehn bis zwölf Zyklen selbst bei hohen Temperaturen und eine Betriebsspannung von 1,8 V. Die Forscher verwendeten diese AFE-Kondensatoren in einer neuartigen Speicherarchitektur für ultrahohe Bitdichten: ein vertikaler Stapel, der auf einem Zugriffstransistor mit mehreren parallel geschalteten AFE-Kondensatoren basiert. Jeder Kondensator repräsentiert ein einzelnes Speicherbit. Durch das vertikale Stapeln von vier AFE-Kondensatoren konnte eine signifikante Erhöhung der Dichte erreicht werden, ohne dass die Fläche vergrößert wurde (Paper 28.1)

Eine neue Kraft in ferroelektrischen Tunnel-Junction-Speichern:

Ferroelektrische Tunnelübergänge (FTJs) sind vielversprechende Kandidaten für nichtflüchtige Speicher (NVMs), wie z.B. für Ultra-Low-Power-Datenspeicher und neuromorphes Computing. Sie verfügen über eine ultradünne ferroelektrische Barriereschicht, die zwischen zwei Elektroden liegt. Die Modulation des Barrierewiderstands oder der „Höhe“ durch die Steuerung der Polarisation verhindert oder ermöglicht das Quantentunneln von Elektronen durch die Barriere und gewährleistet so die Speicherung oder den Abruf von Daten. Die Suche nach einem optimalen Barrierematerial war bisher jedoch eine Herausforderung. Auf der IEDM diskutierte ein Team unter der Leitung der University of Florida seine Arbeit, bei der es einen ferroelektrischen Tunnelübergang simulierte und baute, indem es dünne Schichten (ca. 4 nm) eines Van-der-Waals-Materials ($CuInP_2S_6$ – CIPS) auf einer Graphenschicht vertikal stapelte, um atomare Heteroübergänge an der CIPS-Graphen-Grenzfläche zu erzeugen.

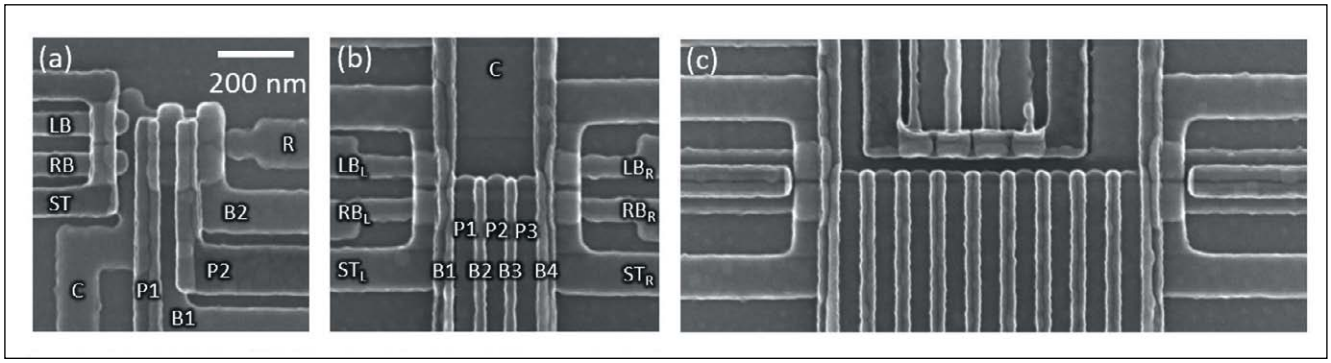
Die Heteroübergänge sind zwischen einem SiO_2-Substrat und einem Topmetall (Gold)-Kontakt eingebettet. (Van-der-Waals-Kräfte sind schwache Anziehungs-/Abstoßungskräfte zwischen Atomen, Molekülen und Oberflächen.) Simulationen der Leistung dieser Heteroübergänge, die durch Laborexperimente verifiziert wurden, zeigten ein rekordverdächtiges Tunnel-Elektrowiderstands-Verhältnis von $-6x10^7$, was den Weg zu einer möglichen neuen NVM-Speicherbausteinstruktur mit einem exponentiell höheren On/Off-Verhältnis als bei bestehenden Bausteinen und 1 ns Leselatenz aufzeigt (Paper 4.1).

QUANTEN-COMPUTING

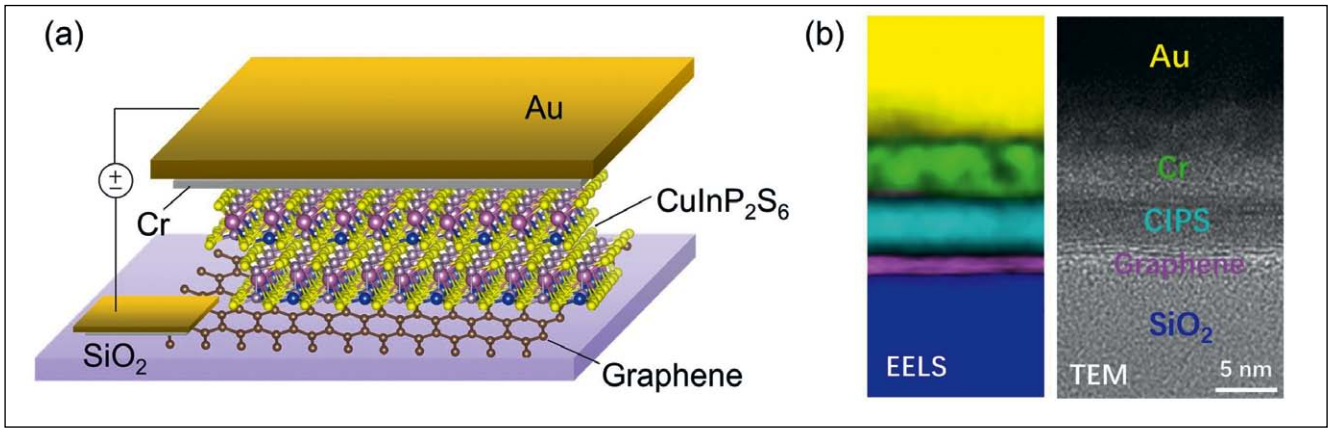
Quantencomputer nutzen die Prinzipien der Quantenmechanik, um Daten auf eine neuartige Weise zu verarbeiten. Während heutige Computer Bits aus den Ziffern 0 und 1 manipulieren, verarbeiten Quantencomputer Quantenbits (Qubits), die 0, 1 oder beides gleichzeitig darstellen, dank ihrer Fähigkeit, sich im Quantenzustand der „Superposition“ zu befinden. Ein Computer mit vielen Qubits könnte eine immense Anzahl von Berechnungen parallel ausführen, was zu einer unglaublich schnellen, energieeffizienten Leistung führt. Allerdings sind Qubits instabil, mit kurzen „Kohärenzzeiten“ (d.h. wie lange sie in einem Quantenzustand bleiben können). Es gibt bereits einige Quantencomputer, aber sie verwenden nur wenige Qubits, sind fehleranfällig und instabil und arbeiten bei kryogenen Temperaturen.

Qubits beginnen, vom Labor in die Fabrik zu kommen:

Qubits werden oft aus Quantenpunkten hergestellt, Partikel von wenigen Nanometern Größe, die aus Halbleitern bestehen. Quantenpunkt-Qubit-Systeme auf Siliziumbasis sind für den potenziellen Einsatz in großen Quantenprozessoren attraktiv, weil sie relativ lange Kohärenzzeiten und einen hochgradig zuverlässigen Betrieb in Laborumgebungen gezeigt haben, und weil die Siliziumtechnologie im Vergleich zu anderen Material-



Imec-Forscher stellten eine Plattform zur Untersuchung von Silizium-Qubits vor, die auf der industrieüblichen 300-mm-Silizium-Wafer-Fertigungstechnologie anstelle von speziellen Laborprozessen basiert. (Bild: IEDM | Imec)



(Bild: IEDM | University of Florida)

Ein Team der University of Florida simulierte und baute einen ferroelektrischen Tunnelübergang, indem es ca. 4 nm dicke Schichten eines Van-der-Waals-Materials ($CuInP_2S_6$ – CIPS) auf einer Graphenschicht vertikal stapelte, um atomare Heteroübergänge an der CIPS-Graphen-Grenzfläche zu erzeugen.

systemen weit verbreitet und kostengünstig ist. Aber die kryogenen Materialeigenschaften und andere Aspekte des Qubit-Designs sind immer noch nicht gut verstanden, und es wird eine Designplattform benötigt, die flexibel genug ist, um sie für Untersuchungen der Eigenschaften von Silizium-Qubits einzusetzen.

Imec-Forscher beschrieben eine erste derartige Plattform, die auf der industrieüblichen 300-mm-Silizium-Wafer-Fertigungstechnologie anstelle von speziellen Laborprozessen basiert. Sie nutzt sowohl optische als auch Elektronenstrahl-Lithographie zur Herstellung von Silizium-Spin-Qubits und ermöglicht spontane Layoutänderungen für Bauelemente mit ohmschen Implantationen vom n- oder p-Typ, Abständen <100 nm und einheitlichen kritischen Abmessungen bis hinunter zu 30 nm. Die Forscher sagen, dass sie mit der Designplattform eine nahezu hundertprozentige Ausbeute für Qubits mit 30 nm Abständen erreichen konnten. Sie planen, die Plattform zu nutzen, um weitere Materialien und Strukturen in Qubits einzubauen und die kryogenen Charakterisierungen zu verbessern. (Paper 38.3)

In weiteren Präsentationen ging es weiter mit den Themen Bildgebung, HF-Technik und Leistungselektronik bis hin zur Medizinelektronik. GS

NIEDRIGENERGIE-WEITVERKEHRSNETZE (LPWAN)

FUNKPROTOKOLL FÜR MASSIVE IOT

Zur Embedded World 2020 gründeten sechs Unternehmen und das Fraunhofer Institut für Integrierte Schaltungen (IIS) die Mioty Alliance, um das LPWAN-Protokoll Mioty bekannt zu machen. Nach einem Jahr lohnt sich ein Blick auf die Palette der verfügbaren Mioty-Produkte.

Von Harry Schubert

(Bild: Krunja | Shutterstock)

Das Funkprotokoll Mioty [1, 2] für Niedrigenergie-Weitverkehrsnetze kann zur zweiten Generation der LPWAN-Protokolle gezählt werden. Es wurde für Massive-IoT-Anwendungen entwickelt, d.h. für Netzwerke mit tausenden von Endgeräten, die Millionen von Nachrichten pro Tag transportieren müssen.

EINFACHER START MIT SYSTEMEN

Für den Einstieg in die Mioty-Netzwerkwelt bieten die Firmen Behr Tech, Radiocrafts, Swissphone und Texas Instruments Entwicklungskits an. Behr Tech und Swissphone liefern damit leistungsfähige Basisstationen (**Bild 1**) aus. So basiert die *MYTHINGS Base Station* von Behr Tech zum Beispiel auf dem Industrie-PC ARK-2250L von Advantek, in dem Intel-Prozessoren der Core-i3- oder Core-i5-Reihe verbaut sind. Auf ihm läuft die Mioty-Potokollsoftware *MYTHINGS Central*. Zum Entwicklungskit gehören: zwei Funksensoren *MYTHINGS Smart Sensor*, eine Antenne, Zubehör sowie eine Anleitung.

In seinem Mioty-Entwicklungskit liefert Swissphone die Basisstation *MBS20* mit, die auf einem Arm-Prozessor basiert und auf dem die Protokollsoftware *Demo Service- & Application Center* läuft. Es enthält weiter: ein Entwicklungsmodul, das kompatibel zu Arduino-UNO auf einem Mikrocontroller von STMicroelectronics basiert, ein bidirektionales Mioty-Modem und einen Sensor. Dieses Mioty-Entwicklungskit bietet Swissphone nur limitiert an.

Texas Instruments setzt in seinem Mioty-Entwicklungskit *MIOTY-HW-BDL* (**Bild 2**) den Wireless-Mikrocontroller CC1352R ein. Es besteht aus Entwicklungsmodul *LAUNCHXL-CC1352R* und drei Funksensormodulen *LPSTK-*

CC1352R, einer Image-Datei für Applikationen mit dem Mioty-Protokollstapel und einer Anleitung.
Radiocrafts dagegen verzichtet im Entwicklungskit *RC1882-MIOTY1-DK* auf eine eigene Basisstation. Das Unternehmen stellt nur einen Bootloader zur Verfügung, um mit den Funkmodulen *RC1882CEF-MIOTY1* die Netzwerkeigenschaften zu testen. Für ein komplettes Netzwerk wird noch ein Mioty-Gateway benötigt, das Radiocrafts jedoch nicht anbietet. Das Entwicklungskit *RC1882-MIOTY1-DK* enthält: zwei Entwicklungsmodule mit den Funkmodulen *RC1882CEF-MIOTY1*, auf denen alle Anschlüsse der Funkmodule leicht zugänglich herausgeführt sind und die mit einem USB-zu-UART-Schnittstellen-IC von FDTI ausgerüstet sind; zwei USB-Kabel; den Bootloader sowie Hinweise wo weitere Tools und eine Dokumentation zu finden sind.

MODULE FÜR ENTWICKLER

Das Entwicklungsmodul von Behr Tech, *MYTHINGS Click Board* (**Bild 3**), basiert auf einem Funkmodul von TDnext – TD1207R für 868 MHz mit 14 dBm Sendleistung oder TD1508 für 915 MHz und einer maximalen Sendeleistung von 24 dBm – vorkonfektioniert mit dem Mioty-Protokollstapel. Behr Tech hat sein Entwicklungsmodul kompatibel zum mikroBUS-Standard ausgeführt, um das Modul mit dem umfangreichen mikroBUS-Angebot an Sensor-, Schnittstellen- und Display-Modulen kombinieren zu können. Das *MYTHINGS Click Board* wird über AT-Kommandos gesteuert.
Radiocrafts bietet sein Entwicklungsmodul (**Bild 4**) in zwei Versionen an: als *RC1882CEF-MIOTY1* mit UART-Interface und AT-Befehlssatz sowie als *RC1882CEF-MIOTY2* mit API (Application Programming Interface), das über das eigene ICI Framework (Intelligent C-programmable I/O) in C programmiert werden kann. Beide Ausführungen enthalten den Mioty-Protokollstapel und sind für Europa (868 MHz) und Nordamerika (915 MHz) vorzertifiziert mit einer Sendeleistung von 14 dBm und einer Empfindlichkeit von –129 dBm.

MIOTY-FUNKMODULE FÜR ENDGERÄTE

Für den direkten Einbau in Endgeräte gedacht ist das Mioty Modul von Swissphone (**Bild 5**). Es enthält die *SWION* genannte Mioty-Software von Swissphone als Firmware und wird per AT-Kommandos über UART- oder SPI-Schnittstelle gesteuert. Seine maximale Sendeleistung liegt bei 18 dBm. Es kann für die unidirektionale und bidirektionale Datenübertragung eingesetzt werden.
Weptech Elektronik bietet zwei Funkmodule mit dem Mioty-Protokollstapel an: *COUA-M* auf der Basis des CC1310 von Texas Instruments für die bidirektionale Datenübertragung bei 868 MHz und *PHOENIX-M* (**Bild 6**) auf Basis des STM32L071RBH6 von STMicroelectronics für die unidirektionale Datenübertragung mit einer Sendeleistung von bis zu 16 dBm bei 868 MHz. Beide Funkmodule verfügen über eine UART-Schnittstelle und einen Antennenanschluss und für beide bietet Weptech Elektronik Entwicklungskits.

MIOTY-ZENTRALE: BASISSTATIONEN

Die Mioty-Basisstation *MYTHINGS Base Station* liefert Behr Tech auch mit seinem Entwicklungskit aus. Sie basiert, wie oben bereits erwähnt, auf einem Industrie-PC (ARK-2250L) von Advantech mit Intel-Core-i3-Prozessor und der Software *MYTHINGS Central*, die auf einem Ubuntu OS läuft. In der Basisstation ist ein Softwaregesteuerter Funk-Transceiver (868 und 915 MHz) eingebaut. Komplettiert wird die Basisstation mit einer Dipol-Antenne (Rundstrahler) mit Magnetfuß und Filtern für die Einsatzregion. Die *MYTHINGS Base Station* kann Millionen von Nachrichten pro Tag verarbeiten und mehrere Tausend Knoten in einem Mioty-Netzwerk verwalten.
Das *Mioty Premium Gateway* von Diehl ist für die bidirektionale Datenübertragung in Netzwerken mit bis zu 25.000 Endgeräten ausgelegt. Es wird mit Mioty-Lizenz, Stromversorgung und Anleitung ausgeliefert.

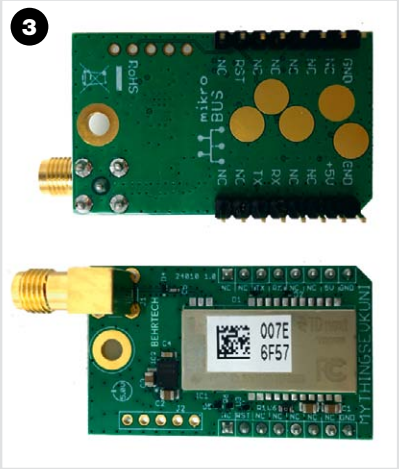


Bild 1. Einen Industrie-PC mit Mioty-Software als Basisstation und zwei mobil einsetzbare Funksensoren packt Behr Tech in sein Entwicklungskit für Mioty-Netzwerke. (Bild: Behr Tech)
Bild 2. Drei Funksensoren und ein Entwicklungsmodul – alle auf Basis des Wireless-Mikrocontrollers CC1352R – enthält das Mioty-Entwicklungskit *MIOTY-HW-BDL* von Texas Instruments. (Bild: Texas Instruments)
Bild 3. In seinem Entwicklungsmodul *MYTHINGS Click Board* setzt Behr Tech auf Funkmodule von TDnext und den mikroBUS-Standard. (Bild: Behr Tech)

Für die Basisstation *MBS20* – sie ist auch Teil des Mioty-Entwicklungskits von Swissphone – nutzt Swissphone ein Modul mit Arm-Prozessor (**Bild 7**). Sie enthält einen Funk-Transceiver für die bidirektionale Datenübertragung im Netzwerk und kann über einen Mini-PCIe-Slot erweitert werden. Die Basisstation *MBS20* kann über PoE (Power over Ethernet) und per externem Netzteil mit Strom versorgt werden und Swissphone bietet eine maßgeschneiderte Anpassung der Hard- und Software an.

Als Low-Cost-Alternative bewirbt Weptech Elektronik sein Mioty-Gateway *AVA* (**Bild 8**) für den Einsatz in Europa (868–870 MHz) und den USA (915–917 MHz). Sie arbeitet mit einer Sendeleistung von 14 dBm und einer Empfindlichkeit von –135 dBm, wird über eine Ethernet-Schnittstelle angeschlossen und gibt Informationen per Web-Interface aus. Versorgt wird das Gateway *AVA* mit 5 V über eine USB-C-Buchse.

ENDGERÄTE FÜR ANWENDUNGEN

Funksensoren zählen zu den klassischen Endgeräten in einem LPWAN. Mit *Climavi* bietet das Unternehmen Agvolution eine Reihe von energieautarken Umweltsensoren für die Land- und Forstwirtschaft sowie den Gartenbau an. Sie werden von der Sonne mit Energie versorgt und senden alle 15 min Messwerte – zur Feuchtigkeit und Temperatur des Bodens, Luftfeuchtigkeit und -temperatur, Windgeschwindigkeit und -richtung, Niederschlag, UV- und Sonnenstrahlung sowie zur Konzentration von Gasen wie CO_2.

Für den stationären und mobilen Einsatz bis 120 km/h bietet Behr Tech den *MYTHINGS Smart Sensor* an. Er kann Beschleunigung, Temperatur, Feuchtigkeit und Druck messen sowie GPS-Daten empfangen. Zur Stromversorgung ist ein Akku eingebaut, der über eine USB-Buchse geladen wird. Nicht benötigte Sensoren lassen sich deaktivieren, um Energie zu sparen. Über eine serielle Schnittstelle kann der *MYTHINGS Smart Sensor* mit anderen Geräten verbunden werden, um deren Daten als Nutzdaten zur Mioty-Basisstation zu übertragen.

Der *Multisensor MS2* von Comtac (**Bild 9**) kann Temperatur, Luftfeuchtigkeit, Magnetfelder, Helligkeit und die Beschleunigung messen. Zusätzlich verfügt der Multisensor über ein Mikrofon zur Lärmmessung, einen GPS-Empfänger zur Positionsbestimmung und über digitale Eingänge. Er wird über Batterien oder von einem externen 24-V-Netzteil versorgt und

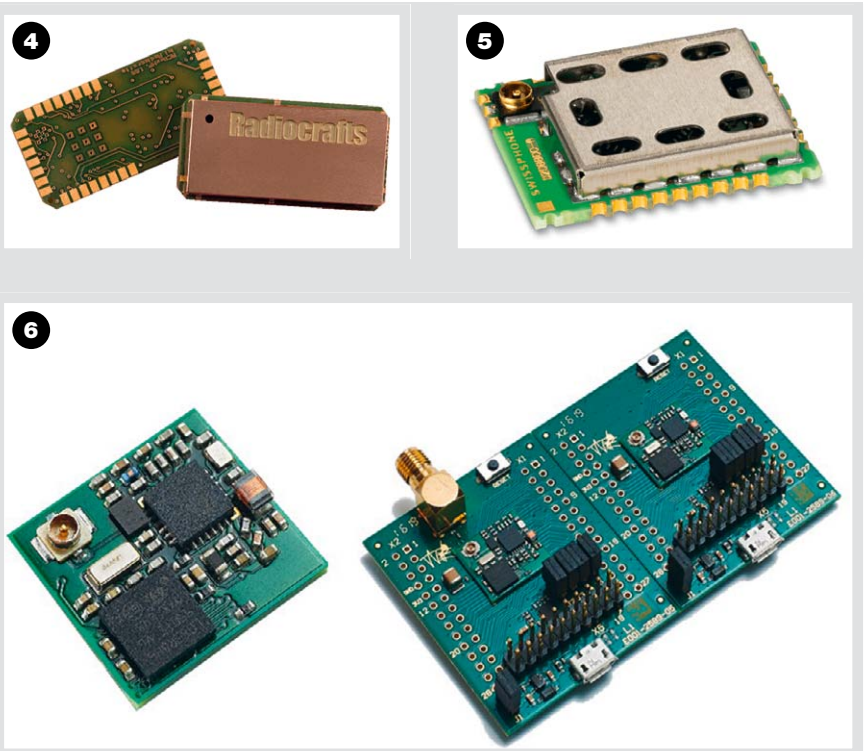


Bild 4. Die Mioty-Funkmodule von Radiocrafts *RC1882CEF-MIOTY1* und *RC-1882CEF-MIOTY2* unterscheiden sich in der Programmierschnittstelle. (Bild: Radiocrafts)
Bild 5. Für den Einbau in Mioty-Knoten bietet Swissphone ein Funkmodul mit der Mioty-Protokollsoftware *SWION* an. (Bild: Swissphone)
Bild 6. Für Anwendungen, in denen ein Endgerät nur senden muss (unidirektionale Datenübertragung), hat Weptech Elektronik das Funkmodul *PHOENIX-M* entwickelt. Es arbeitet mit einem STM32L071RBH6 von STMicroelectronics. (Bild: Weptech Elektronik)

wird per USB-Anschluss konfiguriert. Um in Räumen die Temperatur und die Luftfeuchtigkeit zu messen, eignet sich der Sensor *MUNIA-M* von Weptech Elektronik. Er ist mit zwei AA-Primärzellen bestückt, deren Kapazität für zehn Jahre Betrieb ausreicht. Für den Einsatz im Außenbereich bietet Weptech Elektronik den Sensor *ROBIN-M* an, der ebenfalls Temperatur und Luftfeuchtigkeit erfasst, jedoch in einem erweiterten Messbereich. Er ist in einem für Außenbereiche geeigneten Gehäuse eingebaut und wird von einer Lithium-Primärzelle mit Energie versorgt, deren Kapazität für zehn Betriebsjahre ausgelegt ist.

FUNKKNOTEN MIT EINGÄNGEN

Zwei digitale Eingänge – 0/24 V sowie S0-Pulse – oder zwei analoge Eingänge – 10 V, 20 mA sowie PT1000 – abfragen können die Knoten *DI-2* oder *AI-2* von Comtac (**Bild 10**). Sie sind in einem IP65-Gehäuse eingebaut, benötigen 24 V (DC) für den Betrieb und können auch auf DIN-Schienen montiert werden. Konfiguriert werden die Knoten per USB-Schnittstelle. Beide Knoten können die am Eingang detektierten Signalwerte übertragen, sie können aber auch den Mittelwert, die Minima und Maxima berechnen.

BRÜCKEN IN DIE AUTOMATISIERUNG

Eine Bridge zu Modbus hat Comtac im Angebot. Sie arbeitet nur als Mioty-Sender (unidirektional) und kann als Modbus RTU-Master (Remote Terminal Unit) bis zu 16 Registerwerte von Modbus-Slaves abfragen, die über RS485 angeschlossen sind. Die Mioty-Modbus-Bridge benötigt 24 V (DC) für den

Bild 7. Swissphone bietet an, seine Basisstation *MBS20* individuell anzupassen, sie kann auch unter der Marke des Kunden verkauft werden. (Bild: Swissphone)
Bild 8. Als Low-Cost-Alternative bietet Weptech Elektronik sein Mioty-Gateway *AVA* mit Ethernet-Schnittstelle an. (Bild: Weptech Elektronik)
Bild 9. Der *Multisensor MS2* von Comtac kann zusätzlich zu Temperatur, Luftfeuchtigkeit und Beschleunigung auch Magnetfelder, Helligkeit und Lärm messen sowie GPS-Daten empfangen, um seine Position zu bestimmen. (Bild: Comtac)

Betrieb, verfügt über ein IP65-Gehäuse, das auf DIN-Schienen montiert werden kann, und lässt sich per USB-Schnittstelle konfigurieren.

ENDGERÄTE FÜR FORSCHUNG UND ENTWICKLUNG

Für den Einsatz im Transport- und Baugewerbe hat Diehl den *Mioty Tracking Beacon* entwickelt (**Bild 11**). Er erfasst die Temperatur und die Beschleunigung mit seinen Sensoren und bestimmt seine Position über den Signal-Rauschabstand (SNR). Mit seiner Batterie ist der Sensor für zehn Jahre Betrieb ausgelegt.
Für den Einsatz in der Umgebung von Schaltstationen in elektrischen Verteilnetzen hat Friendcom einen batteriebetriebenen universellen Sensorknoten mit Mikrocontroller entwickelt. Er ist in einem Industriegehäuse verbaut und lässt sich mit vielen Sensoren bestücken, z.B. zum Detektieren von SF_6 und zur Zugangskontrolle.

SOFTWARE FÜR MIOTY-NETZWERKE UND -KNOTEN

Für Basisstationen bietet nur das Fraunhofer Institut für Integrierte Schaltungen (IIS) eine Referenzsoftware und Unterstützung bei der Implementierung an. Die Software *MYTHINGS Central* von Behr Tech kann das Netzwerk und die Knoten verwalten. Das Programm ist plattformunabhängig und verfügt über eine Cloud-Integration, z.B. für Azure und AWS. Es erlaubt die Funktionen über Plug-ins zu erweitern.
Für die Verwaltung der im Mioty-Netzwerk verbundenen Knoten und Gateways bietet Comtac eine Integration in das Programm Enerchart an. Mit *Diehl Backend* bietet Diehl ein Programm zur Verarbeitung und Darstellung der Sensordaten an. Es lässt sich mit dem eigenen Mioty-Gateway einsetzen, kann aber auch mit anderen Gateways arbeiten.

UNTERSTÜTZUNG FÜR ENTWICKLER

Für die Entwicklung eigener Mioty-Knoten können Entwickler mit dem Fraunhofer Institut für Integrierte Schaltungen (IIS) zusammenarbeiten, auch um Machbarkeitsstudien und Prototypen schnell zu realisieren. Stackforce bietet mit seinem Mioty-Protokollstapel auch Unterstützung bei der Implementierung an. Er wird als Firmware und Bibliothek angeboten, mit API (Application Programming Interface) und HAL (Hardware Abstraction Layer). HS

(Bild: Comtac)

Bild 10. Mit den Funkknoten *AI-2* und *DI-2* von Comtac können zwei analoge bzw. zwei digitale Eingänge abgefragt werden und die Werte an die Mioty-Basisstation übertragen werden.
Bild 11. Der *Mioty Tracking Beacon* von Diehl in einem robusten Gehäuse erfasst Temperatur und Beschleunigung. (Bild: Diehl)

Literatur
[1] *Sikora, Dr. A.:* Funkprotokoll für Massive IoT – Standard für skalierbare Netzwerke. *Elektronik* 2020, H. 16–17, S. 34–37.
[2] *Bernhard, J.; Dünkler, R.; Kneißl J. und Otte, L.:* Funknetzwerke – Mioty – die Revolution des IoT. *Elektronik*, 2019, H. 7, S. 26–30.

EMBEDDED WORLD CONFERENCE 2021 DIGITAL

DAS INTERNET OF THINGS – EINE WELT VOLLER MÖGLICHKEITEN

Beim Internet der Dinge greifen viele Technologien ineinander: Hardware, Vernetzung, Security, System- und Anwendungs-Software. Wie all das zusammenspielt und wohin der Trend geht, das wird auf der embedded world Conference 2021 DIGITAL thematisiert. Von Prof. Dr. Dirk Pesch

(Bild: Immersion Imagery | Shutterstock)

Das Internet of Things (IoT) steht ganz oben auf der Agenda. Es ist der Schlüssel, um unsere Häuser intelligenter zu machen, unsere Gesundheit und unser Wohlbefinden kontinuierlich zu überwachen, unsere Städte effizienter zu gestalten, unsere Autos zu vernetzen und die Vision von Industrie 4.0 zu verwirklichen. Viele sehen das IoT als große Chance, die Digitalisierung von vielen Branchen und Dienstleistungen im öffentlichen Bereich voranzutreiben. Mit der Möglichkeit, die physische Welt mit digitalen Diensten zu verbinden, treiben Entwickler den Einsatz einer immer größeren Anzahl von Embedded-Geräten voran. Prognosen über die Anzahl der mit dem Internet verbundenen „Dinge" schwanken zwischen 21 und 75 Mrd. Geräten bis zum Jahr 2025. Glaubt man IoT Analytics, scheint die Corona-Pandemie dem Ausbau der IoT-Infrastruktur im Jahr 2020 nicht geschadet zu haben [1].

DATEN AM EDGE VERARBEITEN

Es gibt eine Vielzahl von IoT-Plattformen auf dem Markt, von denen viele über das gesamte Spektrum vom Endgerät bis zur Cloud-basierten Serviceplattform zum Einsatz kommen. Schlüsselaspekte für IoT-Plattformen sind das zuverlässige Verbinden von Geräten mit der Cloud, das Orchestrieren von Diensten sowie die Leistung, insbesondere für Echtzeitdienste. War die Cloud anfangs für das Erfassen von Daten sowie das Bereitstellen von Services zuständig, wird die Echtzeit-Performance für IoT-Dienste immer wichtiger.
Da die Cloud oft weit entfernt ist und die Verbindung zu weit entfernten Orten eine große Verzögerung mit sich bringt, wird Edge Computing immer bedeutender. Hierbei werden Cloud-Dienste am Netzwerkrand, also näher an den eigentlichen IoT-Geräten, bereitgestellt. Ein Verarbeiten der Daten in der Cloud oder am Edge ist ein wichtiges Thema, da die Geräte viele Informationen über uns und unsere Umgebung erfassen und sammeln.
Ebenso spielen maschinelles Lernen und künstliche Intelligenz (KI) eine Schlüsselrolle. Mit ihnen ist es möglich, Informationen aus den Daten zu extrahieren und dem Benutzer intelligente Dienste anzubieten. Ebenfalls ein heißes Thema im Zuge des IoT ist Blockchain. Hierbei geht es vor allem um Sicherheit, Vertrauen und Datenprovenienz innerhalb von IoT-Plattformen.

SOFTWARE FÜR DAS IOT

Das Entwickeln von Software für das IoT begann als reine Embedded-System-Programmierung, unter Verwenden von Low-Level-Programmiersprachen. Um die Softwareentwicklung für das IoT

zugänglicher zu machen, haben höhere Programmiersprachen, ein Virtualisieren und clevere Softwareentwicklungswerkzeuge Einzug gehalten. So ist für Entwickler derzeit unter anderem Java für Embedded-Systeme, virtuelle Maschinen und modellbasierte Werkzeuge verfügbar.

Viele IoT-Produkte haben eine Lebensdauer von vielen Jahren und erfordern ein Warten der Geräte und Software. Aufgrund der hohen Anzahl und der oft schwierigen Zugänglichkeit der Geräte sind „Over the Air" (OTA)-Software-Updates zur Norm geworden. Das ist ein anspruchsvoller Prozess und kann dazu führen, dass sich das System in einem labilen oder nicht funktionierenden Zustand befindet, wenn etwas schief geht. Entscheiden für den langfristigen Erfolg des IoT ist hierbei die Vorgehensweise bei OTA Updates.

ERFOLGSFAKTOR SECURITY

Sicherheit ist ein großes Thema für alle vernetzten digitalen Systeme, so auch für das IoT. In der Vergangenheit haben Hacker IoT-Geräte genutzt, um Botnets einzusetzen und alle Arten von Angriffen zu starten, zum Beispiel verteilte Denial-of-Service- oder Daten-Angriffe. Der Aufbau sicherer IoT-Systemsoftware ist ein Schlüsselthema beim Entwickeln von Embedded-Systemen und IoT-Diensten. In letzter Zeit sind sichere Elemente und eSIMs in den Bereich der Embedded-Systeme vorgedrungen, um ein Autorisieren von Software und Diensten zu unterstützen. Es sind neue IoT-Architekturen aufgetaucht, die den Anspruch erheben, Sicherheit in ihren Kern zu implementieren. Außerdem werden Bedrohungsmodelle und sichere Kommunikationsmechanismen entwickelt, um Sicherheitsbedenken gegenüber dem IoT zu zerstreuen.

BEGRENZT LEDIGLICH VON DER VORSTELLUNGKRAFT

Das IoT ist lediglich von unserer Vorstellungskraft begrenzt. Es gibt bereits eine Fülle von Anwendungsfällen und Produkten und jeden Tag werden es mehr. Die Frage ist, ob das zugrunde liegende Geschäftsmodell einer neuen IoT-Anwendung solide ist und die beteiligten Anbieter und Nutzer daraus einen Wert schöpfen. Viel Interesse erfahren derzeit die Vorhersage und das Management der Leistungsaufnahme, digitale Zwillinge, Diagnosemethoden sowie das Asset Management. Letzteres ist eng mit der Gerätelokalisierung verbunden. Zu wissen, wo sich Fahrzeuge, Waren oder Gegenstände befinden, ist ein wichtiger Treiber für verbesserte Logistik und Asset-Tracking.

Die angesprochenen Themen stellen lediglich einen kleinen Ausschnitt dessen dar, was das IoT ausmacht. Es ist eine breite und interdisziplinäre Technologie und bildet einen Schwerpunkt der embedded world Conference. Themen wie die oben angesprochenen sowie Konnektivität, Betriebssysteme, Software-Engineering, eingebettete KI sowie eingebettete Hardware für das IoT werden auf der embedded world Conference in Nürnberg vom 1. bis 5. März 2021 präsentiert, diskutiert und weiterentwickelt. TS

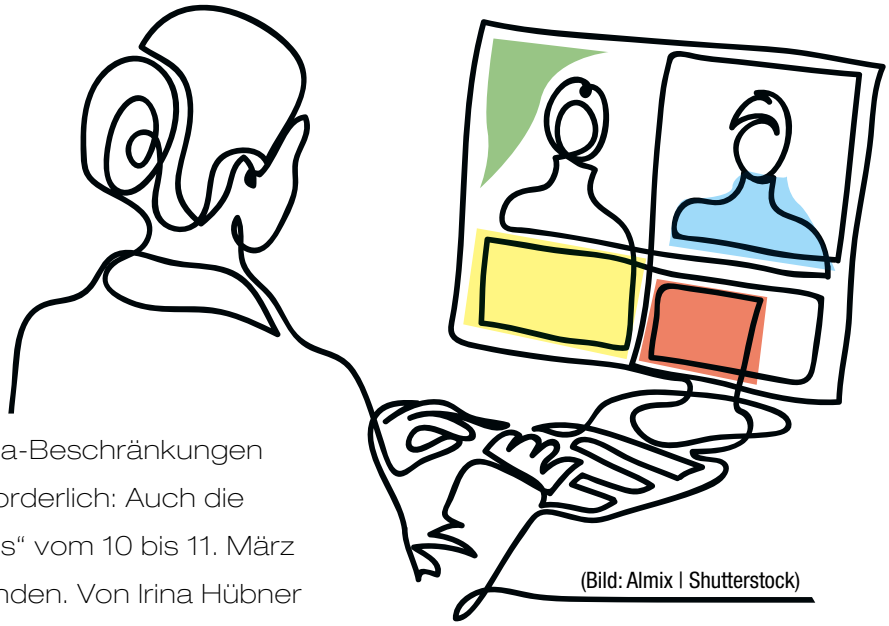
Literatur
[1] IoT Analytics. 2020. https://iot-analytics.com/iot-2020-in-review/

EMBEDDED WORLD CONFERENCE 2021 DIGITAL

Vom 1. bis 5. März 2021 findet die embedded world Conference 2021 DIGITAL statt. Das Konferenzprogramm besteht aus insgesamt 239 Vorträgen und 19 Classes. Die Vorträge können auch in den 14 Tagen nach der Veranstaltung noch „on demand" angesehen werden.
Programm und Anmeldung: www.embedded-word.eu
Gleichzeitig finden die embedded world Exhibition (www.embedded-world.de) und die electronic displays Conference (www.electronic-displays.de) statt.

12. GMM-SYMPOSIUM
„AUTOMOTIVE MEETS ELECTRONICS“

AME 2021 ERSTMALS ONLINE


(Bild: Almix | Shutterstock)

Die noch immer bestehenden Corona-Beschränkungen machen neue Konferenzformate erforderlich: Auch die „AmE – Automotive meets Electronics“ vom 10 bis 11. März wird 2021 als Onlinekonferenz stattfinden. Von Irina Hübner

Wie von den AmE-Präsenzveranstaltungen aus der Vergangenheit gewohnt, bietet auch die Onlinekonferenz ein umfangreiches zweitägiges Vortragsprogramm. Dr. Michael Wahl von der Universität Siegen führt durch die Veranstaltung. Highlights der diesjährigen „Automotive meets Electronics“ sind sicherlich die Keynotes, für die namhafte Speaker gewonnen werden konnten.

Am ersten Konferenztag um 14:15 Uhr widmet sich Prof. Dieter Schramm, Inhaber des Lehrstuhls für Mechatronik an der Universität Duisburg-Essen, in seinem Vortrag dem „Automatisierten Fahren zu Lande und auf dem Wasser“. Denn nicht nur beim motorisierten Straßenverkehr, sondern auch bei der Weiterentwicklung des Verkehrs auf Binnenwasserstraßen spielt das automatisierte Fahren zunehmend eine wichtige Rolle. Der Vortrag stellt die aktuellen Entwicklungen in beiden Mobilitätsbereichen gegenüber und befasst sich darüber hinaus mit Projekten und neuen Forschungseinrichtungen auf dem Gebiet der Binnenschifffahrt.

Eine zweite Keynote findet am zweiten Konferenztag, dem 11. März, ebenfalls um 14:15 Uhr statt. Berthold Hellenthal, Head of Computing Platform and Semiconductors bei Car.Software Org referiert in dieser über „Umbrüche in Architektur, Eigenkompetenz und Wertschöpfung“. Fahrzeugarchitekturen wandeln sich ausgehend von der dezentralen Organisation mehr und mehr hin zu einer zentralen Recheneinheit und Domänencontrollern. Dieser Umbruch erfordert jedoch gravierende Änderungen sowohl in Hard- als auch in Software, die in der Keynote thematisiert werden.

RECHTSRAHMEN ZUM AUTONOMEN FAHREN

Am Nachmittag des 11. März hält Dr. jur. Wolfgang Schneider von der Universität Duisburg-Essen einen weiteren Keynote-Vortrag mit dem Titel „Autonomes Fahren – wie das Recht der Technologie folgt“. Er informiert darin über den Rechtsrahmen für autonomes Fahren und bringt die Teilnehmer zu dieser Thematik auf den neuesten Stand.

Zu den weiteren Themen der Onlinekonferenz zählen unter anderem der Einsatz von neuronalen Netzen, die modellbasierte Entwicklung und Simulation sowie neuartige Sensortechnologien. Die AmE 2021 endet mit der Honorierung der besten Konferenzbeiträge.

