06/2017
www.iot-design.de
TeDo Verlag GmbH
November
€ 7,80

Sicherer Fernzugriff per VPN

IoT DESIGN

Smarte Systeme für das Internet of Things

SMARC 2.0 testen

4 SQL4AUTOMATION
The smart database connection

SQL4automation

Energie aus Wellen: Datenanalyse mit SQL4automation auf dem Meer

SPS IPC Drives 2017

Unsere Highlights zur Messe

NAND-Flash

Welchen Speicher brauchen Automatisierer?

Wissen ist Macht

Maschinen und Anlagen als Datenquelle nutzen – So werden Sie IoT-ready

Hitzefrei

Mit dem richtigen Gehäuse Wärme ableiten

CANopen FD

Alles rund um die neue Spezifikation

Besuchen Sie uns auf der
SPS/IPC/Drives 2017
Halle 7A · Stand 7A-302

IO-Link – we connect you!

Gewährleistung 5 Jahre auf ifm-Produkte

Mehr Funktionalität: Smarte IO-Link-Sensoren von ifm

IO-Link-Geräte schützen vor Manipulationen, übertragen den Messwert ohne Verluste, erlauben einfachen Austausch ohne Vor-Ort-Parametrierung und sind ohne Aufpreis verfügbar. Sie sehen, es gibt gute Gründe, IO-Link-Sensoren einzusetzen.
ifm als Technologieführer im Bereich IO-Link bietet Ihnen die größte Anzahl smarter Sensoren mit IO-Link im Markt. Machen Sie den richtigen Schritt in eine innovative Zukunft und profitieren Sie von der langjährigen Erfahrung, die Maßstäbe in Sachen Funktionalität und Service gesetzt hat. ifm – your IO-Link system partner. ifm – close to you!

www.io-link.ifm
ifm-Service-Telefon 0800 16 16 16 4

Innovation ist Pflicht

Industriegesellschaften sind ohne Halbleiter nicht denkbar. Ob Mobiltelefone, Autos oder medizinische Geräte – nahezu kein technisches Erzeugnis kommt ohne diese Kernelemente der Elektronikfertigung aus. Mitte des Jahres sagten Analysten von Gartner dem weltweiten Halbleitermarkt nach einem mäßigen Zuwachs von 1,5 Prozent im vergangenen Jahr, für 2017 ein deutliches Plus von 16,8 Prozent voraus. Der Umsatz soll dabei auf über 400 Milliarden US-Dollar steigen. Verantwortlich sind explodierende Preise für Speicherbausteine. Zusätzlich erreicht laut IC Insights der Wert des Halbleiteranteils in elektronischen Geräten in diesem Jahr den Rekordwert von 28,1 Prozent.

Zudem ist die komplette Halbleiterindustrie im Umbruch. Nach gut fünf Jahrzehnten verliert der 'Moore'sche Fahrplan', wonach alle zwei Jahre doppelt so viele Transistoren auf einen Mikroprozessor gepackt werden, allmählich seine Gültigkeit. Die Physik spielt nicht mehr mit, die Halbleiterwerke (Fabs) für die nächsten Chip-Generationen sind kaum mehr zu bezahlen, und für immer weniger Chips macht es Sinn dem moore'schen Gesetz zu folgen.

Energieeffizienz, Mobilität und Konnektivität fordern laufend neue Lösungen. Und speziell das Internet der Dinge, in dem bald Milliarden vernetzter Geräte miteinander kommunizieren werden, hat die Geschwindigkeit noch einmal erhöht. So entscheidet neben dem Preis und neuen Features vor allem 'Time-to-Market' über den Erfolg eines Produktes. Da wundert es nicht, dass die Halbleiterbranche zu den am meisten von Innovationen getriebenen Branchen gehört.

Und auch die SPS IPC Drives verändert sich. In diesem Jahr gibt sie in Halle 6 der Software & IT ihren eigenen Raum. Microsoft Deutschland hat das erste mal seit drei Jahren wieder einen eigenen Stand. Die Fachmesse für elektrische Automatisierungstechnik setzt damit virtuelle Produktentwicklung, IT/OT-Technologien, Cyber-Security und Fog-, Edge- und Cloud-Computing in den Fokus. Automatisierer und Produzenten können sich über Software, Cloud-Dienste, Künstliche Intelligenz und Mixed Reality informieren. Was Sie aus unserer Sicht auf gar keinen Fall auf der Messe verpassen sollten, lesen Sie ab Seite 8.