Eine Stärke der „Automotive meets Electronics“ ist, dass sie sich sowohl an Vertreter aus der Industrie als auch aus der Forschung richtet. Dadurch fördert sie die Kommunikation zwischen beiden Welten und hilft dabei, neue Ideen zu kreieren. Alle Beiträge der AmE werden als GMM-Fachbericht herausgegeben. Die Konferenzteilnehmer erhalten den Tagungsband etwa eine Woche vor Veranstaltungsbeginn zum Download. IH

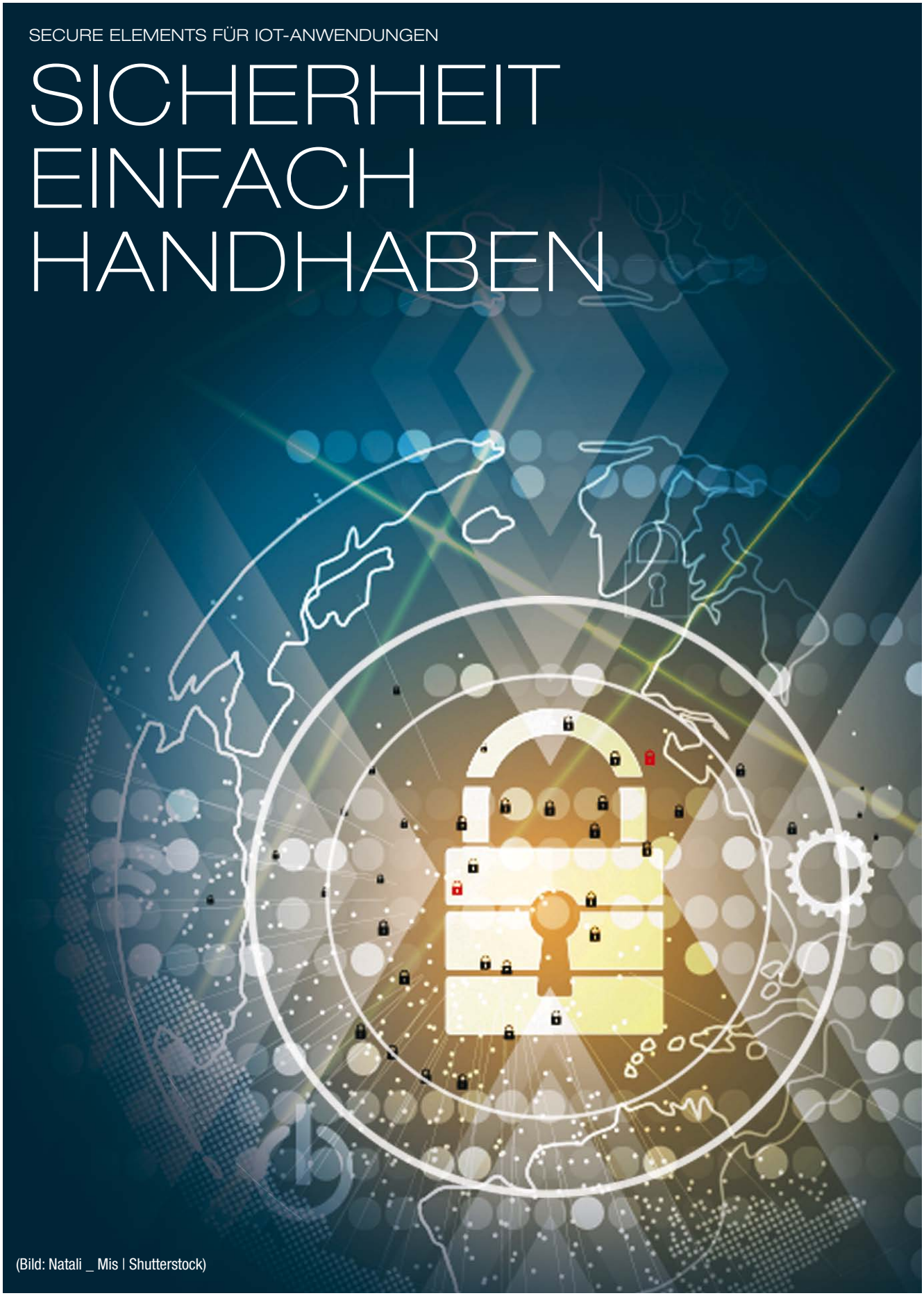
AUTOMOTIVE MEETS ELECTRONICS

AME 2021 – AUTOMOTIVE MEETS ELECTRONICS

12. GMM-Symposium
Termin: 10. bis 11. März 2021
Format: Onlinekonferenz
Anmeldung und weitere Infos:
www.ame-konferenz.de

SECURE ELEMENTS FÜR IOT-ANWENDUNGEN

SICHERHEIT EINFACH HANDHABEN



(Bild: Natali _ Mis | Shutterstock)

Sicherheits-ICs (Secure Elements) schützen Daten und Geräte vor Angriffen und vor Manipulationen. Ihr bisheriger Nachteil einer komplexen Implementierung beschränkte den Einsatz auf Geräte, die in hoher Stückzahl hergestellt wurden. Mit der Trust-Plattform vereinfacht Microchip nun die Anwendung von Sicherheits-ICs deutlich. Von Xavier Bignalet

Mit der Einführung des Internets der Dinge (IoT, Internet of Things) hat sich die Bedrohungslage im Bereich Cybersicherheit in allen Marktsegmenten dramatisch verschärft. Jedes dem Internet hinzugefügte IoT-Gerät/-System stellt gleichzeitig einen neuen Angriffspunkt dar – nicht nur auf das Gerät selbst, sondern auch auf die lokalen und in der Cloud befindlichen Systeme, mit denen es verwaltet wird.

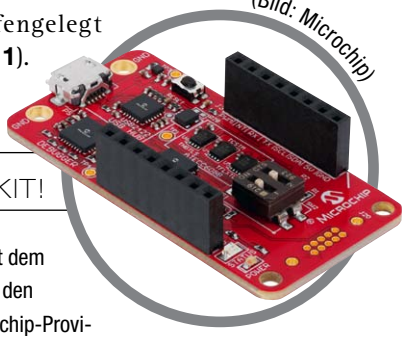
Angriffe können schwerwiegende Folgen haben, da durch das erfolgreiche Eindringen in ein IoT-Gerät neue Firmware geladen werden kann, mit der Angreifer das Gerät böswillig verwenden können. Einige Angriffe stören dabei einfach nur den Betrieb des Geräts, sodass es auf eine neue Art und Weise verwendet wird, z.B. als Knoten in einem Botnet zum Ausführen von Denial-of-Service-Angriffen. Andere Attacken hingegen können das kompromittierte System nutzen, um in das Netzwerk eines Diensteanbieters einzudringen.

Ein Eindringen wird durch reine Software-Anmeldeinformationen wie Passwörter erleichtert. Mit diesen grundlegenden Zugangsdaten kann ein Angreifer, der ein Gerät erfolgreich kompromittiert hat, diese Informationen verwenden, um Zugriff auf Dienste zur Steuerung und Verwaltung aus der Ferne zu erhalten und leichter Angriffe auf diese ausführen. Mit Hardware erzwungene Sicherheit verhindert zusammen mit einer sicheren Identität, dass Geräte ausgenutzt werden. Die Wahrscheinlichkeit, dass die ersten Angriffe erfolgreich sind, verringert sich damit erheblich.

SICHERHEIT DURCH HARDWARE

Mit per Hardware erzwungener Sicherheit lassen sich eine gültige Identität und Zugangscodes für das Gerät nur während der Herstellung mithilfe von PKI-Mechanismen (Public Key Infrastructure) erstellen. Bei einer PKI verfügt jedes Gerät über einen eindeutigen geheimen Schlüssel (Private Key), der mathematisch mit einem bekanntermaßen zuverlässigen digitalen Zertifikat verknüpft ist, das vom Hersteller sicher aufbewahrt wird. Dieser geheime Schlüssel wird verwendet, um eine Abfrage (Challenge) zu signieren, um das Gerät gegenüber jedem Server, der Zugriff auf den entsprechenden öffentlichen Schlüssel (Public Key) hat, eindeutig zu identifizieren. Der öffentliche Schlüssel ist ein einsehbarer Satz an Informationen und stellt daher kein Risiko dar, wenn er an nicht autorisierte Benutzer verteilt wird. Im Zusammenhang mit einem IoT-Gerät wird die Identität des Geräts durch Verwendung eines geheimen Schlüssels nachgewiesen. Der zugehörige öffentliche Schlüssel wird in Protokollen verwendet, die feststellen, ob die beanspruchte Identität gültig ist. Diese Identität kann während des gesamten Lebenszyklus des Geräts verwendet werden, um etwaige Firmware-Updates sowie die Identität des Geräts beim Zugriff auf Dienste zu authentifizieren.

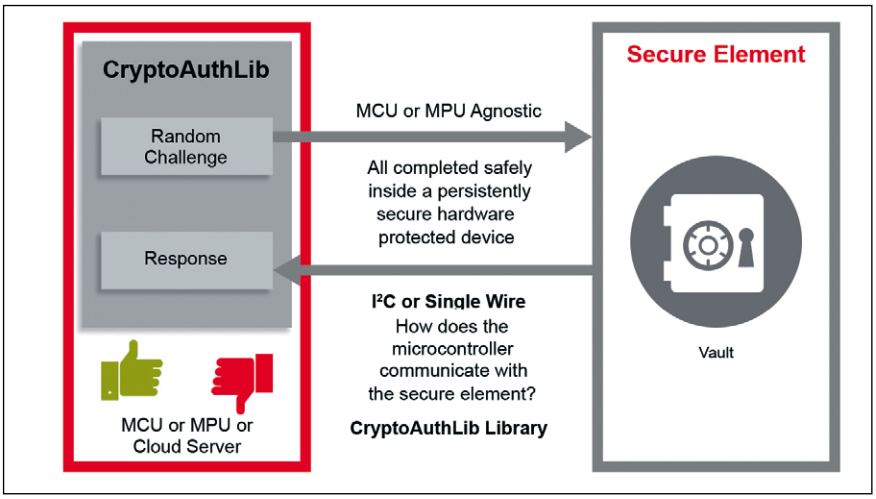
Aufgrund ihrer zentralen Rolle dürfen die geheimen Schlüssel des Geräts weder für physische Angriffe noch für Angriffe über das Netzwerk anfällig sein. Im Idealfall werden die kryptografischen Schlüssel in einem Sicherheits-IC (Secure Element) gespeichert, das eine isolierte sichere Grenze auferlegt, sodass die Schlüssel niemals offengelegt werden (**Bild 1**).


(Bild: Microchip)

GEWINNEN SIE EIN CRYPTOAUTH-TRUST-PLATFORM-ENTWICKLUNGSKIT!

Die CryptoAuth Trust Platform ist die neueste Ergänzung zu den Crypto-Authentication Evaluation Kits von Microchip für den IoT-Bereich. Dieses Kit ermöglicht den Test und die Implementierung einer sicheren Authentifizierung mit einem vorbereitetem Sicherheits-IC ATECC608B Trust&GO, einem vorkonfigurierten Sicherheits-IC ATECC608B TrustFLEX und vollständig anpassbaren Sicherheits-IC ATECC608B TrustCUSTOM. Die Trust&GO- und TrustFLEX-Sicherheits-ICs wurden entwickelt, um IoT-Cloud-Anwendungen sehr einfach mit Hardwaresicherheit, Zubehörauthentifizierung, IP-Schutz und Firmware-Verifizierung zu versehen. Mit dem CryptoAuth-Trust-Platform-Entwicklungskit, den Microchip-Entwicklungstools und den Microchip-Provisioning-Systemen können Entwickler selbst in Geräten, die in kleiner Auflage hergestellt werden, eine sichere Authentifizierung einfach und problemlos implementieren.

Ergreifen Sie die Chance, ein CryptoAuth-Trust-Platform-Entwicklungskit zu gewinnen, auf https://page.microchip.com/CTP



(Bild: Microchip)

Bild 1. Das Sicherheitsmodul der Trust-Plattform von Microchip speichert sensible Daten wie Schlüssel und Zertifikate, die während der Herstellung in den gesicherten Fertigungsstätten des Unternehmens generiert und während des gesamten sicheren Bereitstellungsprozesses niemals offengelegt werden.

Dies ist nicht ganz einfach. Die Schaltung erfordert Manipulationssicherheit und Schutz vor Lauschangriffen wie z.B. Seitenkanalanalyse. Um den Schlüssel auf diese Weise angemessen zu schützen, ist ein hohes Maß an Sicherheits-Know-how erforderlich. Außerdem verlängert sich dadurch die Entwicklungsdauer der IoT-Anwendung. Verzichten sollte ein Entwickler darauf jedoch nicht. Der Schutz des Schlüssels ist ein äußerst wichtiger Sicherheitsaspekt. Für Hersteller von IoT-Geräten sind daher Sicherheits-ICs wie der ATECC608 von Microchip mit den erforderlichen Schutzstufen erhältlich.

SICHERER UMGANG MIT SICHERHEITS-ICs

Obwohl es solche Bauelemente gibt, bleiben Herausforderungen beim hardwareerzwungenen Identitätsmanagement bestehen. Die Notwendigkeit, die sichere Identität so anzuwenden, dass sie von einem gut ausgestatteten Angreifer nicht kompromittiert werden kann, war für die meisten Geräteherstellen, Systemintegratoren und Dienstanbieter nur schwer zu erreichen. Der herkömmliche Ansatz besteht darin, ein Sicherheits-IC in der Schaltung während der Herstellung mit den entsprechenden geheimen Schlüsseln zu konfigurieren. Überlegungen rund um die Logistik in der Lieferkette haben diesen Ansatz jedoch auf große Stückzahlen beschränkt. Um jedem Gerät eine sichere Identität zu verleihen, muss der Herstellungsprozess angepasst werden, was sehr kostspielig sein kann – es sei denn, die Anpassung wird über hohe Stückzahlen amortisiert, was die Kosten pro Gerät minimiert.

Heute ist es jedoch möglich, die erforderliche Konfiguration des Sicherheits-ICs selbst bei einer Mindestbestellmenge von nur zehn Stück kostengünstig bereitzustellen, indem die Bauelemente für IoT-Geräte vorkonfiguriert bzw. vorinstalliert werden. Mit diesem Modell, das über die Trust-Plattform von Microchip unterstützt wird, lassen sich sogar einfache IoT-Überwachungskameras, Gateways, Klimaanlagen oder ähnliche Anwendungen durch vorgenerierte, gerätespezifische Zertifikate schützen. Die Gesamtkosten pro Gerät für die Bereitstellung dieses hardwarebasierten sicheren Schlüsselspeichers mit einem spezifischen Zertifikat sind geringer als die Kosten, die PKI-Diensteanbieter und Zertifizierungsstellen von Drittanbietern bieten können – und der Ansatz verringert die Komplexität und die Zeit bis zur Markteinführung erheblich.

ANPASSUNG AN HERSTELLERANFORDERUNGEN

Da IoT-Geräte, die in kleinen bis mittleren Stückzahlen hergestellt werden, mit Sicherheits-ICs ebenfalls kostengünstig mit einem sicheren Identitätsmanagement ausgestattet werden können, ist der nächste Schritt, das Sicherheits-IC so zu konfigurieren, dass es für die jeweilige Anwendung am besten geeignet ist. Dem Sicherheits-IC müssen die Anmeldeinformationen und andere Verschlüsselungsgrundlagen bereitgestellt werden, die für das jeweilige Authentifizierungsmodell zum Einsatz kommen. Neben der Identität des Kerngeräts lassen sich zusätzliche geheime Schlüssel und sensible Informationen in das Sicherheits-IC einfügen, z.B. solche, die nicht vom Root-Schlüssel abgeleitet sind, um Zubehör, Peripherie, Inhalte von Drittanbietern und Hosts zu authentifizieren, damit deren Anmeldeinformationen separat verwaltet werden können.

Das Sicherheits-IC kontrolliert den Zugriff auf wichtige Ressourcen und überwacht das IoT-Gerät, um nicht autorisierte Aktivitäten zu verhindern, z.B. Versuche, die vom Hersteller zugelassene Firmware durch bösartigen Code zu ersetzen, der möglicherweise versucht, die sensiblen Informationen des Geräts für weitere Angriffe zu verwenden.

Eine wichtige Voraussetzung, um sicherzustellen, dass Angreifer nicht in ein Gerät eindringen und es umprogrammieren können, ist eine Strategie für sicheres Booten (Secure Boot), die wiederum durch ein Sicherheits-IC geschützt ist. Durch das sichere Booten wird garantiert, dass sich auf dem IoT-Gerät nur autorisierter Code ausführen lässt. Unter diesen Bedingungen kann das Gerät nur Codeblöcke laden, die gehasht und mit einem privaten Schlüssel des Herstellers signiert sind. Muss der Mikrocontroller Code aus dem Boot-ROM laden, fordert er eine Überprüfung durch den unveränderlichen öffentlichen Schlüssel an, der im Sicherheits-IC gehalten wird. Nur wenn diese Überprüfung erfolgreich ist, wird der Mikrocontroller beginnen, den Code zu laden. Stößt der Baustein auf einen falsch signierten Codeblock, wird die kompromittierte Software nicht mehr geladen und versucht, in den werkseitig programmierten Zustand zurückzu-

kehren oder, falls dies nicht möglich ist, das Gerät zu deaktivieren. Solange der Bootloader-Code nicht geändert werden kann, indem er im ROM oder geschützten Flash abgelegt wird, kann die Überprüfung selbst nicht umgangen werden.

SICHERHEIT ERWEITERN

Ist die Kernsicherheit garantiert, lassen sich andere Anwendungen einfach hinzufügen, z.B. die zertifikatbasierte Authentifizierung auf Servern – ein wichtiger Aspekt bei IoT-Geräten. Diese Fernauthentifizierung verwendet Standardprotokolle wie TLS (Transport Layer Security) für die verschlüsselte Kommunikation sowie X.509, mit dem sich digitale Zertifikate verwalten lassen, die belegen, dass ein Gerät oder ein Dienst echt ist.

Nach dem X.509-Standard beziehen sich alle digitalen Zertifikate über eine Hierarchie von untergeordneten Zertifikaten auf ein OEM-Kernzertifikat. Die von den Zertifikaten übertragenen Informationen bieten die Möglichkeit, den rechtmäßigen Eigentümer jedes Zertifikats zu identifizieren und daraus den öffentlichen Schlüssel des Zertifikats weiter oben in der Hierarchie zu erhalten, damit die Signatur des abhängigen Zertifikats überprüft werden kann.

Kommuniziert ein entsprechend gesichertes IoT-Gerät mit einem Server, verwendet es die Informationen in den darin enthaltenen Zertifikaten, um zu demonstrieren, dass es ein gültiger Nutzer des Dienstes ist. Umgekehrt verwendet der Server seine eigenen Zertifikate, um dem Gerät zu bestätigen, dass er auch echt ist. Solange das Gerät über die erforderlichen Zertifikate verfügt, ist die bidirektionale Authentifizierung sichergestellt.

GESICHERTE INBETRIEBNAHME

Im Rahmen des IoT können digitale Zertifikate den Anmeldeprozess von IoT-Geräten beim ersten Einschalten vereinfachen, bei dem sie versuchen über das Internet eine Verbindung zu ihrem Diensteanbieter herzustellen. Dazu werden die erforderlichen Zertifikate bei der Erstprogrammierung des Sicherheits-ICs an die Server weitergeleitet. Die Zertifikate, mit denen das IoT-Gerät diese Server neben dem geheimen Kernschlüssel des Geräts im Sicherheits-IC authentifiziert, werden ebenfalls gespeichert. Als Beispiel für diesen Ansatz arbeitete Microchip mit Amazon Web Services (AWS) zusammen, damit alle mit der Trust-Plattform erstellten Produkte auf diese Weise in die AWS-IoT-Dienste integriert werden. Durch die Unterstützung von Standardprotokollen und Zertifizierungssystemen lassen sich dieselben Techniken problemlos mit anderen Cloud-Diensten wie Microsoft Azure sowie privaten und hybriden Cloud-Infrastrukturen verwenden.

Eine weitere Anwendung des IoT sind OTA-Firmware-Updates (Over-the-Air)

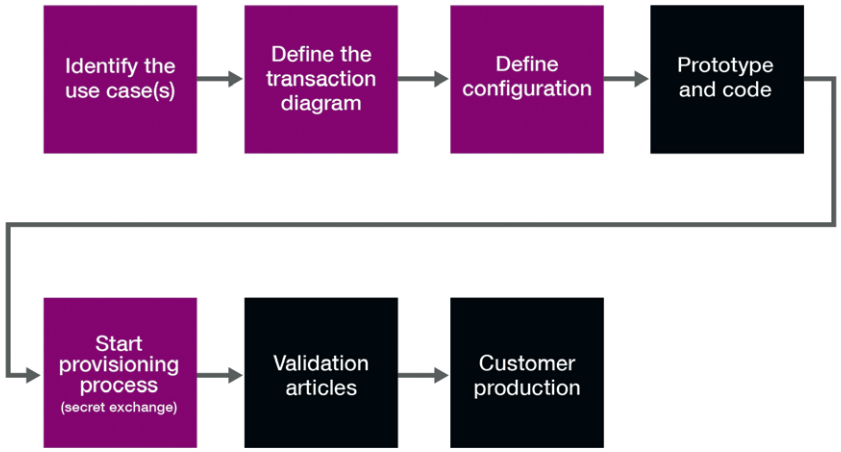


Bild 2. Prozess zur Definition der benutzerdefinierten Schlüsselbereitstellung. Nach dem Prototyp- und Code-Prozess beginnt die Bereitstellung mit einer Schlüsselübergabe und dem Erstellen sensibler Daten. Nach Abschluss des Prototypentests werden die sensiblen Daten im Sicherheits-IC eingeschlossen. (Bild: Microchip)

für IoT-Geräte/-Systeme. Diese Updates bieten die Möglichkeit, Sicherheitslücken zu beheben, ohne zu riskieren, dass die Geräte durch den Update-Prozess selbst beeinträchtigt werden. OTA-gesendete digital signierte Updates können auf ähnliche Weise überprüft werden wie Code, der beim sicheren Booten auf Authentizität überprüft wird, bevor das Update angewendet werden kann. Ist der gespeicherte Code installiert, muss er beim Neustart des Geräts auch Secure-Boot-Tests bestehen.

Weitere Anwendungsfälle sind der Schutz geistigen Eigentums, um die Gültigkeit von Ersatzteilen und optionalem Zubehör sowie den Schutz von Benutzerdaten, die Schlüsselzuweisung und die LoRaWAN-Authentifizierung zu überprüfen. Einige Gerätehersteller benötigen vielleicht anpassbare Optionen, die über diese Kerndienste hinausgehen. Andere benötigen vielleicht einen Sicherheitsansatz mit geringerem Verwaltungsaufwand (Overhead), wenn sie ressourcenbeschränkte IoT-Geräte bereitstellen. Für die Google-Cloud-IoT-Kernautorisierung ist z.B. keine vollständige digitale Zertifizierung erforderlich. Der Dienst verwendet „JSON Web Token“ (JWT), die vom privaten Kernschlüssel im ATECC608B abgeleitet sind, der die herkömmliche kennwortbasierte Anmeldung ersetzt.

SICHERHEIT NACH MASS IMPLEMENTIEREN

Die Flexibilität, diese unterschiedlichen Anwendungen mit geringen Einrichtungskosten zu bewältigen, wird durch die Trust-Plattform von Microchip und deren Unterstützung für verschiedene Einsatzmodelle möglich. Das erste Modell bietet Kunden eine einfache Möglichkeit, um Systeme mit sicheren Anmeldeinformationen über einen Standardablauf zu erwerben. In diesem Modell werden der geheime Schlüssel des Sicherheitsmoduls und die generischen Zertifikate während der Fertigung in einer sicheren Einrichtung von Microchip generiert. Der Schlüssel und die Zertifikate bleiben während des gesamten sicheren Bereitstellungsprozesses geschützt und werden im Sicherheits-IC eingeschlossen, wo sie während des Versands sicher bleiben. Die zugehörigen öffentlichen Berechtigungsnachweise können an Dienste in der Cloud oder an einen Join-Server eines LoRaWAN-Netzwerks weitergeleitet werden.

Da sich viele Gerätehersteller mehr Flexibilität bei der Authentifizierung wünschen und die Möglichkeit haben möchten, Zertifikate basierend auf ihrer eigenen Authentifizierungskette zu erstellen und einzufügen, bietet eine zweite Option eine Reihe vorkonfigurierter Anwendungen, die diese Aktionen automatisch durchführen. Weitergehende Änderungen sind in einem dritten Modell möglich. Bei diesem Ansatz (**Bild 2**) beginnt der Gerätehersteller mit der Bestellung eines leeren Sicherheits-ICs und nutzt dann Tools von Microchip, um die Bereitstellung aufzubauen – u.a. den XML-Code, mit dem in den sicheren Einrichtungen von Microchip die Zustellung privater Schlüssel und Zertifikate an das Sicherheits-IC gesteuert wird.

Durch neueste Entwicklungen bei Onlinetools und Bauelementen für hardwarebasierte Sicherheit können Projekte jeder Größe nun mit einem Sicherheits-IC ausgestattet werden. Die Hindernisse, die eine Konfiguration und Bereitstellung von Sicherheits-ICs erschwerten und kostspielig machten, wurden beseitigt. Der Prozess hat zu einer etablierten sicheren Lieferkette geführt, wodurch Best-Practice-Sicherheitsmodelle nun auf das gesamte IoT-Wirtschaftsökosystem ausgedehnt wurden. HS

XAVIER BIGNALET

ist Produkt Marketing-Manager im Geschäftsbereich Security Products bei Microchip Technology und verfügt über mehr als 13 Jahre Erfahrung in der Halbleiterindustrie. Vor seinem Eintritt bei Microchip begann er seine Karriere in der Entwicklung von Analog-, Mixed-Signal- und Stromversorgungs-ICs. Ab 2012 wechselte er in den kaufmännischen Bereich und wurde Produktlinienmanager für mehrere Mixed-Signal-IC-Reihen, während er zugleich an Integrationsaufgaben mitwirkte. Seit 2015 spezialisierte er sich bei Microchip auf Embedded IoT- und Sicherheitstechniken. Er hat sein Elektrotechnikstudium an der Hochschule CESI (Centre des Études Supérieures Industrielles) in Toulouse, Frankreich, mit einem Master (M. Sc.) abgeschlossen. Xavier.Bignalet@microchip.com

Elektronik automotive

E-VEHICLES & CONNECTED CARS

powered by

ETAS
DRIVING EMBEDDED EXCELLENCE

Zuliefermarkt: Angriff der Cybertech Tiers

Energiemanagement: Neue Architektur für das Bordnetz

Verifizierung: Zufällige Hardwarefehler schnell identifizieren

embeddedworld2021

Exhibition&Conference

DIGITAL

EMBEDDED.
INTELLIGENT. SYSTEMS.

JOIN THE DIGITAL EVENT!

1.–5.3.2021

Jetzt Ticket sichern!
embedded-world.de/ticket

Medienpartner

Markt&Technik
Elektronik
SmarterWorld
Computer & AUTOMATION
DESIGN& ELEKTRONIK
Elektronik automotive
medical-design
elektroniknet.de

NÜRNBERG MESSE

DIE ZEIT IST REIF

2020 ist vorbei und auf dem noch jungen Jahr 2021 ruht trotz eines anstrengenden Januars riesige Hoffnung. Hoffnung darauf, dass man 2021 wieder mehr Normalität erreicht, dass Corona erfolgreich bekämpft werden kann, sich Menschen wieder die Hand reichen können, und sich die Wirtschaft rasch erholt.

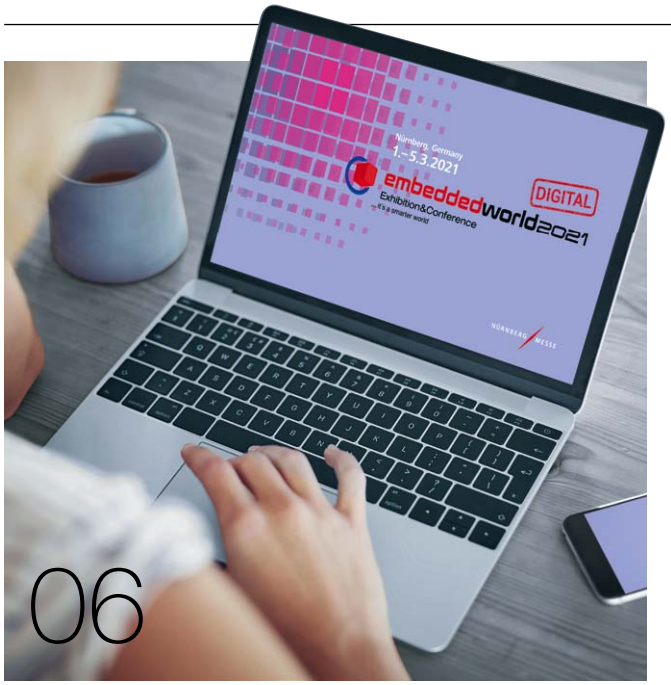
„Back to normal" heißt allerdings nicht, dass jede Privatperson oder jedes Unternehmen so weiter machen kann wie bisher. Denn die Pandemie hat knallhart gezeigt, dass altbewährte und für gut befundene Geschäftsmodelle ganz schnell auf dem Abstellgleis landen, wenn sich damit die Bedürfnisse der Nutzer nicht mehr erfüllen lassen oder diese aufgrund der gegenwärtigen Ein- und Beschränkungen nicht mehr umsetzbar sind. „Die Grenzen traditioneller Geschäftsmodelle, Managementpraktiken und Unternehmenskulturen werden immer deutlicher. Wir benötigen daher dringend neue Ideen und Herangehensweisen", betont Tim Leberecht, Co-Gründer des House of Beautiful Business – neue Ideenfabrik und Plattform des Porsche Digital Company Builder „Forward31". Eine Botschaft, die nicht nur für Porsche gilt, sondern die sich viele Unternehmen zu Herzen nehmen dürfen.

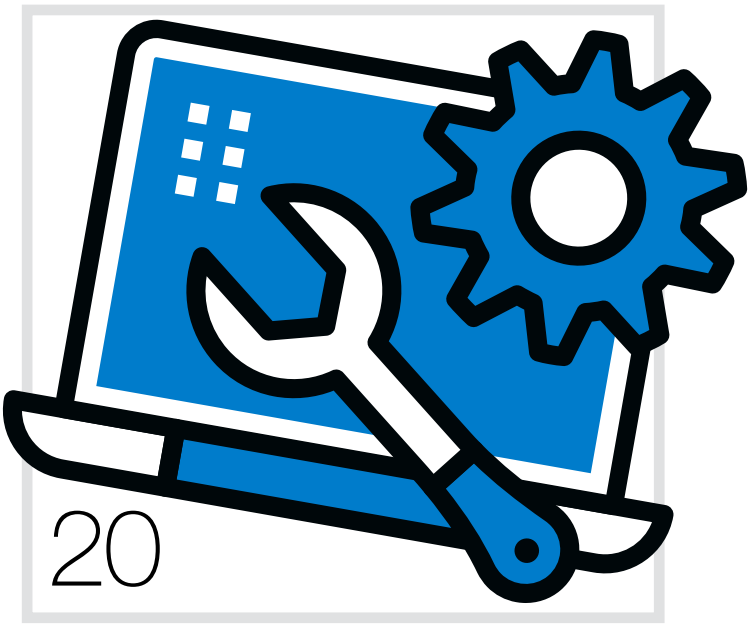
Auch in puncto Klimaschutz lässt sich nicht so weitermachen wie bisher. Zwar konnte Deutschland 2020 sein selbstgestecktes Klimaziel von 40 Prozent weniger Treibhausgase als 1990 erreichen und dieses sogar laut der politisch unabhängigen Denkfabrik Agora Energiewende mit 42,3 Prozent noch etwas überbieten. Doch auf die Schultern muss sich niemand klopfen, denn das Ergebnis sei nicht der Klimaschutzpolitik zu verdanken, sondern Folge der Corona-Pandemie. „Verkehr und Industrie werden wieder mehr Treibhausgase ausstoßen, sobald die Wirtschaft wieder anzieht", ist sich Patrick Graichen, Direktor der Denkfabrik, sicher.

Dem muss die Bundesregierung eigentlich entgegenwirken. Eine wichtige Rolle sollte dabei den öffentlichen Verkehrsmitteln zukommen. Doch wenn ich sehe, dass Pendler, die mit Bahn und Co. unterwegs sind, im Vergleich zu Autofahrern tiefer ins Portemonnaie greifen müssen, dann stimmt mich das nachdenklich. Denn Bahnfahren ist klimafreundlich, wird aber nicht nur finanziell nicht belohnt – sondern im Gegenteil bestraft. Die Kosten sind in den vergangenen Jahren deutlich stärker gestiegen als die Kosten für Autofahrer. Das verdeutlicht eine Auswertung der Allianz pro Schiene auf Basis von Daten des Statistischen Bundesamts. So zahlten Nutzer des Nahverkehrs 2020 im Schnitt 16 Prozent mehr als 2015. Autofahren wurde dagegen nur um vier Prozent teurer. Auch als begeisterte Autofahrerin muss ich sagen, dass das äußerst ungerecht ist und steinzeitliche Ausmaße hat. Die Zeit ist mehr als reif für eine neue Denke, moderne Konzepte und Herangehensweisen. Und für unpopuläre Maßnahmen – auch im Wahljahr.

STEFANIE ECKARDT

Leitende Redakteurin
Twitter: @seckardt2
seckardt@weka-fachmedien.de





E-VEHICLES & CONNECTED CARS

IMPRESSUM

Anschrift für Verlag, Redaktion, Vertrieb, Anzeigenverwaltung und alle Verantwortlichen: WEKA Fachmedien GmbH, Richard-Reitzner-Allee 2, 85540 Haar
Tel.: 089 25556-1000, Fax 089 25556-1399, www.weka-fachmedien.de
Telefondurchwahl im Verlag: Sie wählen 089 25556 und dann die Nummer, die in Klammern zum jeweiligen Namen angegeben ist.
Geschäftsführer: Kurt Skupin, Matthäus Hose

Director Content Electronics: Dr. Ingo Kuss
Markenteam Elektronik automotive: Joachim Kroll (jk/1335), Chefredakteur (verantwortlich für den Inhalt), Markus Kien, Chef vom Dienst (mk/1333)
Redaktionsteam: Heinz Arnold, Editor-at-Large (ha/1253), Stefanie Eckardt, Ltd. Red. (eck/1342), Melanie Erhardt (me/1346), Markus Haller (mha/1371), Ralf Higgelke (rh/1341), Engelbert Hopf, Chefreporter (eg/1320), Ute Häußler (uh/1369), Irina Hübner (ih/1339), Andreas Knoll, Ltd. Red. (ak/1319), Corinna Puhlmann-Hespen (cp/1316), Corinne Schindlbeck, Ltd. Red. (sc/1311), Tobias Schlichtmeier (ts/1368), Harry Schubert (hs/1338), Iris Stroh, Ltd. Red. (st/1326), Kathrin Veigel (kv/1746), Nicole Wörner (nw/1325), Karin Zühlke, Ltd. Red. (zü/1329)
Layoutteam: Wolfgang Bachmaier, Andreas Geyh, Norbert Preiss, Bernhard Süßbauer, Alexander Zach
Bilderdienst: Shutterstock
Redaktionsassistenz: Andrea Seidel (sei), Tel.: 089 25556-1332; Fax: 089 25556-1670
redaktion@elektronik.de
www.elektronik-automotive.de

Director New Business: Marc Adelberg (1572)
Sales Director: Christian Stadler (1375)
Mediaberatung: Petra Beck (1378), Burkhard Bock (1305), Tanja Lewin (1386), Konrad Nadler (1382), Martina Niekrawietz (1309),
International Account Managers: Konrad Nadler (1382), Martina Niekrawietz (1309)
Auslandsrepräsentanz (Foreign Representation):
USA West: Huson International Media, Lanibel Collado, 16615 Lark Avenue, Suite 100, Los Gatos, CA 95032, Tel.: 001 408 879 6666, Fax: 001 408 879 6669, lanibel.collado@husonmedia.com
Anzeigenverwaltung und Disposition: Jeanette Blaukat (1014)
Anzeigenpreise: Es gilt die Preisliste Nr. 21 vom 1. Januar 2021
Teamassistenz: Rosi Böhm, Tel.: 089 25556-1307, Michaela Stolka, Tel.: 089 25556-1376, Fax: 089 25556-1651
media@elektronik.de
www.weka-fachmedien.de/de/medien/elektronik/

Vertriebsleitung: Marc Schneider (1509, mschneider@weka-fachmedien.de)
Leitung Herstellung: Marion Stephan (1442)
Sonderdrucke: Alle in dieser Ausgabe erschienenen Beiträge können für Werbezwecke als Sonderdrucke hergestellt werden. Anfragen an Andreas Hofner, Tel. 089 25556-1450, E-Mail: AHofner@wekanet.de
Technik: JournalMedia GmbH, Richard-Reitzner-Allee 4, 85540 Haar
Druck: L.N. Schaffrath GmbH & Co. KG DruckMedien, Marktweg 42–50, 47608 Geldern

20. Jahrgang

INSERENTEN

SAFETY UND SECURITY IM FOKUS

EMBEDDED WORLD CONFERENCE 2021 DIGITAL

(Bild: NürnbergMesse)

Aufgrund diverser Corona Lockdowns hat sich die Welt im vergangenen Jahr etwas ruhiger gedreht. Die ganze Welt? Nein. Die Embedded-Branche ist durch die Pandemie im Gegenteil herausgefordert, und so sind auch dieses Jahr wieder zahlreiche spannende Entwicklungstrends und Innovationen auf der embedded world Conference zu finden. Unter dem Motto "embedded. intelligent.systems – the innovators' place to be!" trifft sich die Community dieses Jahr digital.
Von Prof. Dr. Peter Fromm

Mehr als 230 Vorträge und 19 Classes u.a. aus den Themengebieten Safety and Security, Software and Systems Engineering, Autonomous Systems, Embedded Vision, Ultra Low Power Designs, FPGA, Operating Systems und viele mehr bieten einen imposanten Überblick über aktuelle Technologien und Trends in der Embedded Community.

Der Trend setzt sich fort: Embedded-Systeme übernehmen zunehmend komplexe Steuerungsaufgaben, die bislang dem Menschen vorbehalten waren. Da bei einer Fehlfunktion dieser Systeme Menschenleben gefährdet werden können, müssen sie unter Berücksichtigung der entsprechenden Sicherheitsnormen entwickelt werden.

Aktuelle Neuerungen in der Normenwelt, unter anderem Arbeiten an einer neuen Version der ISO 61508, liefern den Stoff für den Vortragsreigen im Track Safety and Security. Ein weiterer spannender Schwerpunkt ist die Entwicklung sicherer Architekturen. In der Track Keynote "Taming Timing – Combining Static Analysis With Non-intrusive Tracing to Compute WCET Bounds on Multicore Processors" stellt Dr. Daniel Kästner einen innovativen hybriden Ansatz zur Bestimmung der Worst Case Execution Time auf Multicore Controllern vor. Ein sehr aktuelles Thema, um Zeitbudgets von parallelen Prozessen performant und gleichzeitig sicher definieren zu können.

Eine ebenfalls nach wie vor große Herausforderung ist der Bereich Informationssicherheit oder Security. Immer mehr eingebettete Systeme haben eine Schnittstelle in die Cloud. Besonders bei komplexen Systemen sind diese Schnittstellen unbedingt notwendig, damit bei einem Fehlerfall schnell ein Update eingespielt werden kann bzw. zunehmend auch rechenintensive Dienste quasi in Echtzeit ausgelagert werden können. Es ist zu erwarten, dass solche Over-the-Air-Dienste bei zukünftigen intelligenten

Systemen noch stärker an Bedeutung gewinnen werden.

Gleichzeitig bieten diese Schnittstellen mögliche Angriffsflächen für Hacker, die im Worst Case darüber z. B. komplette Fahrzeugflotten manipulieren können. Besonders kritisch wird es, wenn über eine solche Schnittstelle sicherheitskritische Funktionen wie Lenkung, Motor oder Bremse manipuliert werden können. Das bedeutet, dass der Informationssicherheit in Zukunft ein deutlich höherer Stellenwert eingeräumt werden muss und Security eine wesentliche Architekturanforderung von Beginn an sein wird.

Obwohl immer mehr Controller über Hardware-Kryptofunktionen verfügen, ist die Entwicklung einer langlebigen Security-Architektur nach wie vor nicht einfach. In den Sessions „Security Hardware“ und „Security Architectures“ werden diese Herausforderung u. a. am Beispiel der Entwicklung eines Security Stacks für eine RISC-V-Architektur aufgegriffen sowie aktuelle Security-Hardwareentwicklungen etwa von STM, Infineon und ARM vorgestellt. Praktische Anwendungsfälle aus verschiedenen Industriebereichen, u. a. Medical und Railway, werden in der Session „Security Use Cases“ diskutiert. Ein Blick in die Zukunft wagt die Session „Long Term and Post-Quantum Security“.

Das Thema künstliche Intelligenz in Embedded-Systemen – ob Microcontroller, FPGA oder dedizierte Hardware – nimmt nicht nur im Automobilbereich beeindruckend schnell an Fahrt auf, während gleichzeitig die Themen Connectivity und Cloud-Services eine wesentliche Technologie für die Verarbeitung der dabei anfallenden Datenmengen bilden. Der Einsatz von künstlicher Intelligenz für sichere Systeme bringt neue Herausforderungen mit sich, gerade auch für den Bereich der Qualifikation solcher Lösungen. „Hilfe, ich verstehe mein neuronales Netz nicht“ – eine Erfahrung, die wohl die meisten Entwickler neuronaler Netze mehr als einmal gemacht haben. Ein solcher Kontrollverlust ist insbesondere für sichere Systeme natürlich nicht akzeptabel und wird unter den Überschriften „Safe AI“ und „Explainable AI“ aufgegriffen. Einen guten Einstieg in die Entwicklung von intelligenten Embedded-Systemen bieten die Sessions „Embedded AI“ und „AI Use Cases“. Hier werden praktische Erfahrungen und Herausforderungen von KI-Implementierungen auf FPGA und Microcontrollern adressiert. Einen ersten Einblick in das spannende Themenfeld Bildverarbeitung und künstliche Intelligenz bietet die Session „Embedded Vision: SW Tools & Tooling AI & Tool Chains“. Besonders empfehlenswert ist sicherlich auch die „Track Keynote: Dependable Neural Networks Through Redundancy – Comparing Architectures“ von Prof. Hans Dermot Doran der Hochschule Zürich.

Wie man sieht – auch dieses Jahr spannt die embedded world Conference für Ingenieure (nicht nur) aus der Automotive-Branche ein breites Themenangebot auf: “embedded.intelligent.systems – the innovators‘ place to be!”. Dieses Jahr noch einmal digital und nächstes Jahr wieder vor Ort in Nürnberg! Das ausführliche Programm ist im Web nazulesen unter **www.embedded-world.eu** JK | ECK

NEUE GENERATION ZULIEFERER FÜR DAS CONNECTED CAR

ANGRIFF DER CYBERTECH TIERS

(Bild: Sashkin / Shutterstock)

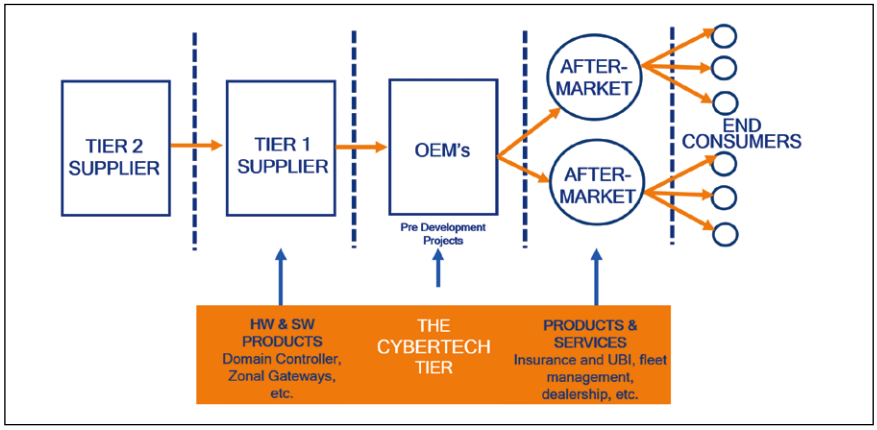
Für die technologischen Herausforderungen des Smartphones auf Rädern braucht es neben neuen softwareorientierten Fahrzeugarchitekturen einen Paradigmenwechsel in der Lieferkette. Cybertech Tiers wollen Services für vernetzte Fahrzeuge schnell und effektiv entwickeln – mit Fahrzeugherstellern, Zulieferern und Aftermarket-Anbietern. Wir befragten Dionis Teshler von GuardKnox: Was sind Cybertech Tiers und wie ordnen sie sich in der im Umbruch befindlichen automobilen Lieferkette ein? Von Ute Häußler

Cybertech Tier klingt futuristisch. Die dahinterliegende Service Oriented Architecture (SOA) für Elektronik im Auto ist nicht neu. Was ist der „Game Changer“ am neuen Ansatz?

SOA ist eine Technologie. Um sie erfolgreich zu implementieren, müssen wir die aktuellen Kundenwünsche und den Wandel bei den Zulieferern betrachten. Heutige Autokäufer wollen digitale Erlebnisse und Konnektivität – OEMs und Tier-1s müssen statt Pferdestärken die beste Software und die beste Computing Power für „User Experience“ liefern. Die Hälfte aller Entwicklungskosten fließt bereits in Software, rund 70% Anteil werden langfristig vorausgesagt. Das ist ein grundlegender Wandel.

Parallel erkennen viele OEMs, dass der Hersteller der ECU-Hardware nicht zwangsläufig der passende Experte für Software oder Computerplattformen sein muss. Der eigentliche Wert der nächsten Fahrzeuggeneration liegt in der besten Technologie und damit bei den Zulieferern, die die besten Lösungen für ein fortschrittliches Benutzererlebnis bieten. Zwei Aspekte sind SOA und Services, weitere zonale Architekturen, Cybersicherheit und High-Performance-Computing. Außerdem natürlich Konnektivität. Statt nach der „eierlegenden Wollmilchsau“ suchen OEMs – bestes Beispiel ist die VW-Gruppe mit der Car.Software Org (CSO) – jetzt nach dem besten Anbieter für eine bestimmte Technologie, der dann Tier-1 für das jeweilige Produkt wird. Das ist Priorität Nummer Eins.