Ich wünsche Ihnen eine informative Lektüre,

CLARA L. JOSUTTIS
Redakteurin IoT Design

Bild: Inasoft GmbH

Bild: © adam121 / Fotolia.com

Titelstory

Sicherheit

Bild: TeDo Verlag GmbH

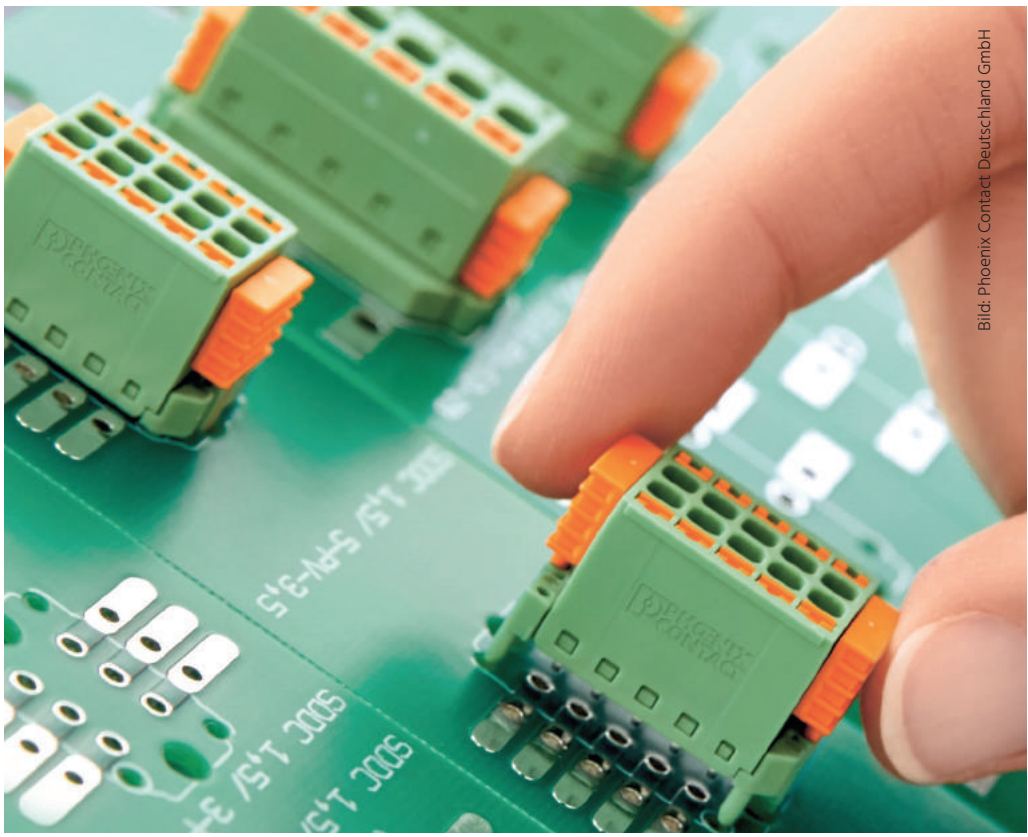


Bild: Phoenix Contact Deutschland GmbH

Sigfox World IoT Expo

Steckverbinder

IoT Must Haves

zur SPS IPC Drives 2017

Ratgeber

IoT News

Service

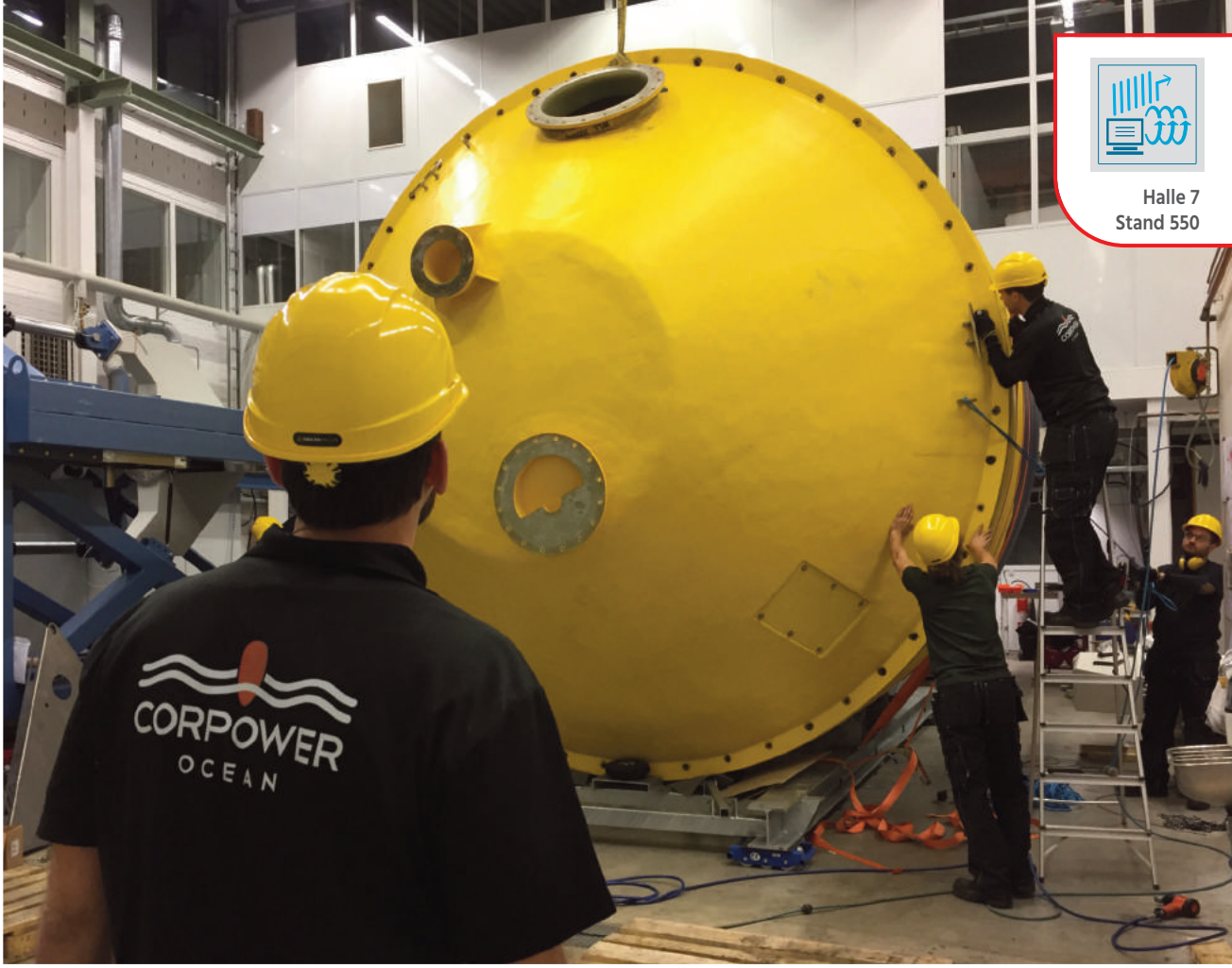
Bilder: Inasoft Systems GmbH

Energie aus Wellen: Datenanalyse auf dem Meer

Von Corpower stammt ein neuer Typ von **Wellenkraftwerken**, die auf See zum Einsatz kommen. Für die **Überwachung und die ständige Verbesserung der Systeme** werden Twincat-Steuerungen von Beckhoff genutzt. Gesammelt und analysiert werden die Daten in **SQL-Datenbanken**. Der SQL4automation Connector **überträgt auf einfache Weise** die **Daten von der Steuerung zur Datenbank**.

INASOFT SYSTEMS GMBH

Die von Corpower AB entwickelten Wellenkraftwerke oder Wave Energy Converter nutzen – inspiriert vom Pump-Prinzip des menschlichen Herzens – Wellenbewegungen des Meeres und setzen sie mittels phasengesteuerter Oszillation in elektrische Energie um. So wird eine bis zu fünfmal höhere Energiedichte als bei herkömmlichen Wellen-Energie-Konvertern ohne Phasensteuerung erreicht. Mit der neuen Technologie kann somit in einer relativ kompakten Anlage eine beachtliche Menge elektrische Energie erzeugt werden. „Aktuell arbeiten wir an einer Anlage, die nur ein Zehntel des Volumens im Vergleich zu herkömmlichen Bojen den gleichen Effekt hinsichtlich der Energiegewinnung erzielt", erläutert Jakob Sagatowski, Senior Software Engineer Control & Communications bei Corpower Ocean AB in Stockholm/Schweden.



Halle 7
Stand 550

Saubere Energie aus Wellen

Die in Bojen integrierten Konverter könnten 2.000TWh bis zu 4.000TWh Energie pro Jahr erzeugen. Immerhin 10 % bis 20 % des weltweiten Stromverbrauchs könnten so effizienter, sauberer und wirtschaftlicher erzeugt werden und zur Schonung von Ressourcen beitragen. Die Herausforderung speziell in der Wave Power-Nutzung sei es „einerseits ein Gerät zu entwerfen, das robust genug ist, um auch härtesten Stürmen zu widerstehen“, so Sagatowski, andererseits müsse gleichzeitig genug Energie erzeugt werden, um es wirtschaftlich einsetzen zu können. „Mit unseren neuen Konvertern ist das möglich“, berichtet er stolz. „Unser Ziel besteht darin, eine neue Generation von Geräten zur wirksamen Nutzung von Wellenenergie für die Energieerzeugung zu schaffen, die mit etablierten Energieressourcen konkurrieren kann.“ Als Steuerungstechnik kommt PC-Control auf Basis von Twincat 3 von Beckhoff Automation zum Einsatz. Im Wave Energy Converter sind jeweils zwei dieser Steuerungen integriert. „Eine Twincat-PLC sammelt alle Sensordaten, die andere dient zur Datenverarbeitung“, erläutert Sagatowski weiter. Von dieser werden die gesammelten Informationen per ebenfalls integriertem SQL4automation Connector an eine SQL-Datenbank übergeben, damit diese dann für die Systemoptimierung genutzt werden können. „Eine Vielzahl von Werten ist für die Analyse und Verbesserung des Systems zu erfassen und zu berücksichtigen“, setzt der Automatisierungsspezialist fort. „Korreliert werden unter anderem Temperaturwerte, Messwerte von Druck- und Feuchtesensoren, die Fließgeschwindigkeit und nicht zuletzt wird die erzeugte elektrische Energie erfasst, um eine sichere Aussage hinsichtlich der Effizienz treffen zu können.“ Die Bewegung der Boje wird ebenso mittels Beschleunigungs- und Vibrationssensoren erfasst.

Mit Datenanalyse bis zu dreimal effektiver

Der SQL4automation Connector kommt dabei „aus mehreren Gründen zum Einsatz“, so Sagatowski: „Einerseits müssen sehr viele Sensordaten erfasst werden, um das korrekte Funktionieren des Systems zu gewährleisten.“ Für einen erfolgreichen Einsatz in der Praxis sind umfangreiche Tests erforderlich. Dies schließt auch die Mechanik ein: So wird zum Beispiel die Temperatur in den Zylindern überwacht. Er setzt fort: „Andererseits gilt es, die Technologie selbst kontinuierlich zu optimieren. Wir arbeiten sozusagen mit einem sich ständig optimierenden Modell, um die Energieausbeute zu maximieren.“ Laut dem Spezialisten wird die Anlage mithilfe der Datenanalyse bis zu dreimal effektiver. „Für die kontinuierlichen Build-In-Tests ist eine ständige Überwachung der Systemparameter unabdingbar. Dies dient nicht nur zur Verbesserung des Systems, sondern reduziert auch die Störanfälligkeit und eventuelle Systemfehler“, schließt der Automatisierungsspezialist an. Möglich ist es damit auch, den Kunden zu gewährleisten, dass die Anlage reibungslos und bestmöglich funktioniert. „Natürlich werden die Bojen auch visuell beobachtet, aber um das komplette System mit all seinen Funktionalitäten und Einflüssen optimieren zu können, ist eine Verarbeitung und Erfassung aller Daten erforderlich. SQL4automation ermöglicht dafür den praktikabelsten Weg. Wir erfassen ca. 3GByte bis 4GByte Daten pro Tag“, erklärt er weiter. Zum Einsatz kommt die Standard-Version für bis zu zehn Verbindungen. Die Daten helfen das System stetig zu optimieren und somit die Performance zu erhöhen. Darüber hinaus wird die Anlage selbst überwacht, denn sie ist selbst erheblichen Temperatur- und Umgebungseinflüssen ausgesetzt. „Die Kombination aus Beckhoff-Steuerungstechnik und Inasoft-Datentechnologie passt dabei perfekt für unsere Anforderungen und bietet Vorteile“, so Sagatowski. „Die SQL-Anbindung von Inasoft ist einfach und komfortabel zugleich. Im bisherigen Einsatz hat das in den letzten zwei Jahren hervorragend funktioniert.“

www.inasoft.ch
www.sql4automation.com/de ■

IoT MUST HAVES

Bild: B&R Industrie-Elektronik GmbH

Industrie-PC mit Xeon

Der Automation PC 910 von B&R ist nun auch optional mit einem Intel-Xeon-Prozessor erhältlich. Gegenüber den bisherigen leistungsfähigen Core-i-Prozessoren ermöglicht die neue Mikroarchitektur einen Performancesprung um 50%. Mit dieser Performance können alle Applikationen bedient werden, die eine schnelle Analyse großer Datenmengen benötigen. Dazu zählen Vision-Systeme, Datenvorverarbeitung für Cloud-Anwendungen sowie Data Mining zur Qualitätsdatenerfassung und -analyse

www.br-automation.com

Halle 7
Stand 114

Für den Dschungel 4.0

Janz Tec bietet mit dem Fully Protected Security Eco System ein Toolkit, das Prozesse und Supply Chains vernetzt und unter dem Aspekt hoher Security für IIoT-Anwendungen entwickelt wurde. Außerdem erweitert das Unternehmen das Embedded-PC-Portfolio und bringt die IoT-Gateway-Serie emIOT auf den Markt. Alle IoT Gateways sind optional auch mit maßgeschneiderten Industrial Security Features aus dem Security Eco System Toolkit von Janz Tec verfügbar. Als erste Produkte der neuen IoT-Gateway-Serie stellt Janz Tec den emIoT-A/iMX6 und emIoT-X vor, denen demnächst beginnend mit dem emIoT-Edge auch kleinerformatige Systeme nachfolgen.

www.janztec.com

Halle 7
Stand 591

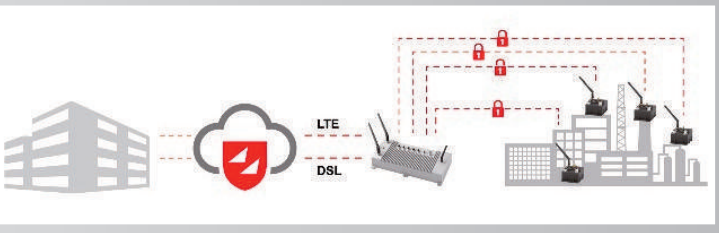


Bild: Janz Tec AG

Auf 100 Metern visualisieren

Bild: Kontron S&T AG

Kontron zeigt erste Systeme mit Kontron-Widelink-Unterstützung. Dieses Übertragungsverfahren ermöglicht es, abgesetzte Industriemonitore und Bedienpanel in einer Entfernung von bis zu 100m vom Steuerungsrechner zu betreiben. Kontron zeigt die Widelink-Technologie erstmals in Verbindung mit der neuen, für den Schaltschrankeinbau vorgesehenen KBox-C-102-Serie sowie dem ebenfalls neuen Kontron Fusionview als dezentralem Industriemonitor. Widelink ist ein vom Betriebssystem unabhängiges Übertragungsverfahren nach der IEEE1911-Norm, mit dem die Datenkommunikation zwischen abgesetztem Visualisierungssystem und Steuerungsrechner über ein Standard-CAT6-Ethernet-Kabel realisiert wird.

www.kontron.de

Halle 7
Stand 193

Bild: Schubert System Elektronik GmbH

Sicher digitalisieren

Schubert System Elektronik und Genua präsentieren das neue GS.Gate. Die Lösung kann herstellerunabhängig an Maschinen angebunden werden, um Zustands- und Leistungsdaten von Maschinen zu erfassen, zu analysieren und zu filtern sowie sicher an Monitoring-Systeme oder in die Cloud weiterzuleiten. Ein zentrales Merkmal des GS.Gate ist das Security by Design, das ein hohes Schutzniveau an der sensiblen Schnittstelle Maschine-LAN bzw. Internet garantiert.