Zu diesen Technologielösungen können viele verschiedene Zulieferer einen Part beitragen, der von einem anderen Zulieferer produziert und wieder vom nächsten implementiert wird. Deshalb haben wir diesen neuen Partnern einen Namen gegeben – Cybertech Tier. Cyber ist alles, was miteinander verbunden ist. Tech steht natürlich für Technologie, zusammen ordnet es sich als neue Kategorie von Technologiezulieferern in die sich verändernde Wertschöpfungskette bei den Tier-1s und Tier-2s ein.



Wie Cybertech Tiers an die automobile Lieferkette andocken wollen. (Bild: Guard Knox | Elektronik)

Welche Vorteile dienen den eher kleinen Cybertech Tiers als Eintrittskarte in der aktuellen Konsolidierungsphase mit Megafusionen, OEM-übergreifenden IT-Partnerschaften und Halbleiterunternehmen als neuen Playern im Automarkt?

Bereits die Frage zeigt, dass es im Automobilsektor Partnerschaften braucht. Alleine geht es nicht, die OEMs müssen für das Connected Car ein Ökosystem erschaffen. Wir als GuardKnox arbeiten bereits mit NXP, Green Hills Software, Xilinx und vielen anderen Partnern zusammen. Diese Firmen sind Lieferanten von Kerntechnologien, die auch Teil unseres Angebotes sind.

Der Weg in die sich neu formende Lieferkette führt über die vertikale Integration, welche die OEMs mit Organisationen wie der CSO oder mit Spin-offs wie dem ZF Software Center bereits geschaffen haben. Cybertech Tiers streben einen Status als Lieferant für diese Entitäten der OEMs und auch Tier-1s an. Wenn es um SOA, einen Software-Stack oder eine Cybersecurity-Lösung geht, wird es zukünftig immer ein gemeinsames Lösungsangebot mehrerer Partner sein. Die wichtigste Änderung ist, dass wir nicht unbedingt die ECU produzieren, stattdessen stellen wir ein spezifisches Modul mit der bestmöglichen Technologie her. Das widerspricht der traditionellen Herangehensweise eines Tier-3- oder Tier-2-Zulieferers. Wir kooperieren direkt mit OEMs und Tier-1s – dazu sind die Softwarekomponenten viel zu wichtig im modernen Auto. Cybertech Tier ist eher eine Frage der Positionierung und des Partnermanagements, wir haben uns das ja nicht ausgedacht. Es sind die OEMs, welche die Lieferkette verändern – das ist an der Art und Weise sichtbar, wie diese sich gerade (um-)strukturieren.

Die Vorteile einer Cybertech-Tier-Kooperation dürften für Tier-1s weit größer sein als für OEMs?

Das würde ich so nicht ausdrücken. Ein Cybertech Tier muss mit beiden Partnern arbeiten, allerdings nicht zwingend traditionell hierarchisch. Der OEM muss sehen, wie er neue Technologien zulassen und integrieren kann, mit beiden Partnern ist eine direkte Zusammenarbeit wichtig. Heute arbeiten Cybertech Tiers hauptsächlich mit Tier-1-Kunden, das ändert sich aber bereits aufgrund von Organisationen wie der CSO stark. Die CSO ist selbst ein Integrator und eine Art Tier-1 geworden. Wenn sie also das Steuergerät integrieren, dann arbeiten wir dort direkt zusammen. Das ist nicht mehr klar voneinander getrennt. Es wird immer mehr zu einer Matrix zwischen den Partnern, um die jeweiligen Stärken zu maximieren und das beste Produkt für den OEM und den Autokäufer zu schaffen. UH

DIONIS TESHLER

ist Co-Gründer und CTO bei GuardKnox. Teshler hält einen Bachelor in Elektroingenieurswesen, einen Master in Computerwissenschaft sowie einen MBA in Globaler Strategie. Er arbeitete als Computer-Vision-Ingenieur und Cyberingenieur bei der israelischen Luftwaffe und leitete folgend die Cybersecurity des F-35-Programms. Seit 2015 widmet er sich bei GuardKnox Technologien für die automobile Zukunft.

BATTERIETECHNIK

LI-IONEN-BATTERIE-MUSTER MIT NUR FÜNF MINUTEN LADEZEIT

StoreDot konzentriert sich auf die Entwicklung von sogenannten XFC-Batterietechniken (Extreme Fast Charging). Nun gibt das israelische Unternehmen bekannt, dass Entwicklungsmuster seiner ersten Batteriegeneration mit nur fünf Minuten Ladedauer verfügbar sind.

Mit seiner Entwicklung weist StoreDot die wirtschaftliche Machbarkeit von XFC-Batterien mit kleinem Formfaktor nach. Damit will das Unternehmen Anwendern die Angst vor geringer Reichweite und langer Ladedauer von Elektrofahrzeugen nehmen. StoreDot gibt nun die erste Produktionscharge mit Musterzellen frei, um die Technik potenziellen Partnern im Bereich Elektromobilität und in der Industrie zu präsentieren. Mit dieser Batterie konnte die vollständige Ladung eines elektrischen Zweirads in nur fünf Minuten demonstriert werden.

Die Batterie könnte sich auch in einer Reihe anderer Industriezweige für ultraschnelles Laden eignen, wie zum Beispiel für das Laden kommerzieller Drohnen und die Unterhaltungselektronik. Die technischen Muster der ersten Batteriegeneration sollen Herstellern von Elektrofahrzeugen und Batterien den erfolgreichen Ersatz von Graphit in der Zellenanode durch metalloide Nanopartikel demonstrieren. Dies könnte einen entscheidenden Durchbruch in der Überwindung wichtiger Probleme darstellen – beispielsweise im Hinblick auf Sicherheit und Zykluslebensdauer.

Die Musterzellen wurden hergestellt von EVE Energy, dem strategischen Partner von StoreDot in China. Konkurrierende Technologien erfordern zum Teil erhebliche Investitionen in spezielle Fertigungsanlagen. Die XFC-Batterien von StoreDot sind hingegen so konzipiert, dass sie in bestehenden Fertigungslinien für Li-Ionen-Batterien bei EVE Energy hergestellt werden können. Die Muster entsprechen der UN 38.3, wodurch die Sicherheit von Li-Ionen-Batterien beim Gütertransport gewährleistet ist.

„StoreDot ist seinem Ziel, das Laden von Elektrofahrzeugen innerhalb von fünf Minuten zu einer wirtschaftlichen Realität zu machen, einen Schritt nähergekommen. Die XFC-Technik wird nun zum ersten Mal in einem kommerziell nutzbaren Produkt eingesetzt, das für die Massenproduktion skalierbar ist. Als nächsten Schritt wollen wir den Prototyp einer Batterie mit Silizium-dotierten Anoden der zweiten Generation für Elektrofahrzeuge noch in diesem Jahr vorstellen“, so Dr. Doron Myersdorf, CEO von StoreDot. IH

Entwicklungsmuster der ersten StoreDot-Batteriegeneration, die mit fünf Minuten Ladezeit auskommt. (Bild: StoreDot)

PORSCHE

TAYCAN-MODELL-PALETTE ERWEITERT

Nach Turbo S, Turbo und 4S hat Porsche mit dem Taycan nun die vierte Version des elektrischen Sportwagens vorgestellt. Dieses Modell vertraut auf Heckantrieb und ist mit zwei Batteriegrößen erhältlich – der serienmäßigen Performance-Batterie und der optionalen Performance-Batterie Plus.

Bild: Porsche

Als jüngster Vertreter der Modellfamilie verfügt der Taycan vom Start weg über die bei den anderen Versionen zum Modelljahreswechsel eingeführten Neuerungen. So erlaubt die Plug-&-Charge-Funktion bequemes Laden und Bezahlen ohne Karte oder App: Sobald das Ladekabel eingesteckt ist, kommuniziert der Taycan verschlüsselt mit der Plug-&-Charge-fähigen Ladestation. In der Folge startet der Ladevorgang automatisch. Gleiches gilt für die Bezahlung.

Als Sonderausstattungen sind wie bei den anderen Versionen unter anderem ein farbiges Head-up-Display und ein On-Board-Ladegerät mit einer Ladeleistung von bis zu 22 kW verfügbar. Mit Functions on Demand (FoD) können Taycan-Fahrer verschiedene Komfort- und Assistenzfunktionen nach Bedarf erwerben oder zeitlich befristet zubuchen. Dies funktioniert auch nachgelagert zum Kauf und zur ursprünglichen Konfiguration des Sportwagens. Ein Werkstattbesuch ist dank Online-Aktivierung nicht erforderlich. Aktuell ist das für die Funktionen Porsche Intelligent Range Manager (PIRM), Servolenkung Plus, Aktive Spurführung und Porsche InnoDrive möglich.

Serienmäßig ist eine einstöckige Performance-Batterie mit einer Bruttokapazität von 79,2 kWh verbaut. Auf Wunsch gibt es die zweistöckige Performance-Batterie Plus. Deren Bruttokapazität ist 93,4 kWh. Die Reichweite nach WLTP beträgt bis zu 431 beziehungsweise bis zu 484 km.

Aus dem Stand beschleunigt der Taycan in beiden Varianten in 5,4 s von null auf 100 km/h. Die Höchstgeschwindigkeit liegt bei ebenfalls einheitlichen 230 km/h. Die maximale Ladeleistung liegt bei bis zu 225 kW (Performance-Batterie) beziehungsweise bis zu 270 kW (Performance-Batterie Plus). Somit können beide Batterien in 22 Minuten und 30 Sekunden von fünf auf 80 Prozent geladen werden.

Das Fahrzeug verfügt über eine permanent erregte Synchronmaschine an der Hinterachse, die mit einer Länge von 130 mm ebenso lang wie die entsprechende Antriebskomponente des Taycan 4S ist. Der Pulswechselrichter an der Hinterachse arbeitet mit bis zu 600 A. Die Antriebsarchitektur umfasst neben der permanent erregten Synchronmaschine an der Hinterachse ein Zweiganggetriebe. Die maximale Rekuperationsleistung beträgt 265 kW.

Darüber hinaus kommt für das Fahrwerk des Taycan ein zentral vernetztes Steuersystem zum Einsatz. Die integrierte Fahrwerkregelung Porsche 4D-Chassis Control analysiert und synchronisiert alle Fahrwerksysteme in Echtzeit. Sowohl die serienmäßige Stahlfederung des Taycan als auch die optionale adaptive Luftfederung mit Dreikammer-Technologie werden durch die elektronische Dämpferregelung Porsche Active Suspension Management (PASM) ergänzt. ECK

SMARTE KOMPONENTEN OPTIMIEREN DAS ENERGIEMANAGEMENT

NEUE ARCHITEKTUR FÜR DAS BORDNETZ

(Bild: Shutterstock)

Das Automotive-Bordnetz steht vor tiefgreifenden Änderungen. Leoni unterstützt mit intelligenten elektronischen Komponenten neue Architekturkonzepte, die dabei helfen, Zukunftsthemen wie etwa das automatisierte und autonome Fahren auf die Straße zu bringen.

Von Lars Nilsson

Die Revolution bei den Antriebstechniken ist nicht der einzige Umbruch im Automobilbau. Themen wie das autonome Fahren und die Vernetzung der Fahrzeuge mit ihrer Umgebung sind weitere Megatrends, die wiederum den Wandel im Energie- und Daten-Bordnetz beschleunigen. Hybridantriebe mit 48-V-Elektromotor und elektrisch angetriebene Nebenaggregate benötigen eine sichere Energieversorgung, ebenso die Systeme zur Lenk- und Bremsunterstützung. Plug-in-Hybridantriebe oder rein batterieelektrische Antriebe stehen buchstäblich unter Hochspannung. Funktionen für automatisiertes und autonomes Fahren müssen ausfall- und funktionssicher sein, da sie zeitweise oder ganz die Fahrverantwortung übernehmen. Das heißt: Energieversorgung und Datenverteilung dürfen nicht ausfallen.

Diese Anforderungen kann das bisherige Bordnetz nicht erfüllen. Weder weist es die für funktionale Sicherheit geforderte Ausfallsicherheit auf, noch kann es das Energiemanagement so gewährleisten, dass immer und überall ausreichend elektrische Energie zur Verfügung steht. Auch bei der Bandbreite und Rechenleistung sind noch deutliche Fortschritte nötig, um den stark wachsenden Datenverkehr im Automobil sicher zu managen.

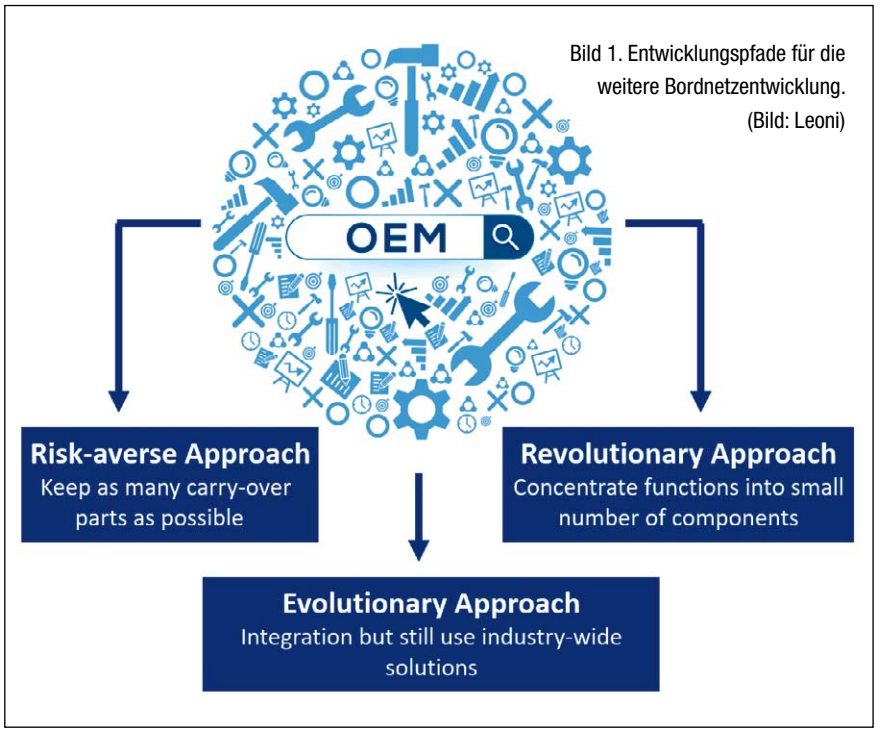


Bild 1. Entwicklungspfade für die weitere Bordnetzentwicklung. (Bild: Leoni)

ZUKUNFTSFÄHIGKEIT DURCH SYSTEM-KNOW-HOW

Der auf Bordnetzsysteme spezialisierte Zulieferer Leoni arbeitet bereits intensiv an neuen Lösungen. Grundlage ist eine von Intedis durchgeführte Studie, in der 34 Bordnetzarchitekturen – von realen Fahrzeugen sowie aus Vorentwicklungsprojekten und Konzeptstudien – gründlich auf ihre Zukunftsfähigkeit hin analysiert wurden. Etwa die Hälfte der Bordnetze erfüllte die künftigen Anforderungen an robuste Energieversorgung, Fehlertoleranz und praxisgerechte Funktionalität nicht. Bezüglich ihrer Architektur ließen sich die Bordnetze in drei Kategorien einteilen (**Bild 1**):

➔ Herkömmliche risikominimierte Architekturen, die sukzessiv erweitert werden, dabei aber rasch ihre

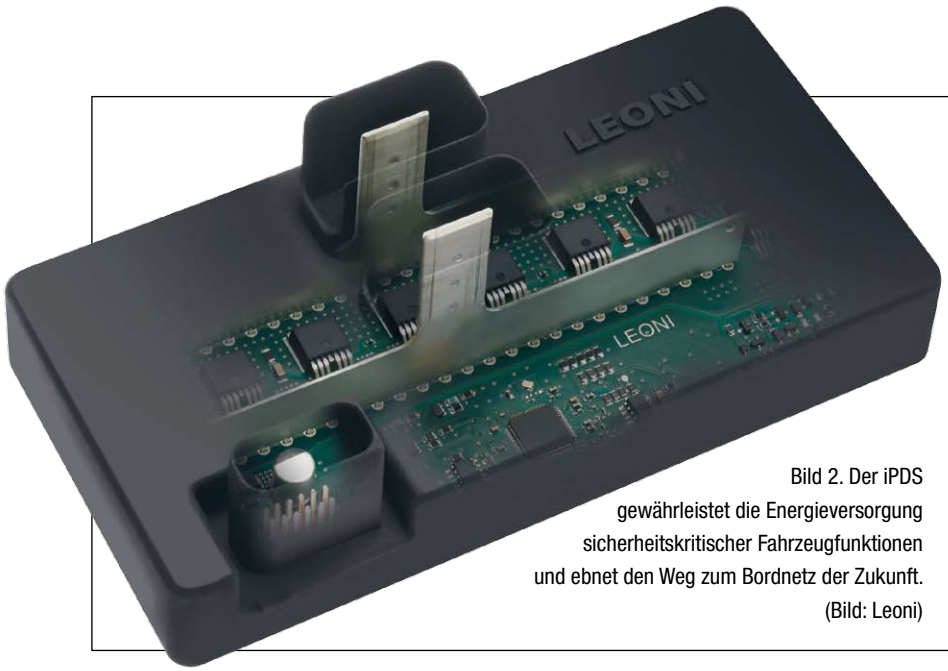


Bild 2. Der iPDS gewährleistet die Energieversorgung sicherheitskritischer Fahrzeugfunktionen und ebnet den Weg zum Bordnetz der Zukunft. (Bild: Leoni)

Komplexitäts-, Gewichts- und Kostengrenzen erreichen werden.

➔ Architekturen mit einer verstärkten Integration von Funktionen in größeren Steuergeräten, um deren Anzahl und somit die Komplexität des Bordnetzes zu reduzieren (evolutionärer Ansatz).

➔ Ein völlig neuer, revolutionärer Ansatz sind Architekturen mit wenigen großen Zentralrechnern, in denen die meisten Funktionen für Daten- und Energieverteilung integriert sind, ergänzt um kleinere Zonen-Controller für den Datenverkehr und das Energiemanagement in der Fahrzeugperipherie.

Sowohl die Studie als auch die eigenen Marktkenntnisse haben Leoni davon überzeugt, dass Architekturen mit wenigen großen Zentralrechnern die künftigen Anforderungen an das Bordnetz am besten abbilden. Als Zwischenschritt dahin integrieren bereits etliche Kunden mehr Elektronikfunktionen in bestehende Steuergeräte, um die Komplexität etwas einzudämmen.

Sein Know-how zieht Leoni aus zahlreichen Kundenprojekten. So wächst permanent die Kompetenz sowie die Erfahrung, an welcher Stelle der Bordnetzarchitektur und in welcher Form Elektronikkomponenten den besten Nutzen erbringen. Daneben arbeitet Leoni in mehreren Arbeitskreisen und Konsortien mit, die Einzelaspekte zum Bordnetz der Zukunft erforschen. Dazu zählen Arbeitskreise des VDA und der Gesellschaft für Innovation und Wissenstransfer „Bayern Innovativ“, in denen Empfehlungen und Standards definiert werden, mit denen das Bordnetz für die Anforderungen des automatisierten bzw. autonomen Fahrens nach Level 3, 4 oder 5 ertüchtigt wird.

DIE PRODUKT-ROADMAP

Die Basis auf dem Weg hin zur modernen Bordnetzarchitektur ist für Leoni das Energiemanagement. Schon heute bedienen die Sicherungs- und Relaisboxen die Kundenbedürfnisse nach Netzstabilität, Funktionsintegration und Kompaktheit. Mit – je nach Kundenanforderung – elektromechanischen Schmelzsicherungen, Relais oder elektronischen Sicherungskonzepten entsprechen sie den Kostenanforderungen der Kunden.

Aus den klassischen Sicherungsboxen heraus hat Leoni eine Roadmap für zukünftige Stromverteilungssysteme entwickelt. Die nächste Entwicklungsstufe verfügt über eine gewisse Intelligenz: Der iPDS (Intelligent Power Distribution Switch) und das Stromverteilungsmodul iPDM (Intelligent Power Distribution Module) sind bereits serienreif und Umfang von Vorentwicklungsprojekten. Sie unterstützen Kunden beim Übergang zu evolutionären und revolutionären Architekturkonzepten.

Nächster Entwicklungsschritt sind umfangreiche Zonen-Controller mit Energie- und Datenverteilungsfunktion. Diese komplexeren Module umfassen alle Funktionen von iPDS und iPDM sowie viele weitere mehr. Sie sollen ab der Mitte dieses Jahrzehnts den Übergang zu revolutionären Architekturen mit nur noch wenigen großen Zentralrechnern und einigen Zonen-Controllern beschleunigen.

Für Leoni könnte ein weiterer Entwicklungsschritt die Ergänzung der Zonen-Controller um eine kleine Stützbatterie und/oder einen DC/DC-Wandler sein. Pro Spannungsebene (12/24/48 V) im Fahrzeug würde eine solche Power Unit für Spannungsstabilität und somit für eine gewisse Autarkie sorgen.

KUNDENWÜNSCHE MODULAR ERFÜLLEN

Mit iPDS (**Bild 2**) und iPDM (**Bild 3**) lässt sich die gesamte Energieversorgung im Fahrzeug managen. Der elektronische Schalter iPDS trennt bei Ausfällen, Fehlern oder Kurzschlüssen

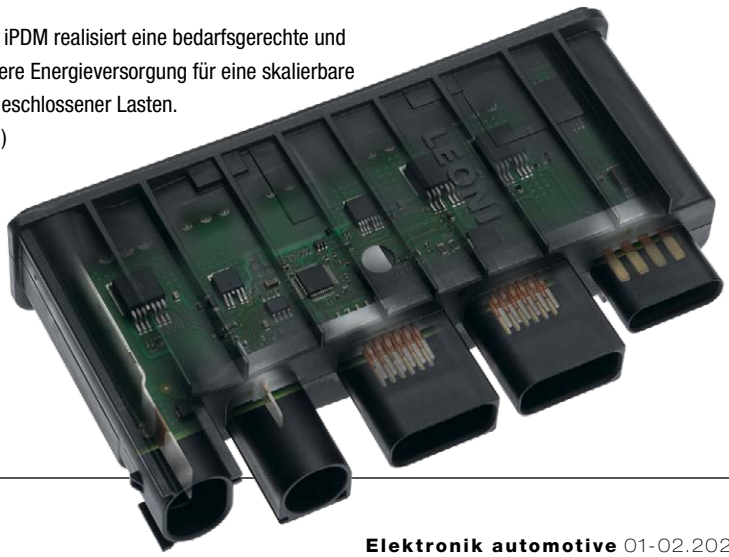


Bild 3. Das iPDM realisiert eine bedarfsgerechte und ausfallsichere Energieversorgung für eine skalierbare Anzahl angeschlossener Lasten. (Bild: Leoni)

nicht-sicherheitskritische Bordnetzteile schnell ab und stabilisiert so die Energieversorgung sicherheitskritischer Funktionen – etwa der elektrisch angetriebenen Lenk- und Bremsunterstützung oder von assistierenden oder automatisierten Fahrfunktionen.

Der intelligente elektronische Stromverteiler iPDM löst diese Aufgabe noch eleganter. Er regelt bei einer skalierbaren Anzahl von Verbrauchern im Fahrzeug die elektrische Energiezufuhr, kann bei Bedarf angeschlossene Leitungen auch gegen thermische Überlast absichern und so eine Rückwirkungsfreiheit erreichen.

Die Module iPDS und iPDM sind jeweils einzeln, aber auch in Kombination miteinander einsetzbar. Beide Komponenten bauen auf modularen Standardeinzelteilen auf. Das iPDM verfügt beispielsweise über folgende Kerneigenschaften:

➔ Die Temperaturfestigkeit liegt zwischen -40 °C und +105 °C. Die Dichtigkeitsklassen betragen entsprechend IPX9K/5K2.

➔ Durch den modularen Aufbau können verschiedene Spannungsebenen (12/24/48 V) problemlos realisiert werden; ebenso werden ASIL-Sicherheitsanforderungen von Level B bis D erfüllt.

➔ Die Modularität ermöglicht ferner die Aufnahme verschiedener Kommunikationsschnittstellen wie CAN, LIN, CAN-FD bis hin zu Automotive Ethernet und gewährleistet eine freie Wahl der Anzahl der Ausgänge (von 1 bis 50) und der nominalen Gesamtleistung (von 150 A bis 300 A) je nach Kundenanforderung.

Zudem entsprechen die Module iPDS und iPDM sämtlichen Anforderungen der internationalen OEMs sowie gängigen Standards (etwa ISO 26262 oder Automotive Spice 3) und erfüllen damit die Sicherheitsanforderungen für automatisiertes Fahren. Neben der Energieabschaltung und -verteilung verfügen sie über weitere Funktionen – beispielsweise Eigendiagnose, Leitungsdiagnose sowie eine Vorladefunktion für kapazitive Lasten. Die nachträgliche Erweiterung des softwaregestützten Funktionsumfangs sowie die Wahl zwischen dem Leoni-Betriebssystem und einem Autosar-konformen Betriebssystem sorgen für weitere Flexibilität.

Hinzu kommen interessante Sekundäreffekte. Dank der reversiblen elektronischen Absicherungsfunktion des iPDS und des iPDM ist kein Wartungszugang mehr erforderlich, was völlig neue Freiheiten beim Fahrzeugbauraum eröffnet. Zudem sind die beiden intelligenten Komponenten bis zur Hälfte kleiner und leichter als die herkömmlichen Sicherungs- und Relaisboxen. Ihre integrierte Leitungsdiagnose erlaubt es, Kabel mit kleineren Leitungsquerschnitten zu wählen, was weiteres Gewicht sowie Bauraum und Kosten einspart.

SYNERGIEN FÖRDERN SPAREFFEKT

Eine gut abgestimmte Gesamtlösung der Architektur könnte – abhängig vom spezifischen Kundenprojekt – bis zu 50 Prozent Bauraum und Gewicht sparen. Die durch Sicherheitsanforderungen und den Einsatz von Elektronik verursachten Mehrkosten lassen sich durch Einsparungen an anderen Orten des Bordnetzes teilweise kompensieren. Um derartige valide Einschätzungen treffen zu können, berücksichtigt Leoni das Gesamtsystem. In die Betrachtungen fließen nicht nur der Architekturentwurf samt Spezifikation, sondern auch Themen wie die Simulation, Software, Hardware, funktionale Sicherheit und die Erkenntnisse aus der Mitarbeit in maßgeblichen Standardisierungsgremien ein. IH

LARS NILSSON

studierte Elektrotechnik mit den Schwerpunkten Regelungs- & Steuerungstechnik sowie Informatik an der Universität Lund und an der Technischen Universität München. Im Anschluss war er bei Continental unter anderem für die Abteilung System Design in der Business Unit Hybrid and Electrical Vehicles verantwortlich. Dann wechselte er zu Faurecia, wo er für die Division Clean Mobility den Bereich New Technologies leitete. Seit 2018 arbeitete er bei Leoni und leitet das Tech Center Energy & Data Solutions.
Lars.Nilsson@leoni.com

PRÄVENTION MIT BATTERIEÜBERWACHUNG UND ZELL-BALANCING

MEHR AUSDAUER FÜR DAS E-MOBIL

(Bild: Shutterstock)

Die neue Generation an Elektrofahrzeugen überzeugt mit einer höheren Reichweite. Eine wichtige Rolle dafür spielt die Batterie als Herzstück des Stromers. Damit man weiß, dass diese ordnungsgemäß funktioniert, kommt ein Batterie-Managementsystem zum Einsatz. Hochspezialisierte ICs helfen bei der Umsetzung. Von Ralf Hickl

Selfcare boomt – der Markt für Produkte und Dienstleistungen, die zur Optimierung des Wohlbefindens und zur Steigerung der Leistungsfähigkeit beitragen, wächst konstant. Denn nur ein gut gepflegtes System, in das ein gewisser Vorsorgeaufwand gesteckt wird, kann auch langfristig die gewünschten Funktionen liefern. Gleiches gilt auch für die Lithium-Ionen-Batterie. Nicht nur, dass das Fahrzeug ohne sie nicht fahrtüchtig wäre, macht sie zudem einen erheblichen Anteil an den Gesamtkosten aus. Durch ihre Speicherkapazität ist sie maßgeblich für die Reichweite des Autos verantwortlich. Ihre Speicherkapazität, ihr Ladeverhalten und ihre tatsächliche Lebensdauer sind erfolgskritisch für Kaufentscheidungen – und die User Experience des Fahrers. Ladezeiten, Ladehäufigkeit und Betriebstemperaturen spielen für die optimale Nutzung der Batterien eine wesentliche Rolle.

BESTANDTEILE DES BATTERIE-MANAGEMENTSYSTEMS

Das Batterie-Managementsystem (BMS) besteht aus einer Battery-Management-Unit (BMU), die wiederum mit mehreren Cell Supervisory Circuits (CSC) kommuniziert. Die CSCs sind für die Überwachung der Vitalparameter und die gleichmäßige Ladungsverteilung zwischen mehreren Li-Ion-Zellen zuständig (**Bild 1**). Von zwei bis zu 240 Zellen lassen sich damit kontrollieren.

Durch den Mikrocontroller in der Battery-Management-Unit kommuniziert das BMS über den Fahrzeugbus mit übergeordneten Steuergeräten. Eine weitere Schnittstelle, die iso UART, sorgt für die Kommunikation mit der

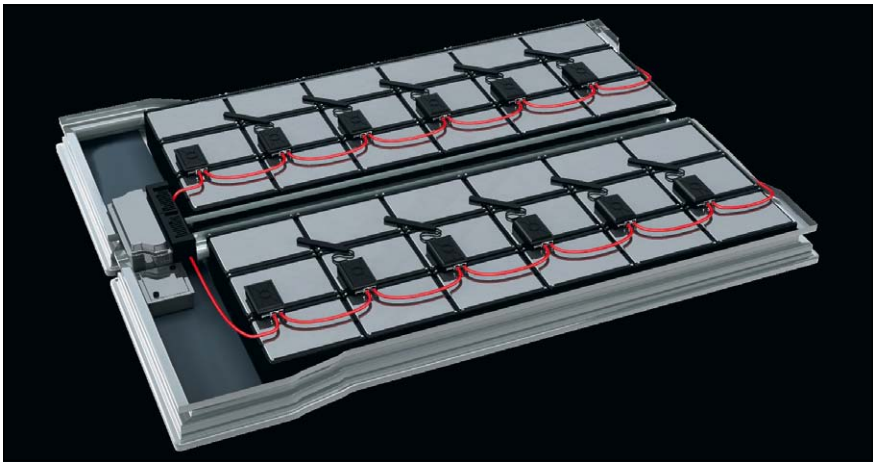


Bild 1. Batterie-Managementsystem mit Batterieüberwachungs- und Zell-Balancing-IC TLE9012AQU von Infineon. (Bild: Infineon)

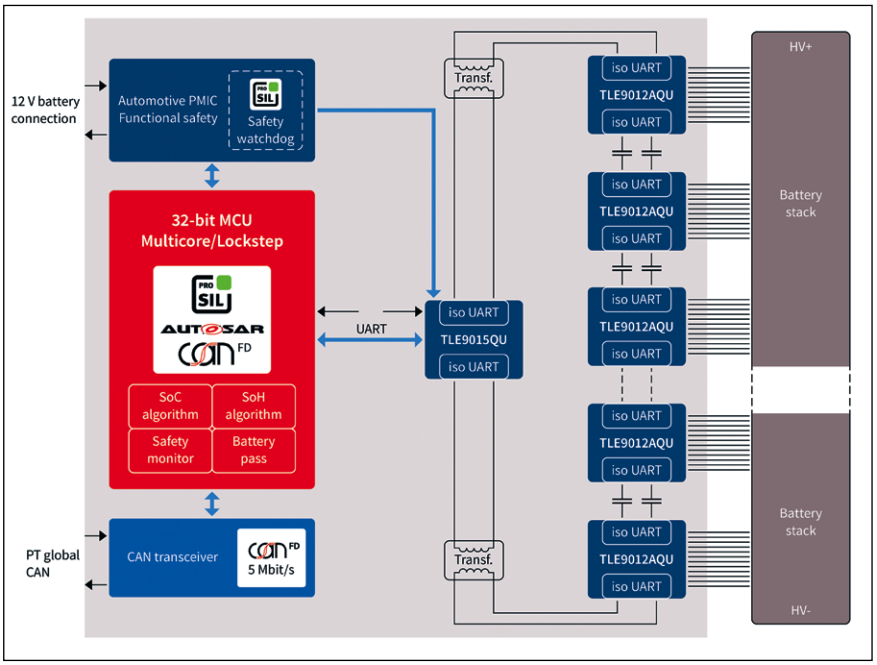


Bild 2. Blockschaltung des BMS mit Battery-Management-Unit (BMU) und Cell-Supervisory-Circuits (CSC). (Bild: Infineon)

Kette aus CSCs (**Bild 2**). In der BMU laufen die Messwerte jeder einzelnen Batteriezelle zusammen. Daraus ermittelt die BMU den Batteriestatus mithilfe spezieller Verfahren wie der Impedanzspektroskopie und stellt Zustandswerte wie den Ladezustand (State of Charge, SoC) und den Alterungszustand (State of Health, SoH) fest.

Für die Messung der Zellspannungen werden die CSCs eingesetzt. Die Lithium-Ionen-Zellen an einem CSC bilden einen Block. Dieser wird, als Gesamtheit und jede Zelle für sich, von einem Balancing-IC wie dem TLE9012AQU von Infineon überwacht und gesteuert. Der Baustein kann maximal zwölf Lithium-Ionen-Zellen überwachen. Der IC misst parallel jede einzelne Zellenspannung und verwendet dazu zwölf Sigma-Delta-Analog-Digital-Umsetzer (ADCs) mit maximal 16 bit Auflösung. Alle Zellspannungen werden zeitgleich, also synchron, mit großer Präzision gewandelt. Infineon spezifiziert eine Messgenauigkeit von +/-2 mV bei Raumtemperatur und eine Langzeitstabilität von +/-5 mV über die gesamte Temperatur und Lebensdauer. Ermöglicht werden diese langfristigen und engen Toleranzwerte durch Temperaturkompensation und den Einsatz eines Stresssensors auf dem Chip. Der Stresssensor hilft bei der Kompensation von Einflüssen durch das Verlöten und durch mechanische Belastungen auf der Platine.

Bei einer sehr genauen 16-bit-Messung für ein System mit 100 Zellen kann eine Abtastrate von 10 ms verwendet werden, trotz gleichzeitiger Ausführung von Diagnose und sicherheitsrelevanter Aufgaben.

Als weiteres Sicherheitsmerkmal des TLE9012AQU, und deshalb unabhängig von den Sigma-Delta-ADCs, überwachen zwölf Komparatoren jede einzelne Zelle auf Unter- oder Überspannung. Die Schwellwerte dafür sind über einen Digital-Analog-Wandler mit eigener Referenzspannungsquelle per Software einstellbar.

Ein weiterer Sigma-Delta-ADC wandelt die Blockspannung über allen Zellen an einem TLE9012AQU. Sind alle Spannungsmessungen in Ordnung, stimmt der gemessene Spannungswert über dem Block mit der Summe der erfassten Zellenspannungen des Blocks überein. Dieser zyklisch wiederkehrende Spannungsvergleich wird von der Komponente für Diagnosezwecke ausgewertet. Der Batterieüberwachungs- und Zell-Balancing-IC ist robust und übersteht die Kontaktierung an die geladenen Zellen (Hot-Plugging) ohne zusätzliche Schutzbeschaltung durch Zenerdioden.

LADUNGSAUSGLEICH AUF ZELLEBENE

Beim passiven Balancing wird einer Zelle mit Ladevorsprung per Halbleiterschalter, zum Beispiel einem integriertem N-Kanal-MOSFET, ein Widerstand zeitweilig parallelgeschaltet. Dadurch überlagert sich der Entladestrom dem Ladestrom so lange, bis die anderen Zellen aufgeholt haben. Dafür besitzt der TLE9012AQU integrierte Schalter mit einer Strombelastbarkeit von 150 mA pro Zelle. Alle Zellen lassen sich gleichzeitig balancieren. Reicht das nicht aus, dann kann der IC auch externe MOSFETs mit höherer Belastbarkeit ansteuern.

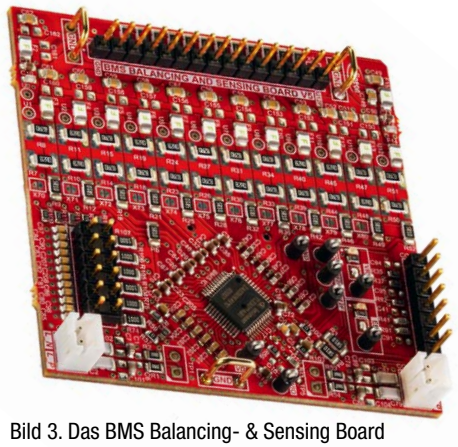


Bild 3. Das BMS Balancing- & Sensing Board TLE9012AQU_DTR_BMS2. (Bild: Infineon)

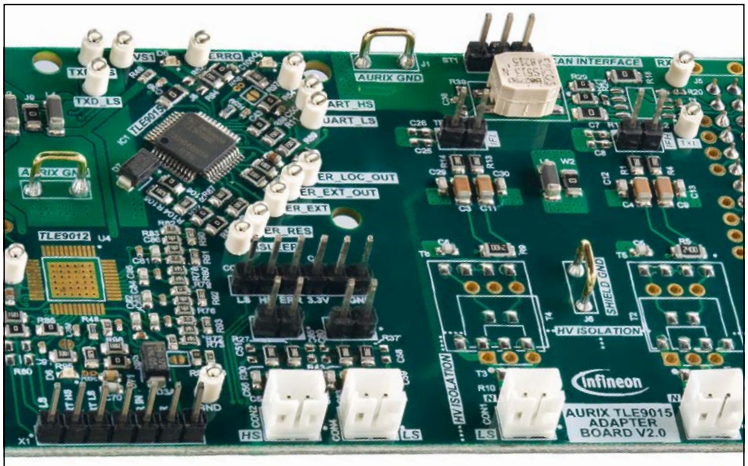


Bild 4: Das Interface-Board TLE9015QU_TRX_BRG. (Bild: Infineon)

Die Eigendiagnose des ICs erkennt Überstrom bezogen auf den Ausgleichsstrom beim Balancing, Zellüber- und Unterspannung sowie einen Bruch der Verbindungen (Open Load) zwischen den Batteriezellen und den Messeingängen des TLE9012AQU.

GERINGE EIGENERWÄRMUNG DURCH AUTOMATISCHE ANPASSUNG

Die Temperatur innerhalb der Batterie ist eine entscheidende Größe für deren Lebensdauer, die Sicherheit und für die Berechnungen ihres mathematischen Modells. Der TLE9012AQU ermöglicht Temperaturmessungen mit bis zu fünf NTC-Sensoren. Die AD-Wandlung führt der Sigma-Delta-ADC durch, der auch für die Wandlung der Blockspannung zuständig ist. Die Messungen erfolgen zyklisch ohne externe Anforderung/Auslösung über den Bus. Diese Eigeninitiative spart Bandbreite auf dem Kommunikationsbus. Der TLE9012AQU passt den Messstrom automatisch an den Widerstandswert der NTCs an. Durch dieses Autoranging entsteht ein Minimum an Eigenerwärmung an den Temperatursensoren.

SICHERE KOMMUNIKATION DANK CRC

Die Kommunikation zwischen CSCs mit unterschiedlichen Bezugspotenzialen oder einem übergeordneten Mikrocontroller auf BMU-Ebene (Host-Communication) basiert auf differenziellen Signalpegeln von Infineons iso UARTs. Die Datenübertragungsrate beträgt 2 Mbit/s. Für die sichere Kommunikation werden alle Nachrichtenrahmen mit einem 8-bit-Cyclic-Redundancy-Check (CRC) zur Verifikation der übertragenen Daten abgeschlossen. Für die galvanische Trennung zwischen den iso UARTs eignen sich wahlweise Kondensatoren oder Übertrager. Diesen empfiehlt Infineon auch zur Trennung von BMU- und CSC-Stapel. Als Leitungstreiber für die UARTs in der BMU sieht der Hersteller den iso UART Transceiver TLE9015QU vor.

Die einzelnen TLE9012AQU können in einer Ketten- oder Ring-Topologie verschaltet werden. Die Datendurchlaufzeit durch einen IC in der Kette beträgt dabei weniger als 100 ns. Die Ring-Topologie bietet Fail-Operational-Betrieb bei einer Unterbrechung im Ring. Die Kommunikation von bis zu 20 Slaves in der Kette/im Ring ist von Infineon getestet und wird gewährleistet. Die Ausbaustufe mit 20 Slaves reicht für nominale Bordnetzspannungen von 800 V. Das Kommunikationsprotokoll selbst unterstützt die Adressierung von bis zu 62 Stück der Bausteine in einer Reihe.

Die Kommunikation zwischen einem Mikrocontroller und einem der Transceiver auf gleichem Bezugspotenzial ist per UART auch ohne galvanische Trennung möglich. Die Kommunikationsrichtung ist Halbduplex über eine Leitung.

IT-SICHERHEIT PLANEN

Weil der Zellstapel sowohl geladen als auch entladen werden kann, muss die Strommessung bidirektional ausgelegt werden. Bei Systemen mit mehreren hundert Volt werden zwar mehrere CSCs und damit mehrere TLE9012AQU benötigt – aber wegen der Reihenschaltung der Zellen nur eine Stromsensorik. Um Chipfläche und damit Kosten zu sparen, ist deren Signalaufbereitung mit AD-Umsetzer normalerweise zentral ausgelagert und deshalb nicht im TLE9012AQU enthalten.

Die Komponente ist konform zu ISO 26262 und unterstützt Systeme bis ASIL C. Das Safety-Konzept beinhaltet zwei unabhängige Spannungsreferenzen auf dem Chip und einen separaten ADC für die Messung der Blockspannung an einem IC. Dazu kommen konfigurierbare Komparatoren, welche die Unter- und Überspannung an jeder Zelle erkennen. Zusätzlich ist die Kommunikation über die seriellen Schnittstellen mit CRCs abgesichert.

PASSENDE EVALUATION BOARDS

Die Zeit bis zur Marktreife ist gerade für innovationsgetriebene Unternehmen, wie im E-Mobility-Segment, eine elementare Komponente in der Projektplanung. Um ihren Kunden Optionen zur Optimierung dieses Zeitraums zu präsentieren, empfiehlt die Rutronik Automotive Business Unit unter ande-

```
Code Listing 1

001 !TABLE_START
002
003 ;CMD  Slave  addr   data   Delay  CAN_OUT
004 ;     (DEC)  (HEX)  (DEC)  (DEC)  (0/1)
005 ;=========================================
006 !SN                 8
007 !IH               300      5
008
009 ;CMD  Slave  addr   data   Delay  CAN_OUT
010 ;     (HEX)  (HEX)  (HEX)  (DEC)  (0/1)
011 ;=========================================
012 !WH      00     36  0001       0
013 !WH      00     36  0002       0
014 !WH      00     36  0003       0
015 !WH      00     36  0004       0
016 !WH      00     36  0005       0
017 !WH      00     36  0006       0
018 !WH      00     36  0007       0
019 !WH      00     36  0a08       0      1
020 !BWH     BF     01  0fff       0           // Enable all ADC channels
021 !BWH     BF     32  000c       0           // Read all Cell 0 -Cell 11 voltage
022
023 ;1st loop
024 ;CMD  Slave  addr   data   Delay  CAN_OUT
025 ;     (HEX)  (HEX)  (HEX)  (DEC)  (0/1)
026 ;=========================================
027 !CSTART
028 !BWH     BF      9  8044       5      0    // Round robin sync
029 !BWH     BF     18  ee00       5      1    // 16bit ADC sampling
030 !BRH     3F      1             0      1
031 !RH       1     31             0
032 !RH       2     31             0
033 !RH       3     31             0
034 !RH       4     31             0
035 !RH       5     31             0
036 !RH       6     31             0
037 !RH       7     31             0      1
038 !RH       8     31            20
039 !CYCLE    10000 times
040
041 !DISCONNECT
042 !TABLE_END
043 !EXECUTE

[1] A Reference. See the code examples at www.infineon.com
```

(Bild: Infineon)

Bild 5: Die Funktionen des TLE9012AQU lassen sich durch einfache Script-Befehle auswerten.

rem die Nutzung von, für das jeweilige Produkt passende, Evaluation Boards, wie sie zum Beispiel Infineon zur Verfügung stellt:

Das TLE9012AQU_DTR_BMS2 (**Bild 3**) ist als „BMS Balancing and Sensing Board" das Herzstück eines stapelbaren CSCs. Es bietet die Mess- und Balancing-Anschlüsse an den Stapel aus bis zu zwölf Batteriezellen und die entsprechenden galvanisch getrennten Kommunikationsschnittstellen für den Anschluss an zwei benachbarte CSCs.

Das TLE9015QU_TRX_BRG (**Bild 4**) beherbergt einen TLE9015QU mit zwei iso-UART-Transceivern mit galvanischer Trennung und dient als Bindeglied zwischen einem CSC mit TLE9012AQU und einem Mikrocontroller auf dem Board einer übergeordneten Steuerung, wie z. B. einer BMU.

Die beiden Evaluation Boards können in Kombination mit den Mikrocontroller-Boards KIT_AURIX_TC265_TFT oder KIT_AURIX_TC397_TFT betrieben werden. Für diese beiden Boards stellt der Hersteller spezielle Firmware zur Verfügung, die Advance Scripting beherrscht.

EINFACHE EVALUIERUNG DURCH ADVANCED SCRIPTING

Der Anwender kann die Funktionen des TLE9012AQU durch einfache Script-Befehle auswerten, ohne jedes Mal ein C-Programm kompilieren und einen Mikrocontroller neu flashen zu müssen. Der Script-Interpreter befindet sich in der Firmware auf den AURIX-Boards und erhält seine Befehle über eine serielle Schnittstelle, zum Beispiel von einem Terminalprogramm auf einem PC. Der Funktionsumfang des Interpreters beinhaltet unter anderem die Initialisierung des Bausteins, das Schreiben von Registerinhalten zur Konfiguration und das Auslesen von Messergebnissen während des Betriebs (**Bild 5**).

CELL BALANCING FÜR ELEKTROMOBILITÄT UND E-STORAGE

Der TLE9012AQU von Infineon zielt besonders auf Hochvoltbatterien, die aus mehreren Blöcken bestehen. Der Ladungsausgleich zwischen den Zellen geschieht passiv über Widerstände. Synchronisierte Spannungsmessungen im Zusammenspiel mit flotter Kommunikation ermöglichen die digitale Signalverarbeitung der Messergebnisse beispielsweise im Rahmen einer Impedanz-Spektroskopie. Damit das Gesamtsystem kostengünstig bleibt, sind die Komponenten zur Signalaufbereitung einer Strommessung nicht in jedem IC enthalten, sondern müssen nur einmal extern aufgebaut werden.

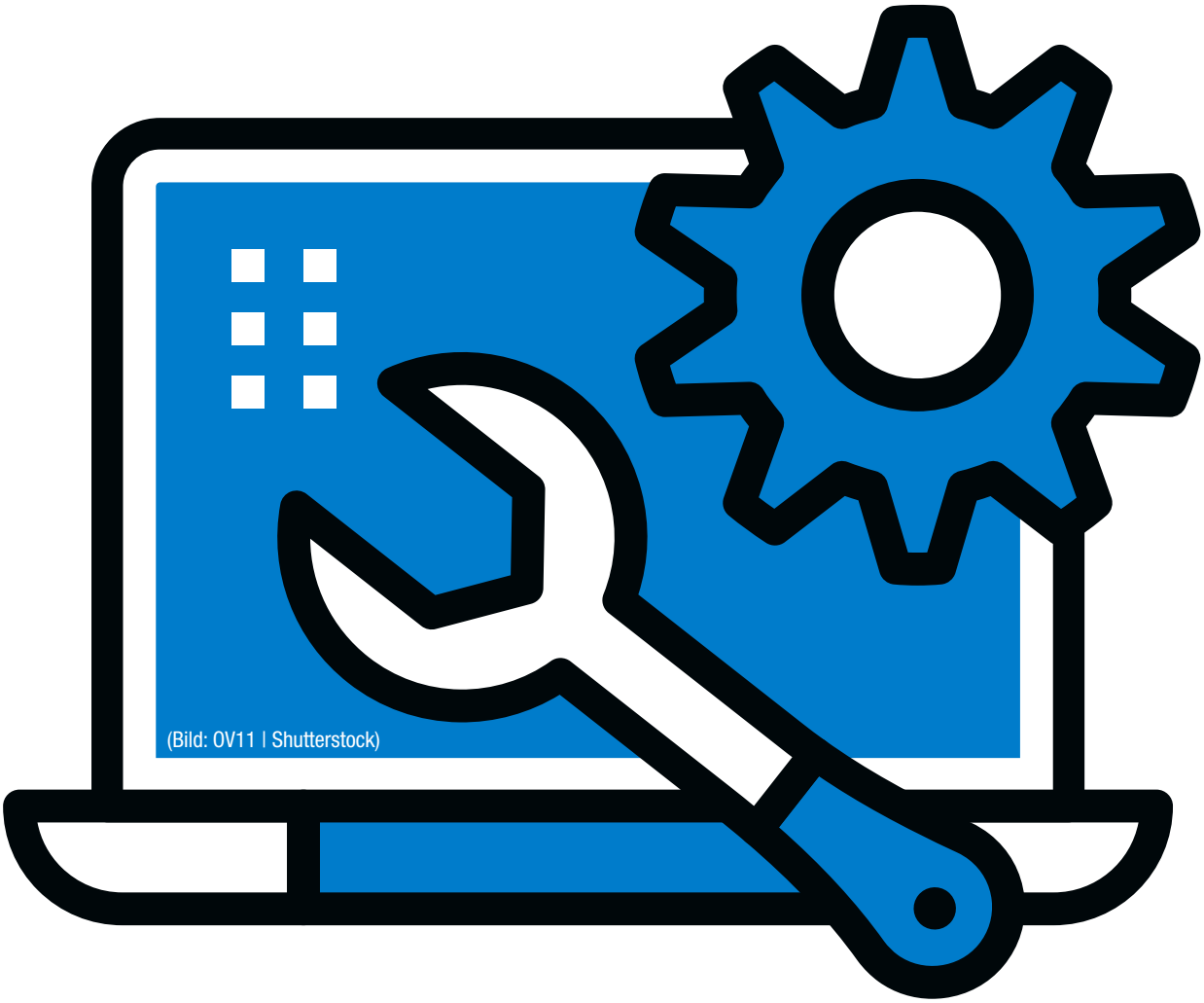
Für Rutronik Elektronische Bauelemente bedeutet der Infineon Cell-Balancing-IC eine wertvolle Ergänzung des Power-Portfolios – nicht nur für den Automotive-Sektor. Der TLE9012AQU ist in erster Linie für die Anwendung bei Hybrid-, Mild-Hybrid- und Plug-in-Hybrid- oder batterieelektrischen Fahrzeugen und E-Bikes gedacht. Er eignet sich aber auch für die Nutzung in Energiespeichersystemen im professionellen wie privaten Umfeld und bietet damit einen interessanten Ansatz zur Optimierung im Smart-Energy-Umfeld. ECK

RALF HICKL

arbeitet als Product Sales Manager in der Automotive Business Unit von Rutronik. Nach seinem Studium an der Universität Karlsruhe begann er als Serviceingenieur für elektrische Antriebe bei ABB. Nach sieben Jahren im Außendienst wechselte er 1998 zu Rutronik, wo er langjährige Erfahrungen im Produktmarketing von Mikrocontrollern sammelte.

REDUZIERUNG DER STRAHLUNGSEFFEKTE AUF AUTOMOBIL-ICs DURCH FORMALE ANALYSE

FEHLER SCHNELL IDENTIFIZIEREN



(Bild: OV11 | Shutterstock)

Unternehmen stehen vor der Herausforderung, funktionsreiche Produkte frist- und budgetgerecht zu liefern und gleichzeitig eine hohe Verfügbarkeit und einen einwandfreien Betrieb unter allen Bedingungen zu gewährleisten. Die Forderung nach hoher Verfügbarkeit treibt daher die Notwendigkeit einer robusteren Verifizierung zufälliger Hardwarefehler voran. Ein automatisierter, systematischer Ansatz zur Identifizierung der Anfälligkeit für Einzelereignisstörung durch strukturelle und statische Analyse ist dabei von großem Vorteil. Von Jacob Wiltgen

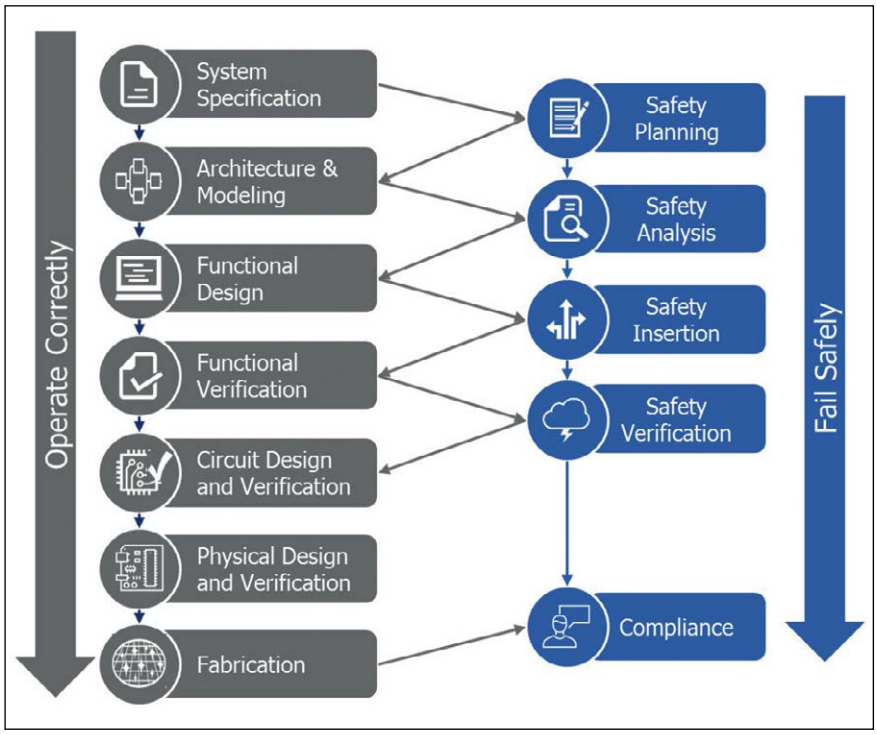


Bild 1. ASIC-Entwicklungsablaufänderungen für ISO 26262-Konformität. (Bild: Siemens EDA)

Die ISO 26262 ist der aktuelle Sicherheitsstandard, der die Sicherheitsaktivitäten und Arbeitsprodukte für die in einem Automobilsystem eingesetzte Elektronik regelt. Er verlangt, dass ein Design vor den Auswirkungen von strahlenbasierten Ereignissen geschützt ist, die ein Sicherheitsziel verletzen können. In Automobilanwendungen fallen strahlenbasierte Ereignisse unter den Begriff zufällige Hardwarefehler, die während der gesamten Nutzungsdauer eines Fahrzeugs unvorhersehbar sind. **Bild 1** zeigt einen allgemeinen ASIC-Entwicklungsablauf (in Grau dargestellt). Bei der Entwicklung einer ASIC nach ISO 26262 gibt es zusätzliche Phasen, die blau dargestellt sind.

Traditionell wurde eine fachkundige Beurteilung angewendet, um Fehlermodi aufgrund zufälliger Hardwarefehler zu identifizieren. Die Erstellung einer Failure Modes Effects Diagnostic Analysis (FMEDA) ist sowohl ein gängiger Ansatz als auch das Arbeitsprodukt bei der Abschätzung von Fehlermodi. Eine FMEDA berechnet anhand von Einsatzumgebung, Daten zur Ausfallrate und Zieltechnologie die Fehleranfälligkeit des Designs.

Es gibt verschiedene Nachteile, die mit der ausschließlichen Abhängigkeit von einer expertengesteuerten Fehleranalyse verbunden sind:

➔ Nicht wiederholbar
➔ Nicht gänzlich vollständig
➔ Skaliert nicht gut
➔ Schwierig in Bezug auf Drittanbieter-IP, Legacy-IP oder maschinengenerierten Code

Glücklicherweise wurden eine neue Verifizierungstechnologie und eine dreiphasige Methodik entwickelt, um Experten bei der Analyse, dem Schutz und der Prüfung eines Designs auf zufällige Fehlererkennung und -minderung zu unterstützen. Diese dreiphasige Methodik wird von der Automatisierung geleitet, um ein Design systematisch vor Fehlern zu schützen und anhand von Kennzahlen nachzuweisen, dass dieses vollständig erreicht wurde.

PHASE 1: FEHLERANALYSE

Die Ergänzung der Expertenanalyse um eine automatisierte strukturelle Analyse des Fehlerschutzes und dessen Logik sorgt für ein höheres Maß an Sicherheit und reduziert die für die Entwicklung eines robusten Designs erforderlichen Iterationen. Solche Lösungen ermöglichen es Ingenieuren, Metriken wie die Fehlerabdeckung (Diagnostic Coverage, DC) genau abzuschätzen, die angibt, wie viel des Designs vor Fehlern geschützt ist. Dieser stärker automatisierte, strukturelle Ansatz bietet im Vergleich zu manuellen Fehleranalyseansätzen viele Vorteile.

Die Fehleranalyse lässt sich in zwei Aktivitäten unterteilen. Die erste Aktivität ist eine erste Design-Bewertung, die die Genauigkeit von Expertengutachten und Kennzahlen wie die Ausfallrate (Failure in Time, FIT) und DC validiert. Die Informationen zur strukturellen Konnektivität werden verwendet, um Bereiche der Konstruktion zu identifizieren, die von Fehlern betroffen sein können, und um entsprechend zu ermitteln, wie effektiv die Fehlerschutzlogik bei der Abschwächung ist. Dieser Bottom-up-Ansatz punktet mit einer hohen Genauigkeit verglichen mit einer Top-down-Analyse, die von Experten durchgeführt wird. Durchgehende Analyse (**Bild 2**) und Instanzanalyse stellen die beiden Analysearten dar, die zur Berechnung von FIT und DC verwendet werden.

Die durchgehende Strukturanalyse schätzt die Fehlerabdeckung von End-to-End-Schutzmechanismen, die die Mehrzykluslogik abdecken. Mit dieser Technik wird die Fehlerabdeckung für alle Gates und Zustandselemente zwischen Erzeugungs- und Prüfpunkten von Schutzmechanismen berechnet. Datenpfad-Parität und CRC sind gängige Beispiele für mehrzyklische Schutzmechanismen.

Die Instanzanalyse (**Bild 3**) schätzt die Wirksamkeit des Fehlerschutzes auf Hardwaremechanismen, die einzelne Instanzen wie Module oder Flip-Flops schützen. Mit dieser Technik wird die Fehlerabdeckung für die Schutzmechanismen zum Schutz von Zustandselementen, Modulen und deren lokalisierten Logikkegeln abgeschätzt. Drei gängige Beispiele für den Schutz auf Instanzebene sind Flip-Flop-Paritätsketten, Duplizierungen auf voller Modulebene und Speicher-ECCs.

Falls bei der anfänglichen Abdeckungsbeurteilung Lücken im Fehlerschutz festgestellt werden, muss eine Strategie zur Schadensminderung abgeleitet

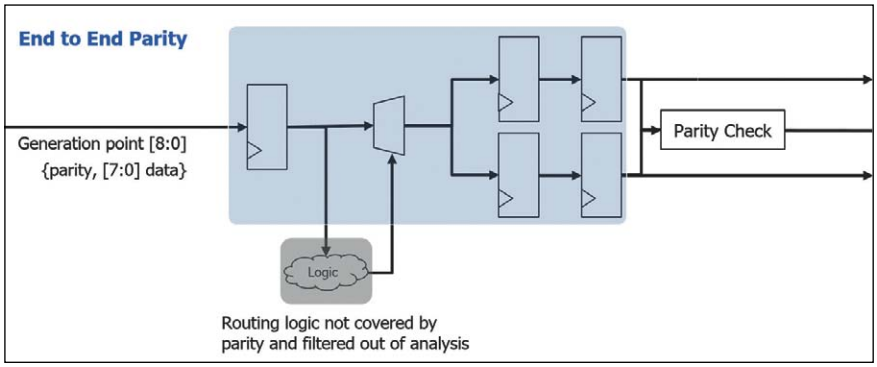


Bild 2. Durchgehende Strukturanalyse (Bild: Siemens EDA)

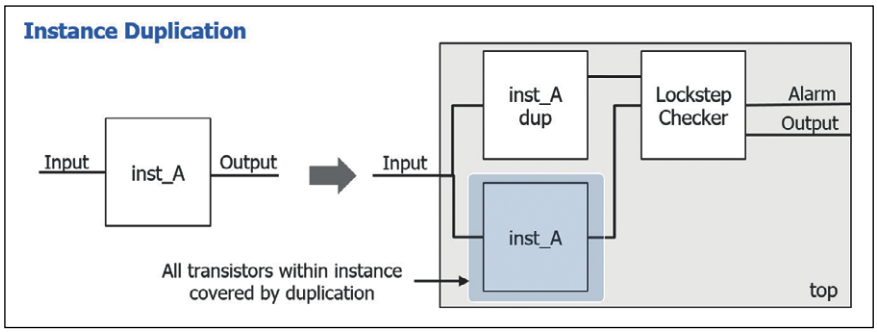


Bild 3. Instanz-Strukturanalyse (Bild: Siemens EDA)

werden. Diese Strategie besteht in der Regel darin, vorhandene Hardware zum Fehlerschutz zu modifizieren oder zusätzliche Hardware vorzusehen.

Die zweite Aktivität ist die Sicherheitsuntersuchung. Ziel der Untersuchung ist es, eine Schadensminderungsstrategie zu identifizieren, die das gewünschte Maß an Fehlerschutz bietet und gleichzeitig die Anforderungen an Leistung und Bereich erfüllt. Bei der Entscheidung für eine Sicherheitsstrategie stehen viele verschiedene Sicherheitsmechanismen zur Auswahl, die jeweils ein einzigartiges Maß an Effektivität und Einfluss auf Leistung und Bereich haben. Das Verständnis dieser unterschiedlichen Wirksamkeiten und Auswirkungen ist entscheidend für die Erforschung verschiedener Minderungsstrategien. Einige Fehlerminderungstechniken können Fehler auch erkennen, während andere fortschrittlicher sind und einzelne Bitfehler korrigieren können.

In diesem Schritt führen Ingenieure eine Reihe von „Was-wäre-wenn"-Experimenten durch, um die Auswirkungen verschiedener Fehlerminderungsstrategien auf die Leistungs-, Bereichs- und Fehlerabdeckung zu verstehen. Diese Untersuchung wird ohne Modifikation des Designs durchgeführt, sodass mehrere parallele Analysen möglich sind. Das Ergebnis der Erforschung ist ein klares Verständnis für die Design-Verbesserungen, die erforderlich sind, um die Sicherheitsanforderungen zu erfüllen.

PHASE 2: FEHLERSCHUTZ

Fehlerschutzschaltungen gibt es in verschiedenen Ausführungen, jede mit einem eigenen Grad an Effektivität bei der Erkennung von Fehlern. In der Regel werden Schutzmechanismen als ausfallsicher oder betriebssicher eingeteilt. Ausfallsichere Mechanismen sind in der Lage, Fehler zu erkennen, garantieren jedoch nicht den korrekten Betrieb. Betriebssichere Schutzmechanismen sind in der Lage, zufällige Hardwarefehler zu erkennen und zu beheben. Der Ausfallschutz erfordert in der Regel Redundanz und eine höhere Ressourcenauslastung, bietet jedoch den zusätzlichen Vorteil, dass das Design durch den Fehler weiterhin ordnungsgemäß funktioniert. Nach dem Einfügen muss eine logische Äquivalenz zwischen dem ursprünglichen und dem erweiterten Design durchgeführt werden, um sicherzustellen, dass keine funktionale Abweichung eingeführt wurde.

PHASE 3: FEHLERVERIFIZIERUNG

Fehleranalysen können belegen, dass ein Design geschützt ist, sobald Schutzmechanismen vorhanden sind. Aber es ist wichtig nachzuweisen, dass das Design in einem fehlerfreien Zustand funktioniert. Die Fehlerverifizierung muss durch Simulation des Verhaltens des Designs im fehlerhaften Zustand erfolgen, um den ordnungsgemäßen Betrieb zu gewährleisten. Ein einfaches Beispiel wäre ein CRC-Fehler, der zum Ausfall eines Wiederherstellungsmechanismus führt. Selbst wenn die CRC-Logik korrekt implementiert wurde, könnte ein Wiederherstellungsmechanismus, der die erneute Übertragung eines Pakets verursacht hat, fehlerhaft sein. Die Fehlerverifizierung schließt den Kreis, indem sicherstellt wird, dass die Konstruktion robust ist und auch bei Fehlern korrekt funktioniert.

Primäres Ziel der Fehlerverifizierung ist es, Fehler in ein Design zu injizieren, die Fehler in der Simulation zu propa-

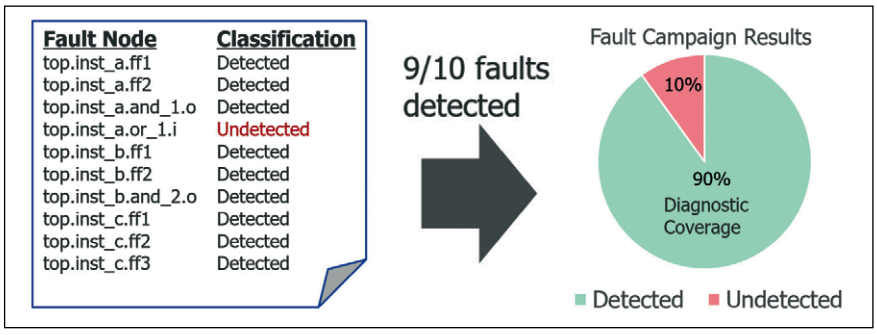


Bild 4. Berechnung der Fehlerabdeckung aus der Fehlerklassifizierung. (Bild: Siemens EDA)

gieren und festzustellen, ob der Fehler erkannt wird. Anhand der Ergebnisse der Fehlerinjizierung wird die Gesamtfehlerabdeckung berechnet, indem die von den Schutzmechanismen erkannten Fehler mit dem gesamten Fehlerzustandsraum verglichen werden (**Bild 4**). Es ist nicht ungewöhnlich, dass Konstruktionen Millionen potenzieller Fehlerknoten aufweisen. Daher müssen alle Mittel ergriffen werden, um die Fehlerliste auf ein Minimum an Fehlerknoten zu reduzieren und dann die Automatisierung zu nutzen, um Fehler so effizient und effektiv wie möglich zu injizieren. Um diese Lücken und Herausforderungen anzugehen, wurden spezielle Fehlersimulatoren entwickelt. Zum Erzielen der maximalen Leistung werden drei Stufen der Gleichzeitigkeit eingesetzt. Zunächst werden Fehler mit einem simultanen Fehlerinjektionsalgorithmus injiziert, der Parallelität über einen einzelnen Thread bietet. Multithreading und Multicore sorgen für eine weitere Stufe der Fehlerinjizierung. Schließlich werden Fehlerinjektionsaufträge weiter über das größere Maschinenraster verteilt. Das Fehlermanagement überwacht die Auftragsverteilung und die Zusammenführung der resultierenden Daten.

AUTOMATISIERTE PROZESSE MIT VORTEILEN

Die zunehmende Größe und Komplexität von Designs erfordert den Einsatz stärker automatisierter und skalierbarer Techniken bei der Entwicklung von ICs, die in Automobilanwendungen zum Einsatz kommen. Manuelle Prozesse zur Entwicklung und Validierung von Sicherheitsmechanismen skalieren nicht für sehr große Designs, sind nicht schlüssig oder erschöpfend und lassen sich nicht leicht wiederholen. Mentor, ein Siemens-Unternehmen, bietet eine Reihe von automatisierten, formalen Verifizierungs- und Analysetools sowie Apps, die einen viel effektiveren, hochwertigeren und wiederholbaren Prozess für Fehleranalyse, Schutz und Verifizierung bieten. Als Teil des Siemens Xcelerator-Portfolios stattet diese Lösung Projektteams mit der Technologie und den Informationen aus, die sie benötigen, um heute fehlertolerante Designs der nächsten Generation zu schaffen. ECK

JACOB WILTGEN

ist Functional Safety Solutions Manager bei Siemens EDA und verantwortlich für die Definition und Ausrichtung von Technologien für funktionale Sicherheit im gesamten Portfolio der IC-Verifizierungslösungen. Er besitzt einen Bachelor of Science in Elektro- und Computertechnik der University of Colorado Boulder. Vor seiner Tätigkeit bei Siemens EDA (ehemals Mentor) hatte Wiltgen verschiedene Design-, Verifikations- und Führungspositionen im Bereich der IC- und SoC-Entwicklung bei Xilinx, Micron und Broadcom inne.


(Bild: Shutterstock)

ISO/SAE 21434 UND CYBERSICHERHEIT IM FAHRZEUG

HAND IN HAND

Es gibt keine funktionale Sicherheit ohne Datensicherheit. Die Norm ISO/SAE 21434 flankiert daher zukünftig die Norm ISO 26262 und fordert Maßnahmen zur Sicherstellung der Cybersicherheit über den gesamten Lebenszyklus elektronischer Produkte hinweg. Entsprechend sind alle Unternehmen der Wertschöpfungskette von der neuen Norm betroffen.

Von Sergio Marchese

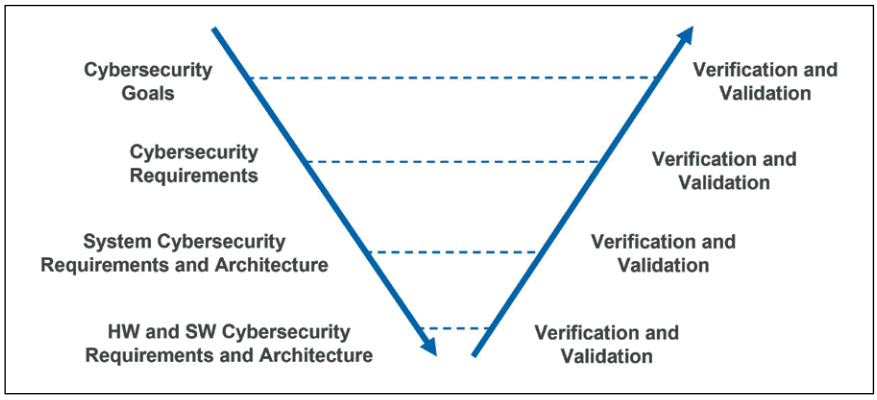
Elektronische Systeme für vernetzte autonome Fahrzeuge (Connected Autonomous Vehicles, CAVs) und fortgeschrittene Fahrerassistenzsysteme (ADAS) verwenden ICs. Ein modernes Fahrzeug kann mehr als 100 darauf aufbauende Steuergeräte (ECUs) enthalten, die sicherheitsrelevante Systemfunktionen wie Bremsen und Lenkung steuern. Die Norm für funktionale Sicherheit ISO 26262 stellt strenge Anforderungen an die verwendeten elektronischen Komponenten, etwa ASICs oder FPGAs. Sicherheit lässt sich dabei nicht durch nachträgliche Maßnahmen gewährleisten. Dementsprechend deckt die Norm den gesamten Lebenszyklus von ICs, einschließlich der Designphase vor der Produktion des ersten Siliziums ab. Obwohl noch viele Herausforderungen bewältigt werden müssen, haben die Lieferanten von Halbleiter-IP (Intellectual Property) und Automotive-Chips enorme Fortschritte bei der Ausrichtung ihrer Prozesse und Organisationen an die Anforderungen der ISO 26262 gemacht. Die nächste große Herausforderung ist nun die Gewährleistung der Datensicherheit.

WARUM CYBERSECURITY?

Cyberangriffe auf Fahrzeugsysteme können katastrophale Folgen haben. Der berühmte Jeep-Hack von Charlie Miller und Chris Valasek rückte dieses Thema ins Rampenlicht. Ein erfolgreiches Car-Hacking könnte auf eine ganze Fahrzeugflotte ausgedehnt werden und viele Menschenleben gefährden. Darüber hinaus geht es auch um die Privatsphäre der Autobesitzer und den Schutz des geistigen Eigentums und anderer Assets der Autohersteller und ihrer Lieferkette. Im Gegensatz zur funktionalen Sicherheit steckt die Cybersicherheit im Automobilbereich jedoch noch in den Kinderschuhen. Die kommende Norm ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering verspricht eine Modernisierung und Harmonisierung der Cybersicherheitsaktivitäten entlang der gesamten Wertschöpfungskette der Automobilindustrie. Die Norm befindet sich derzeit noch in der Entwicklung. Eine Entwurfsversion steht jedoch bereits zur Verfügung. Die Veröffentlichung der ersten Ausgabe, die eigentlich für Ende 2020 erwartet wurde, wird sich aber aufgrund der COVID-19-Situation bis in den Jahresanfang 2021 verzögern.

Dieser Artikel beschreibt die zentralen Aspekte der Norm ISO/SAE 21434, darunter die Anforderungen an eine Bedrohungsanalyse sowie Risikobewer-

tung (Threat Analysis and Risk Assessment, TARA) und erklärt die Konzepte des Risikowerts und der Cybersicherheits-Gewährleistungsstufen (Cybersecurity Assurance Levels, CAL). Darüber hinaus beleuchtet er die Notwendigkeit einer Strategie zur Reaktion auf Cybersicherheitsvorfälle, die mehrere Beteiligte der Wertschöpfungskette betreffen können. Im Folgenden wird die ISO/SAE 21434 mit der ISO 26262 verglichen, was insbesondere den Ingenieuren den Einstieg erleichtern wird, die sich bereits mit der funktionalen Fahrzeugsicherheit beschäftigt haben. Schließlich wird auch auf den Bedarf an neuen Werkzeugen und automatisierten Lösungen eingegangen, welche die Entwicklung von ICs in Übereinstimmung mit der ISO/SAE 21434 unterstützen.



(Bild: OneSpin)

Bild 1. Cybersicherheitsmaßnahmen während der Produktentwicklung werden auf den verschiedenen Abstraktionsebenen ergriffen. Es ist denkbar, einem V-Modell-Ansatz zu folgen, bei dem die Anforderungen nach und nach verfeinert werden, um Hardware- und Softwarekomponenten abzudecken.

HARDWARESICHERHEIT

Die Norm ISO/SAE 21434 befasst sich mit dem gesamten Lebenszyklus elektrischer und elektronischer Systeme, die für den Einsatz in Straßenfahrzeugen bestimmt sind – von der Konzeptphase bis zur Außerbetriebnahme. Anders als die ISO 26262 hat die Norm keine separaten Abschnitte für Hardware-, Software- und Systementwicklung. Diese Themen werden jedoch alle abgehandelt. Ähnlich wie die ISO 26262 enthält die Norm Bestimmungen für die Entwicklung kontextunabhängiger Komponenten, die in unterschiedlichen Systemen und Anwendungen verwendet werden könnten. In der ISO 26262 und im Sicherheitsbereich werden sie als Safety Elements out of Context (SEooCs) bezeichnet.

Die Produktentwicklung kann einem V-Modell-Ansatz folgen (**Bild 1**), bei dem jede Phase, von der Definition des Elements und seiner Sicherheitsziele bis hin zum Hardware- und Softwaredesign, eine entsprechende Validierungs- und Verifikationsaktivität und damit verbundene Arbeitspunkte aufweist, ähnlich der ISO 26262.

Während sich die Datensicherheit in der Vergangenheit vornehmlich mit der Software beschäftigte, hat sich gezeigt, dass Angriffe zunehmend Schwächen und Verwundbarkeiten der Hard- und Firmware nutzen. Die MITRE CWE-Datenbank hat kürzlich mit der Version 4.0 einen Abschnitt eingeführt, welcher der Hardware gewidmet ist. In der Version 4.2 der Datenbank sind dort bereits 75 Einträge zu finden. Die Hardwareentwicklung ist auf eine globale, fragmentierte Lieferkette angewiesen, an der Dienstleistungsunternehmen, Halbleiter-IP- und IC-Lieferanten, Foundries und Distributoren mitwirken. Die Vertrauenswürdigkeit und Qualität von Third-Party-Komponenten lässt sich dabei nicht als gegeben voraussetzen, sondern muss durch geeignete Verfahren und Nachweise belegt werden. Eine „Security-by-Design"-Methodik und eine strenge Verifikations- und Zuverlässigkeitsstrategie vor der Produktion des ersten Siliziums sind entscheidend, um die Vertrauenswürdigkeit zu stärken und objektive, auditierbare Metriken und Berichte zu erstellen. Dedizierte EDA-Lösungen, die auf die Absicherung der funktionalen Korrektheit und der Vertrauenswürdigkeit sowie der Datensicherheit von Halbleiter-IP und ICs abzielen, wie sie von OneSpin Solutions angeboten werden, können zur Implementierung automatisierter, skalierbarer Prozesse zur Gewährleistung der Hardwaresicherheit verwendet werden.

BEDROHUNGSANALYSE UND RISIKOBEWERTUNG

Threat Analysis and Risk Assessment (TARA) ist das sicherheitsrelevante Gegenstück zum Hazard Analysis and Risk Assessment (HARA) nach ISO 26262. Es ist wichtig, die Assets eines Systems und deren Cybersicherheitseigenschaften, einschließlich der Vertrauenswürdigkeit, Integrität und Verfügbarkeit, aufzulisten. Vielleicht noch anspruchsvoller ist die Identifizierung von Bedrohungsszenarien, die die Ziele der Cybersicherheit verletzen könnten, sowie die Durchführung einer Risikobewertung. Die ISO/SAE 21434 fordert, dass für jedes identifizierte Bedrohungsszenario ein Risikowert bestimmt wird. Das ist eine Zahl zwischen 1 (geringstes Risiko) und 5 (höchstes Risiko). Das mit einem Bedrohungsszenario verbundene Risiko hängt von der Durchführbarkeit des Angriffs und seinen Auswirkungen ab. Wenn für den Angriff ein Team fachkundiger Hacker und kostspielige Ausrüstung erforderlich ist, dann ist das Risiko geringer als bei einem Angriff, den jeder ausführen kann und der zum gleichen Schaden führt. Im schlimmsten Fall ist der Angriff leicht durchführbar und hat schwerwiegende Folgen. Die Norm schreibt keine bestimmte Methode zur Analyse des Systems und zur Berechnung von Risikowerten vor, aber sie gibt einige Orientierungshilfen und nennt Beispiele. Wie nicht anders zu erwarten, verdienen Bedrohungsszenarien, die zu schwerwiegenden Folgen führen könnten, mehr Aufmerksamkeit und erfordern möglicherweise die Spezifikation und Implementierung von Kontrollmechanismen zur Risikominderung (**Bild 2**).

Der CAL ist ein Attribut, das mit einem System, einer Komponente oder einem

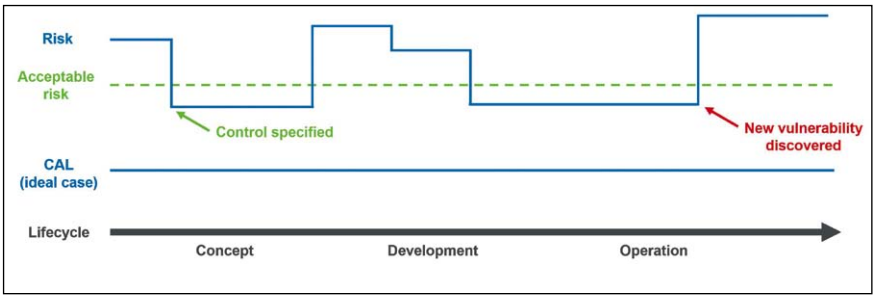


Bild 2. Der mit einem Bedrohungsszenario verknüpfte Risikowert kann sich während des Lebenszyklus eines E/E-Systems ändern. Wenn zum Beispiel eine neue Schwachstelle entdeckt wird, kann er plötzlich steigen. CALs hingegen bleiben, zumindest im Idealfall und falls sie ursprünglich korrekt bestimmt wurden, konstant. (Bild: OneSpin)

bestimmten Cybersicherheitsziel verknüpft werden kann. Er drückt den Grad an Sicherheit aus, der für Assets erforderlich ist. Es gibt vier CALs – wobei CAL1 das niedrigste und CAL4 das anspruchsvollste Level ist. Je nach CAL-Zielvorgabe können bestimmte Cybersicherheitsaktivitäten ausgelassen oder weniger strikt durchgeführt werden. Eine als CAL4 klassifizierte Komponente deutet darauf hin, dass auf ihr gegebenenfalls kritische Funktionen ausgeführt werden, die einen hohen Sicherheits- und Schutzlevel für die Assets erfordern. CALs sind wichtig, um Cybersicherheitsaktivitäten entsprechend der angestrebten Sicherheitsstufe zuzuschneiden und die Kommunikation zwischen den Beteiligten und Parteien der Lieferkette zu vereinfachen. Ingenieure, die mit ISO 26262 vertraut sind, werden starke Ähnlichkeiten zwischen CALs und Automotive Safety Integrity Levels (ASILs) erkennen.

Obwohl CALs und Risikowerte verwandte Konzepte sind, weisen sie erhebliche Unterschiede auf. CALs werden in einem Anhang der Norm beschrieben – einem informativen, aber nicht normativen Abschnitt. Das könnte sich aber in der ersten Auflage der Norm ändern. Offenbar sind CALs ein kontroverses Thema innerhalb des Ausschusses, der die Norm entwickelt, und Gegenstand einer anhaltenden Debatte. Das Konzept des Risikowerts und seine Bestimmung ist dagegen Teil der Anforderungen der ISO/SAE 21434. Außerdem sind CALs, zumindest im Idealfall, konstant, während sich die Risikowerte während des Produktlebenszyklus ändern können. Ein Risikowert, der als zu hoch erachtet wird, kann zusätzliche Kontrollen erfordern, bis er auf ein akzeptables Niveau reduziert ist.

Es gibt Software-Tools zur Unterstützung und Automatisierung von TARAs bei Automobil- und anderen Anwendungen, zum Beispiel Yakindu Security Analyst von Itemis. Sie können zur Modellierung komplexer Systeme sowie ihrer Sicherheitsressourcen und -eigenschaften, zur Bestimmung von Sicherheitszielen, zur Analyse von Bedrohungen, zur Risikobewertung und zur Verfolgung von Abhängigkeiten zwischen Komponenten (Hardware- und Software) verwendet werden.

REAKTION AUF VORFÄLLE

Es ist von entscheidender Bedeutung, neue Schwachstellen, die in Hardware- und Softwarekomponenten von Automotive-Systemen stecken, zu entdecken, kontinuierlich zu überwachen und die Risikowerte neu zu bewerten. Falls erforderlich, müssen Abhilfemaßnahmen ergriffen werden. Das ist ein Bereich, in dem sich die ISO/SAE 21434 grundlegend von der ISO 26262 unterscheidet, weil letztere kein Konzept für die Reaktion auf Sicherheitsvorfälle kennt. Berücksichtigt man, dass bei Automotive-Hardwarekomponenten zwischen dem Einsatz und Ende des Supports viele Jahre liegen können und eine komplexe Lieferkette dahintersteht, stellen die Überwachung der Cybersicherheit und die Reaktion auf Sicherheitsvorfälle eine Herausforderung dar. Eine gründliche Verifikation der Designs und die Durchführung von Absicherungsmaßnahmen im Pre-Silicon-Zeitraum können helfen, die Kosten dafür deutlich zu senken. Eine effiziente, von geeigneten Werkzeugen unterstützte Post-Silicon-Analyse ist ebenfalls von entscheidender Bedeutung, um die zugrunde liegende Ursache einer Schwachstelle zu ermitteln und Abhilfemaßnahmen zu entwerfen bzw. zu validieren. Die Werkzeuge von OneSpin werden zum Beispiel auch zur Analyse und Fehlerbeseitigung von Post-Silicon-Fehlern und Mängeln im Hardwaremodell eingesetzt.

FRÜHZEITIG AGIEREN

Cybersicherheit im Automobilbereich ist ein heißes Thema. In den kommenden Jahren werden alle Beteiligten der Elektronikwertschöpfungskette ihre Prozesse und Organisationen entsprechend der ISO/SAE 21434 gestalten müssen. Eine frühzeitige Adaption verschafft einen erheblichen Vorteil gegenüber der Konkurrenz. ECK

SERGIO MARCHESE

ist Technical Marketing Manager bei OneSpin Solutions. Er begann seine Karriere bei Infineon Technologies, wo er die TriCore CPU, eine weit verbreitete Architektur für Automobil-SoCs, mithilfe von Simulationen und formalen Methoden verifizierte. Seitdem hat er an unterschiedlichen Projekten in den Bereichen Kommunikation, Konsumgüter, Industrie und Luft- und Raumfahrt mitgearbeitet. Zuletzt war er als Verifikationsexperte bei Huawei Technologies tätig und leitete weltweit formale Verifikationsaktivitäten für ARM-CPU- und Consumer-SoC-Designs. Er hat einen Master of Electronic Engineering der Universität Catania (Italien) und ist seit 18 Jahren in der Halbleiter- und Elektronikdesign-Automatisierung (EDA) tätig.

ALLE AUSGABEN JETZT AUCH ALS **E-PAPER** LESEN!

Offen für alles.
Außer für Kompromisse.

Im Zeitalter des autonomen Fahrens steigt der Aufwand an Entwicklung und Validierung sprunghaft an. Es wird immer wichtiger, die Systeme effizient ins Automobil zu integrieren – ganz ohne Kompromisse bei Funktionalität, Sicherheit und Qualität.

Mit den offenen und skalierbaren Lösungen von ETAS treffen Sie die richtige Wahl. Umso mehr, wenn Sie offen sind für eine effiziente Entwicklung: Wir begleiten Sie kompetent von Beratung und Design über Test und Validierung bis hin zur Integration der Software am PC, im Labor und im Fahrzeug.

Überzeugen Sie sich selbst auf www.etas.com/solutions

ETAS

DRIVING EMBEDDED EXCELLENCE

MARTIN DANZER

ist Director Product Management bei Congatec und studierte Elektrotechnik an der Technischen Hochschule Deggendorf. Seit gut 20 Jahren hat er Erfahrung im technischen Service, der Entwicklungsleitung und im Produktmanagement für Computer-on-Modules, inklusive seiner Zeit bei Kontron und JUMPtec.