www.schubert-system-elektronik.de

Halle 7
Stand 290

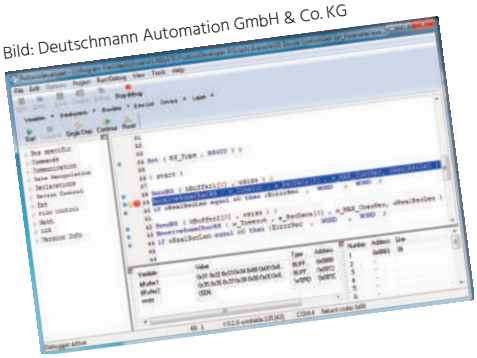
Applikationen abbilden

Deutschmann Automation vereinfacht die flexible Protokollanbindung zwischen seinen Unigate-Modulen und unterschiedlichen Endgeräten. Das Unternehmen zeigt die verbesserte Version V3 seines Protocol Developers. Das kostenfrei erhältliche Entwicklungs-Tool ist speziell für die Buskommunikation ausgelegt und leicht zu handhaben.

www.deutschmann.de

Halle 2
Stand 550

Bild: Deutschmann Automation GmbH & Co. KG



I/O-Modul für IIoT-Gateways

RS Components stellt das neue Simatic-IOT2000-Modul von Siemens vor. Besucher können am Stand das Arduino-kompatible Modul, das zusätzliche digitale und analoge Ein-/Ausgabe-Konnektivität in einem industriellen Umfeld ermöglicht, unter die Lupe nehmen. Im Einsatz mit den Simatic-IOT2020- und IOT2040-Industrie-IoT-Gateways kann das neue Modul direkt an lokale Sensoren angeschlossen werden. Ansprechbar über Allzweck-I/O und programmierbar über Hochsprachen ist das robuste Modul Schield CE- und UL-zertifiziert und für den industriellen 24/7 Betrieb konzipiert. Der I/O-Bereich umfasst fünf digitale 24V-Eingänge und zwei Ausgänge. Hinzu kommen zwei wählbare Analogeingänge mit 9Bit-Auflösung und für Spannungen von 0 bis 10V oder Ströme von 0 bis 20mA. Das IOT2020 eignet sich für den Einsatz im Bildungs- und Ausbildungsbereich.

de.rs-online.com

Bild: RS Components GmbH

Halle 1
Stand 624

Systemboard für Kiosk und Digital Signage

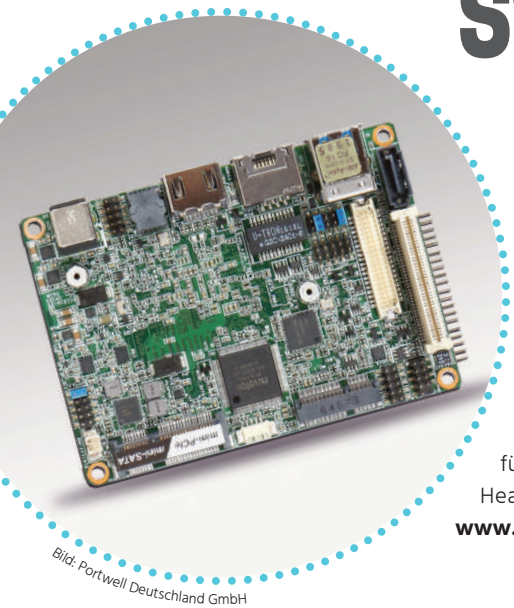


Bild: Portwell Deutschland GmbH

Portwell kündigt das PICO-6260 (100mmx72mm) Pico-ITX Embedded System Board, basierend auf der Intel-Atom-Prozessor-E3900-Serie und dem Intel-Celeron-Prozessor N3350, früherer Codename Apollo Lake, an. Die Intel-Atom-Prozessor-E3900-Serie und der Intel-Celeron-Prozessor N3350 integrieren die Intel Gen-9-3D-Grafikengine mit bis zu 12 Ausführungseinheiten (kurz EUs), was die Leistung verbessert und 4K Codec De- und Encode unterstützt. Zudem wird ein 24-Bit-Dual-Channel-LVDS-Anschluss und ein HDMI auf der hinteren I/O mit einer Auflösung von bis zu 3840x2160, unterstützt. Das 204-PIN Non-ECC SO-DIMM bietet Speicherunterstützung bis zu 8GB DDR3L. Es verfügt über insgesamt zwei COM-Ports, drei USB-Ports (1xUSB3.0 auf der rückseitigen I/O, 2x2.0 Onboard Header) und einen Gigabit Ethernet Port.

www.portwell.de

Halle 8
Stand 120

Robuste Connectivity

Der NB800 EcoRouter von Netmodule zielt auf alle Anwendungen im Umfeld von Industrie 4.0 ab, bei denen robuste Connectivity und Zuverlässigkeit Voraussetzungen sind. Der Fokus liegt auf einfacher Integration und Remote-Konfiguration/Management. Zu den Features gehören ein 3G/4G-zu-Ethernet-Gateway und eine VPN-Protokoll-Suite. Das hochkompakte Gerät ist als UMTS und als LTE&WLAN-Version erhältlich sowie in kundenspezifischen OEM-Varianten, z.B. als Tagfinder zum Freight Tracking, weitere Adaptierungen sind in Arbeit. Speziell für OEM-Versionen bieten neue Hardware-Shields zusätzliche Flexibilität, indem diese kleinen, aufsteckbaren Erweiterungsmodule auf den jeweiligen Einsatzbereich abgestimmt werden können.

www.netmodule.com

Halle 6
Stand 140E

Deep-Learning trainieren

MVTec Software zeigt im VDMA-Pavillon die neuen Releases Halcon 17.12 und Merlic3. Ein Schwerpunkt liegt dabei auf Deep-Learning-Funktionalität. Die neue Halcon-Version bietet eine große Auswahl an standardisierten Funktionen für den sofortigen Einsatz von Deep Learning. Anwender sind damit in der Lage, Convolutional Neural Networks (CNNs) mit vertretbarem Aufwand selbst zu trainieren. Besucher können dieses Feature direkt am Messestand anhand von Beispielanwendungen live erleben und bei einer neu produzierten Videopräsentation tiefer in das Thema Deep Learning einsteigen.

www.mvtec.de

Halle 3A
Stand 151

LTE-Module für M2M

Atlantik Elektronik präsentiert mit der neuen auf Qualcomm basierenden Produktfamilie LTE-A Cat.-6-Module und erweitert damit das LTE-Portfolio. Quectel stellt diese neuen LTE-Module in drei verschiedenen Formfaktoren vor: EG06, EP06 und EM06, um einen größeren Bereich an Anwendungen abdecken zu können. Das EG06 ist ein im LGA-Format ausgeführtes Modul für eine SMD-Bestückung. Mit den Modulen EP06 als Mini-PCIe-Bord und EM06l im M.2-Format können Applikationen mit optionalen LTE-Einsatz ermöglicht werden. Die auf der 3GPP-Rel.-12-LTE-Technologie und auf Carrier Aggregation basierende Produktfamilie ermöglicht Datenraten von 300Mbps im Download und 50Mbps im Upload.