CONGATEC AUF DER EMBEDDED WORLD DIGITAL

VON ARM BIS X86

Im Vorfeld zur virtuellen embedded world 2021 gab Congatec seine kommenden Produkt-Launches bekannt. Im Fokus stehen Edge- und Fog-Computer für COM-HPC, ein SMARC-Modul sowie das 8-Core-V2000-CoM auf AMD-Basis. Wie das alles zusammenpasst, erklärt Martin Danzer. Von Tobias Schlichtmeier


(Bild: Shutterstock)

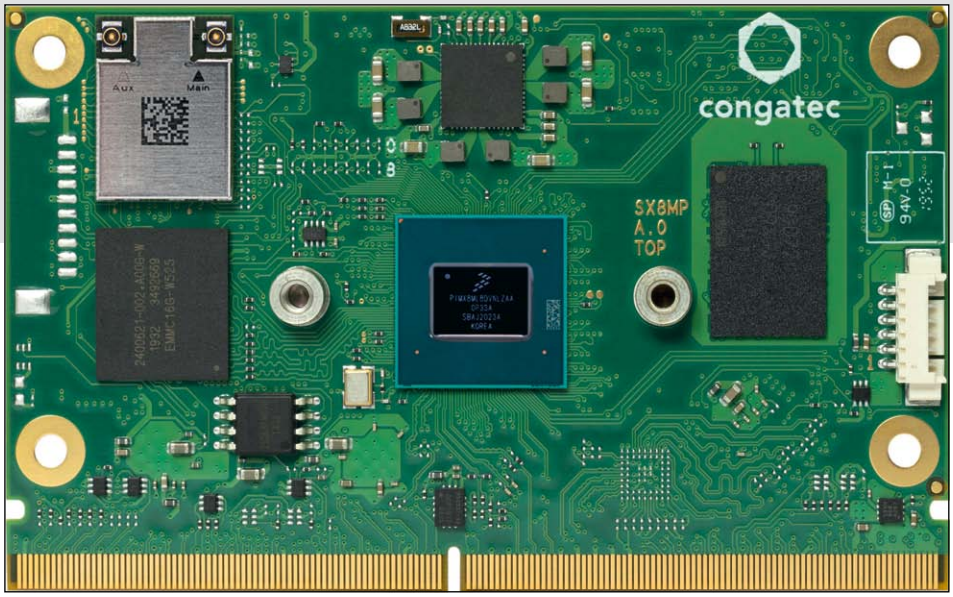
Herr Danzer, auf welche vertikalen Märkte zielt das SMARC-Modul mit dem neuen Prozessor von NXP?

Unsere SMARC-Module der i.MX-8M-Plus-Familie von NXP konzentrieren sich auf industrielle Produkte in Kombination mit Embedded Vision, Machine Learning (ML) und künstlicher Intelligenz (KI) sowie Multimedia-Geräten. Sie zielen somit auf Industrie 4.0 und IIoT, visuelle Inspektions- und Überwachungssysteme sowie smarte Infrastrukturen und Smart Cities ab. Weitere Einsatzbereiche finden sich jedoch ebenso in der Land- und Bauwirtschaft sowie der Gebäudeautomation.

Eines der größten Anwendungsfelder sehen wir im Bereich HMIs, denn nahezu jedes Gerät erhält heute eine grafische Bedienoberfläche und Multimedia-Funktionen. Die i.MX-8M-Plus-Prozessorfamilie bietet hierzu neben der hohen Rechenleistung und der zusätzlich integrierten Neural Processing Unit (NPU) ein umfassendes Set an Embedded-Schnittstellen, welches optimal zum SMARC-Formfaktor passt. Hiermit ergänzt NXP unser Portfolio an AMD- und Intel-basierten Modulen.

Welche Plattformen bieten Sie für Embedded Vision an?

Die SMARC-Module mit i.MX-8M-Plus-Prozessoren sind wichtig für unsere Embedded-Vision-Systeme. Bereits 2019 haben wir mit Basler und NXP ein Proof-of-Concept für Retail-Deep-Learning-



SMARC-Module mit NXP i.MX-8M-Plus-Prozessor für Temperaturen von -40 bis +85 °C. (Bild: Congatec)

Anwendungen erstellt. So beinhaltete die Plattform bereits KI, um den Check-out-Prozess im Einzelhandel vollständig zu automatisieren. Im Zuge der pandemiebedingt aufkommenden kontaktlosen Geräte ist das Kit heute aktueller denn je. Mit dem NXP-Prozessor bietet das Kit für solche Produkte ein gelungenes Featureset. Es besitzt beispielsweise zwei integrierte Image-Signal-Prozessoren (ISP), die es bei den 8X-, 8Mini- und 8QM-Varianten nicht gibt. Infolgedessen können Entwickler günstige MIPI-Kamerasensoren sowie das Software-Ökosystem von NXP für die ISP verwenden – das reduziert die Kosten sowie den Entwicklungsaufwand.

Können Sie ein paar technische Highlights der neuen SMARC-Module nennen?

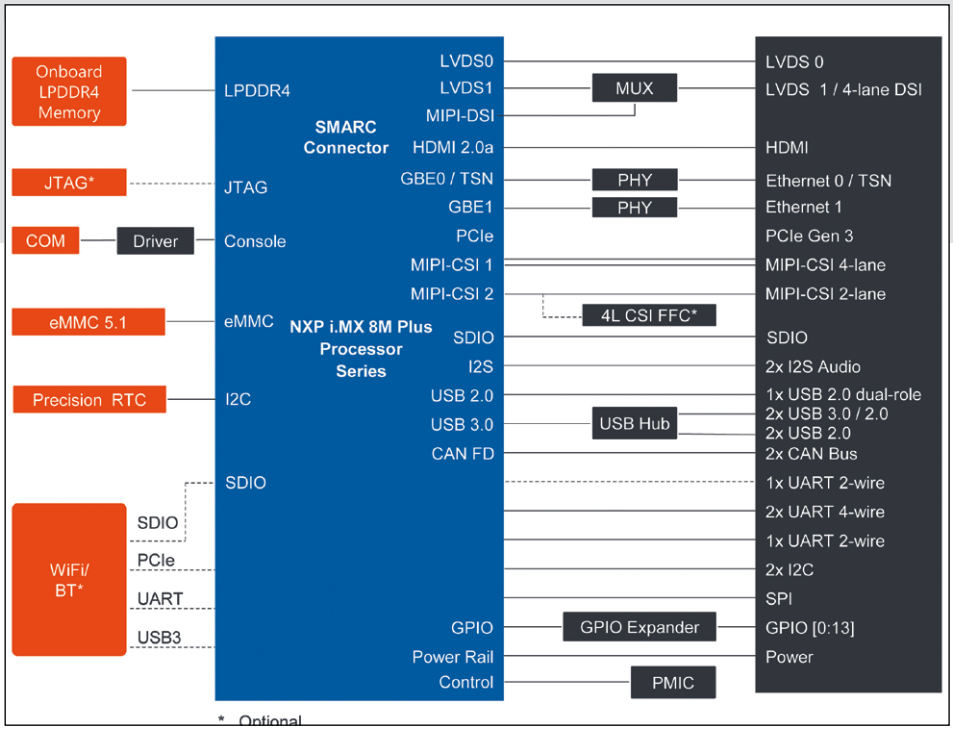
Zum einen die vier Arm-Cortex-A53-Prozessor-Kerne mit der zusätzlichen NPU, die bis zu 2,3 Billionen Operations per Second (TOPS) an KI-Rechenleistung addiert. Sie sind speziell für KI-Inferenzen entwickelt und somit sehr effizient, um beispielsweise die Daten des Dual-Kamera-Bildsignalprozessors zu verarbeiten.

Außerdem gibt es umfassende Multimedia-Funktionen. Zum Beispiel 3D/2D-Grafikbeschleunigung sowie Video-De- und Encodierung einschließlich H.265. Hohe Auflösungen werden sowohl in Inspektions- als auch Überwachungssystemen immer wichtiger, um Details besser auswerten zu können. Die NPU kann hier bei der Voranalyse helfen, damit nicht die Rohdaten das Netzwerk überlasten. Interessant ist zudem der hochwertige digitale Signalprozessor (DSP) für Audio- und Sprachfunktionen. Über die Kombination mit den Rechenwerken ist zum Beispiel eine nutzerspezifische Spracherkennung mit rund 40.000 unterschiedlichen Wörtern möglich. Anders als bei Produkten wie Alexa, Google oder Siri, funktioniert das rein lokal und ohne Cloud.

Was sind also die Vorteile für Entwickler?

So wie alle Computer-on-Modules (CoMs) sind sie für Entwickler attraktiv, weil sie bereits fertig entwickelt und alle Funktionen bereits validiert sind. Das spart Zeit und Geld. Es gibt zudem von Anfang an ein umfassendes Ökosystem für Hard- und Software, um das Entwickeln zu erleichtern und zu beschleunigen. Im weiteren Verlauf des Produktlebenszyklus kann der Kunde eine Skalierung mittels Leistungsvarianten bilden. Außerdem sind die Module einfach austauschbar und lange Zeit verfügbar. So kann man bei Abkündigen eines Prozessors mit geringem Aufwand auf die nächste Generation wechseln und den Return on Invest verlängern. Aus dem Grund sind CoMs im Markt der Embedded-Computer führend. Attraktiv bei SMARC ist zudem die Tatsache, dass der Standard sowohl Arm als auch x86 unterstützt.

„Arm wird im Low-Power-Computing-Bereich vom Funktionsumfang und der Leistung immer ähnlicher zu x86“



Das Blockdiagramm des iMX-8M-Plus-Prozessormoduls. (Bild: Congatec)

Spielt Migration von einer Technologie zur anderen eine große Rolle?

Wir wissen alle, dass die Devise gilt: „Never change a running system“. Entwickler verlassen den eingeschlagenen Pfad lediglich ungerne, denn jeder Wechsel kostet Zeit und Geld. Es ist jedoch immer gut, Optionen zu haben. Letztlich ist niemand mit einer einzigen Technologie oder einem einzelnen Prozessorhersteller verheiratet. Das ist auch gut so und wir wollen und müssen unseren Kunden mögliche neue Wege immer wieder öffnen. Interessant ist hierbei die Tatsache, dass Arm im Low-Power-Computing-Bereich vom Funktionsumfang und der Leistung immer ähnlicher zu x86 wird. Zwar ist der initiale Integrationsaufwand immer noch höher als bei x86, jedoch sehen wir Arm speziell bei hochvolumigen Projekten mehr und mehr als Option. SMARC bietet hier die Möglichkeit, zwischen beiden Architekturen zu wählen.

Welcher ist der wichtigste Wachstumsmarkt für 2021?

Definitiv der Markt für COM-HPC-Module. COM-HPC entwickelt sich zum zukünftigen Standard für den High-End-Embedded-Computing-Markt und bietet darüber hinaus die Möglichkeit, rechenintensive Anwendungen zu adressieren. Allen voran robuste Edge- und Fog-Server. Sie werden in unterschiedlichen industriellen sowie kritischen Netzwerken eingesetzt – und befinden sich in der Netzwerk-Computing- und Kommunikationspyramide oberhalb des Edge-Geräte-Levels.
Sie bedienen den Edge-Computing-Markt mit Echtzeit-Cloudserver-Leistung, die sowohl in On-Premise- als auch in kritischen Netzwerkinfrastrukturen bereitgestellt wird. Zusammen bilden die Fog- und Edge-Geräte den Echtzeit-Edge-Computing-Markt, der im Bereich des Embedded-Computings für raue Umgebungen bedeutender wird.

Wo liegt der Schwerpunkt bei COM-HPC?

Wir stehen kurz vor dem offiziellen Launch der COM-HPC-Spezifikation. Congatec stellt den Vorsitzenden der PICMG COM-HPC Working Group und deshalb ist es selbstverständlich, dass wir bereits mit Hochdruck an ersten Produkten und dem dazugehörigen Ökosystem arbeiten. Wir haben bereits COM-HPC-Client-Module mit Intels Core-Prozessoren der elften Generation gelauncht und zeigen sie auf der embedded world. Mit aktuellen Techniken wie PCIe und USB der jeweils vierten Generation bieten die Intel-Tiger-Lake-UP3-Plattformen ein gelungenes Featureset für High-End-Anwendungen. Darüber hinaus arbeiten wir bereits an den ersten COM-HPC-Server-Modulen und stellen unsere 2021er-Roadmap hierzu ebenfalls vor.

Wo kommen die neuen COM-HPC-Module mit Intels Tiger-Lake-Prozessoren zum Einsatz?

Typische Anwendungsfälle für die neuen COM-HPC- und COM-Express-Module finden sich in robusten Anwendungen, Outdoor-Edge-Geräten und Installationen im Fahrzeug. Typische Einsatzgebiete sind zum Beispiel die Industrieautomation, das Schienenverkehrs- und Transportwesen sowie smarte Infrastrukturen inklusive missionskritischer Anwendungen wie im Energie-, Öl- und Gassektor. Es sind also vergleichbare Anwendungen wie jene, die man mit dem neuen SMARC-Modul umsetzen kann, jedoch auf deutlich höherem Leistungsniveau.

Vielen Dank für das Gespräch Herr Danzer.

QSEVEN, SMARC ODER COM

EINS, ZWEI ODER DREI?

(Bild: MinJan | Shutterstock)

Vom IoT-Gerät über den Box-PC bis zur Systemplattform: Computermodule verhelfen Embedded-Anwendungen zum Erfolg. Jedoch gibt es inzwischen eine breite Palette an Modulen in vielen verschiedenen Formfaktoren. Da stellt sich schnell die Frage: Welches Modul nehmen? Von Alexander Jäger.

Aufsteckmodule – genauer Computer-on-Modules (CoMs) – haben inzwischen den Markt erobert, denn ihre Vorteile zeigen sich sehr schnell: Zusammen mit einem Träger-Board kann ein Entwickler ein CoM passgenau in eine Anwendung implementieren – und das mit geringem Aufwand und niedrigen Kosten. Das reichhaltige Angebot am Markt birgt viele Optionen – jedoch hat der Entwickler hiermit ebenso die Qual der Wahl zwischen verschiedenen Standards und Anbietern. **Bild 1** zeigt, welche Standards zu welcher Zeit entstanden sind.

Die unterschiedlichen Modultypen spielen ihre Vorteile bereichsbezogen aus, deshalb sollte zuerst eine genaue, das jeweilige Produkt betreffende Bedarfsanalyse erfolgen. Folgende Fragen sind hierbei zu beantworten:

➔ Was ist bei der Wahl des passenden Boards zu berücksichtigen?

➔ Welche Vor- und Nachteile weisen die jeweiligen Standards auf?

➔ Welcher Standard ist für die jeweilige Anwendung ideal?

QSEVEN ODER SMARC?

Produkte aus dem Bereich der Konsumgüter besitzen meist einen geringen Leistungsanspruch. In erster Linie geht es hierbei um das Entwickeln eines kompakten und günstigen Produkts. Hierbei ist der CoM-Standard QSeven eine gute Wahl. Sind die Ansprüche allerdings komplexer, sollten Entwickler den Bedarf genau analysieren und mit den Eigenschaften der unterschiedlichen Modulstandards abgleichen.

Human Machine Interfaces (HMI) beziehungsweise computergestützte Mensch-Maschine-Benutzerschnittstellen bestehen meist aus Display, Eingabefeld, Hardware und spezieller Software. Sind sie in einer Fertigungsanlage eingesetzt, erfordern sie oft eine hohe IP-Schutzklasse. Verfügten die ersten HMIs über einfache Funktionen, geht der Trend derzeit zu komplexen, programmierten Systemen. Außerdem gehen die Trends von lokalen Tastensystemen hin zu dezentralen, vernetzten und mobilen Anwendungen mit berührungsloser Bedienmöglichkeit – oder einer Kombination aus allem.

Es kann von Vorteil sein, Funktionen auf ein Modul auszulagern. Beispielsweise wenn der Entwickler das Board erweitern, optimieren oder sicherer gestalten will. Gesetzt sind hierbei allerdings die Rahmenbedingungen für Module, und zwar:

➔ kompakter Formfaktor

➔ geringe Leistungsaufnahme

➔ geringes Gewicht

➔ gute Verfügbarkeit

Selbst wenn die Anforderungen hinsichtlich PCI-Express (PCIe)-Schnittstellen und hoher Leistung nicht gegeben sind, ist die Leistungserwartung normalerweise zu hoch für QSeven. Neuartige Funktionen, die Visualisieren, Steuern und multiple Bedienmöglichkeiten bieten, erfordern eine flexible Softwarekonfiguration. Sie ist wichtig für ein Priorisieren der Prozesse, die zwischen reinen Bedien- und Verarbeitungsvorgängen entscheiden müssen. Eine höhere Leistung erzeugt gewöhnlich ebenso höhere Verluste und somit Wärme. Jedoch bleiben die Verluste übersichtlich, da viele HMIs mit Power over Ethernet (PoE) beziehungsweise PoE+ zu versorgen sind und somit Leitungen und Stromanschlüsse einsparen.

Eine gute Option ist hier der Smart Mobility Architecture (SMARC)-Standard. Es handelt sich um kompakte, vielseitige Computermodule für Anwendungen mit übersichtlicher Investitionstiefe und geringer Leistungsaufnahme, die dennoch eine beachtliche Leistung abliefern. Auf SMARC-Modulen kommen oft effiziente Arm-Prozessoren zum Einsatz. Genauso jedoch Low Power System-on-Chips (SoCs) oder niedriger performante x86-kompatible Geräte. Allerdings sind sie nicht beliebig erweiter- oder aufrüstbar. Typischerweise liegt die Leistungsaufnahme unter 6 W, obwohl Designs bis zu etwa 15 W möglich sind. Es sind grundsätzlich zwei Größen – „small“ im Format 82 x 50 mm² sowie „large“ in 82 x 80 mm² – verfügbar. Vorzugsweise wird das Modul für stationäre und tragbare Embedded-Systeme eingesetzt und beinhaltet:

➔ die CPU einschließlich DRAM

➔ Boot-Flash

➔ Power-Sequencing

➔ Netzteile

➔ Gigabit (Gb)-Ethernet

➔ zweikanalige LVDS-Display-Sender

Auf dem Trägerboard befinden sich weitere Funktionen wie Touchcontroller, Audio-Codecs und Anschlüsse

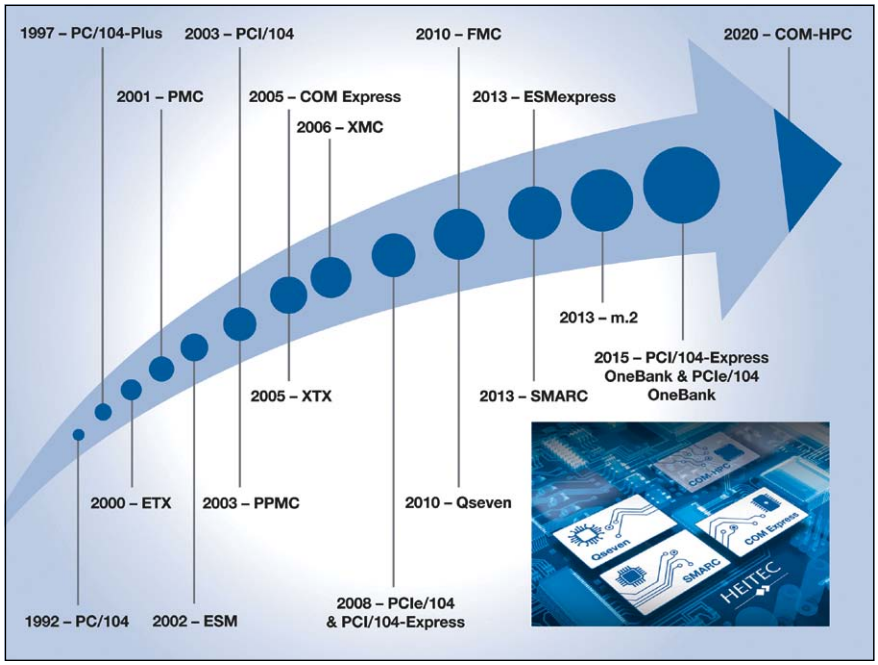


Bild 1. Der Zeitstrahl zeigt die Historie der Modulstandards, die in den letzten Jahrzehnten entwickelt wurden. (Bild: Heitec)

für drahtlose Geräte. Hiermit erfüllen sie ebenso alle Anforderungen von typischen HMIs: Aufgrund ihrer Skalierbarkeit sind sie flexibel und erweiterbar, erzielen eine schnelle Marktreife bei geringen Kosten, sind energieeffizient und weisen einen kleinen Footprint auf.

HOHE LEISTUNGEN MIT COM EXPRESS

Wie sieht es dagegen bei Anwendungen mit einer höheren Leistungserwartung aus, zum Beispiel dem autonomen Fahren? Längst ist der Autopilot nicht mehr auf herkömmliche Kraftfahrzeuge beschränkt, sondern spielt ebenso eine immer größere Rolle in der Landwirtschaft, bei öffentlichen Verkehrsmitteln sowie beim Überwachen von Flugräumen. So leiten beispielsweise Landwirte Mähdrescher mit optimierter und kraftstoffsparender Route. Außerdem wird mithilfe von Drohnen die Getreidereifung ausgewertet. So wird lediglich das Terrain befahren, das aktuell nötig ist. Sensorik spielt hierbei eine unerlässliche Rolle. Zum Beispiel überwachen hochauflösende (Wärmebild)-Kameras und Infrarotsensoren Bereiche vor dem Fahrwerk und der Mäheinheit, um Lebewesen wie Rehe im hohen Getreidefeld zu schützen.

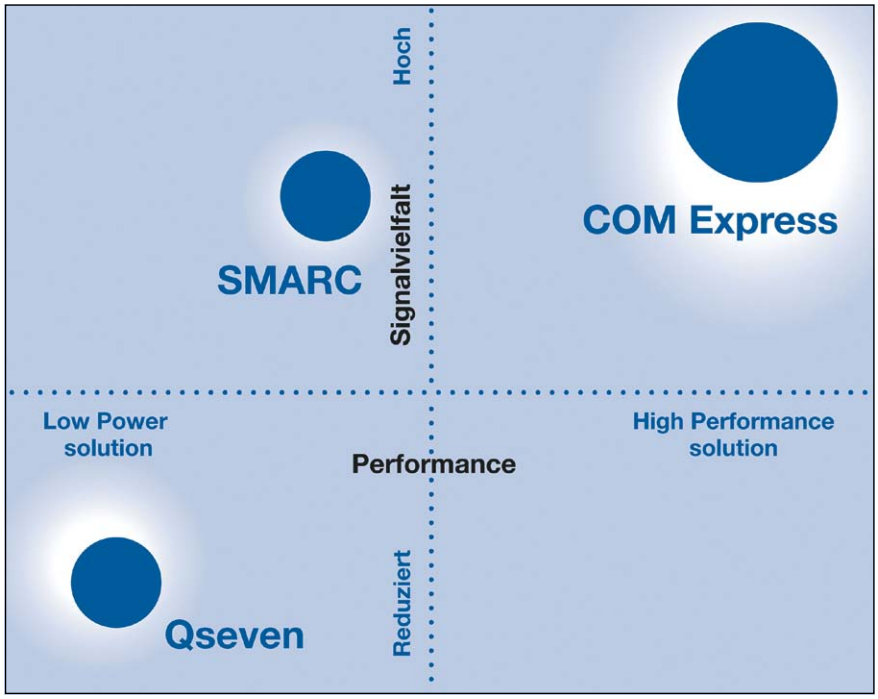


Bild 2. Qseven, SMARC und COM Express im Vergleich. (Bild: Heitec)

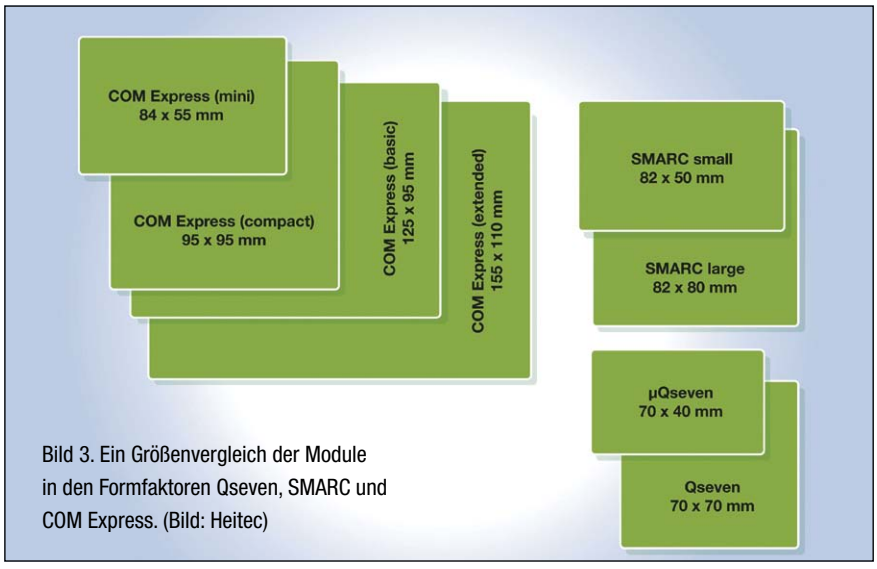


Bild 3. Ein Größenvergleich der Module in den Formfaktoren Qseven, SMARC und COM Express. (Bild: Heitec)

Performante Anwendungen wie diese verfügen zwar ebenfalls über eine Struktur mit Controller und Bediengerät, dennoch reicht die Leistungsfähigkeit von SMARC-Modulen bei solchen Anwendungen meist nicht mehr aus. So nutzen Entwickler Vision und Logik auf Basis künstlicher Intelligenz (KI), um ein Situationsbewusstsein zu etablieren. Hierzu ist es nötig, verschiedene Aufgaben zu implementieren, die eine komplexe Elektronik, Software und Kommunikation nötig machen. Zu den Aufgaben zählen zum Beispiel:

➔ eine genaue Motorsteuerung
➔ umfangreiche Sensorik und Bildverarbeitung
➔ Algorithmen und Sicherheitsfunktionen
➔ eine anspruchsvolle Datenverarbeitung wie das Berechnen von Erntezeitaufwand, Reifegrad, Mengen oder Flächen

Algorithmen sind in Echtzeit zu berechnen, so kann die Anwendung unter anderem aus Sicherheitsgründen sofort reagieren und unter Umständen den Betrieb einstellen. Das Gleiche gilt für kollaborative Roboter (Cobots). Alle genannten Beispiele erfordern verschiedene Vernetzungs- und Multifunktionsmöglichkeiten. Für eine große geforderte Anzahl an Schnittstellen und entsprechend hohe Rechenleistungen, bietet sich COM Express an. Einen Vergleich mit SMARC und Qseven zeigt **Bild 2**.

COM Express definiert eine Familie von „Small Form Factor“ (SFF)- und CoM Single-Board-Computern (SBCs), die die nötige Leistungsvielfalt liefern und genau auf die jeweiligen Bedürfnisse adaptierbar sind. COM Express wurde für die aktuellen Chipsätze und seriellen Signalisierungsprotokolle konzipiert. Es schließt PCI-Express der dritten Generation, 10 GbE, SATA, USB 3.0 sowie hochauflösende Videoschnittstellen – etwa für das Erfassen der Umgebung – mit ein.

Nicht zu vernachlässigen ist außerdem die Kompaktheit von COM-Express-

Modulen. Ihr Alleinstellungsmerkmal ist, dass die Module einerseits eigenständig als SBC operieren, andererseits als Prozessor-Mezzanine auf einem Basisboard ihren Dienst verrichten können. Letzteres reduziert den Zeit- und Kostenaufwand beim Produktdesign. Der Anwender muss die Details der Signalverarbeitung in Hochgeschwindigkeit nicht verstehen und der rasanten Entwicklung der Chipsätze nicht folgen. Für den Anwender bedeutet das Zukunftssicherheit, da neue COM-Express-Module einfach auf das Trägerboard aufsteckbar sind und so die Leistung erhöhen sowie die Produktlebenszeit verlängern.

Von den acht erhältlichen Typen sind die vier neuesten Pin-out-Typen relevant. Sie sind in der Spezifikation 3.0 der COM-Express-Module beschrieben. Mit dem sogenannten „Mini"-Formfaktor (84 x 55 mm²) sind Designs hinsichtlich COM Express Typ 10 realisierbar, „Compact" (95 x 95 mm²) findet vor allem bei Typ 6 Anwendung, „Basic" (95 x 125 mm²) dient Typ 6 und Typ 7 als Basis **(Bild 3)**. Der „Extended"-Formfaktor ist insbesondere für Server-Anwendungen relevant, von denen in der Folge die Rede ist.

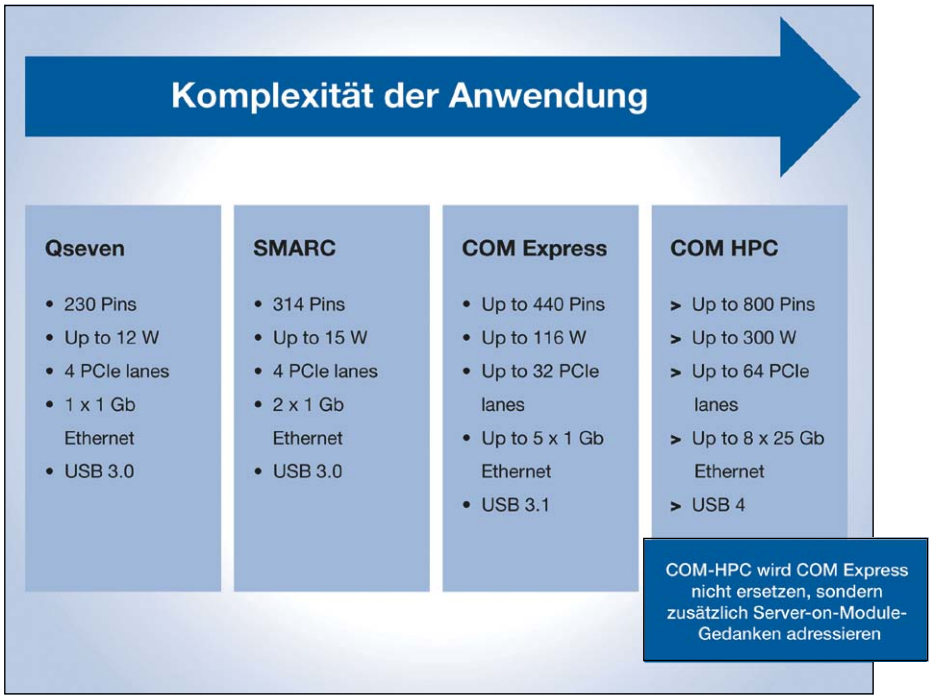


Bild 4. COM-HPC wird die Server-Leistungsklasse erschließen. (Bild: Heitec)

DATEN AM EDGE VERARBEITEN

IIoT-Anwendungen erfordern oft eine hohe Konnektivität – sowohl drahtgebunden als auch per Funk. Nach „oben" ins Internet beziehungsweise in die Cloud und nach „unten" zu unterschiedlichen Sensoren und Aktoren.

Sind viele Informationen vor Ort auszuwerten und anschließend weiterzugeben, ist oft eine Gateway-Funktion mit umfassender Leistung gewünscht. Ein Aufbereiten und Ergänzen der Daten vor dem Weitergeben führt zu einer verbesserten Konnektivität und Bedarfsoptimierung. Daten lassen sich gegebenenfalls im laufenden Betrieb umgehend an veränderte Anforderungen anpassen. Wesentliche Bestandteile der Architektur sind Gateways, die die zeitlich deterministisch zu erfassenden Daten in Echtzeit puffern, asynchron vorverarbeiten und an nachgeschaltete Dienste weitergeben. Über passende Schnittstellen, industrielle Datenmodelle und Standardprotokolle werden die lokalen Daten abgerufen. Ein sicheres und korrektes Verarbeiten der Signale verschiedener Datenprotokolle wird im Gateway anhand der Schnittstellenphysik und Softwarealgorithmen gewährleistet.

Abhängig von den zu analysierenden Datenpunkten und Auslastungen erzeugt eine Maschine mehrere hundert GB an Daten. Würde die Datenmenge an ein Rechenzentrum übertragen, käme es zu hohen Kosten aufgrund der benötigten Leitungskapazitäten, langen Latenzzeiten oder überlasteten Netzen. Um eine unterbrechungsfreie Funktion der involvierten Systeme zu gewährleisten, sammeln, überwachen und analysieren Edge-Computing-Systeme Datenmengen dort, wo sie erzeugt werden – in der physischen Nähe zu den Maschinen, welche die Daten generieren. Hiermit ergeben sich mehrere Vorteile:

➔ Die Analyse von Livedaten funktioniert lokal erheblich schneller als in virtuellen Speichern oder auf Ebene des Datenzentrums

➔ Die Kosten für das Übertragen der Daten sind gering, da die Daten vor Ort ausgewertet werden

➔ Es werden lediglich die relevanten Daten in die Cloud oder ein Rechenzentrum geschickt

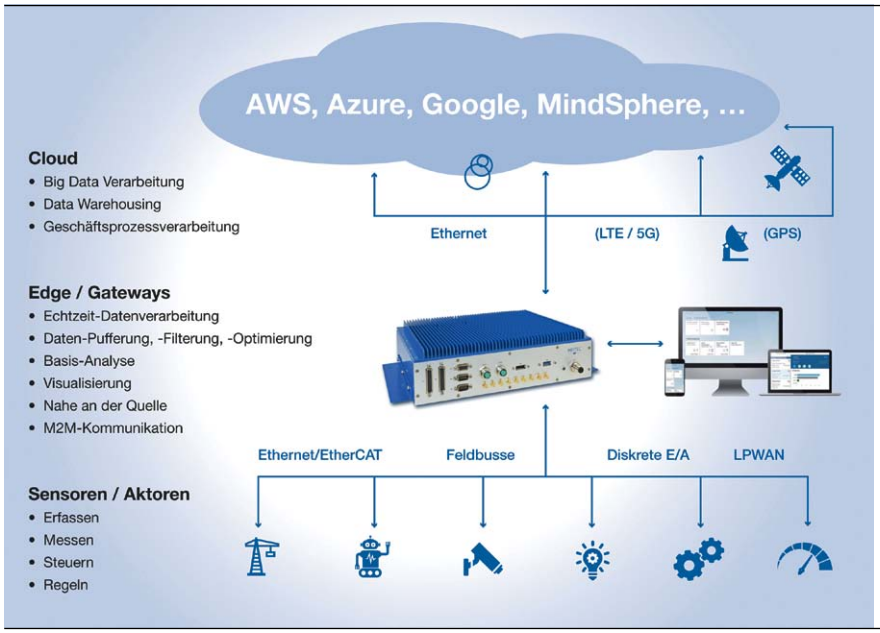
➔ Die Datensicherheit ist höher, da sensible Daten die Fertigung nicht verlassen

Bei den hohen Anforderungen an Bandbreite, Rechenleistung, Signalvielfalt und Stromaufnahme sind COM-Express-Module eine gute Wahl. Mit ihren vier aktuellen Grundtypen können Entwickler leistungsgerechte Designs – je nach Verlustleistung und Leistungsaufnahme – exakt umsetzen.

AUF DEM WEG ZU COM-HPC

Noch höhere Ansprüche als im IIoT entstehen bei Server-Anwendungen mit ihren immer größeren Datendichten, die beträchtlich mehr DRAM-Speicherkapazität und CPU-Funktionen benötigen. Eine immer größere Akzeptanz am Markt kommt hierbei der vierten definierten COM-Express-Modulgröße „Extended" mit 110 x 155 mm² zu. Sie ist in COM Express Rev. 3.0 mit dem Server-orientierten Pin-out-Typ 7 definiert. Jedoch gilt es ab einem gewissen Leistungsprofil andere Möglichkeiten zu finden.

Ergänzend für Hochleistungs-CoMs ist COM-HPC zu sehen, dessen Freigabe für



DIE SYSTEMPLATTFORM „HEISYS“

Eine All-in-One-Anwendung, die Gateway und Rechenzentrale in einem darstellt, liefert der Embedded-Spezialist Heitec. Die Systemplattform „HeiSys“ ist hinsichtlich Rechenleistung und Modularität skalierbar und bietet kabelgebundene I/O-Schnittstellen. Flexibilität bei kabellosen Übertragungstechniken bietet Heitec über integrierte M.2-Module. Hinsichtlich Wireless bietet HeiSys viele Übertragungsmöglichkeiten, darunter WLAN, LTE, 5G, UMTS, WiFi oder Bluetooth. Ebenso ist ein GPS/GLONASS-Multiband-Funkmodul integriert. Somit eignet sich die Plattform als zukunftsorientierte, adaptierfähige Grundlage für passgenaue Module. (Bild: Heitec)

das erste Quartal dieses Jahres erwartet wird **(Bild 4)**. Pin-out, Footprint und der Großteil der Funktion haben die Genehmigungsprozesse bereits passiert. Der neue Standard wird Bereiche abdecken, bei denen COM Express in puncto Übertragungsleistung, Highspeed-Schnittstellen und Netzanbindung an seine Grenzen stößt. Während COM Express lediglich 440 Pins aufweist, bietet COM-HPC 800 Pins. COM-HPC verdoppelt die PCIe-Lanes von 32 auf 64. Im Vergleich zu PCIe der dritten Generation mit 8 Gb/s, über PCIe der fünften Generation mit bis zu 32 Gb/s je Lane, erreichen sie somit eine vierfach höhere Datenrate. Bislang sieht der COM-HPC-Standard fünf Formate vor:

➔ COM-HPC „Server“ mit Size E (160 x 200 mm²) sowie Size D (160 x 160 mm²)

➔ COM-HPC „Client“ mit Size A (95 x 120 mm²), Size B (120 x 120 mm²) und Size C (120 x 160 mm²)

Die unterschiedlichen Formate unterscheiden sich vor allem in der Größe und der Anzahl beziehungsweise Art der Schnittstellen voneinander.

Die Client-Module verfügen über Video/Embedded-Display-Schnittstellen, worauf die Server-Variante verzichtet. Sie bietet jedoch für Server-Anwendungen wesentliche 10-Gb-Ethernet-Schnittstellen. Ein in der Grundfläche größeres COM-HPC-Server-Modul verfügt über bis zu acht DIMM-Sockel für Arbeitsspeicher und 64 PCIe-Lanes für zusätzliche GPUs und NVMe-Speicher. Bei den Netzwerkanschlüssen erreicht COM-HPC einen ebenso großen Leistungsanstieg und ist hoch skalierbar. Profitieren könnten davon Anwendungen wie:

➔ Edge-Server in der Telekomunikation, mit ihren stetig wachsenden Übertragungsraten

➔ Eine neue Klasse an Headless Edge Servern, welche zunehmend als verteilte Systeme in rauen industriellen Umgebungen und erweiterten Temperaturbereichen zum Einsatz kommen sowie

➔ Medizinische Diagnosegeräte mit leistungsstarker CPU, KI und parallelen Datenverarbeitungskapazitäten

Im Vergleich zu COM Express erreicht COM-HPC Datenraten bis zu 200 Gb/s anstatt 10 Gb/s. Somit eröffnen sich entsprechend mehr Anwendungsmöglichkeiten.

„THE PERFECT MATCH“

Der Markt für CoMs wird bisher im Wesentlichen von drei Standards beherrscht. Sie decken im Wesentlichen das Gros der Bedürfnisse und Anforderungen der geschilderten Anwendungen ab. Low-Power-Module wie SMARC oder Qseven (bis 12 W) eröffnen die Möglichkeit, einfache Anwendungen umzusetzen, während performante Module mit bis zu 116 W bei Typ 6/7 sowie 58 W bei Typ 10 mit einem COM-Express-Modul gut zu realisieren sind. Für ein optimales Design ist es nötig, bereits in der Konzeptphase alle Anforderungen genau zu evaluieren. So können Entwickler langfristig die passenden Schnittstellen bereitstellen und gegebenenfalls leistungsfähigere Prozessoren einsetzen. Ein COM-Express-Design ist dann sinnvoll, wenn bereits die Obergrenze an Schnittstellen und Leistung mit SMARC oder Qseven erreicht ist, da dies „Luft nach oben“ garantiert. TS

ALEXANDER JÄGER

ist Portfolio Solution Manager für das Geschäftsgebiet Elektronik bei Heitec in Eckental. Nach seinem Eintritt bei Heitec war er zunächst als Produktmanager für das Unternehmen tätig. Davor war er Produktmanager für ausfallsichere 19“-Systeme für Rail/Transportation und Industrial Solutions bei MEN Mikro Elektronik. Er besuchte die Rudolf-Diesel-Fachschule sowie die Georg-Simon-Ohm-Hochschule in Nürnberg und hat einen Abschluss als staatlich geprüfter Elektrotechniker.
elektronik@heitec.de

IMPRESSUM

Anschrift für Verlag, Redaktion, Vertrieb, Anzeigenverwaltung und alle Verantwortlichen:
WEKA Fachmedien GmbH, Richard-Reitzner-Allee 2, 85540 Haar
Tel.: 089 25556-1000, Fax 089 25556-1399, www.weka-fachmedien.de
Telefondurchwahl im Verlag: Sie wählen 089 25556 und dann die Nummer, die in Klammern zum jeweiligen Namen angegeben ist.
Geschäftsführer: Kurt Skupin, Matthäus Hose

Director Content Electronics: Dr. Ingo Kuss
Markenteam Elektronik: Joachim Kroll (jk/1335), Chefredakteur (verantwortlich für den Inhalt), Markus Kien, Chef vom Dienst (mk/1333)
Redaktionsteam: Heinz Arnold, Editor-at-Large (ha/1253), Stefanie Eckardt, Ltd. Red. (eck/1342), Melanie Erhardt (me/1346), Markus Haller (mha/1371), Ralf Higgelke (rh/1341), Engelbert Hopf, Chefreporter (eg/1320), Ute Häußler (uh/1369), Irina Hübner (ih/1339), Andreas Knoll, Ltd. Red. (ak/1319), Corinna Puhlmann-Hespen (cp/1316), Corinne Schindlbeck, Ltd. Red. (sc/1311), Tobias Schlichtmeier (ts/1368), Harry Schubert (hs/1338), Iris Stroh, Ltd. Red. (st/1326), Kathrin Veigel (kv/1746), Nicole Wörner (nw/1325), Karin Zühlke, Ltd. Red. (zü/1329)
Mitarbeiter dieser Ausgabe: Gerhard Stelzer (gs)
Layoutteam: Wolfgang Bachmaier, Andreas Geyh, Norbert Preiss, Bernhard Süßbauer, Alexander Zach
Bilderdienst: Shutterstock
Redaktionsassistenz: Andrea Seidel (sei), Tel.: 089 25556-1332; Fax: 089 25556-1670
redaktion@elektronik.de
www.elektronik.de

Director New Business: Marc Adelberg (1572)
Sales Director: Christian Stadler (1375)
Mediaberatung: Petra Beck (1378), Burkhard Bock (1305), Tanja Lewin (1386), Konrad Nadler (1382), Martina Niekrawietz (1309),
International Account Managers: Konrad Nadler (1382), Martina Niekrawietz (1309)
Auslandsrepräsentanz (Foreign Representation):
USA West: Huson International Media, Lanibel Collado, 16615 Lark Avenue, Suite 100, Los Gatos, CA 95032, Tel.: 001 408 879 6666, Fax: 001 408 879 6669, lanibel.collado@husonmedia.com
Anzeigenverwaltung und Disposition: Jeanette Blaukat (1014)
Anzeigenpreise: Es gilt die Preisliste Nr. 56 vom 1. Januar 2021
Teamassistenz: Rosi Böhm, Tel.: 089 25556-1307, Michaela Stolka, Tel.: 089 25556-1376, Fax: 089 25556-1651
media@elektronik.de
www.weka-fachmedien.de/de/medien/elektronik/

Vertriebsleitung: Marc Schneider (1509, mschneider@weka-fachmedien.de)
Bestell- und Abonnement-Service: WEKA FACHMEDIEN GmbH, c/o Zenit Pressevertrieb GmbH, Postfach 810640, 70523 Stuttgart, Tel.: 0711 7252-210, Fax: 0711 7252-333, E-Mail: abo@weka-fachmedien.de
Bestellungen Schweiz: Thali AG, Industriestr. 14, CH-6285 Hitzkirch, Tel.: 041 9196611, Fax: 041 9196677, abo@thali.ch, www.thali.ch
Organschaft: Die Elektronik ist Organ der VDE/VDI-Gesellschaft Mikroelektronik, Mikrosystem- und Feinwerktechnik (GMM). Die Mitglieder der GMM erhalten die Elektronik im Rahmen ihrer Mitgliedschaft.
Erscheinungsweise: 26 Ausgaben

Jahresabonnement Print Inland: 179,00 €, davon 115,30 € Heft, 63,70 € Versand, inkl. MwSt.
Jahresabonnement Print Ausland: 201,10 €, davon 115,30 € Heft, 85,80 € Versand, inkl. MwSt.
Einzelausgabe Print: 8,00 € inkl. MwSt., zzgl. 3,00 Euro Versandkosten
Jahresbezug digitales E-Paper (Inland/Ausland)**:** 69,99 € inkl. MwSt., ohne Versandkosten
Einzelausgabe digitales E-Paper (Inland/Ausland)**:** 2,99 € inkl. MwSt., ohne Versandkosten
Heftbestellung online: shop.weka-fachmedien.de

Bankverbindung: HypoVereinsbank
IBAN: DE37 7002 0270 0035 7049 81
BIC: HYVEDEMMXXX

Leitung Herstellung: Marion Stephan (1442)
Sonderdrucke: Alle in dieser Ausgabe erschienenen Beiträge können für Werbezwecke als Sonderdrucke hergestellt werden. Anfragen an Andreas Hofner, Tel. 089 25556-1450, E-Mail: AHofner@wekanet.de
Technik: JournalMedia GmbH, Richard-Reitzner-Allee 4, 85540 Haar
Druck: L.N. Schaffrath GmbH & Co. KG DruckMedien, Marktweg 42–50, 47608 Geldern

70. Jahrgang, ISSN 0013-5658, Vertriebskennzeichen ZKZ 2594

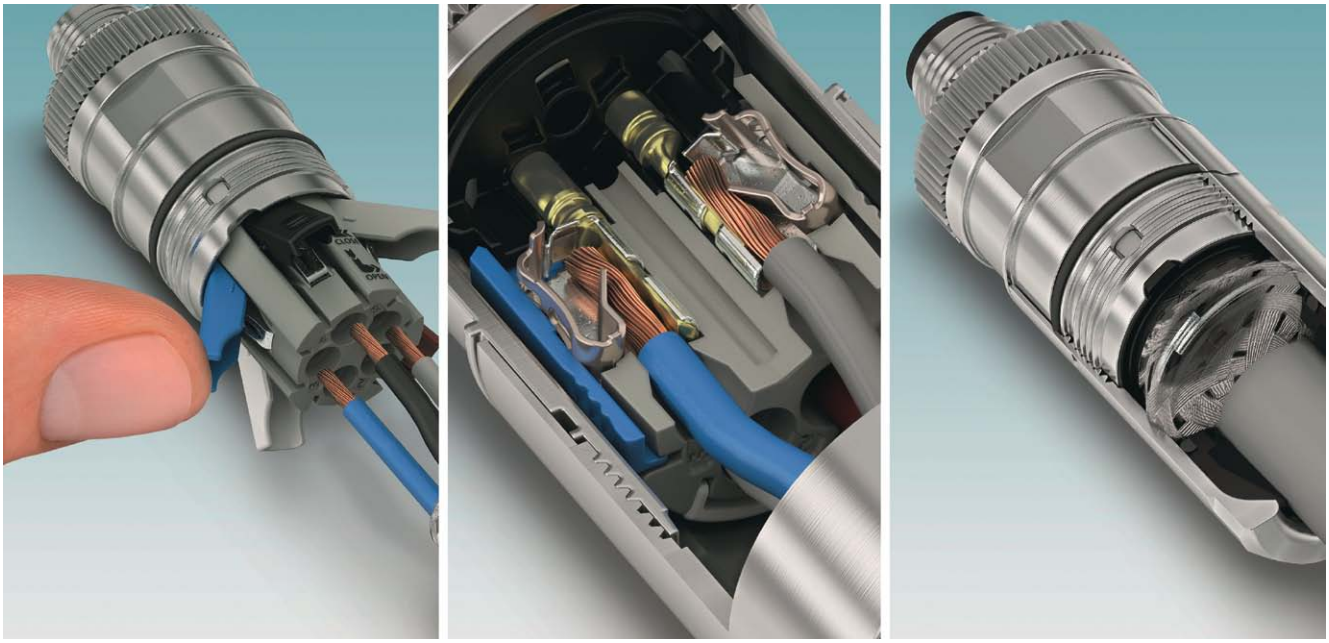
LA ELFA
LESERANALYSE ELEKTRONIK-FACHMEDIEN

INSERENTENVERZEICHNIS

Dieser Ausgabe liegt teilweise eine Beilage der Firma Nürnberg Messe GmbH bei. Wir bitten freundlich um Beachtung!

M12-VERKABELUNG FÜR POWER-ANWENDUNGEN

VIEL LEISTUNG AUF WENIG RAUM



(alle Bild: Phoenix Contact)

Der M12-Steckverbinder gilt als Universalgenie der industriellen Anschlusstechnik – neben der Signal- und Datenübertragung wird auch immer häufiger Leistung über diese kompakte Schnittstelle übertragen. Durch die Push-Lock-Anschlusstechnik können Anwender Leiterquerschnitte bis 2,5 mm² komfortabel, sicher und schnell konfektionieren. Von Tobias Dietel und Jörg Hohmeier

Ein wichtiger Aspekt der digitalen Transformation, die sich vor dem Hintergrund von Industrie 4.0 vollzieht, ist die dezentrale Energieverteilung. Dazu ist das M12-Power-Verkabelungssystem wie geschaffen **(Bild 1)**. Dazu gibt es seit 2011 die Produktnorm IEC 61076-2-111 für die Energieübertragung über M12-Steckverbinder. Bei Einbausteckverbindern beispielsweise für I/O-Module mit Schutzart IP67, bei vorkonfektionierten Leitungen, bei Verteilern sowie bei konfektionierbaren Steckverbindern sind stets die normativen Anforderungen zu beachten. Neben den gängigen Anforderungen – wie etwa Tauglichkeit für die Schutzart IP67 – wurde bei der Konzeption der M12-Power-Komponenten ein besonderes Augenmerk auf die Verstecksicherheit sowie auf die Einhaltung der Luft- und Kriechstrecken gelegt. Nur so werden die erhöhten Ströme von bis zu 16 A sowie die Spannung von bis zu 690 V sicher übertragen.

Dazu hat Phoenix Contact fünf spezielle Codierungen entwickelt und in die Norm IEC 61076-2-111 eingebracht. Diese Norm beschreibt, welche Eigenschaften ein solcher Steckverbinder haben muss und welche Anforderungen an ihn gestellt werden können. Die T- und L-Kodierungen sind für DC-Anwendungen mit einem Strom von bis zu 16 A pro Pin ausgelegt. Die L-Kodierung verfügt gegenüber der T-Kodierung über einen separaten FE-Kontakt. Die S-, K- und M-Codierungen dienen

Bild 1. Durchgängige Energieverteilung bei jeder Topologie: Durch die Push-Lock-Anschlusstechnik lassen sich Leiterquerschnitte bis 2,5 mm² passgenau konfektionieren.

zur Versorgung von AC-Endverbrauchern. Ein- und dreiphasige AC-Geräte – wie etwa Motoren – lassen sich dann mit Spannungen von bis zu 690 V und bis zu 16 A versorgen.

EINE LÖSUNG FÜR ZAHLREICHE APPLIKATIONSFELDER

Unabhängig vom jeweiligen Applikationsfeld ist es für den Anwender immer besonders komfortabel, wenn er seine Energieverkabelung vollständig mit Plug-and-play-Lösungen umsetzen kann. Zu diesem Zweck sind auch vorkonfektionierte Leitungen mit M12-Power-Steckverbindern im Markt verfügbar. Besonders in den letzten Jahren wurden zahlreiche Steckverbinder für diese Leitungen entwickelt. Parallel

NERVENSYSTEM DER ALL ELECTRIC SOCIETY – STECKVERBINDER UND LEITUNGEN

Der Klimawandel erfordert eine globale Energiewende, die nur durch die Digitalisierung und Vernetzung aller Lebensbereiche möglich ist. In der All Electric Society wird der Energiebedarf daher lediglich aus erneuerbaren Energien gedeckt und elektrischer Strom zum zentralen Energieträger. Dazu bedarf es auch einer umfassenden Kopplung der Sektoren Energie, Mobilität, Infrastruktur, Gebäude und Industrie. Die weltweite Infrastruktur muss physikalisch und datentechnisch vernetzt werden.
Bislang sind die einzelnen Sektoren durch unterschiedliche technische Standards gekennzeichnet, was ihre Kopplung erschwert. Allerdings stehen bereits Basistechnologien wie Single-Pair-Ethernet, TSN oder 5G zur Verfügung, um eine nahtlose Kommunikationsinfrastruktur zwischen den unzähligen installierten Geräten aufzubauen. Elektromechanische Produkte – etwa Steckverbinder oder Reihenklemmen – dienen als Basis für die Elektrifizierung von Maschinen und Anlagen. Phoenix Contact engagiert sich aktiv in vielen Nutzerorganisationen, Gremien und Verbänden, damit die (Weiter-) Entwicklung dieser Standards anforderungsgerecht vorangetrieben und die All Electric Society Wirklichkeit wird.

Bild 2. Produktprogramm M12 Power von Phoenix Contact: Konfektionierbare Federkraft-Steckverbinder sowie fertig konfektionierte Kabel und Verteiler bieten für jede Applikation die richtige Lösung.

dazu hat sich auch das Angebot an applikationsspezifischen Leitungen massiv ausdifferenziert. Leider kann längst nicht jeder Anwender auf vorkonfektionierte Leitungen zurückgreifen. In der Praxis muss die Power-Leitung häufig Geräten zugeführt werden, die kein Kabeleinführungssystem – wie beispielsweise CES von Phoenix Contact – umfassen, sondern nur eine Standard-Kabelverschraubung nutzen können. Einige Geräte sind auch bereits selbst mit einer Leitung ausgestattet, die ein offenes Leitungsende aufweist.
Zahlreiche Anwender rund um den Globus möchten ihre eigene interne Standard-Energieleitung einsetzen. Gerade dann sind die konfektionierbaren M12-Power-Steckverbinder der benötigte Baustein für eine durchgängige M12-Energieverkabelung. Um die Energieverteilung flexibler zu gestalten sowie Anzahl und Länge der Leitungen zu minimieren, lohnt sich der Einsatz von Energieverteilern. Früher mittels „Verteilerdose“ und Klemmkasten realisiert, sind mit dem Verkabelungskonzept von M12 Power derartige Anwendungen jetzt einfach und steckbar geworden **(Bild 2)**. Geringerer Leistungsabfall, übersichtliche Installation und eine einfache Diagnose im Fehlerfall sind Vorteile, die für den Einsatz dieser neuartigen Technologie sprechen.

ANSCHLUSSTECHNIKEN FÜR M12 POWER

Zurzeit sind am Markt bereits folgende Anschlusstechniken für Signal- und Datenanwendungen verfügbar: Schraub-, Federkraft-, Crimp-, Pierce- und Schneidklemm-Anschluss. Jede diese Anschlusstechniken ist seit langer Zeit im Einsatz und bietet je nach Anwendung ihre ganz spezifischen Vorteile. Werden die Anschlusstechniken untereinander verglichen, lässt sich das Resultat nicht ohne weiteres auf die Energieverkabelung übertragen. Denn Leiterquerschnitte von 1,5 mm² und besonders 2,5 mm² erfordern vom Installateur ein höheres Maß an Kraftaufwand und Sorgfalt. Vor allem bei AC-Anwendungen von bis zu 690 V ist eine sorgfältige Installation ein nicht zu unterschätzender Faktor **(Bild 3)**. Die Steckverbinder-Norm IEC 61076-2-111 sieht vor, dass M12-Leistungssteckverbinder nur spannungsfrei steckbar sind, und auch das Gehäuse darf nur spannungsfrei geöffnet werden. Hier kennt der Markt unterschiedliche Ansätze und darauf sollte der Anwender achten, wenn er einen Steckverbinder auswählt. Einige Steckverbinder lassen sich beispielsweise nicht wiederbeschalten, da die Gehäuse bei der Installation verklebt werden. Steckverbinder mit Schneidklemmanschluss lassen sich nur erneut wiederbeschalten, wenn die Leitung erneut abgesetzt wird und die Schneidklemme an anderer Stelle die Leiter kontaktiert.

M12-FEDERANSCHLUSS MIT MEHRWERT

Mit dem Federkraftanschluss lassen sich sowohl Reihenklemmen und Rundsteckverbinder als auch Leiterplatten-Steckverbinder anschließen. In den vergangenen Jahren wurde dieser Anschluss kontinuierlich weiterentwickelt und eignet sich daher mittlerweile für zahlreiche Anwendungsfälle. Während bei der Leiterplatten- oder Hutschienenmontage der Steckverbinder fixiert ist, muss der konfektionierbare M12-Steckverbinder beim Anschluss von Hand gehalten werden. Im Bereich der Signal- und Datenverkabelung hat sich bereits eine hebelbedienbare Lösung etabliert. Der Hebel bietet den Vorteil, dass die Klemmkammer geöffnet bleibt und man den Leiter mit beiden Hände zuführen kann. Beim Anschluss von Querschnitten wie 1,5 mm² und 2,5 mm² wird jeder Installateur diese Eigenschaft zu schätzen wissen. Dieser Anschluss bietet somit eine erhebliche Erleichterung und macht den Federkraftanschluss auch im M12-Bereich zu einer schnellen und einfachen Anschlussmöglichkeit.

SICHER MIT PE-ANSCHLUSS

Ein besonderes Augenmerk gilt dem PE-Anschluss (Protection Earth, Schutzerde) bei AC-Anwendungen. Um auf dem kleinen Raum die hohen Spannungen von bis zu 690 V umzusetzen, sind gewisse Luft- und Kriechstrecken sowie Wandstärken des isolierenden Materials notwendig. Dabei ist zu berücksichtigen, dass im Fehlerfall kein leitendes Material unter Spannung stehen darf, das der Anwender berühren könnte. Ein Fehlerfall wäre beispielsweise der Auszug der Leitung aus dem Steckverbinder. Dabei können einzelne Leiter aus dem Anschlussbereich gerissen werden. Hier ist von der Konstruktion her darauf zu achten, dass der PE-Leiter als Letztes getrennt wird. Dadurch ist sichergestellt, dass bei einem Spannungsdurchschlag von der herausgerissenen Phase zu leitenden Gehäuseteilen die Sicherung auslöst. Da sich in den meisten Fällen die Anschlussklemmen auf einer Ebene befinden, wird diese Anforderung durch einen 2 mm längeren PE-Leiter umgesetzt. Ebenso gibt es Konzepte am Markt, die konstruktiv gleiche Längen der Leiter zulassen. Die sind dann so konstruiert, dass der PE-Leiter die höchste Haltekraft im System besitzt.

Bild 3. Der M12-Power-Steckverbinder ermöglicht mit seinem Push-Lock-Anschluss eine schnelle und komfortable Leistungsverkabelung ohne Werkzeug: die Klemmkammern des Steckverbinders werden mittels Hebel geöffnet und geschlossen – der Anwender hat beide Hände für die Leiterzuführung frei.

Üblicherweise ist der PE-Leiter in der Anwendung stromlos – nur im Fehlerfall können kurzzeitig hohe Ströme fließen. Bei geschirmten Anwendungen fließen diese zusätzlich über die Schirmkontaktierung des Steckverbinders. Somit ist im Gegensatz zu den geschirmten Signal- und Datensteckverbindern der Schirmanschluss ein wichtiges Sicherheitselement. Je nach Zulassung werden bei den Freigabeprüfungen Ströme im dreistelligen Amperebereich angelegt, um die Sicherheit des Systems im Fehlerfall zu prüfen. Dabei ist der Querschnitt der PE-relevanten Komponenten – wie PE-Kontakt, PE-Kontaktierung zum Gehäuse und die Anbindung des Leitungsschirmes – am Steckverbinder ausschlaggebend für die sichere Funktion. Demzufolge sollte bei der Kontaktierung das Schirmgeflecht der Leitung großflächig mit dem Steckverbindergehäuse verbunden werden.

FAZIT

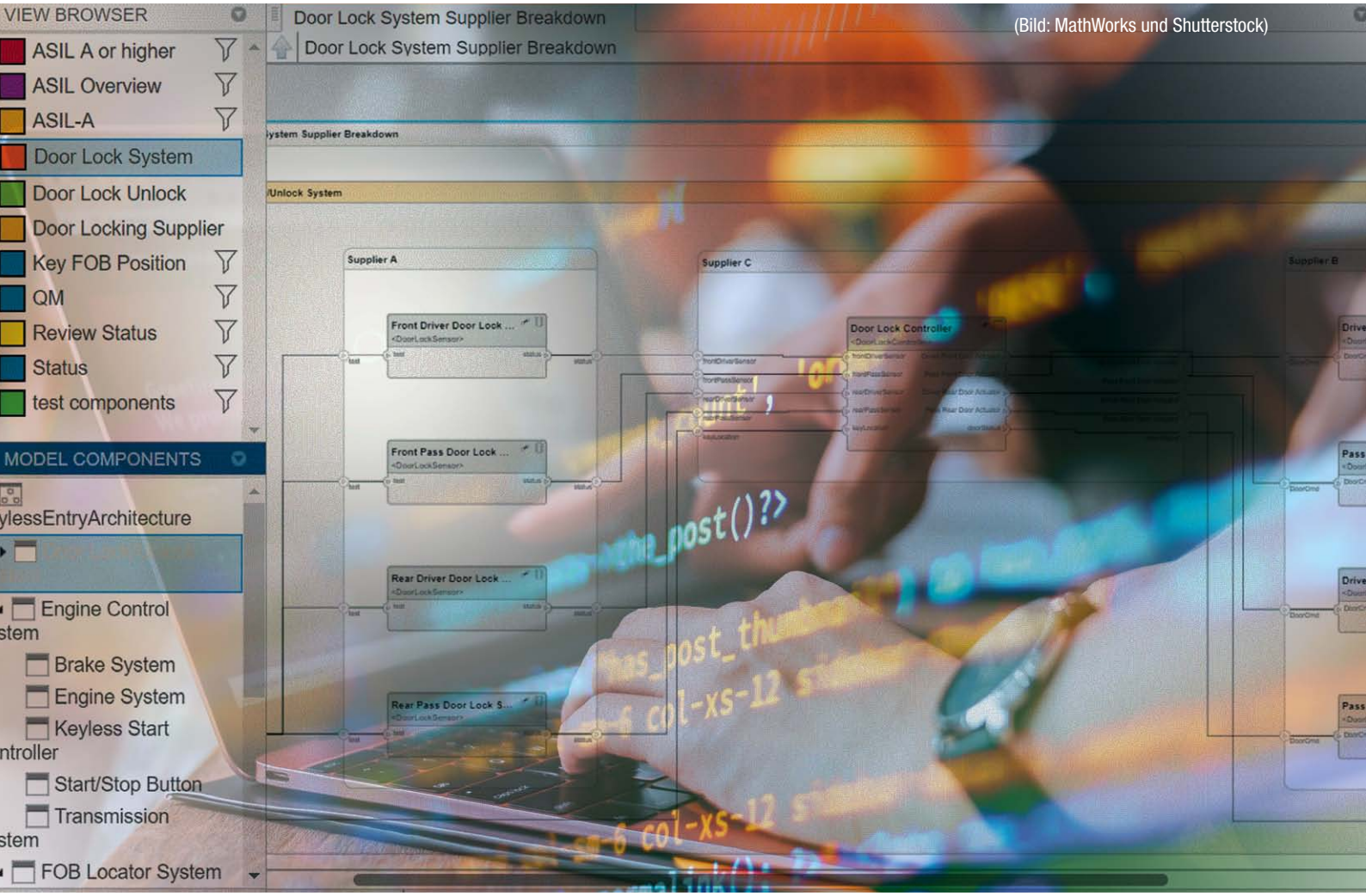
Bei Spannungen bis zu 690 V und Strömen bis zu 16 A ist eine sorgfältige Installation erforderlich. Standardisierte Komponenten wie konfektionierte Leitungen, Energieverteiler und konfektionierbare Steckverbinder vereinfachen die sonst aufwendige Energieverteilung erheblich. Mit der Push-Lock-Anschlusstechnik von Phoenix Contact wird der Leistungsanschluss im Feld komfortabel und zeitsparend. RH

TOBIAS DIETEL
ist staatl. gepr. Elektrotechniker, Phoenix Contact.

JÖRG HOHMEIER
ist Diplomingenieur (FH) und zuständig im Produkt-Marketing Industrial Field Connectivity, Phoenix Contact.

MODEL-BASED DESIGN

DIE BESTE ARCHITEKTUR GEWINNT



(Bild: MathWorks und Shutterstock)

System- oder Software-Architekturen zu erstellen ist nicht immer leicht. Mit zunehmender Komplexität steigen die Anforderungen. Helfen können hierbei Tools von MathWorks.

Von Marc Segelken

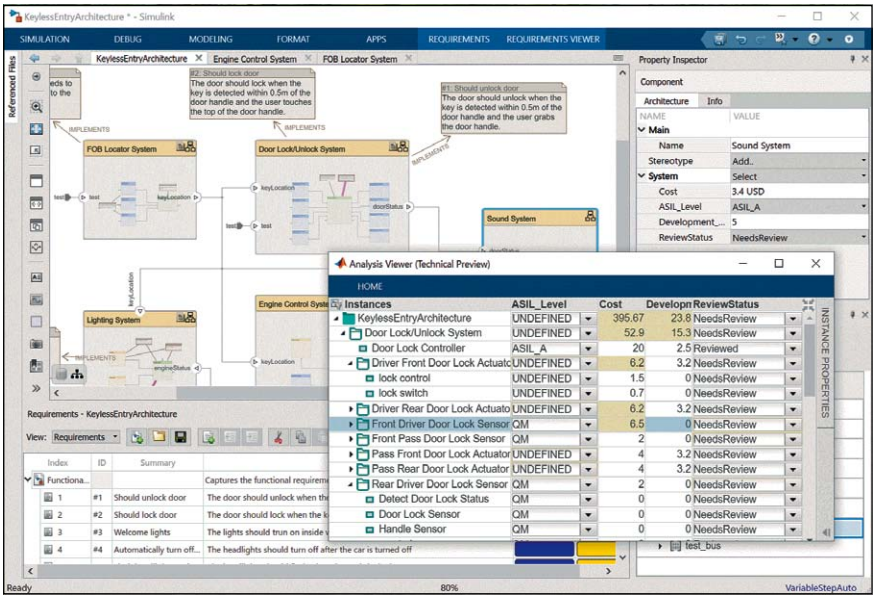


Bild 1. Der System Composer mit eingeblendeten Anforderungen und Komponenteneigenschaften wie Kosten oder ASIL-Level. Eine Analyse zeigt errechnete Kenngrößen der Architektur. (Bild: MathWorks)

Das Entwickeln großer Systeme wird immer komplexer. Ein Schlüssel zum Rationalisieren von groß angelegten Programmen ist, sie über alle Designebenen hinweg zu verfolgen und zu synchronisieren. Häufig fehlt jedoch das Bindeglied zwischen der Systemtechnik und dem Implementieren des Designs.

Herausfordernd ist außerdem der Entwurf von Systemarchitekturen. Hierbei sind verschiedene Faktoren zu berücksichtigen, zum Beispiel Leistung, Kosten, Markteinführungszeit, Leistungsaufnahme sowie Gewicht. Ergebnis des Entwicklungsprozesses sind in der Regel verschiedene Ausgangspunkte für das Design der Unterkomponenten. Zum Beispiel Schnittstellenbeschreibungen, abgeleitete Randbedingungen und Anforderungen.

Schwer ist außerdem, sich auf Systemdetails zu konzentrieren, ohne den Überblick zu verlieren. Entscheidend sind:

➔ Informationen zum Kontext einzuholen

➔ Anforderungen auf System- und Komponentenebene rückzuverfolgen

➔ Gefilterte Ansichten für das Handhaben der Systemkomplexität bereitzustellen

Ein einfacher Übergang zum Weiterentwickeln des Systems und eine garantierte Beständigkeit sind weitere Schlüssel zum Erfolg.

ERSTELLEN EINER ARCHITEKTUR

Ein Systemtechnikprojekt beginnt meist mit Forderungen auf hoher Ebene und optional einem Altsystem, das teilweise oder strukturell bis zu einem gewissen Grad wiederzuverwenden ist. Die Hauptaufgabe ist, eine Architektur mit Unterkomponenten zu erstellen, die jeweils abgeleiteten Anforderungen zugeordnet sind. So erfüllen sie ihren Anteil an der Gesamtfunktion, wobei so viele Hierarchieebenen wie nötig beteiligt sind. Ein strukturelles Zerlegen geht also mit einem zugehörigen Zerlegen der Forderungen und Randbedingungen einher – so sind am Ende des Schritts die Einschränkungen jeder Unterkomponente ausreichend definiert.

Meist erstellen Entwickler anfangs mehrere alternative Architekturen, welche es anschließend auszuwerten und zu vergleichen gilt. So wird die beste Architektur für das weitere Entwickeln ausgewählt. Beispielsweise können Entwickler im Bereich der Sensorik unterschiedliche Konzepte umsetzen, oder bei sicherheitskritischen Systemen unterschiedliche Ansätze zur Sicherheitsdekomposition gegenüberstellen. Das kann zum Beispiel das Verwenden einzelner Komponenten höherer Sicherheitsstufen gegenüber mehreren diversitär redundanten Komponenten niedrigerer Sicherheitsstufen betreffen. Prämissen, welche beim Aufbau einer Architektur den Komponenten zuzuordnen sind, können sowohl nichtfunktionaler als auch funktionaler Natur sein.

AUSWAHL DER RICHTIGEN KOMPONENTEN

Wie im vorangehenden Beispiel ersichtlich, gibt es nichtfunktionale Anforderungen, die beim Entscheiden für eine Architektur zu berücksichtigen sind. Neben Sicherheitsstufen können das beispielsweise Forderungen an den Lebenszyklus oder andere nicht-funktionale Einschränkungen sein. Mögliche Komponenten sind über Eigenschaften wie Gewicht, Kosten, Zuverlässigkeit, Entwicklungsaufwand und andere domänenspezifische Designdaten charakterisiert. Sie müssen den nicht-funktionalen Anforderungen – sowie deren Zusammensetzung – auf jeder Hierarchieebene entsprechen. Um solche Größen einzubeziehen, wird eine Hierarchie von Stereotypen definiert. Sie repräsentiert jede benötigte

Komponente und erfasst nach Bedarf die nicht-funktionalen Eigenschaften. So können Entwickler in einer Architektur alle Komponenten typgerecht mit den relevanten Daten versehen. Alle Architekturdaten sind für Systemanalysen nötig. So können Entwickler beurteilen, ob alle Randbedingungen erfüllt sind. Außerdem lassen sich so verschiedene Architekturen miteinander vergleichen.

Bei Model-based System Engineering (MBSE)-Werkzeugen wie dem „System Composer“ von MathWorks wählen Nutzer die Stereotypen zu jeder Komponente aus und geben die Größen der dazugehörigen Typeigenschaften ein. So sind zu jeder Komponente der Architektur alle spezifischen Daten verfügbar. Wie in **Bild 1** zu sehen, kann der System Composer die Daten jederzeit auswerten und die resultierenden architekturspezifischen Systemgrößen ermitteln. So kann ein Entwickler frühzeitig das Einhalten der Randbedingungen überprüfen oder die beste Architektur zum weiteren Entwickeln selektieren.

SIMULATION ERÖFFNET NEUE MÖGLICHKEITEN

Abgesehen von zeitlichen Leistungseinschränkungen werden funktionale Anforderungen in der Regel nicht speziell auf der Architekturebene behandelt, außer dass sie parallel zum Erstellen der Architektur in abgeleitete Prämissen zerlegt und den Architekturkomponenten zugeordnet werden. Mit Werkzeugen zum Verwalten der Anforderungen wie „Simulink Requirements“ erfolgt das per Drag-and-drop auf die Komponenten und ist direkt im Diagramm einzublenden **(Bild 1)**. Inkonsistenzen oder fehlende Prämissen sind bei so eng integrierter Datenhaltung schnell auffällig. Für ein Präzisieren können Anwender an der Stelle ebenso Sequenzdiagramme nutzen und später zu Verifikationszwecken wiederverwenden.

Erst ein vollständiges Formalisieren aller Prämissen der Komponenten würde bereits auf Architekturebene eine frühe funktionale Analyse erlauben. Aufgrund des hohen Aufwands wird das Verfahren jedoch sehr selten durchgeführt. Stattdessen greift zum Beispiel das MBSE-Werkzeug System Composer auf Simulation von Komponenten- und Architekturebene zurück. So können Anwender die Konsistenz der Anforderungen sowohl lokal als auch im Gesamtsystemverhalten validieren. Jede Komponente, für die ein Simulink-Modell hinterlegt ist, wird in die Gesamtsystemsimulation einbezogen. Hiermit eröffnen sich alle Möglichkeiten der Testeinrichtung und -automatisierung selbst auf oberster Architekturebene, ohne hierfür ein Extramodell erstellen zu müssen **(Bild 2)**. Schnittstellen und Verbindungen werden somit simulativ mit einbezogen und potenzielle Fehlerquellen ausgeschlossen.

UMGANG MIT KOMPLEXEN SYSTEMEN

Per Definition sind Systeme komplexer als lediglich die Software, die Hardware oder jede andere Segmentierung. Das alleinige Konzentrieren auf Teile des Systems während jeder Entwurfstätigkeit ist zwingend erforderlich, um sich nicht in Komplexitätsfragen zu verlieren. Fehlen jedoch wichtige Kontextinformationen über die Rolle einer Komponente oder ihrer systeminternen Umgebung, sind Spezifikations- oder Designfehler unvermeidlich.

Es ist also eine geeignete Teilmenge (Ansicht) des Systems einzurichten, um ein spezifisches Design- oder Analyseanliegen zu verstehen. Hierbei dürfen lediglich die minimal erforderlichen Kontextinformationen enthalten sein. Alles, was für die vorliegende Aufgabe nicht relevant ist, ist auszublenden. Ein manuelles Erstellen einer geeigneten Ansicht, die den oben genannten Kriterien entspricht, ist sehr aufwendig und bei Änderungen im System der Gefahr der Inkonsistenz ausgesetzt. Zudem reicht es in der Regel nicht aus, lediglich eine Ansicht für einen Teil des Systems zu erstellen, da verschiedene Perspektiven der Systembetrachtung verschiedene Ansichten erfordern, die sich darüber hinaus überlappen können. Beispielsweise sind das Ansichten für funktionale oder organisatorische Abhängigkeiten, Engpassansichten, Lieferantenabhängigkeiten, Reifegrade oder Ansichten zur Ausfallwahrscheinlichkeit, um nur einige zu nennen.

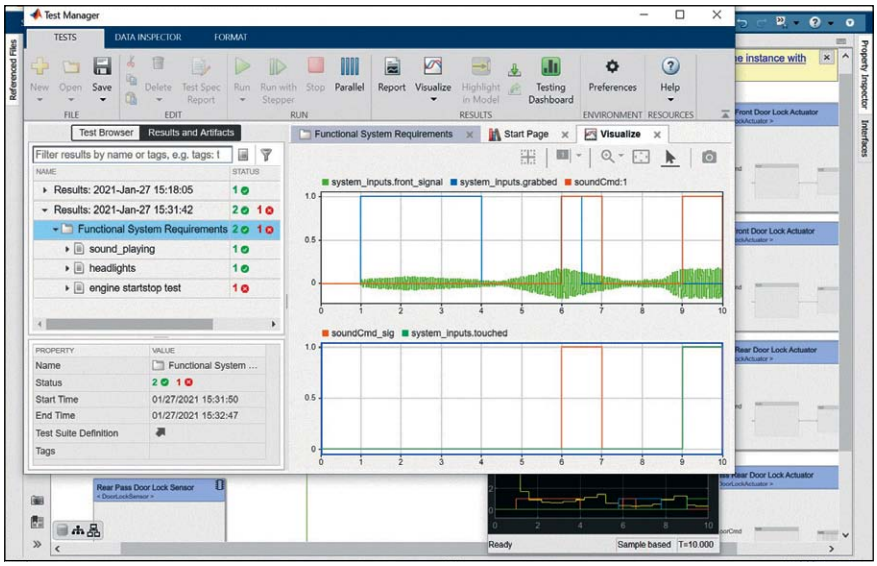


Bild 2. Simulation der Architektur im Rahmen einer Testautomatisierung. (Bild: MathWorks)

Ein vollständiges Verständnis eines bestimmten Design- oder Analyseanliegens erfordert ein schnelles Umschalten zwischen der großen Anzahl verschiedener Gruppen und Filter, die die Systeme benötigen.

Da all jene unterschiedlichen Sichtweisen auf ein System konsistent sein müssen, ist die Tool-Hilfe für das Einrichten und Verwenden von Sichtweisen entscheidend. Beispielsweise erlaubt der System Composer hierfür das Einrichten beliebiger Ansichten über multiple Filterbedingungen und optionale

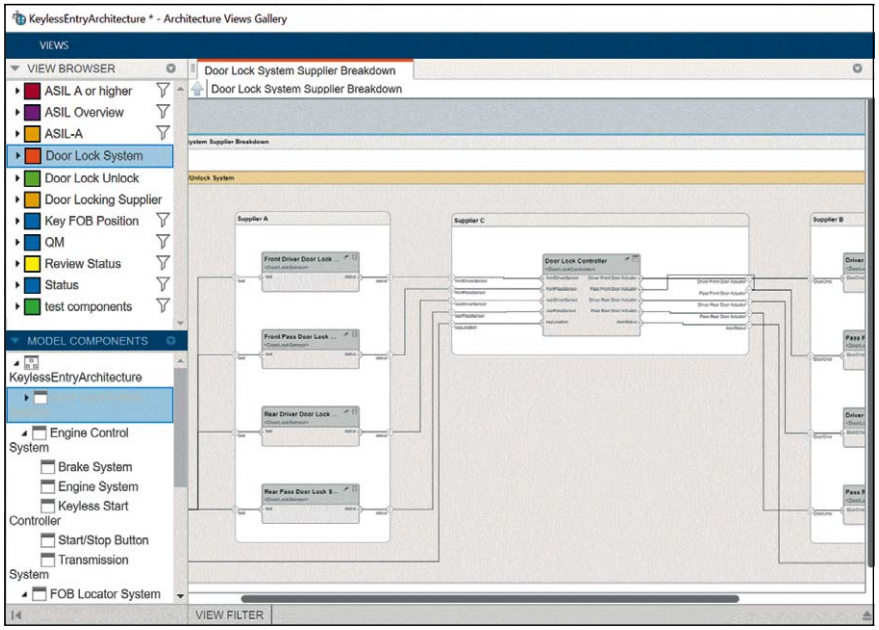


Bild 3. Ansichten zum Betrachten von Teilaspekten der Architektur, hier zum Beispiel Abhängigkeiten von den Zulieferern. (Bild: MathWorks)

Gruppierungskriterien **(Bild 3)**. So sind Teile der Architektur unter ausgewählten Gesichtspunkten darstellbar. Beispielsweise alle Komponenten von bestimmten Zulieferern und deren Beziehungen zum Betrachten von Lieferantenabhängigkeiten. Hier sind beliebige Kriterien möglich. Unnötige Komponenten oder Signalverbindungen sind zum Beispiel entfernt, hingegen sind optionale Gruppen einbezogen und im automatischen Layout berücksichtigt.

Bei entsprechender Werkzeugunterstützung sind die Sichten basierend auf den Filterbedingungen automatisch generiert und somit immer konsistent zur Gesamtarchitektur. Änderungen sowohl in der Struktur als auch in den Komponenteneigenschaften sind in allen Ansichten automatisch synchronisiert und somit aktualisiert.

Ebenfalls wichtig in der Systemtechnik sind sogenannte Allokationen. So beziehen sich beispielsweise Softwarefunktionen auf die logische oder physikalische Ausführungsebene. Zum Bearbeiten und Visualisieren der Allokationszuordnung haben sich Matrizendarstellungen bewährt.

DER EINSATZ VON MBSE-WERKZEUGEN

Aufgrund der Größe und Komplexität von Systemen sind klassische Ansätze mit Zeichentools und Tabellenkalkulationen zum Berücksichtigen benutzerdefinierter Eigenschaften und entsprechender Analysen nicht mehr angemessen. Probleme im Zusammenhang mit Einheitlichkeit oder veralteten Daten sind sehr wahrscheinlich. Gerade wenn keine spezielle Werkzeugunterstützung in Anspruch genommen wird, um die Daten zusammen und konsistent zu halten. Umso mehr gilt das für jeden manuellen Ansatz, mit dem eine Sicht auf das System geschaffen wird. Aus dem Grund sind MBSE-Werkzeuge oder Entwicklungsumgebungen für Software und für Hardware sehr zu empfehlen.

Für den Entwurf der Verhaltensspezifikation wird außerdem empfohlen, die Systemtechnikfunktionen in eine Entwicklungsumgebung zu integrieren. Sie ermöglicht ein nahtloses Fortsetzen der Arbeit auf Komponentenebene, ein automatisches Integrieren in die Architektur sowie ein Simulieren des Systems beim Validieren.

Für Model-based Design stehen dem Entwickler solche Systemtechnikfunktionen mit den Produkten System Composer und Simulink Requirements offen. Bereits während dem Architekturaufbau können Nutzer für jede Komponente mit Simulink ein zugehöriges Verhalten modellieren. Schnittstellen werden hierbei automatisch übernommen und sind somit immer identisch zur Architektur, ebenso bei Änderungen. Laufen die Verhaltensmodelle in Simulink, können Entwickler die Gesamtintegration der Architektur simulieren und testen. Mit diesen Systemtechnikfähigkeiten bietet Model-based Design somit einen vollständigen Workflow – von den Systemanforderungen über die Architektur und den Verhaltensmodellen bis hin zum virtuellen Produkt. TS

MARC SEGELKEN

ist Applikationsingenieur bei MathWorks im Bereich Systems Engineering und Verifikation sicherheitskritischer Systeme. Zuvor war er als wissenschaftlicher Mitarbeiter am Forschungsinstitut „OFFIS“ in der Abteilung für sicherheitskritische Systeme tätig. Er hat im Themenfeld der formalen Verifikation eingebetteter Systeme an der Universität Oldenburg promoviert.

LEISTUNGSMODELLIERUNG UND VALIDIERUNG VON PROTOTYPEN – TEIL 2

Portierbare Stimuliermethode für Post Silicon Validation

(Bild: Lightspring | Shutterstock)

Dass sich der Portable Stimulus Standard (PSS) mit den üblichen Standardmethoden zur Verfifikation, wie der Universal Verification Methodolgy (UVM), kombinieren lässt wird im zweiten Teil gezeigt. Am Beispiel eines Interconnect Bus wird verdeutlicht, welche Vorteile die Kombination bietet.

Von Gaurav Bhatnagar und Courtney Fricano

Die Leistungsanalyse der Interconnect Fabric ergibt die beste Konfiguration bezüglich Leistungsfähigkeit, Stromaufnahme und Flächenbedarf. Ist die Struktur der internen Verbindungen einmal festgelegt, kann sie benutzt werden, um mit einem konfigurierbaren automatischen Ablauf RTL-Code für den AMBA-Interconnect-Bus (AMBA, Advanced Microcontroller Bus Architecture) zu generieren. Allerdings kann dieser Ablauf wegen Konfigurationseinschränkungen, Softwarestruktur und manueller Interpretation der Spezifikationen fehleranfällig sein. Deshalb muss er verifiziert werden, um einen einwandfreien Entwicklungsprozess zu erhalten. Dies wird traditionell mit Einsatz der Industriestandard-UVM-basierten Methode erzielt.

UVM-BASIERTE VERIFIKATION DES INTERCONNECT-BUSSES

Die UVM-Umgebung zur Verifikation des Interconnect-Busses ist in **Bild 5** zu sehen. Sie besteht aus unterschiedlichen Arten von AMBA-Mastern (AXI, AHB, APB) und UVC-Slaves (UVC, Universal Verification Component) in anwendungsspezifischen Konfigurationen, die mit den Slaves bzw. Mastern des Prüflings verbunden sind. Diese Umgebung kann generisch konfiguriert werden. Die Rangfolgetabelle (SB, Scoreboard) meldet die Transaktionen und zeigt Fehler bei jeder Art von Datenabweichung an.