Bild: Atlantik Elektronik GmbH

www.atlantikelektronik.de

Halle 10
Stand 422D

IoT MUST HAVES

Bild: Data I/O GmbH

Sicher programmieren

Data I/O präsentiert die neue Provisioning-Umgebung SentriX zur sicheren Erzeugung und Programmierung von Schlüsseln und Zertifikaten für authentifizierbare Bausteine, Secure Elements und Secure-Mikrokontroller. SentriX lässt sich nahtlos in den Programmier- und Handling-automaten PSV7000 von Data I/O einbinden und sowohl mit der Programmiertechnologie LumenX als auch der smarten Software ConneX kombinieren. Außerdem wird erstmals in Europa die neue webbasierte Software ConneX live demonstriert. Das Programmiermodul ermöglicht umfangreiche Nachvollziehbarkeit in Echtzeit und detailliertes Prozess-Monitoring. ConneX integriert die automatische Bausteinprogram-mierung mit Industrie-4.0-Fertigungsumgebungen, indem es die Programmierhandler der PSV-Serie von Data I/O mit Produktionssystemen und Applikationen von Drittanbietern verbindet.

www.dataio.de

productronica
Halle A2 | Stand 205

Messen und Testen

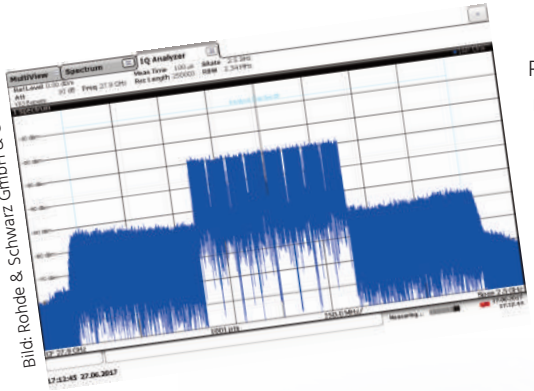


Bild: Rohde & Schwarz GmbH & Co. KG

Rohde & Schwarz stellt Mess- und Testlösungen für die Technologien der drahtlosen Kommunikation in den Mittelpunkt. Dazu zählen das IoT, die fünfte Mobilfunkgeneration (5G) sowie Automotive Radar und Infotainment-Systeme. Für Entwickler im Bereich 5G oder Breitbandkommunikation im Allgemeinen präsentiert das Unternehmen eine Testlösung bestehend aus dem R&S-SMW200A-Vektorsignalgenerator und dem R&S-FSW43-Signal- und -Spektrumanalysator. Der Messaufbau unterstützt Verizon-5GTF-Signale und zahlreiche 5G-Wellenform-Kandidaten im Frequenzbereich bis 40GHz.

www.rohde-schwarz.com

productronica
Halle A1 | Stand 375

Kostenloser EMS-Design-Guide

Das Hardware-Design ist der Grundstein für eine kostengünstige Serienproduktion von elektronischen Baugruppen. Die Kosten dieser Baugruppen werden durch viele verschiedene Faktoren in der Produktion beeinflusst. Der größte Kostenhebel wird jedoch viel früher, beim Layout der Platinen und der Positionierung von Bauelementen, definiert. Ginzinger hat mehr als 25 Jahre Erfahrung in der Produktion von elektronischen Baugruppen in einer nützlichen Broschüre zusammengefasst, die Sie am Unternehmensstand auf der Productronica kostenlos erhalten.

www.ginzinger.com

productronica
Halle A2 | Stand 543

Bild: Ginzinger Electronic Systems GmbH

IoT STATEMENT

Nur Mut, Logistik

STATEMENT VON MATHIAS MITTMANN, SOFTWARE AG

Investitionen im IoT-Bereich sind für Unternehmen nicht nur sinnvoll, sondern auch unvermeidbar, wollen sie wettbewerbsfähig bleiben. Die Logistik-Branche wird nach Experteneinschätzungen einer der Vorreiter sein: Laut einer BCG-Studie werden Unternehmen aus dem Transport- und Logistikbereich bis zum Jahr 2020 jährlich 40 Milliarden Dollar für IoT-Technologie und Lösungen ausgeben, um ihre Supply Chain, ihre Fahrzeugbewegungen oder ihren Waren- und Güterverkehr zu optimieren.

Die grüne IoT-Wiese

In der Logistik bergen mehrere Bereiche großes Optimierungspotenzial, etwa das Flotten- und Transportmanagement, das Einsatzzeiten, Routen, aber auch Beladungen steuert. So hat ein deutsches Logistikunternehmen Sensoren an LKWs befestigt, die Geschwindigkeit, Ort und Neigungswinkel des Fahrzeugs ermitteln und in Echtzeit übertragen. Auf Basis dieser Daten erhalten die Fahrzeugführer – ergänzt um Verkehrsinformationen, Wetterdaten oder Treibstoffpreise – aktuelle Empfehlungen zu Fahrweise und -route. Dies erhöht die Sicherheit und reduziert den Treibstoffverbrauch. Die Auswertung aller Faktoren und Übermittlung einer Empfehlung muss in Echtzeit vonstatten gehen, damit die Verantwortlichen zeitnah geeignete Maßnahmen ergreifen können. Auch im Transportation & Warehouse Management können IoT-Technologien Mehrwerte schaffen. Hier lässt sich wiederum mehrmals unterteilen, in welchen Disziplinen Hebel für Mehrwerte angesetzt werden können. In Sachen Diebstahlprävention können Sensoren etwa überprüfen, ob Container oder einzelne Pakete auf ihrer Reise oder während der Lieferung geöffnet wurden, Gewicht verloren haben oder Licht zu ungewöhnlichen Zeiten eingefallen ist – und wenn ja, wann. Durch Asset & Item Tracking wiederum können einzelne, sensorbestückte Gegenstände individuell geortet werden, selbst innerhalb eines Lagers, eines Hafens oder Flughafens. So kann die Position einer Lieferung exakt bestimmt werden. Doch auch den Aspekt Arbeitssicherheit bringt das IoT voran: Sensorische Wearables können LKW-Fahrer beispielsweise vor Übermüdung oder vor sich anbahnenden Kollisionen von Fahrzeugen, Personen oder Objekten warnen.