Die Tests beinhalten diverse Sequenzen, die die Funktionen der grundlegenden UVC und Schnittstellen steuern. Die Tests laufen in Übereinstimmung mit dem Testplan, der von den Spezifikationen festgelegt ist, mit den gesteuerten und zufälligen Testfällen. Die funktionellen Abdeckungspunkte werden auch bezüglich des Verifikationsplans kreiert, um sicherzustellen, dass die Spezifikation auch erreicht wird. Danach werden die Simulationen gemacht und eine Abdeckungsdatenbank erstellt, um Code und funktionale Abdeckung zu erfassen. Diese Datenbank wird analysiert und Abdeckungslücken werden überprüft. Danach laufen die Regressionen ab und damit werden Berichte

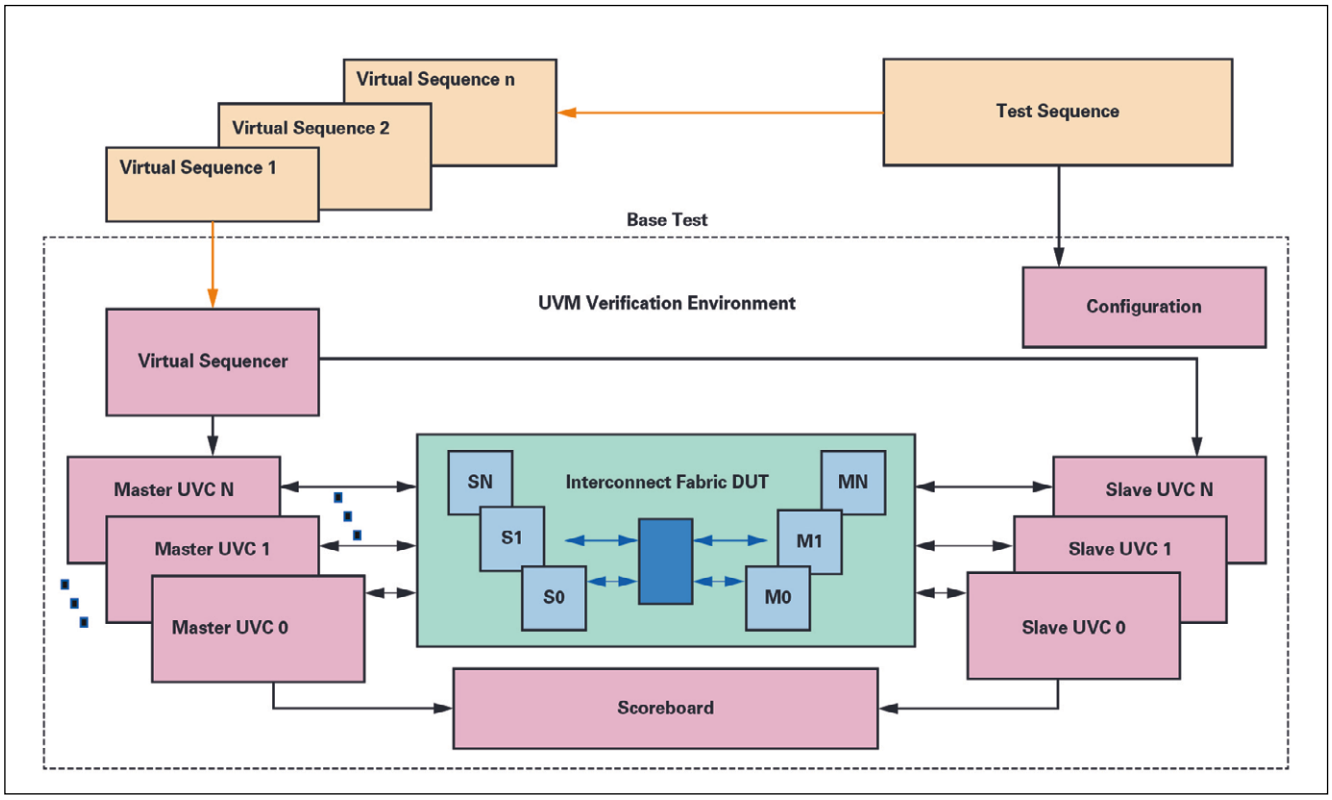


Bild 5. Die UVM-Umgebung zur Verifikation eines Interconnect-Bus-IPs besteht aus unterschiedlichen AMBA-Mastern (AXI, AHB, APB) und anwendungsspezifisch konfigurierten UVC-Slaves. (Bild: Analog Devices)

generiert und analysiert. Dieser Prozess wird solange wiederholt, bis die gewünschten Abdeckungsziele erreicht sind, um eine Verifikation hoher Qualität sicherzustellen.

Zusammen mit den gesteuerten Tests als Teil des Verifikationsplans, hängen die UVM-basierten Techniken auch von den zufälligen Tests ab, um die gewünschte Zielabdeckung zu erreichen. Sie beginnen mit einem Zufallsstimuli und verschärfen schrittweise die Einschränkungen bis die Zielabdeckung erreicht ist. Dies ist abhängig von der Leistungsfähigkeit der Randomisierung und der Rechenleistung der Server, um den Zustandsraum abzudecken. Ist die Codeabdeckung das quantitative Maß, so ist die funktionelle Abdeckung das qualitative Maß der Codeausführung des Prüflings. Typischerweise ist diese Qualität begrenzt durch die Sorgfalt und Gründlichkeit der Menschen, die den Verifikationsplan erstellen und die Testabdeckung analysieren. Der andere Faktor, der die Qualität der Verifikation entscheidet, ist die effektive automatische Überprüfung. Eine Kombination der Paketvergleiche mit den Rangfolgetabellen und festgelegten Prüfpunkten (Assertions) kann die Anzahl der Fehler in den gefertigten Bausteinen bestimmen, die später im Entwicklungsprozess entdeckt werden. Die UVM-basierte Verifikationstechnik ist unabhängig und sorgt für eine qualitativ hochwertige Verifikation. Dennoch verbessert die Einführung der PSS-basierten Techniken mit ihren umfangreichen Eigenschaften den Verifikationsablauf noch weiter.

PSS-BASIERTE VERIFIKATION DES INTERCONNECT-BUSSES

Die PSS-basierte Verifikation beginnt mit der Erstellung des Verifikationsplans laut der Entwurfsspezifikation und dem Aufbau der Verifikationsumgebung. Der Testzweck wird mit portierbaren Stimuli-Modellen, Einschränkungen und Konfigurationsdateien erfasst. Die Werkzeuge, die diesen Standard unterstützen, generieren dann die Tests für eine vorgegebene Verifikationsumgebung, wobei eine Graph-basierte Abdeckung aufgenommen wird. Die Analyse dieser Art der Testabdeckung kann die Lücken in den Testeinschränkungen und der Konfiguration anzeigen wobei dieser Vorgang erneut durchgeführt werden kann.

Bild 6 zeigt den Verifikationsablauf mit PSS-basierten Modellen. Dabei ist besonders wichtig zu beachten, dass die PSS-basierten Modelle die UVM-basierte Umgebung (siehe Bild 5) nicht ersetzen. Stattdessen werden sie zur bestehenden UVM-basierten Umgebung hinzugefügt, um deren Fähigkeiten zu erhöhen. Die UVM-Verifikationsumgebung hat weiterhin die

Test	Testläufe	Gut	Fehler	Kein Testlauf	Code Abdeckung insgesamt
nur UVM	125	125	0	0	298034/388949 (76,6 %)
UVM PSS	75	75	0	0	298034/388949 (76,6 %)

Tabelle 2. Im Vergleich zur UVM-basierten Verifikation erreicht die UVM-PSS-basierte Verifikation die gleiche Testabdeckung mit weniger Testläufen. (Quelle: Analog Devices)

Master- und Slaves-UVCs mit Rangfolgetabelle (SB) und Konfiguration, wobei die virtuellen Sequenzen mit der UVM-SV-Infrastruktur umgangen werden. Die Umgebung wird über einen UVM-Test auf der obersten Ebene gesteuert, der auf der einen Seite die virtuellen Sequenzen aufruft, um den UVC-Betrieb zu steuern. Auf der anderen Seite interagiert sie über PLI- oder DPI-basierte (DPI, Direct Programming Interface) Systemaufrufe mit dem vom portierbaren Stimulus generierten Format. Das PSS-basierte Modell wird im SystemC-basierten Prozess zur Leistungsmodellierung vollständig wiederverwendet. Die vom PSS-basierten Modell generierte Testlogik steuert alle Operationen zwischen den UVCs. Die Simulationen auf IP-Ebene nutzen die generierten Tests und erfassen die Abdeckung.

Tabelle 2 zeigt die Ergebnisse des Regressionslaufs mit PSS- und UVM-basierten Verifikationsumgebungen. Die Anzahl der eingeschränkten Zufallstests, die durchgeführt werden müssen, um die maximal mögliche Testabdeckung (mit Waivers) zu erzielen, wird mit der Anwendung einer UVM-PSS-basierten Methode signifikant reduziert. Der Zufallsmechanismus in der PSS-basierten Verifikation beginnt mit der abstrakten Beschreibung der gültigen Übergänge zwischen den Zuständen auf oberer Ebene des Prüflings. Er spezifiziert automatisch den minimalen Satz an Tests, die nötig sind, um die Pfade durch diesen Zustandsraum abzudecken. Die Graph-basierte Testabdeckung erlaubt es dem Anwender die Traversenpfade zu betrachten und Tests zu generieren, sodass die maximale Länge des Graphen abgedeckt ist.

Die Testqualität ist ein weiterer Faktor, der von der Verifikationsmethode mit portierbarem Stimulus besser gesteuert werden kann. Der Test kann visuell dargestellt werden, was es den Anwendern erlaubt, die Steuerung und den Datenfluss besser zu verstehen. Auch erlauben es einige Tools, aktive Prüfungen während der Runtime zu platzieren, was ein effektives automatisches Prüfen ermöglicht. Dies verbessert, kombiniert mit Scoreboard-Checking und Assertion-basierten Prüfpunkten die Qualität der Verifikation.

Die Methode mit portierbarem Stimulus arbeitet auf höherer Abstraktionsebene und integriert dann den darunter angeordneten Verifikationsprozess. Obwohl dies eine definitive Verbesserung in der Test- und Stimulus-Generation ist, schleppt diese Verifikationsmethode immer noch den grundlegenden Prozess in seiner ursprünglichen Form mit. Im Falle der Integration mit UVM-basierten Umgebungen wird einerseits von der Wiederverwendung von Verifikationskomponenten profitiert und anderseits wird dadurch seine Komplexität begrenzt. Auch ist die Qualität der Verifikation begrenzt von der Qualität des Verifikationsplans und der Analyse der Abdeckungsreports.

SoC-VERIFIKATION DES INTERCONNECT-BUSSES

Wenn der Interconnect-Bus als Teil des SoC integriert ist, ist es wesentlich,

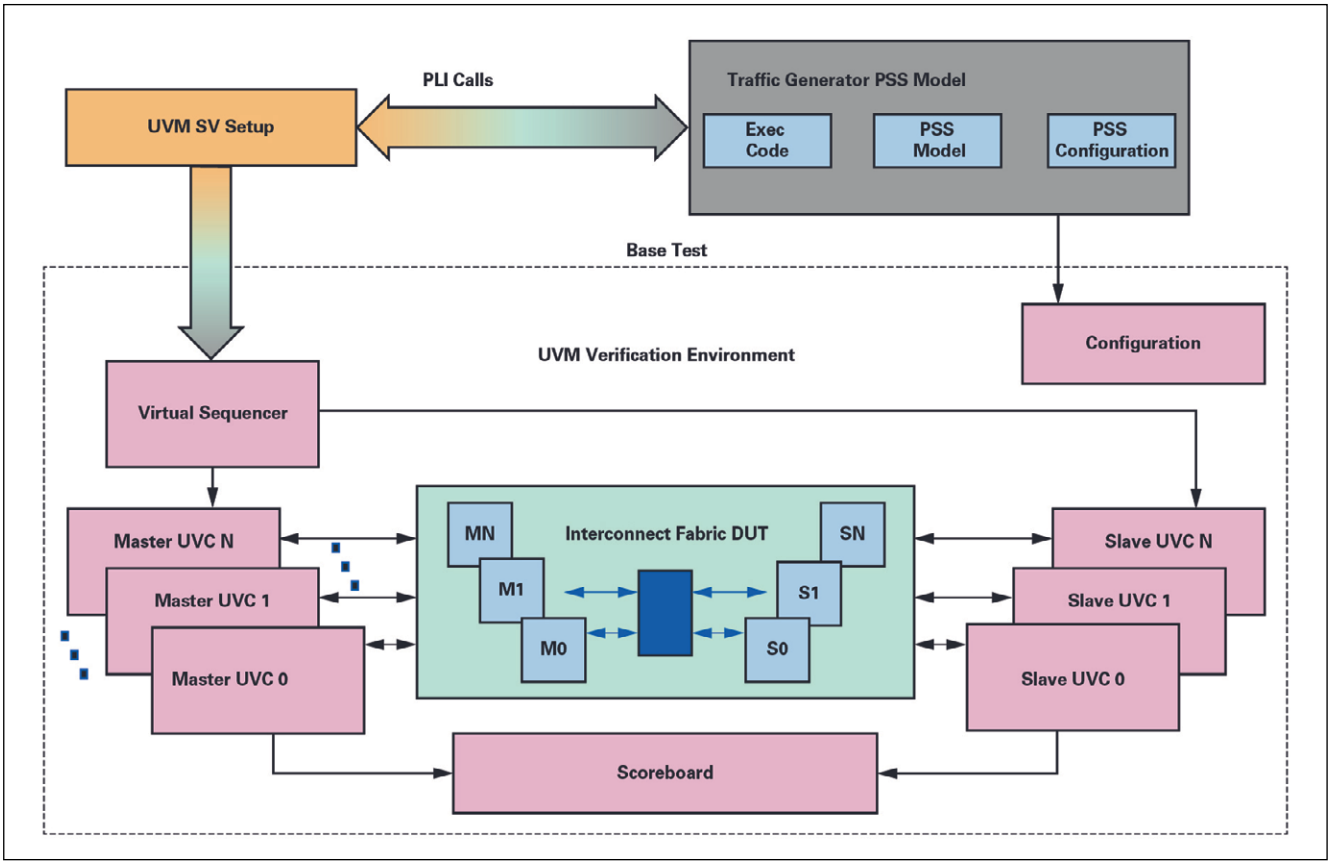


Bild 6. PSS-basierte Verifikation des Interconnect-Busses nutzt die aus Bild 5 bekannte UVM-Umgebung. (Bild: Analog Devices)

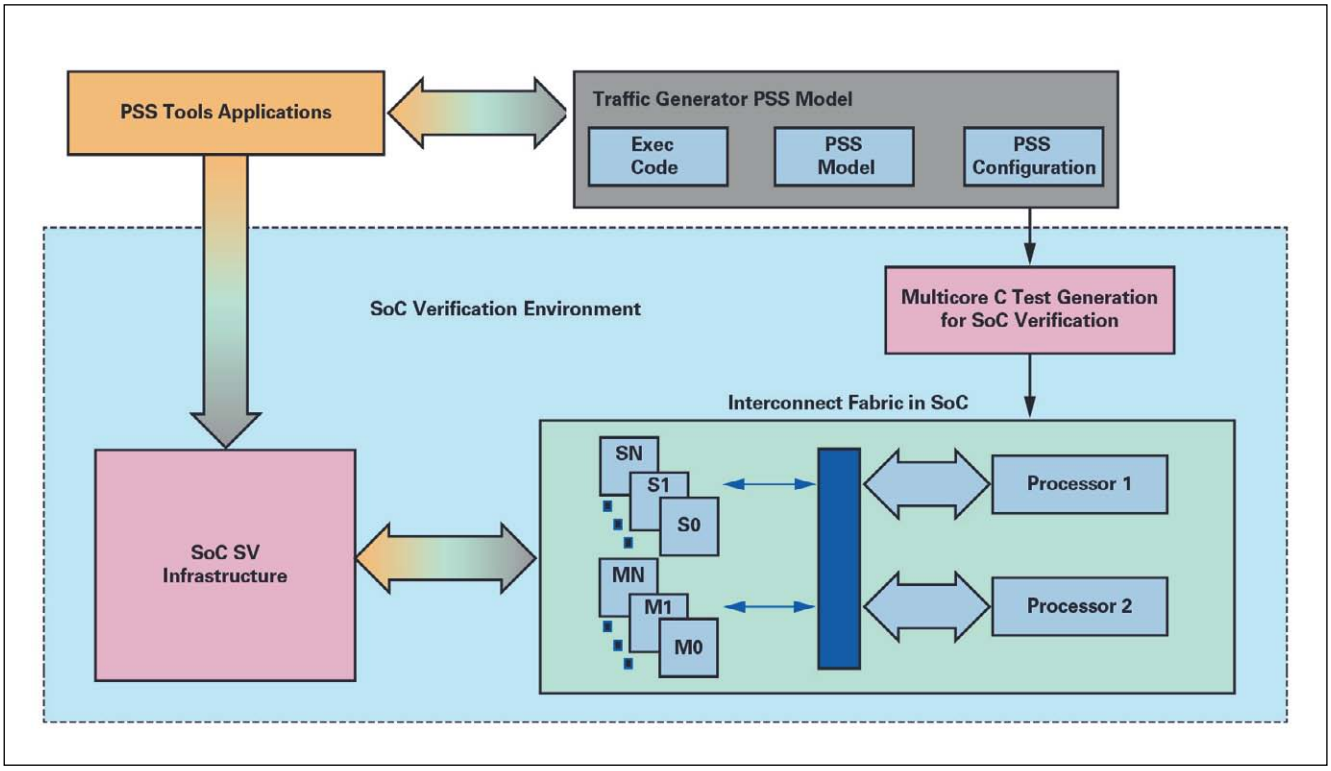


Bild 7. PSS-basierte Verifikation des Zwischenbusses in einem SoC. (Bild: Analog Devices)

seine Integration mit den unterschiedlichen Mastern und Slaves im System zu überprüfen. Dies wird üblicherweise mit C-basierten Tests gemacht, die auf dem Prozessor ablaufen, um die Integration des Interconnect-Busses zu überprüfen. Die generischen Master auf IP-Ebene wechseln zu spezifischen Bus-Mastern, wie Mehrfach-Prozessoren, DSP, DMA-Controllern und seriellen Protokoll-Mastern wie SPI, I²C, CAN und vielen weiteren anwendungsspezifischen Mastern und Slaves. Dies erfordert spezielle Sequenzen oder Makros, die dazu dienen, diese unterschiedlichen Master und Slaves im SoC zu steuern. Diese Makros oder Sequenzen sind üblicherweise Register-programmiert, um es zu ermöglichen, Sende- und Empfangstransaktionen von den Mastern, wie DMA-Controllern, Speichern etc., zu ermöglichen. Es gibt auf dieser Ebene keine eingeschränkte Randomisierung, sodass jedes Szenario untersucht und manuell geschrieben werden muss. In Bezug auf die Wiederverwendung können einige der UVM-Monitore aus der IP-Ebene genutzt werden, das Protokoll oder die Scoreboards anzuzeigen, um die besonders interessierenden Punkte zu überprüfen. Jedoch müssen die Tests und Sequenzen, die große Teile der Spezifikation beinhalten, mit einem anderen Fokus in C erneut erstellt werden.

Die PSS-basierte Verifikationstechnik wurde für die Wiederverwendung von Tests der IP bis zum fertigen SoC entwickelt. **Bild 7** stellt die Wiederverwendung des PSS-Modells des Traffic-Generators in der Verifikation auf SoC-Ebene dar. Die auf IP-Ebene codierten Modelle sind gemäß der SoC-Spezifikation für unterschiedliche Adress-Maps konfiguriert und zielen auf die Generierung von C-Tests ab. Der gleiche Satz an Sequenzen, geschrieben auf IP-Ebene mit der Graph-basierenden eingeschränkten Randomisierung, ist für die Wiederverwendung nutzbar.

Nahezu alle Sequenzen im Modell – ausgenommen die Teile, die für den Exec-Code gedacht sind – sind wiederverwendbar, wenn das Modell für Prozessor-basierte Applikationen geschrieben wird. Allerdings ist der Exec-Code in diesem Fall komplexer und enthält komplette Enable- und Disable-Makros für eine Vielzahl von Mastern wie DMA- und Speichercontroller, die die Single- oder Burst-Transaktionen auf dem Interconnect-Bus initiieren können.

Für jeden generischen Master muss der Exec-Code neu geschrieben werden, sodass er in die Vielzahl von Mastern im SoC integriert werden kann. Die Tool-Randomisierung erlaubt mehrfache Kombinationen von Master- und Slave-Transaktionen. Die Einschränkungen zum Erstellen von gesteuerten Tests zur Überprüfung der Integration auf SoC-Ebene kann mit der visuellen Repräsentation des Tests gut verwaltet werden. Sind die C-Tests einmal kreiert, werden sie über eine systemspezifische Standardinfrastruktur in die SoC-Konfiguration integriert. Diese C-Tests werden dann kompiliert und laufen auf dem Prozessor, um Transaktionen zu generieren.

Bild 7 zeigt ebenfalls die Erstellung von Mehrkerntests mit den PSS-Werkzeugen, die manuell nur schwierig zu kreieren sind. Unterschiedliche Teile des Testzwecks können so ausgelegt sein, dass sie auf unterschiedlichen Prozessorkernen laufen, was das Generieren interessanter Szenarien erlaubt. Dies ist besonders in dem Fall hilfreich, in dem mehrere Busmaster vorhanden sind. Das Programmieren unterschiedlicher Master wird durch diese Funktionspalette möglich.

Die Fähigkeit, Graph-basierte eingeschränkte Zufallstests auf SoC-Ebene

zu reproduzieren, ohne die Notwendigkeit Szenarien tatsächlich neu zu codieren, ist auch ein großer Vorteil. Sie erlaubt auch die Testgenerierung für unterschiedliche Fälle derselben IP mit verschiedenen Adress-Maps. Damit ist die Kreation von komplexen Szenarien möglich, wenn unterschiedliche Arten von PSS-Modellen für verschiedene IPs auf SoC-Ebene kombiniert werden. Manuell wären sie sonst nur sehr schwer zu codieren.

VALIDIERUNG DES INTERCONNECT-BUSSES

Die Validierung ist nötig, um die Übereinstimmung des Produkts mit den Spezifikationen, der Nutzbarkeit und der Abnahmeprüfung sicherzustellen. Traditionell benötigt ein Evaluation-Board C-basierte Tests, die aus der Originalspezifikation manuell erstellt wurden. Dieser doppelte Aufwand kann mit Einsatz einer PSS-basierten Methode, mit der C-Tests, die kompatibel mit der Evaluierungssoftware sind, generiert werden können, wesentlich reduziert werden.

Bild 8 repräsentiert den Validierungsprozess mit der PSS-basierten Methode. Das PSS-Modell für den Traffic-Generator kann entsprechend der SoC-Spezifikation für unterschiedliche Adress-Maps konfiguriert sein und auf die Erstellung von Eval-C-Tests abzielen. Die PSS-Werkzeuge haben üblicherweise die Fähigkeit, Tests für mehrfache Prozessorkerne zu generieren, was den Test spezifischer Szenarien einschließt. Die erstellten C-Tests werden von den Debuggern kompiliert und der Code wird mit Schnittstellen wie JTAG auf das Evaluation Board geladen. Die Tests können dann ablaufen und die Ergebnisse werden auf dem Evaluierungs-Board und dem Debugger-Interface angezeigt.

Derselbe Satz von Sequenzen, der auf SoC-Ebene mit der Graph-basierten eingeschränkten Randomisierung geschrieben wurde, kann komplett wiederverwendet werden. Zusätzlich erweist sich die visuelle Repräsentation des Testzwecks und die Fähigkeit Beschränkungen einzubinden als nützlich, um festgelegte Szenarien zu kreieren. Dies ist eine einzigartige und kontrollierbare Methode, um Tests in der Validierungsphase zu generieren und erfolgte traditionell komplett manuell. Auch hier muss der Exec-Code für die spezifischen Anforderungen der Validierung des Bausteins neu geschrieben werden. Die grundlegenden Softwaretreiber von der Validierungsplattform, die genutzt werden, um die unterschiedlichen Master auf dem Bus wie DMA- und Speichercontroller zu steuern, können typischerweise auch für diese Art von Anwendung genutzt werden. Der generierte Code muss jedoch in ein Format übersetzt werden, das von den Evaluierungsplattformen akzeptiert wird. Dieser Prozess beinhaltet typischerweise die Wiederverwendung des Kopfes (Header) und nimmt Dateien von bereits vorher geschriebenem Validierungscode und verwendet ihn in dem generierten Integrationscode. Dieser Code wird dann kompiliert

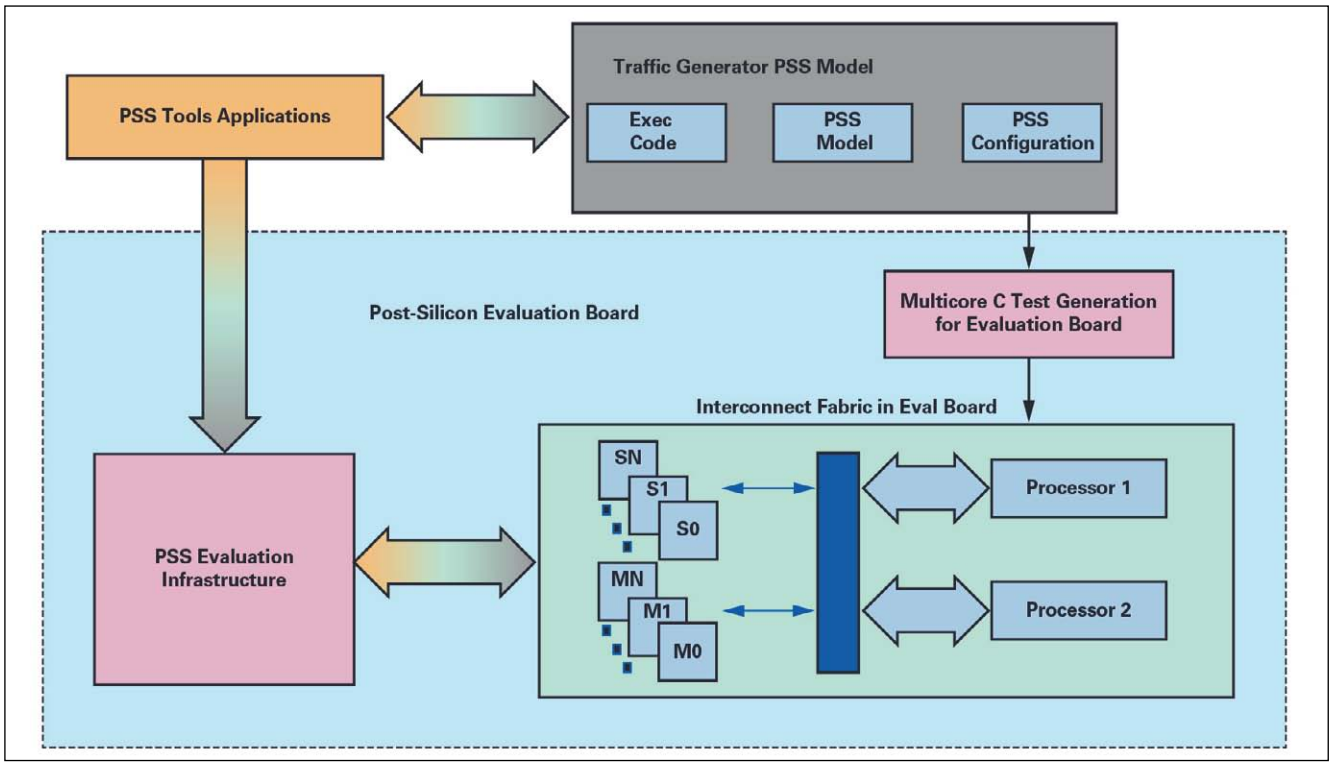


Bild 8. PSS-basierte Validierung des Interconnect-Busses im gefertigten Chip. (Bild: Analog Devices)

und läuft auf dem Ziel-Debugger, um einen sauberen Test auf dieser Ebene sicherzustellen.

Die PSS-Tools bieten üblicherweise die Fähigkeit, die Ergebnisse des Prüflaufs mit Applikationen auf den fertigen Bausteinen zu analysieren. Die visuelle Analyse der Testergebnisse zeigt entweder Gut oder fehlerhaft an und mit speziellen Codesegmenten lassen sich Ergebnisse ausgeben. Dies ist besonders im Validierungsprozess hilfreich, weil hier die traditionellen Debugging-Fähigkeiten sehr eingeschränkt sind.

Obwohl hier die C-Tests für das Traffic-Generator-Modell für die Applikationen auf den fertigen Bausteinen nicht wiederverwendet werden, lässt sich mit Sicherheit sagen, dass sie auf jeder Evaluierungsplattform eingesetzt werden können, die C-basierte Tests beinhaltet. Tatsächlich haben sich die Arten von Modellen, bei denen SoC-basierte PSS-Modelle für Post-Silizium-Evaluierungsboards wiederverwendet werden, für andere prozessorbasierte Anwendungen bewährt. Diese Wiederverwendung ist einzigartig und nur mit portierbaren Stimulus-basierten Methoden möglich. HS

Literatur

[1] *Bhatnagar, G.; Fricano, C.:* Leistungsmodellierung und Validierung von Prototypen – Teil 1 – Portierbare Stimuliermethode für Post Silicon Validation. *Elektronik*, 2021, H. 3, S.32–36.

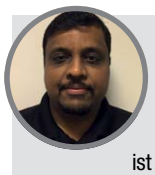
[2] *Ajamian, T.:* AMBA Interconnect Design Flow Automation. Synopsys, Inc., 2015, www.synopsys.com/news/pubs/snug/2015/boston/F1.2_Ajamian_paper.pdf

[3] *Gaurav, B.; Brownell, D.:* Portable Stimulus vs. Formal vs. UVM: A Comparative Analysis of Verification Methodologies Throughout the Life of an IP Block." Design and Verification Conference (DVCon), 2018, Konferenzband, http://events.dvcon.org/2018/proceedings/papers/02_1.pdf

[4] Portable Stimulus Working Group. Website, Accellera Systems Initiative, 2019, https://www.accellera.org/activities/working-groups/portable-stimulus

[5] TrekUVM: Eliminating UVM Overhead. Website, Breker Verification Systems, 2019, https://brekersystems.com/products/trekuvm

[6] Download UVM (Standard Universal Verification Methodology). Website, Accellera Systems Initiative, 2019, https://accellera.org/downloads/standards/uvm



GAURAV BHATNAGAR

ist Staff Design Verification Engineer in der Engineering Enablement (EE) Group bei Analog Devices (ADI). Er ist Elektronikingenieur mit 15 Jahren Erfahrung und kam 2015 zu ADI. Er arbeitet an universellen, Format- und portierbaren Stimulus-Verifikationsmethoden.
gaurav.bhatnager@analog.com.

COURTNEY FRICANO

ist Staff Verification Engineer in der Engineering Enablement (EE) Group bei Analog Devices (ADI). Sie leitet das Verification-Subteam des Engineering Systems and Verification Center of Excellence. Courtney hat einen Bachelor-Abschluss von der Penn State University und einen Master vom MIT.
courtney.fricano@analog.com

1.–5.3.2021

DIGITAL

embeddedworld2021

Exhibition&Conference

... it´s a smarter world

CONFERENCE PROGRAM

www.embedded-world.eu

Organized by

DESIGN& ELEKTRONIK
KNOW-HOW FÜR ENTWICKLER
design-elektronik.de

NÜRNBERG MESSE

Conference Sponsors

axivion
stopping software erosion

Green Hills SOFTWARE

HARWiN
Connect with confidence

Texas Instruments

Overview
Conference Program

embeddedworld2021 Exhibition&Conference ...it's a smarter world DIGITAL

DAY 1

	1. Internet of Things – Platforms & Applications		2. Connectivity Solutions		3. Embedded OS	4. Safety & Security		5. Board Level Hardware Engineering	6. Software & Systems Engineering	
morning	IoT Architectures & Platforms 1		Wired Fieldbus 1		OS Basics 1	Safety Processes and Standards 1		Hardware Basics	Languages & Standards	
afternoon	IoT Architectures & Platforms 2	Class 1.1 The Power of APIs and Containers on Embedded Switching	TSN 1	Class 3.1 Build Your Own Embedded Linux CI/CD Pipeline Using the Cloud	OS Basics 2	Safety Processes and Standards 2	Class 4.1 Security Beyond Cryptography: Security Enclave for Asymmetric Multi-processing	Hardware Development	Languages & Standards: MISRA	Class 6.1 Effective Use Cases, User Stories, and Scenarios
	Localisation		Conformance Testing		OS Virtualization	Safety Processes and Standards 3		Hardware Power	Development Process	

DAY 2

	1. Internet of Things – Platforms & Applications	2. Connectivity Solutions	3. Embedded OS	4. Safety & Security	5. Board Level Hardware Engineering	6. Software & Systems Engineering			10. System-on-Chip (SoC) Design	
morning	Software for IoT 1	Wired Fieldbus 2	OS Automotive, Android, AutoSAR	Security Processes and Standards	Class 5.1 Ultra Low Power Hands-on Workshop	Development Process			Embedded AI 1	Class 10.1 FPGA-Design Using C/C++ and High-Level Synthesis
afternoon	Software for IoT 2	Bluetooth 1	OS Open Source	Safety Architectures 1		Measures & Metrics	Class 6.2 Agile for Embedded Systems	Class 6.3 The Greg Davis Class – Advanced C/C++ Coding and Debugging Techniques	Embedded AI 2	
	Data Management	TSN 2	ROS	Safety Architectures 2		Requirements Engineering			Embedded AI 3	

DAY 3

	1. Internet of Things – Platforms & Applications	2. Connectivity Solutions		4. Safety & Security	5. Board Level Hardware Engineering	6. Software & Systems Engineering				8. Autonomous & Intelligent Systems	9. Embedded Human-Machine-Interface
morning	OTA Firmware Updates	Wired Fieldbus 3	Class 3.2 Embedded Android Workshop	Safe AI		DevOps	Class 6.4 Creating Domain-Specific Modeling Languages: Hands-on			AI Hardware	HMI Libraries
afternoon	Low Energy Devices	Bluetooth 2		Security Hardware	Class 5.2 Easy Design of IoT Wireless Devices Embedding Antennas	DevOps / MBD		Class 6.5 Advanced Behavioral Modeling with UML/SysML: Activities	Class 6.6 Modern C++ for Embedded Development	AI Use Cases	HMI Design Methods 1
	Edge Computing	Wired Fieldbus 4		Security Use Cases		Software & System Quality					HMI Design Methods 2

DAY 4

	1. Internet of Things – Platforms & Applications	2. Connectivity Solutions		4. Safety & Security	5. Board Level Hardware Engineering	6. Software & Systems Engineering			7. Embedded Vision	8. Autonomous & Intelligent Systems	10. System-on-Chip (SoC) Design
morning	Security im IoT 1	Class 3.3 Introduction to Embedded Linux in Theory and Practice – Short Crash Course	Class 3.4 Fast Track to Yocto Project	Security Architectures 1		Software Quality	Class 6.7 How to Improve Software Quality Through Test Automation		Application Case Studies		Complex IC & System Solutions
afternoon	Security im IoT 2			Security Architectures 2	Class 5.3 Production Optimized Hardware Design	Software Quality: Static Analysis		Class 6.8 Advanced Behavioral Modeling with UML/SysML: State Machines	Systems Integration 1	Class 8.1 Developing Artificial Intelligence Using Machine Learning at the Edge with Embedded µSoC FPGAs	IP Core Design & Integration
	IoT Use Cases 1			Hacking		Software Quality: Coding			Systems Integration 2		Mixed Signal & Energy Optimization

DAY 5

	1. Internet of Things – Platforms & Applications	4. Safety & Security	6. Software & Systems Engineering	7. Embedded Vision	10. System-on-Chip (SoC) Design
morning	Security im IoT 3	Security Architectures 3	Testing & Debugging 1	SW Tools & Tooling AI & Tool Chains	Core Integration & Tools 1
afternoon	IoT Use Cases 2	Long Term and Security	Testing & Debugging 2	Embedded Vision	Core Integration & Tools 2

embeddedworld2021
Exhibition&Conference
... it´s a smarter world

DIGITAL

Prof. Dr.-Ing. Axel Sikora
Chairman of embedded world Conference

embedded world Conference 2021 DIGITAL

embedded.intelligent.systems – the innovators' place to be

The world has been changing rapidly during the last year. The embedded world Exhibition & Conference in 2020 will certainly be remembered by a lot of us, as it was the last big event in the last year that allowed physical presence with personal interaction discussions, smalltalk, professional meetings and much more.

In these months, however, a lot of experience showed that digital platforms have improved significantly and that – with thoughtful preparation – excellent events can be performed. Even though they cannot replace all aspects of an intense human interaction, they can enable excellent background learning and knowledge transfer, can foster lively discussions with partners that you might not access in the physical world, and can allow new and yet unknown formats of exchange of ideas.

For a thorough preparation of the 19th thrilling edition of the embedded world, we decided already in November to go for embedded world 2021 DIGITAL. Together with this digital format, embedded world will be held during five full days. Ten tracks will feature 78 sessions with 234 presentations. They will be garnished with additional elements to help a maximum interaction and liveliness.

- We will have five first-class keynotes from top notch industry leaders, including Dr. Reinhard Ploss, CEO Infineon Technologies, Kevin Dallas, CEO Wind River, Randall Restle, Restle LLC, Strategic Advisor to Digi-Key, Prof. Dr. Peter Liggesmeyer, Director Fraunhofer Institute for Experimental Software Engineering (IESE), and Paul Gray, Senior Research Manager Omdia.
- Also, we will feature four plenary panel discussions on hot topics, like Embedded AI, Embedded Vision, Safety & Security, and Connectivity in the IoT.
- All sessions will not only include the presentations, but also discussions and Q&A in each session amongst the speakers and the participants.
- 19 half- or full day classes will cover in-depth knowledge transfer and actual topics.

We see more and more Artificial Intelligence (AI) and Machine Learning (ML) in real applications using embedded and Internet of Things (IoT) architectures: from autonomous vehicles to image recognition and embedded vision systems to preventive and demand-driven maintenance in Industrial IoT systems, from small edge computers to high-performance cloud servers. And increasingly, these applications are interconnected, balancing edge, cloud, and fog computing – with all its challenges for software, hardware and system design, device and application management, security, safety, connectivity, verification and testing, and more. These developments do not only continue to promise immense possibilities and extensive business opportunities, but are also closely associated with many technical, economic, social and ethical issues.

The embedded world Conference 2021 DIGITAL is clearly structured along 10 tracks, which are represented in different colors throughout the program: 1. Internet of Things, 2. Connected Systems, 3. Embedded OS, 4. Safety & Security, 5. Hardware Engineering, 6. Software & Systems Engineering, 7. Embedded Vision, 8. Autonomous & Intelligent Systems, 9. Embedded GUI & HMI, and 10. System-on-Chip.

The embedded world 2021 DIGITAL will cover all aspects of the development and application of embedded systems, from fundamental technologies to development processes and special fields of applications. It is one of the central strengths of the event to be cross-sectoral and interdisciplinary. The conference provides a platform to bring together experts from different domains and application areas of embedded systems in order to promote a holistic system design approach, to identify synergies and commonalities, and to strengthen the exchange of knowledge and experience.

The steering board of the embedded world 2021 DIGITAL wishes you and all participants stimulating discussions about new ideas and solutions enabling you to cope more easily and efficiently with the immense challenges that lie ahead. You are welcome to gain great insights in a pulsating atmosphere.

Best wishes & stay safe

Sign-up & Registration:
www.embedded-world.eu

The Conference Keynotes

embeddedworld2021 Exhibition&Conference ...it's a smarter world DIGITAL

The Conference Keynotes feature prominent speakers on major trends in the industry. These highlight presentations have an exclusive time slot within the busy event schedule.

Monday, 01 March, 10:15

How to Build Embedded Intelligent Systems for a Post-Pandemic World

Dr. Reinhard Ploss, CEO, Infineon Technologies

COVID-19 has accelerated the digitalization process. While large-scale cloud-based systems are already very advanced, embedded intelligence systems are just about beginning to gain traction. Embedded intelligent solutions combine the best of both cloud and edge. The edge keeps personal data local, enables real-time responses, and provides cost-efficiencies by not requiring centralization of all data. Meanwhile, the cloud provides device access to an infinite amount of information allowing for better decision-making. This keynote will focus on three challenges, that IoT edge developers will face and how to address them.

Tuesday, 02 March, 10:15

Engineering Smart Ecosystems

Prof. Dr. Peter Liggesmeyer, Director Fraunhofer IESE

On the one hand, many standards in software and systems engineering are based on assumptions that are currently no longer fulfilled: Systems are treated as closed, static artefacts, with no autonomy and typically the underlying development process is assumed to be traditional and phase-oriented. On the other hand, systems in many domains – e.g. Industry 4.0, autonomous driving, energy management – are different: They are open, they do dynamic adaption in an autonomous way and they are large and heterogenous. This influences the systems engineering solutions that are to be applied in order to master these challenges

Wednesday, March 03, 10:15

Display Disruption: How New Display Technologies are Changing the Industry

Paul Gray, Senior Research Manager, Omdia

Paul Grey is Speaker of the electronic display Conference and will share his thoughts with the entire embedded community in this keynote. 2020 saw seismic changes in the display industry as 2019 plans came to fruition from some companies, while the overall display industry rode the waves of COVID-19. As a result, the industry has evolved rapidly through the year and a new form is beginning to take shape. The talk will examine the new realities, investigate why the surge in R&D especially on new display technologies and offer a viewpoint on future commercial and technical developments

Wednesday, 03 March, 15:30

Modern Embedded Engineering: Where we Are and our Exciting Future

Randall Restle, former Vice President of Applications Engineering at Digi-Key Electronics, now Strategic Advisor at Restle, LLC

Nearly anyone today can feel like an embedded engineer. A plethora of new electronic systems are being developed by individuals outside of our profession. Though initially this trend could be viewed as concerning to professionals, Randall is excited by the prospects for the professional engineer. He predicts embedded engineering will increase in importance as it continues to create leverage for all developers. Electronic systems will become even more important as the backbone of modern economies. In this keynote, he aims to describe the technical details which enabled this change to occur and explains the role of the modern embedded engineer in reducing integration complexity to attract new customers and traditional ones alike.

Thursday, 04 March, 15:30

Challenges of Digital Transformation for the New Intelligent Edge

Kevin Dallas, CEO, Wind River

Edge computing comes with challenges. Edge devices have vast variations between devices, many of them having been tailor-made for a specific purpose. Another example is security. While access to physical data centers can be limited, edge devices are located in disparate locations, where they can be accessed and dismantled. To combat all of these issues, digital frameworks and architectures have to be examined and restructured to adapt to the new workspace. This requires new skills. Combining skills, toolchains, methods from both cloud environments and embedded domains becomes increasingly important. We need to rethink how these systems are built and retool ourselves to prepare for them.

The presentations of the embedded world Conference are running in ten tracks. Each track represents one of the main conference topics. Track keynotes have been chosen based on their high innovation and relevance for the selected track.

Monday, 01 March, 13:30
TRACK KEYNOTE Internet of Things
Get More Productivity with Cloud Services
Reinhard Keil, Arm

Today most embedded applications are still created on desktop computers. For other applications cloud computing is well established. During this talk you will learn how cloud-based tools can help to improve the development flow for embedded. It starts during product evaluation, includes model- or simulation-based validation with continuous integration flows, model optimization for machine learning, up to device provisioning for deployment.

Monday, 01 March, 13:30
TRACK KEYNOTE Connectivity
TSN as the Key Enabler for Converged Networks: Current Status and Challenges
Florian Frick, University Stuttgart

Time Sensitive Networking (TSN) is the key enabling technology for future converged real-time networks across industries. But real-world deployments are still rare. A key reason for this is that TSN itself can only be a part of a solution and further standards are required to create an interoperable eco-system up to the application layer. While reviewing these aspect, the presentation will also help to understand where opportunities are.

Monday, 01 March, 11:00
TRACK KEYNOTE Embedded OS
Using Future Proofed Microcontroller Designs with FreeRTOS
Richard Barry, Amazon Web Services

There is an amazing dynamic between the edge and the cloud. Many applications rely on the physical world around us where microcontrollers are dominating. This talk will discover how to overcome challenges in development acceleration while ensuring firmware integrity and longevity and what that means for an open source project that has been in development for more than 15 years.

Tuesday, 02 March, 16:15
TRACK KEYNOTE Safety & Security
Taming Timing - Combining Static Analysis with non-intrusive Tracing to Compute WCET Bounds on Multicore Processors
Daniel Kästner, AbsInt Angewandte Informatik GmbH

For safety-relevant real-time applications, worst-case execution time (WCET) bounds have to be determined in order to demonstrate deadline adherence. We present a hybrid method that combines static analysis with non-intrusive instruction-level tracing to automatically compute WCET bounds - including interference effects. This will be show using the Infineon AURIX as a reference architecture.

Tuesday, 02 March, 16:15
TRACK KEYNOTE Hardware Engineering
Power Management in Embedded Systems
Colin Walls, Mentor, a Siemens Business

We will discuss design considerations that should be made when starting a new power sensitive embedded design, which include choosing the hardware with desired capabilities, defining appropriate power usage profiles, choosing an appropriate operating system and drivers, and providing power goals to the software development team to track throughout the development process.

Tuesday, 02 March, 16:15
TRACK KEYNOTE Software & Systems Engineering
The Application of Open Source Technologies to Embedded Systems
Mike Milinkovic, Eclipse Foundation, Inc.