Entscheidungen in Echtzeit

Verschiedenartige Daten in Echtzeit zu sammeln, zu korrelieren und auszuwerten, macht es wie bei den genannten Beispielen möglich, Entscheidungen schneller zu treffen und Folgeprozesse frühzeitig einzuleiten. Die technische Voraussetzung dafür ist die reibungslose Integration von Systemen, Anwendungen und Geräten. Dies gelingt bestmöglich auf einer agilen Plattform, auf der sich alle Anwendungen und Geräte über Standardschnittstellen anbinden und ein reibungsloser Datenfluss sicherstellen lassen. In dieser Plattform werden auch standardisierte Prozesse und Abläufe für bestimmte Ereignisse festgelegt. Durch die Verbindung der Integrationsplattform mit Echtzeittechnologien wie einer Streaming-Analytics-Plattform können auf Basis von Kontextinformationen und aktuellen Ereignissen anhand dynamischer Muster automatisch Entscheidungen getroffen und Verantwortliche entsprechend benachrichtigen werden. Logistikunternehmen müssen nach wertschöpfenden Anwendungsfällen suchen und den Mut haben, schnell den Schritt aus der Konzeptionsphase heraus in die Umsetzung zu machen. Mit agiler und plattformbasierter Technologie wird es gelingen, theoretische Überlegungen in praktische Anwendungsfälle umzuwandeln.

www.softwareag.com ■

IoT MUST HAVES

Bild: Premier Farnell Ltd.

Mit Gesten steuern

Farnell Element14 bietet ab sofort das neue 3D-Tracking- und Gestensteuerungs-HAT ('Hardware on Top') im Rahmen der Raspberry-Pi-Zubehörreihe an. Der Flick Hat ermöglicht es Entwicklern, die Steuerungsoptionen für Raspberry-Pi- und -I2C-gestützte Projekte zu erweitern. So können Benutzer ihre Geräte ganz einfach bedienen, indem sie wischen, tippen oder ihr Handgelenk schütteln. Durch die 3D-Gestenerkennungstechnologie erkennt das System Gesten in bis zu 10cm Entfernung – das ist doppelt so weit wie bei ähnlichen Produkten. Damit erhalten Benutzer eine hochgradig flexible Lösung. Durch eine lötfreie Installation ist das Gerät schnell einsatzbereit. Die Software-Bibliotheken ermöglichen es Entwicklern, alle Funktionen der 3D-Tracking- und Gestenerkennungstechnologie im vollen Umfang zu nutzen.

de.farnell.com

Selbstlernender KI-Chip

Intel hat einen experimentellen Chip namens Loihi vorgestellt, der durch 130.000 Neuronen sowie 130 Millionen Synapsen wie ein menschliches Gehirn lernen können soll. Die Neuronen und Synapsen sind natürlich nur nachgebildete Strukturen, sollen aber beim autonomen Lernen in KI-Systemen helfen. Intel sieht die Einsatzmöglichkeiten für den selbstlernenden Chip in fast allen Bereichen, darunter bei Automotive, in der Industrie oder in persönlichen Robotern. Entsprechende Algorithmen zur sparsamen Kodierung, zur Wegfindung oder zum Wörterbuchlernen hat Intel bereits programmiert. Die Produktion soll im November starten, der Einsatz ab Ende des Jahres in Universitäten beginnen.

www.intel.com

Bild: Intel Deutschland GmbH

Mini-PC auf 43mm

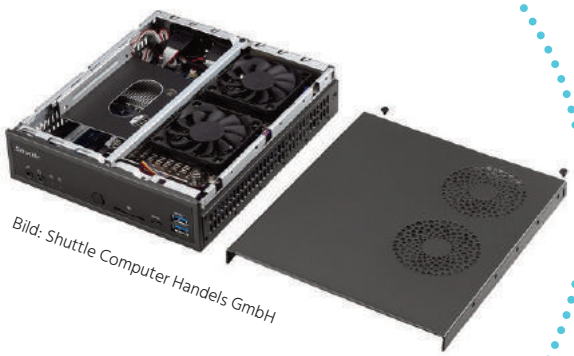


Bild: Shuttle Computer Handels GmbH

Mit dem DH270 hält, durch einen Intel-H270-Chipsatz, nun auch bei Shuttle-Mini-PCs für gesockelte LGA1151-Desktop-Prozessoren der HDMI2.0-Anschluss Einzug. Das platzsparende Stahlgehäuse trotzt Umgebungstemperaturen bis +50°C und ist durch Vesa-Halterung und diverse Gewindeöffnungen auch für individuelle Befestigungskonzepte an Bildschirmen und Oberflächen geeignet. Dabei ist die Betriebsposition völlig egal. Das XPC Barebone DH270 bietet neben Platz für ein 2,5"-Laufwerk und eine NVMe-SSD auch zwei SO-DIMM-Slots für bis zu 32GB DDR4-Speicher. Es eignen sich beliebige Intel-Core-Prozessoren (LGA1151) der siebten und sechsten Generation bis 65W TDP. Mit 1x HDMI2.0 und 2x HDMI 1.4b ermöglicht dieses Modell Multi-Bildschirm-Arbeitsplätze oder Digital-Signage-Szenarien mit bis zu drei 4K-Monitoren (1x60Hz, 2x30Hz).

www.shuttle.eu

Smart zum Ziel – ohne Umwege!

SQL4AUTOMATION – die smarte Datenbankanbindung!

Daten einfach, schnell und sicher zwischen SPS, Robotersteuerungen und Datenbanken auszutauschen war bisher ohne großen Aufwand, selbst programmierte Zwischentools sowie Performanceverlusten nicht möglich.
Der smarte SQL4AUTOMATION Connector schafft das mit wenigen Clicks.

www.sql4automation.com

sps ipc drives
Besuchen Sie uns in Halle 7, Stand 550

SQL4AUTOMATION
The smart database connection

Halle 6
Stand 129

Echtzeitfähiger Embedded-PC

Der Single-Board-Computer lässt sich als Standard-Controller für schnelle **Steuerungs- und Regelungsaufgaben in Maschinen und Anlagen** flexibel einsetzen. Als Embedded-Lösung hat er eine lange Produktverfügbarkeit und bietet damit einen hohen Investitionsschutz.

RENATE KLEBE-KLINGEMANN, esd electronics gmbh

In vielen Branchen werden schnelle und industrietaugliche Steuerungen gefordert, beispielsweise in der Industrieautomatisierung, der Pharmaindustrie, dem Transport- und Verpackungswesen, dem Maschinenbau oder im Bereich Automotive. Der ursprünglich für einen Kunden aus dem Maschinenbau entwickelte Single-Board-Computer EPPC-T10 von ESD Electronics bietet eine solide Basis für schnelle Steuerungs- und Regelungsaufgaben. Durch ein Expertenteam im Hintergrund hat die kompakte Embedded-Lösung eine lange Produktverfügbarkeit und bietet damit einen hohen Investitionsschutz. Als High-End PowerPC mit QorIQ CPU und drei GB-Ethernet-Schnittstellen kann er in Ethercat-Applikationen mit bis zu drei unabhängigen Netzwerken eingesetzt werden. Damit lässt er sich als Maschinensteuerung in der Industrie oder generell als flexible Steuereinheit in Maschinen mit industriellem Feldbus einsetzen. In Kombination mit der Ethercat-Master-Funktion erreicht er eine kurze Zykluszeit bis auf 100µs hinunter.

Standard-Produkt vom Systemhaus

Bei der Entwicklung neuer Projekte oder bei der Erweiterung bestehender Systeme greifen viele Unternehmen auf eigene, erfahrene Entwicklungsteams zurück. Müssen aber komplett neue Technologien eingeführt werden, arbeiten immer mehr Unternehmen mit externen Dienstleistern wie ESD Electronics zusammen, um zeitliche und finanzielle Risiken zu reduzieren. Hierbei profitieren die Unternehmen von der Flexibilität des Ingenieurteams, das täglich auf der Basis aktuellster Technologien entwickelt. Das verbessert die Time-to-Market von Produkten, so dass komplexe Prototypen bereits innerhalb von drei bis vier Monaten lieferbar sein können. Bei den leistungsstarken Fertigkomponenten eines Distributors muss der Anwender hingegen für Funktionalitäten bezahlen, die er häufig gar nicht benötigt. Mit einem Standard-Produkt wie dem EPPC-T10 reduzieren sich Risiko und Kosten, da er sich aktueller, gleichzeitig aber auch bewährter Technologien bedient. Außerdem bleibt die Option einer auf den Kunden zugeschnittenen Modifikation erhalten.

Leistungsstarker Embedded-PC

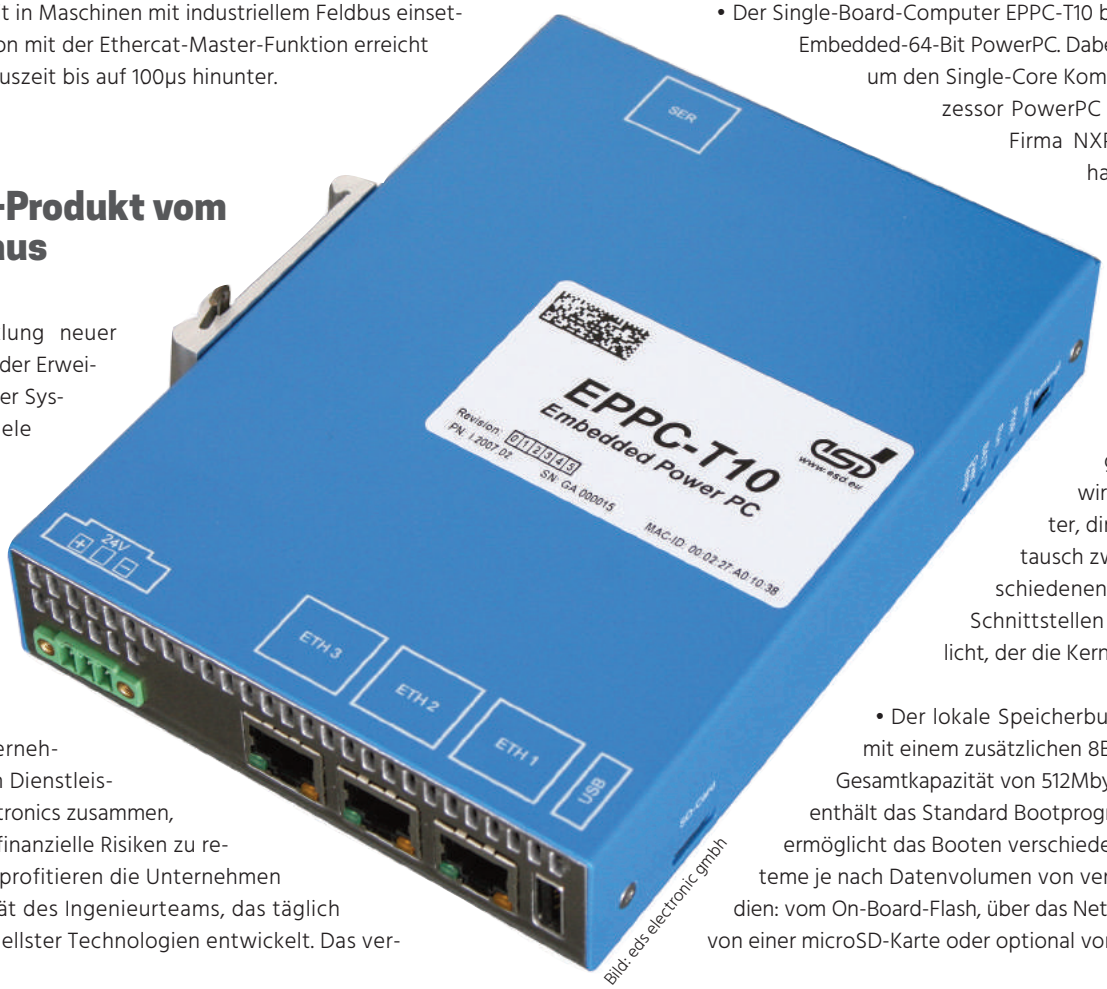


Bild: esd electronic gmbh

• Der Single-Board-Computer EPPC-T10 basiert auf einem Embedded-64-Bit PowerPC. Dabei handelt es sich um den Single-Core Kommunikationsprozessor PowerPC QorIQ T1014 der Firma NXP mit 1,2GHz. Er hat einen 64-bit-Kern auf Basis der Power-Architektur-Technologie und lässt sich bis auf vier Kerne erweitern. Durch die integrierte DPAA wird ein performanter, direkter Datenaustausch zwischen den verschiedenen integrierten Schnittstellen der CPU ermöglicht, der die Kerne entlastet.

• Der lokale Speicherbus ist 64Bit breit, mit einem zusätzlichen 8Bit ECC und einer Gesamtkapazität von 512Mbyte. Der EPPC-T10 enthält das Standard Bootprogram 'U-Boot' und ermöglicht das Booten verschiedener Betriebssysteme je nach Datenvolumen von verschiedenen Medien: vom On-Board-Flash, über das Netzwerk, über USB, von einer microSD-Karte oder optional vom SATA-SSD.

- Außerdem verfügt der Single-Board-Computer über eine Double-Precision Floating-Point-Einheit und ist mit einer Batterie-Backup-RTC ausgestattet. Der kompakte Computer hat die Maße 117mmx31mmx160mm (LxBxH) und ist für die Montage auf der DIN-EN-Tragschiene (TS 35) geeignet. In der Standardversion läuft der EPPC-T10 unter Linux, andere (Echtzeit-) Betriebssysteme sind auf Anfrage erhältlich.

- Für Ethercat-Anwendungen hat ESD Electronics den Ethercat-Master-Stack entwickelt, der für Linux sowie mehrere Echtzeit-Betriebssysteme verfügbar ist wie OS-9, QNX oder VxWorks. Dieser Master-Stack lässt sich auch auf Computern anderer Hersteller mit dem unterstützten Betriebssystem einsetzen.

- Drei 1GB-Ethernet-Schnittstellen sind im Frontpanel über RJ45-Buchsen anschließbar. Außerdem bietet der Single-Board-Computer eine RS232-Schnittstelle, eine USB-2.0-Schnittstelle (Host), einen microSD-Kartensteckplatz sowie einen internen PCI Express Mini-Steckplatz für Hardwareerweiterungen.

- Der sichere Betrieb in Industrieumgebungen wird in erster Linie durch die Überwachung der lokalen Spannungen und Temperaturen sowie ein ausfallsicheres Firmware-Update mittels Fallback-Flash erreicht. In zweiter Linie erhöhen der garantierte Betriebstemperaturbereich von 0°C bis +55°C, eine Watchdog-Funktion sowie ein mehrstufiger Übertemperaturschutz die Betriebssicherheit.

Kundenspezifisch

Reichen diese Leistungsmerkmale für die gewünschte Anwendung nicht aus, so lassen sich auch kundenspezifische Forderungen berücksichtigen, wie z.B. alternativ die Verwendung des Power-Saving Dual-Core Prozessors PowerPC QorIQ T1022, eines parallelen oder seriellen MRAM mit 512Kbyte, eines erweiterten DDR3 RAM mit 2GB, eines größeren Flash-Memorys bis zu 2x128Mbyte. Auch ist ein PCI Express-Steckplatz integrierbar, beispielsweise zur Erweiterung von I/Os mit Hilfe von PMC-Baugruppen über eine PMC Add-on-Baugruppen, inklusive der erforderlichen Gehäuseanpassung sowie die Nachrüstung eines internen SATA-SSD. Optional ist der EPPC T10 auch für die Betriebssysteme OS9, QNX, VxWorks, Linux und andere erhältlich.

www.esd-electronics.com

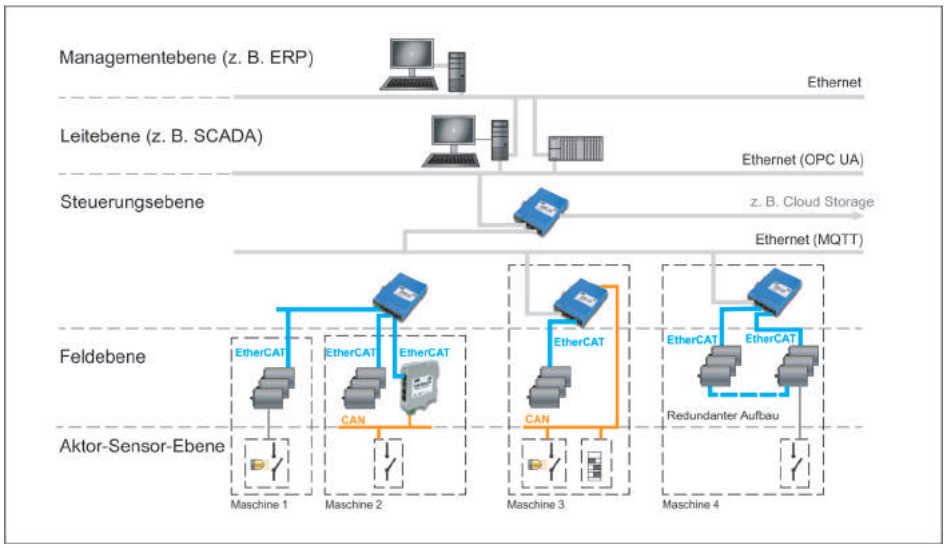


Bild: eds electronic gmbh

Als High-End PowerPC mit QorIQ CPU und drei GB-Ethernet-Schnittstellen kann er in Ethercat-Applikationen mit bis zu drei unabhängigen Netzwerken eingesetzt werden.

Halle 10
Stand 236

Mit AWS sicher in die Cloud

Der Beginn von Industrie 4.0 hat dazu geführt, dass **Fabriken** weit mehr **automatisiert und mit Remote-Fertigungs- und Steuerungskonzepten** ausgestattet sind. Dies setzt Anlagen auch dem Risiko eines ungewollten Zugriffs aus. Wenn die Fabrik, wie üblich, mit einer **öffentlichen oder privaten Cloud verbunden** ist, bestehen inhärente **Sicherheitsrisiken**.

XAVIER BIGNALET, Microchip Technology GmbH

Ein guter Ausgangspunkt ist es, festzulegen, ob die Lösung eine kabelgebundene, drahtlose oder eine Kombination aus beidem sein soll. Davon ausgehend ist es empfehlenswert, Verbindungstechnologien zu nutzen, die über Standardprotokolle verfügen, wie beispielsweise WiFi, Bluetooth oder Ethernet, um die im industriellen Bereich bekanntesten Technologien zu nennen. Der Einsatz von Standard-Sicherheitsverfahren verringert das Risiko einer Gefährdung der Verbindungen. Das widerstrebt zuweilen den historischen Gepflogenheiten, die in der Industrie üblich sind, die auf proprietäre Lösungen setzt. Die Infrastruktur muss so gebaut sein, dass sie über viele Jahre genutzt werden kann. Eines der Probleme ist jedoch, dass selbst die am höchsten qualifizierten Embedded-Ingenieure nur wenig Wissen über IT-Sicherheitskonzepte haben. Sie sind keine IT-Sicherheitsexperten, und diese Wissenslücke hindert sie daran, eine robuste und sichere IoT-Infrastruktur zu schaffen. Sobald die Verbindung zwischen Fabrik und Cloud hergestellt ist, vertrauen die Ingenieure plötzlich der Welt von Amazon Web Services (AWS), Google, Microsoft Azure usw. und kommen schnell dahinter, dass sie Hilfe von IT-Fachleuten benötigen, um die vielfältigen Sicherheitsbedrohungen, denen sie nun gegenüberstehen, zu bewältigen. Eines der Hauptziele von Hackern ist das Aushebeln eines einzelnen Zugriffspunkts, um Fernzugriff auf eine große Zahl von Systemen zu erhalten. Remote-Angriffe können großflächige Schäden anrichten, wie zum Beispiel der Distributed Denial of Service (DDoS)-Angriff gezeigt hat. Die Schwachstelle in einem IoT-Netzwerk sind gewöhnlich die Hardware und deren Anwender am Endknoten, – die Techniker, die ihn betreuen, verfügen in der Regel nicht über das IT-Wissen, um sich dem Problem annehmen zu können. Um so wichtiger ist es, Ingenieure und Techniker darin schulen, wie eine sichere End-to-End-Infrastruktur aussehen sollte. Außerdem sind große Cloud-Anbieter, wie AWS, Google und Microsoft wichtige Know-how-Träger. Die große Lektion besteht darin, das Thema Sicherheit nicht zu vernachlässigen oder zu umgehen, und die Sicherheit erst als zusätzliches Add-On zu betrachten, nachdem ein IoT-Netzwerk konzipiert worden ist. An diesem Punkt ist es bereits zu spät. Sicherheit ist etwas, das von Beginn einer jeden IoT-Konzeption an implementiert werden muss. Sicherheit beginnt bei der Hardware und kann nicht einfach als nachträgliche Idee eingefügt oder in der Software ergänzt werden.