IoT developers expect many technologies to be open source. While businesses appreciate the cost savings of the model, what they value about it is the control and flexibility it gives them. This presentation will examine the application of open source technologies to embedded systems across a host of industries, from smart manufacturing, automotive, cyber-physical systems and smart cities.

Tuesday, 02 March, 16:15
TRACK KEYNOTE Embedded Vision
The State of Khronos Standards Powering the Future of Embedded Vision & Inferencing
Neil Trevett, The Khronos Group

This presentation will provide a state-of-the-industry update on the family of Khronos open standards for programming and deploying accelerated inferencing and embedded vision including OpenCL, Vulkan, OpenVX, SYCL and NNEF. The talk will include future directions for these standards and provide attendees insights into which of these standards may be relevant to their embedded vision and inferencing projects.

Thursday, 04 March, 11:00
TRACK KEYNOTE Autonomous & Intelligent Systems
Dependable Neural Networks through Redundancy - Comparing Architectures
Hans Dermot Doran, ZHAW

The speaker examines the computational cost of a common ML classification task, based on substantial experimental evidence on both standard GPU and FPGA platforms. We will look at the real-time characteristics of the task, and how this is handled by the platform. Coordination/synchronisation issues between the redundant components will be mentioned and we clearly enumerate the dependability considerations that need to be taken into account in this area as well.

Wednesday, 03 March, 13:30
TRACK KEYNOTE Embedded HMI
Human Factors and User Interface Technology for Embedded Systems
Prof. Robert Oshana, NXP Semiconductors

From a human factors perspective, we must shift the design perspective away from technology as the end all and more towards usability for embedded devices. Topics of this session include the evaluation of an interface and its interaction quality, the study of human characteristics affected by interface design, requirements data collection and analysis, and more. We will use several industry examples to demonstrate these concepts.

Thursday, 04 March, 13:30
TRACK KEYNOTE System-on-Chip Design
Architecture Trends for Sensing and Computing to enable Automated Driving
Robert Schweiger, Cadence Design Systems

The level of automation of a vehicle is the key driver for E/E architectures, sensor architectures and System-on-Chip architectures. Radar, Lidar and Camera sensors still need to be significantly improved but will also evolve to address new compute architectures. A new class of high-performance System-on-Chip (SoC) and/or System-in-Package (SiP) is needed to process all sensor data and fuse them together to enable vehicles to become "aware" of their surroundings.

Monday, 01 March
Conference Program

embeddedworld2021 Exhibition&Conference ... it's a smarter world DIGITAL

	Internet of Things – Platforms & Applications	Connectivity Solutions	Embedded OS
10:00	**Welcome**		Prof. Dr.-Ing. Axel Sikora, Conference Chair
10:15	**Conference Keynote: How to Build Embedded Intelligent Systems for a Post-Pandemic World**		Dr. Reinhard Ploss, Infineon Technologies
	IoT Architectures & Platforms 1	**Wired Fieldbus 1**	**OS Basics 1**
11:00	**The Automotive Paradigm Shift: Connectivity at the Core** Pedro Lopez Estepa, Real-Time Innovations (RTI)	**CAN XL – the Next Generation of CAN** Holger Zeltwanger, CAN in Automation (CiA)	**Track Keynote: Using Future Proofed Microcontroller Designs With FreeRTOS** Richard Barry, Amazon Web Services
11:30	**ACRN: Bridging Orchestrator and Hard Realtime Workload Consolidation** Peter Fang, Intel	**10BASE-T1L Based Connection for Field Devices in Cyber-Physical Systems: A Proof of Concept** Victor Chavez, FH Aachen	**Operating Systems for Embedded Applications** Colin Walls, Mentor, a Siemens Business
12:00	**Architecting Scalable Real-time Systems With Embedded Devices: Connecting the Edge to the Cloud** Thijs Brouwer, Real-Time Innovations (RTI)	**IO-Link as the Catalyst for Industrial IoT** Florian Bader, AIT, Dominik Deschner, Stego	**Increasing Resilience to Cyberattacks Through Advanced Use of Static Code Analysis** Dr. Martin Becker, The MathWorks
12:30	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
12:45	Networking		
	IoT Architectures & Platforms 2	**TSN 1**	**OS Basics 2**
13:30	**Track Keynote: Get More Productivity With Cloud Services** Reinhard Keil, Arm	**Track Keynote: TSN as the Key Enabler for Converged Networks: Current Status and Challenges** Florian Frick, ISW Universität Stuttgart	**How Does an IoT OS Differ to a Traditional RTOS?** Stefano Cadario, Arm
14:00	**Cloud-enabled IoT Device Made Simple!** Stefan Vaillant, Software AG	**Bridging Wired and Wireless Time Sensitive Networking: Opportunities and Challenges** Dr. Dave Cavalcanti, Intel	**Building Secured, Connected, Real-Time Devices, With Micorsoft Azure Sphere and Azure RTOS** Sylvain Ekel, Mike Hall, Microsoft
14:30	**Curl is the Internet Data Transfer Engine** Daniel Stenberg, wolfSSL	**Open Source Software Technology for TSN Resource Management** Boon Leong Ong, Intel	**Design Patterns in RTOS Based Applications** Jacob Beningo, Beningo Embedded Group
15:00	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
15:15	Networking		
15:30	**Panel Discussion: Embedded Artificial Intelligence**		Chair: Prof. Dr.-Ing. Axel Sikora
	Localisation	**Conformance Testing**	**OS Virtualization**
16:15	**Sub-meter Localization Precision Based on Bluetooth** Clement Chaduc, Texas Intruments Norway	**A Versatile Measurement and Debug Tool for NFC Interoperability Testing** Martin Erb, Graz University of Technology	**Achieving Optimum System Performance With Embedded Virtualization** Leo Hendrawan, Randy Martin, BlackBerry QNX
16:45	**Smart Proximity Detection and Data Monitoring Using Bluetooth Low Energy Interface** Saurabh Rawat, STMicroelectronics	**TBA**	**Comparing Methodologies to Improve Security and Reliability of Untrusted Embedded Systems** Dr. Carmelo Loiacono, Green Hills Software
17:15	**Evolution of Location Solutions With Bluetooth LE** Srividya Sundar, Texas Instruments	**UWB Reloaded – Test & Certification Based on IEEE802.15.4z** Joerg Koepp, Rohde & Schwarz	**Hypervisor or Multicore Framework: Which is Best?** Colin Walls, Mentor, a Siemens Business
17:45	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A

Safety & Security	Board Level Hardware Engineering	Software & Systems Engineering	
Welcome		Prof. Dr.-Ing. Axel Sikora, Conference Chair	10:00
Conference Keynote: How to Build Embedded Intelligent Systems for a Post-Pandemic World		Dr. Reinhard Ploss, Infineon Technologies	10:15
Safety Processes and Standards 1	**Hardware Basics**	**Languages & Standards**	
Impact of the 3rd Edition of IEC 61508-1/-2 on Your Development Stephan Aschenbrenner, exida.com	**Interfacing to Current Transformers** George Slama, Wurth Elektronik eiSos	**Selecting a Coding Standard – or Build Your Own?** Mark Richardson, LDRA	11:00
Update on Maintenance of IEC 61508-3 for Safety Software Michael Kindermann, Pepperl+Fuchs	**Reference Potential and Current Displacement on Ground Lines.** Thomas Eichstetter, Essentielle Elektronik Eichstetter	**Managing the Risk of Adopting Third Party Code in a Functional Safety Context** Martin Woodhall, LDRA	11:30
SIL and ASIL – is that Really the Principal Difference Between Safety for Plants and Safety for Cars? Andreas Weber, J. Schmidt, Altran	**Single Pair Ethernet Filter Design (part 2)** Martin Leihenseder, Würth Elektronik eiSos	**Is Golang (Go) a Suitable Programming Language for IoT Applications?** Stefan Wellnitz, DH electronics	12:00
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	12:30
	Networking		12:45
Safety Processes and Standards 2	**Hardware Development**	**Languages & Standards: MISRA**	
Model-based Top-down Flow for Safety related Automotive Battery Management Ics Dr. Ralph Görgen, Mark Hafermalz, NXP Semiconductors Germany	**Fast Prototyping with Embedded Super Computers** Alexey Gromov, ZHAW Institute of Embedded Systems	**MISRA C/C++ Situation Report** Andrew Banks, LDRA Software Technology + MISRA	13:30
A Proposed Risk-based Approach to ISO 26262 Tool Error Detection and Tool Qualification Priyasloka Arya, LDRA	**Bluetooth Commercial Antenna Performance in Real World Wearable Applications** Dr. Matthew Magill, Queen's University Belfast	**How to Put MISRA and AUTOSAR Coding Compliance Into Practice** Dr. Dennis Kengo Oka, Synopsys; Dr. Ralf Huuck, Logilica	14:00
A Showcase for Model Based Code Generation for Multicore Safety Systems Prof. Dr. Peter Fromm, Darmstadt University of Applied Sciences	**Textile Circuits – Making Textiles Smart** Kay Ullrich, Textilforschungsinstitut Thüringen-Vogtland e.V.	**BARR-C:2018 and MISRA C:2012: Synergy Between the Two Most Widely Used C Coding Standards** Prof. Dr. Roberto Bagnara, BUGSENG / University of Parma	14:30
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	15:00
	Networking		15:15
Panel Discussion: Embedded Artificial Intelligence		Chair: Prof. Dr.-Ing. Axel Sikora	15:30
Safety Processes and Standards 3	**Hardware Power**	**Development Process**	
Passing Cyber Security Evaluation – Tips for Embedded Engineers and Product Managers Juho Vesanen, National Cyber Security Centre, Finnish Transport and Communications Agency	**Track Keynote:** **Power Management in Embedded Systems** Colin Walls, Mentor, a Siemens Business	**Track Keynote:** **The Application of Open Source Technologies to Embedded Systems** Mike Milinkovich, Eclipse Foundation	16:15
Hardware Security You Can Touch Mihai Tudosie, Infineon Technologies Austria	**Circuit and Antenna Design of a Simultaneous Wireless Power Transfer and Near Field Communication System** Christian Merz, Würth Elektronik eiSos	**Embedded Systems Go Mainstream** Maarten Koning, Wind River	16:45
Using SESIP to Simplify Security Evaluation and Build Trusted IoT Products Gil Bernabeu, GlobalPlatform	**Meeting the Complex Power Supply Demands of ADAS and Autonomous Driving Functions** Sebastian Scholz, Maxim Integrated	**Guidelines and Best Practices for Managing Open Source Software for Embedded Systems** Prof. Robert Oshana, NXP Semiconductors	17:15
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	17:45

Tuesday, 02 March
Conference Program

embeddedworld2021 Exhibition&Conference ...it's a smarter world DIGITAL

	Internet of Things – Platforms & Applications	Connectivity Solutions	Embedded OS
10:00	**Welcome**		
10:15	**Conference Keynote: Engineering Smart Ecosystems**		Prof. Dr. Peter Liggesmeyer, Fraunhofer IESE
	Software for IoT 1	**Wired Fieldbus 2**	**OS Automotive, Android, AutoSAR**
11:00	**Are High-level Languages and Tools Forbidden Fruit for Embedded Developers?** Valter Minute, Toradex	**Comparative Analysis of CAN, CAN FD and Ethernet for Networked Control Systems** Andrea Reindl, OTH Regensburg	**Progress on the AUTOSAR Adaptive Platform for Intelligent Vehicles** Günter Reichart, AUTOSAR
11:30	**n-Blocks Studio – Model based Low Code Ssoftware Development for Low Power Embedded Devices** Nikolaos Chalikias, Cork Institute of Technology	**Ethernet-APL – Ethernet to the Field of Process Plants** Benedikt Spielmann, Endress+Hauser Digital Solutions	**Functional Safety: Software Partitioning and Functionality Assignment for Complex and High Performance Architectures** Dr. Ahmed Khan, Mathias Fritzson, Siemens Digital Industries Software
12:00	**Native Execution of Java for Embedded Market and IoT** Bruno Caballero, Microdoc Computersysteme	**Extended communication capabilities for embedded networking** Reiner Zitzmann, CAN in Automation (CiA)	**An Introduction to Android Automotive OS** Chris Simmonds, 2net
12:30	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
12:45	Networking		
	Software for IoT 2	**Bluetooth 1**	**OS Open Source**
13:30	**Combine C++ and Java Into a Single ARM Executable Using GraalVM** Vojin Jovanovic, Oracle	**Optimizing Bluetooth Low Energy for Energy Efficiency** Clement Chaduc, Texas Intruments Norway	**What Differs the Android Open Source Project from Other Linux Distributions?** Sergio Prado, Embedded Labworks
14:00	**Cloud Driven CI/CD for Embedded Linux** Richard Elberger, Amazon Web Services	**Reliable Industrial Communication Using Bluetooth Technology** Pelle Svensson, ublox	**Formally Verifying the FreeRTOS IPC Mechanism** Nathan Chong, Amazon Web Services
14:30	**Lightweight Tooling to develop lightweight Systems – Advance your IoT Solution by Web-based Modeling and Code Generation** Marcus Munzert, Generative Software	**Bluetooth Mesh – Lessons Learned and Notes from the Field** Szymon Slupik, Silvair	**Innovation in the Fast Lane: Disrupting Automotive Software Development Through Open Source** Dan Cauchy, The Linux Foundation, Automotive Grade Linux
15:00	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
15:15	Networking		
15:30	**Panel Discussion: Safety and Security**		Chair: Prof. Dr.-Ing. Peter Fromm
	Data Management	**TSN 2**	**ROS**
16:15	**The Evolution from IoT to IoE With the Help of Blockchain and the Example „Smart Data Lake“** Marc Hamperl, infoteam Software	**TSN With Linux – The Challenges Ahead** Kurt Kanzenbach, Linutronix	**Redundant Computer Vision for Fault-Tolerant Autonomous Driving in C++ and ROS2** Prof. Dr. Frank Tränkle, Hochschule Heilbronn
16:45	**Deterministic Database Management in Mission-Critical Applications** Andrei Gorine, McObject	**TBA**	**Design and Deployment of Automated Parking Valet on ROS and ROS2 Networks** Shashank Sharma, MathWorks
17:15	**Data Streams, MQTT and No-code Apps on the Edge, in the Cloud and In-between** Philipp Struß, Cedalo	**Time Sensitive Networking Over 5G and WiFi for Industrial** Anil Keshavamurthy, Dr. Dave Cavalcanti, Intel	**ISO 26262 Certification of ROS 2** Dr. Dejan Pangercic, Mehul Sagar, Apex.AI
17:45	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A

Safety & Security	Software & Systems Engineering	Autonomous & Intelligent Systems	
Welcome			10:00
Conference Keynote: Engineering Smart Ecosystems		Prof. Dr. Peter Liggesmeyer, Fraunhofer IESE	10:15
Security Processes and Standards	**Development Process**	**Embedded AI 1**	
Implementing the 13 Best Practices for Consumer Electronics Security Haydn Povey, Secure Thingz	**Software Lifecycle Activity Costs for Secure Embedded Systems** Marcus Nissemark, Green Hills Software	**Prototyping and Deployment of Deep Neuronal Networks on FPGAs** Dimitri Hamidi, The Mathworks	11:00
Security Risk Assessment Using TARA Nishant Khadria, Deloitte	**Test Driven Development for Mission Critical Embedded Software** Mark Richardson, LDRA	**Democratizing Machine Learning for Embedded Developers** Alessandro Grande, Arm	11:30
Planning for the Protection of Your Product IP Throughout the Volume Curve Clive Watts, Secure Thingz	**Adopting Agile Software Development Best Practices for Functionally Safe System Development** Shrikant Satyanarayan, LDRA	**Change Your Mindset: Embedded Machine Learning for Predictive Maintenance** David Henry, Arm	12:00
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	12:30
	Networking		12:45
Safety Architectures 1	**Measures & Metrics**	**Embedded AI 2**	
Applying Automated Formal CCC Checks for Complex Systems Development Wolfgang Meincke, BTC Embedded Systems	**How to SQuaRE the Circle of Software Quality Measures** Andrew Banks, LDRA	**TinyML for AI at the Very, Very Edge** Rajeev Muralidhar, P. Vyawahare, Amazon Web Services	13:30
Designing Safety In by Extending System Modeling Languages Dr. Juha-Pekka Tolvanen, MetaCase	**Mature Enough? A Maturity Model for Model Based Systems Engineering** Dr. Henning Femmer, Qualicen	**Greater AI Visibility in Embedded Software** Dr. James Hui, Wind River	14:00
How to Bulletproof Systems Built With C++ Martin Woodhall, LDRA	**Embedded Software Development to Manage the Complexities of Today's Automotive Distributed Systems** Brendan Morris, Siemens Digital Industries Software	**Machine Learning at the Edge: From Transfer Learning to Inferencing** Markus Levy, Natraj Ekambaram NXP Semiconductors	14:30
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	15:00
	Networking		15:15
Panel Discussion: Safety and Security		Chair: Prof. Dr.-Ing. Peter Fromm	15:30
Safety Architectures 2	**Requirements Engineering**	**Embedded AI 3**	
Track Keynote: Taming Timing – Combining Static Analysis With Non-intrusive Tracing to Compute WCET Bounds on Multicore Processors Dr. Daniel Kästner, AbsInt Angewandte Informatik	**Requirement Verification and 360 Degree Traceability** Deepu Chandran, Shrikant Satyanarayan, LDRA	**Understanding Artificial Intelligence: Explainable AI with Interpretable KPI Labels** Dr. Rudolf Felix, PSI FLS Fuzzy Logik & Neuro Systeme	16:15
Control-Flow Evaluation on Multicore Controllers Using Real-Time Trace Information Stephan Radke, Hochschule Darmstadt University of Applied Sciences	**A Rigorous but Practical Specification Technique for Embedded Systems** Prof. Robert Oshana, NXP Semiconductors	**Software Driven SoC Architectural Exploration for AI and ML Accelerators With RISC-V** Simon Davidmann, Imperas Software	16:45
Statically Safer Polymorphism With C11 Generics Alex Gilding, Perforce Software	**How COVID-19 has Changed the Requirements Engineering Process Among Embedded Companies** Micaël Martins, Visure Solutions	**Quantizing Edge Neural Networks With Qkeras** Russell Klein, Mentor, A Siemens Business	17:15
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	17:45

Wednesday, 03 March
Conference Program

embeddedworld2021 Exhibition&Conference ... it's a smarter world DIGITAL

	Embedded Human-Machine-Interface	Internet of Things – Platforms & Applications	Connectivity Solutions
10:00	**Welcome**		
10:15	**Conference Keynote: Display Disruption: How New Display Technologies are Changing the Industry** Paul Gray, Omdia		
	HMI Libraries	**OTA Firmware Updates**	**Wired Fieldbus 3**
11:00	**Vulkan SC – Safety Critical Graphics and Compute Library** Michael Pyne, CoreAVI & Industrial	**New Approach to the Over-The-Air Updates for Connected Devices** Sergey Lyubka, Cesanta	**Securing Bridges in CAN/CANopen (FD) Systems** Olaf Pfeiffer, Embedded Systems Academy
11:30	**Standardising Low-cost GPUs for Embedded Industrial Use** Kristof Beets, Imagination Technologies	**Ktwo: Orchestrator Based Firmware Distribution Mechanism** Taimor Imtiaz, Intel Deutschland	**TBA**
12:00	**Cross-Platform HMI Families for Modern Embedded Devices** Andy Walter, macio	**Why Firmware Update Over the Air (FOTA) is an Essential Part of Scaling IoT** Andrew Powers, Arm	**CAN FD Light** Yao Yao, CAN in Automation
12:30	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
12:45	Networking		
	HMI Design Methods 1	**Low Energy Devices**	**Bluetooth 2**
13:30	**Track Keynote: Human Factors and User Interface Technology for Embedded Systems** Prof. Robert Oshana, NXP Semiconductors	**Power Savings for IoT Devices** Hans-Guenter Kremser, Texas Instruments Deutschland	**Improving the Connection Range and Time in Car Access Systems Using Bluetooth Role Switching Techniques** David Lara, Texas Instruments
14:00	**Strike the Right Balance of Performance and Visual Experience for Hi-Res Displays Using MCU Graphics Accelerators** Victor Hugo Osornio, NXP Semiconductors	**Unveiling Scalable and Open Source Energy Star Network Proxying Solution for Greener Connected World** Dr. Yoong Siang Song, Intel	**Next Generation Bluetooth Audio Becomes a Reality** Nick Hunn, WiFore
14:30	**How to Drive Down the Cost and Power of On-device Voice-based Devices** Kobus Marneweck, Arm	**Battery-free LPWAN Nodes for Bridges and Walls** Prof. Dr. Marcel Meli, ZHAW	**Understanding Reliability in Bluetooth Technology** Martin Woolley, Bluetooth SIG
15:00	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
15:15	Networking		
15:30	**Conference Keynote: Modern Embedded Engineering: Where we are and our Exciting Future** Randall Restle, Restle LLC, Strategic Advisor to Digi-Key Electronics		
	HMI Design Methods 2	**Edge Computing**	**Large-Scale Wireless Connectivity**
16:15	**When Embedded Experts are Scarce – Low-code/No-Code Graphics Software to the Rescue** Jeff Stewart, Altia	**Connect Code – Direct, Serverless, Schemaless, Non Intrusive and Asynchronous** Dr. Burkhard Heisen, Cybus and Heisenware	**6LoWPAN Solution for Smart Metering Application Using Sub-1GHz Radio and STM32 Microcontroller** Indar Singhal, STMicroelectronics
16:45	**Accelerating Graphics Rendering Performance for ADAS With Zynq UltraScale+ MPSoC** Alok Gupta, Xilinx	**The Power of AI and Edge Computing in Achieving Defect-Free Factories** Brian McCarson, Intel	**Throughput and Latency Concerns When Designing a Mesh Network With Many Nodes** Marie Hernes, Texas Intruments Norway
17:15	**How to Develop a Low Power, Robust, Secure Embedded Voice Capture Pipeline on a Single Arm Cortex M-class Device** Brian Clinton, Arm	**Edge Computing Architectures for the Management of Embedded IoT Devices** Prof. Robert Oshana, NXP Semiconductors	**Wi-SUN – Key to Unlocking Massive IoT** Soumya Shyamasundar, Abitzen Xavier, Silicon Labs
17:45	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A

Safety & Security	Software & Systems Engineering	Autonomous & Intelligent Systems	
Welcome			10:00
Conference Keynote: Display Disruption: How New Display Technologies are Changing the Industry Paul Gray, Omdia			10:15
Safe AI	**DevOps**	**AI Hardware**	
Standards About AI in Systems with Reference to Functional Safety Frank Poignée, infoteam Software	**Ready for EmbSecDevOps? Enhance your Embedded Product With Security-by-Design Decisions and Maintain Security in Your Development Lifecycle!** Michael Brandl, CYOSS	**Track Keynote: Dependable Neural Networks Through Redundancy – Comparing Architectures** Prof. Hans Dermot Doran, Zürich University of Applied Sciences	11:00
Trustworthy AI-based Systems With VDE-AR-E 2842-61 Henrik J. Putzer, cogitron	**DevOps-Toolchains in Embedded Software Development - Towards Trancparency and Traceability** Dmitry Chibisov, Dr. Chibisov Software Quality	**Transforming IoT Endpoints with AI** Chris Shore, Arm	11:30
Edge Machine Learning for Saftey Cirtical Systems Dr. Rikard König, Ekkono Solutions	**IoT in the Age of DevOps** Florian Bader, Thomas Rümmler, AIT	**Enhancing the Deployment of Quantization Aware DNN for Inference Acceleration With Vitis AI** Alok Gupta, Xilinx	12:00
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	12:30
Networking			12:45
Security Hardware	**DevOps / MBD**	**AI Use Cases**	
Secure IoT Firmware For RISC-V Processors Cesare Garlati, Hex Five Security	**DevSecOps Carves a Path to Digital Transformation for Autonomous Embedded Systems** Bruno Chaves, Wind River	**Algorithms for Distributed Sensor Fusion & Tracking** Dimitri Hamidi, The Mathworks	13:30
Keep Device Data Safe With Secure Erase Thom Denholm, Tuxera	**Securing the DevSecOps Platform: Approaches, Methods, and Tools** Arlen Baker, Wind River	**Optical Flow Odometry** Dr. William Lovegrove, Bob Jones University	14:00
DRAM as Security and Privacy Threat to IoT and Embedded Systems Hans Diesing, Zentel EMEA	**From MATLAB to C Code for Heterogeneous Embedded Systems – Using Abstraction Levels for Specialized Optimizations** Oliver Oey, emmtrix Technologies	**Reducing the Energy Consumption of a Refrigerator Using Reinforcement Machine Learning** Özgür Özkan, Arcelik; Cameron LaFolette, Arm	14:30
Discussion/Q&A	Discussion/Q&A	Discussion/Q&A	15:00
Networking			15:15
Conference Keynote: Modern Embedded Engineering: Where we are and our Exciting Future Randall Restle, Restle LLC, Strategic Advisor to Digi-Key Electronics			15:30
Security Use Cases	**Software & System Quality**		
Seamless integration of Cyber Security with Functional Safety will Make Autonomous Driving for Automotive and Industry Solutions Secure and Robust Thorsten Lorenzen, Texas Instruments Sales	**Finding the Serious Bugs that Matter with Advanced Static Analysis** Paul Anderson, GrammaTech		16:15
Security Testing of a Lithotripter Medical Device Based on MDR and MDCG Wilfried Kirsch, Prof. Dr. Hartmut Pohl, softScheck	**Optimizing Heterogeneous Compute Platforms for Domain Controllers** Florent Lebeau, Arm	**Sign-up & Registration: www.embedded-world.eu**	16:45
A Security Architecture for Protecting Safety-Critical Railway Infrastructure Prof. Dr. Christoph Krauß, Fraunhofer SIT	**Performance Measurement and Testing of Realtime MCU-virtualized Applications** Dr. Stéphane Turlier, OpenSynergy		17:15
Discussion/Q&A	Discussion/Q&A		17:45

Thursday, 04 March
Conference Program

embeddedworld2021 Exhibition&Conference ... it's a smarter world DIGITAL

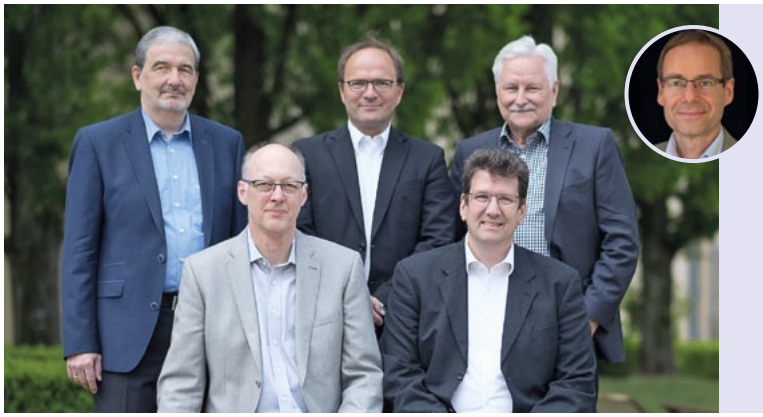
	Internet of Things – Platforms & Applications	System-on-Chip (SoC) Design	Safety & Security
10:00	**Welcome**		
	Security im IoT 1	**Complex IC & System Solutions**	**Security Architectures 1**
10:15	**Panel Discussion: Embedded Vision**		Chair: Prof. Dr.-Ing. Axel Sikora
11:00	**New Aspects of PSA Certified for Securing IoT and Edge Devices** Robert Coombs, Arm	**Maximising Energy Efficiency When Designing SoCs for Endpoint AI** Gergely Kiss, Arm	**Functional Safety and Security for Microcontrollers: Conflict or Cooperation?** Alessandro Bastoni, STMicroelectronics
11:30	**A General IoT Security Classification Framework** Dr. Oana Fabiana Andreescu, Internet of Trust	**FPGA-based Modelling, IP-Implementation and Measurements of Aging Effects Due to TID or Electrical and Thermal Stress** Vidwath Paramesh, Josef J. Schmid, iSyst Intelligente Systeme	**Application of TPM2.0 in Industrial and Automotive Systems Using the Feature API of the Open Source Software Stack** Florian Schreiner, Infineon Technologies
12:00	**OPC UA PubSub IIOT Platform With Secure Embedded Secret** Vincent Lacroix, Systerel	**Automotive and Mobile: Converging Video Content Requirements** Ralph Grundler, Synopsys	**Achieving Mixed Criticality and Cat3 Pld on Single_SoC** Matteo Salardi, Intel
12:30	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
12:45	Networking		
	Security im IoT 2	**IP Core Design & Integration**	**Security Architectures 2**
13:30	**Building Secure Industrial and Embedded Applications with PSA Certified** Simon Butcher, Arm	**Track Keynote: Architecture Trends for Sensing and Computing to Enable Automated Driving** Robert Schweiger, Cadence Design Systems	**Accelerating Security for Linux IoT Endpoints** Michele Riga, Shebu V Kuriakose, Arm
14:00	**Secure IoT Firmware For Cortex-M Processors** Cesare Garlati, Hex Five Security	**Secure Boot Concept on the Zynq Ultrascale+ MPSoC** Thierry Delafontaine, Zürich University of Applied Sciences	**Security Considerations in Linux for the Automotive World** Saurabh Arora, Elektrobit Automotive
14:30	**Analyzing a Real-World Wireless IoT Encryption and Authentication Protocol Using a Threat Modeling Framework** Jakob Buron, Silicon Labs	**Standardizing the TEE – The IoT Opportunity** Gil Bernabeu, GlobalPlatform	**An Architecture For Trusted Operation of IoT Devices** Colin Duggan, BG Networks; K. Thangappan Jasmin, Infotech
15:00	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
15:15	Networking		
15:30	**Conference Keynote: Challenges of Digital Transformation for the New Intelligent Edge** Kevin Dallas, Wind River		
	IoT Use Cases 1	**Mixed Signal & Energy Optimization**	**Hacking**
16:15	**Energy Prediction in Edge Environment for Smart Cities** Oluwatobi Oyinlola, Intel	**The Challenges of Combining Mixed Signal Connectivity IP Into Your SoC** Roger Walker, Imagination Technologies	**Fuzz Attacks for Embedded Network Devices** DeWitt Seward, Silicon Labs
16:45	**Real-time Remote Diagnostics for In-production Automotive Ethernet ECUs** Dr. Ahmed Khan, Siemens Digital Industries Software	**Semiconductor Process Selection from ESD Perspective: FinFET, SOI or CMOS?** Benjamin Van Camp, Sofics	**Sidechannel Analysis in Embedded Devices** DeWitt Seward, Silicon Labs
17:15	**Using MQTT Based Adapters to Enable Testing for Industrial Applications (IIoT)** Prof. Rix Groenboom, Parasoft	**Low Voltage Signal-Chain for the IoT Sensors of the Future** Maurizio Gavardoni, Maxim Integrated	**Security is a System Level Problem: A Case Study** Josh Norem, Silicon Labs
17:45	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A

Software & Systems Engineering	Embedded Vision	
Welcome		10:00
Software Quality	**Application Case Studies**	
Panel Discussion: Embedded Vision	Chair: Prof. Dr.-Ing. Axel Sikora	10:15
Testing, Model Checking and Static Analysis – Dream Team or Rivals? Dr. Sebastian Krings, Axivion	**Embedded Vision in ArgiTech: Livestock Weight Monitoring** Lyubomyr Dutko, Lemberg Solutions	11:00
The Practicalities of Automotive Software Safety Analysis Deepu Chandran, LDRA	**TBA**	11:30
Secure Diagnostics for Connected Vehicles Dr. Ahmed Khan, Dirk Vogel, Siemens Digital Industries Software	**A Vision Based Unsupervised Method for Realtime Anomaly Detection in Welding Process** Tara K. Thimmanaik, Intel	12:00
Discussion/Q&A	Discussion/Q&A	12:30
Networking		12:45
Software Quality: Static Analysis	**Systems Integration 1**	
Static Data and Control Coupling Analysis Dr. Daniel Kästner, AbsInt Angewandte Informatik	**GPU FPGA Accelerated Real time System Implementation for Stereo 3D Mapping and Visual Odometry** Yashwant Kumar Temburu, Indian Institute of Technology Bombay	13:30
Combining Static Unit and Integration Analysis Dr. Daniel Kästner, AbsInt Angewandte Informatik	**Benefits of Industrial Cameras for Embedded Vision Applications** Felix Nikolaus, Allied Vision Technologies	14:00
Maximizing the Value of Static Analysis for Modern Development Miroslaw Zielinski, Parasoft	**Faster Deployments With Software-defined Smart Cameras** Michele Riga, Arm	14:30
Discussion/Q&A	Discussion/Q&A	15:00
Networking		15:15
Conference Keynote: Challenges of Digital Transformation for the New Intelligent Edge Kevin Dallas, Wind River		15:30
Software Quality: Coding	**Systems Integration 2**	
Dynamic Memory Allocation & Fragmentation in C & C++ Colin Walls, Mentor, a Siemens Business	**Track Keynote: The State of Khronos Standards Powering the Future of Embedded Vision & Inferencing** Neil Trevett, The Khronos Group	16:15
Advanced Compiler Optimizations for the Smallest, Fastest Code Greg Davis, Green Hills Software	**Accelerated Computer Vision Processing Pipelines on Versal With AIE and PL Fabric** Alok Gupta, Xilinx	16:45
Hack-proofing your C/C++ Code Greg Davis, Green Hills Software	**A Deterministic Approach to Inferencing on Real Time Safety Critical Embedded Systems** Lucas Fryzek, Core Avionics & Industrial	17:15
Discussion/Q&A	Discussion/Q&A	17:45

Friday, 05 March
Conference Program

embeddedworld2021 Exhibition&Conference ...it's a smarter world DIGITAL

	Internet of Things – Platforms & Applications	System-on-Chip (SoC) Design	Safety & Security
10:00	**Welcome**		
	Security im IoT 3	**Core Integration & Tools 1**	**Security Architectures 3**
10:15	**Panel Discussion: Connectivity in IoT**		Chair: Prof. Dirk Pesch
11:00	**Cyber Secure Communication for Automation Devices – Legal Regulations, Market Trends and Solutions** Thierry Bieber, HMS Industrial Networks	**Jupyosys: From Browser to Silicon in Seconds** Martin Strubel, section5 / Strubel SW solutions	**Implementing the ARM Platform Security Architecture for Robust IoT Devices** Trevor Martin, Hitex UK
11:30	**Firmware Integrity in the Quantum Age – How to Prepare Against Threats of Quantum Computing Now** Martin Schläffer, Infineon Technologies	**Leveraging RISC-V Technology for Industry Use** Prof. Robert Oshana, NXP Semiconductors; Rick O'Connor, OpenHW Group	**uTango: Open Source TEE for TrustZone-M Devices** Dr. Sandro Pinto, Universidade do Minho
12:00	**SIMs, eSIMs and Secure Elements: Providing a Roadmap to Dynamic Security and Flexible Control for Connected Devices** Cyril Caillaud, Trusted Connectivity Alliance	**Working Effectively With Standard and Custom RISC-V ISA Extensions** Felipe Torrezan, IAR Systems	**Porting and Running OP-TEE on ARMv8 devices** Sergio Prado, Embedded Labworks
12:30	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
12:45	Networking		
	IoT Use Cases 2	**Core Integration & Tools 2**	**Long Term and Security**
13:30	**Revolutionary Asset Management Solutions Based on Semtech's LoRa Edge and LoRa Cloud** Pedro Pachuca, Semtech	**Innovate by Customized Iinstructions, But Without Fragmenting the Ecosystem?** Joseph Yiu, Arm	**A Long-term Security Concept for IoT Products** Dr. Hans Herrmann, cogitron
14:00	**TBA**	**The Path to Ultra-low Power AI at the Edge** James Peet, Cambridge Consultants	**Cyber Resiliency is Becoming Critical for All Embedded Systems, Dynamic Firmware Protections, Coupled to Effective Supply Chain Security will Become Mandatory Very Soon** Eric Sivertson, Lattice Semiconductor
14:30	**The Battery Digital Twins** John Milios, Sendyne	**Exploiting Regularity for Compiling Manycore Architectures** Andres Goens, TU Dresden	**Finding N-day Security Vulnerabilities in Third-party Software** Paul Anderson, GrammaTech
15:00	Discussion/Q&A	Discussion/Q&A	Discussion/Q&A
15:15	Networking		



Steering Board

back row (from left to right):
Dr. Bernd Hense,
Prof. Dr. Axel Sikora,
Dr. Klaus Grimm
Prof. Dr. Dirk Pesch

front row:
Joachim Kroll,
Prof. Dr. Peter Fromm

Software & Systems Engineering	Embedded Vision	
Welcome		10:00
Testing & Debugging 1	**SW Tools & Tooling AI & Tool Chains**	
Panel Discussion: Connectivity in IoT	Chair: Prof. Dirk Pesch	10:15
Standardisation of Software Testing... a Necessary Evil? Andrew Banks, LDRA	**Embedded Learning and the Evolution of Machine Vision** Jonathan Hou, Pleora Technologies	11:00
Self-testing in Embedded Systems Colin Walls, Mentor, a Siemens Business	**Using Visual Inference in Edge Computing** Jim White, IoTech	11:30
Risking the New or Preserving the Old? – How to Preserve Treasures in Legacy Code Bases Ingo Nickles, Vector Informatik	**The Best of Both Worlds: Rule-based and AI for Embedded Vision** Christoph Wagner, MVTec Software	12:00
Discussion/Q&A	Discussion/Q&A	12:30
Networking		12:45
Testing & Debugging 2	**Embedded Vision**	
Software Testing Best Practices for Embedded Systems Prof. Robert Oshana, NXP Semiconductors	**Embedded IoT Application with Computer Vision and OpenVINO** Oluwatobi Oyinlola, Intel	13:30
Agile Test Orchestration for Embedded Software Dr. James Hui, Wind River	**Optimising Neural Networks With a Holistic Vie of IoT, Cloud and Edge Using Information Reduction Pipeline Concept** Marc Suhle, Mark Hebbel, Basler	14:00
Dominate Advanced Trace in Your RISC-V Core IP Shawn Prestridge, IAR Systems	**Multimedia Performance Tuning** Marcel Ziswiler, Toradex	14:30
Discussion/Q&A	Discussion/Q&A	15:00
Networking		15:15

Classes
Conference Program

embeddedworld2021 Exhibition&Conference ... it's a smarter world DIGITAL

Monday, 01 March

13:30 - 18:00	**Class 1.1** **The Power of APIs and Containers on Embedded Switching** Florian Pachinger, Cisco Systems	**Class 3.1** **Build Your Own Embedded Linux CI/CD Pipeline Using the Cloud** Richard Elberger, Amazon Web Services	**Class 4.1** **Security Beyond Cryptography: Security Enclave for Asymmetric Multi-processing** Lawrence Case, NXP Semiconductors	**Class 6.1** **Effective Use Cases, User Stories, and Scenarios** Dr. Bruce Douglass, Bruce-Douglass.com

Tuesday, 02 March

09:00 - 13:30	**Class 5.1** **Ultra Low Power Hands-on Workshop** Herman Roebbers, Altran	**Class 10.1** **FPGA-Design Using C/C++ and High-Level Synthesis** Prof. Dr. Frank Kesel, Hochschule Pforzheim		
13:30 - 18:00			**Class 6.2** **Agile for Embedded Systems** Dr. Bruce Douglass, Bruce-Douglass.com	**Class 6.3** **The Greg Davis Class – Advanced C/C++ Coding and Debugging Techniques** Greg Davis, Green Hills Software

Wednesday, 03 March

09:00 - 12:30	**Class 3.2** **Embedded Android Workshop** Karim Yaghmour, Opersys	**Class 6.4** **Creating Domain-Specific Modeling Languages: Hands-on** Dr. Juha-Pekka Tolvanen, MetaCase			
13:30 - 18:00			**Class 5.2** **Easy Design of IoT Wireless Devices Embedding Antennas** Dr. Jaume Anguera, Fractus Antennas	**Class 6.5** **Advanced Behavioral Modeling with UML/SysML: Activities** Dr. Bruce Douglass, Bruce-Douglass.com	**Class 6.6** **Modern C++ for Embedded Development** Greg Davis, Green Hills Software

Thursday, 04 March

09:00 - 12:30	**Class 3.3** **Introduction to Embedded Linux in Theory and Practice – Short Crash Course** Robert Berger, Reliable Embedded Systems	**Class 3.4** **Fast Track to Yocto Project** Chris Simmonds, 2net	**Class 6.7** **How to Improve Software Quality Through Test Automation** Ingo Nickles, Vector Informatik			
13:30 - 18:00				**Class 5.3** **Production Optimized Hardware Design** Stefan Kinzlbauer, Ginzinger electronic systems	**Class 6.8** **Advanced Behavioral Modeling with UML/SysML: State Machines** Dr. Bruce Douglass, Bruce-Douglass.com	**Class 8.1** **Developing Artificial Intelligence Using Machine Learning at the Edge with Embedded µSoC FPGAs** Grant Jennings, GOWIN Semiconductor

ELEKTRONIK 5/2021
ERSCHEINT AM 9. MÄRZ

„Das Ganze ist mehr als die Summe seiner Teile.“ Diese Erkenntnis des griechischen Philosophen Aristoteles hat auch Bestand bei zukunftsweisenden Elektronikdesigns. High-End-Mikroprozessoren und Grafikchips werden erst mit externer Beschaltung zu Embedded-Systemen, etwa für den Einsatz im Internet der Dinge. Mit Blick auf die rauen Umgebungsbedingungen in der Industrie werden Gehäuse und Schalter zu weiteren Puzzleteilen im Gesamtbild. In der kommenden *Elektronik*-Ausgabe greift die Redaktion das Thema Systemkomponenten inklusive der Elektromechanik auf und richtet ein separates Spotlight auf LED/Lighting.

MESSEN UND VERANSTALTUNGEN
https://www.weka-fachmedien.de/de/events/aktuelle-events/

embeddedworld2021 Exhibition&Conference … it's a smarter world DIGITAL	1. – 5. März 2021 Online
electronicdisplays Conference DIGITAL	1. – 5. März 2021 Online
FORUM KÜNSTLICHE INTELLIGENZ	21. April 2021 Online

Änderungen aus aktuellem Anlass möglich.

DIE ELEKTRONIK-MEDIEN AUCH ALS E-PAPER
https://shop.weka-fachmedien.de

BE COOLER.
STAY MAPI!

WÜRTH ELEKTRONIK

© eiSos

WE are here for you!

Nehmen Sie teil an unseren kostenlosen Webinaren: **www.we-online.de/webinare**

Die WE-MAPI ist eine der kleinsten gewickelten Metal-Alloy-Speicherdrosseln der Welt. Ihre Effizienz ist herausragend. In der 4020HT-Produktreihe ist sie jetzt verfügbar mit AEC-Q200 Klasse 0 Qualifikation für Betriebstemperaturen von -55° bis +150 °C. Ab Lager verfügbar. Kostenlose Muster erhältlich.
Erfahren Sie mehr unter: **www.we-online.de/WE-MAPI**

Designen Sie Ihren Schaltregler in **REDEXPERT**, der weltweit genauesten Online Design Plattform zur Berechnung von Spulenverlusten.

- Hohe Strombelastbarkeit bis zu 10 A
- Geringe Spulenverluste
- Geringer RDC bis zu 6,5 mΩ
- Exzellente Temperaturstabilität von -55° bis +150 °C
- Innovatives Design
- Exzellentes EMV-Verhalten

Die WE-MAPI Produktpalette: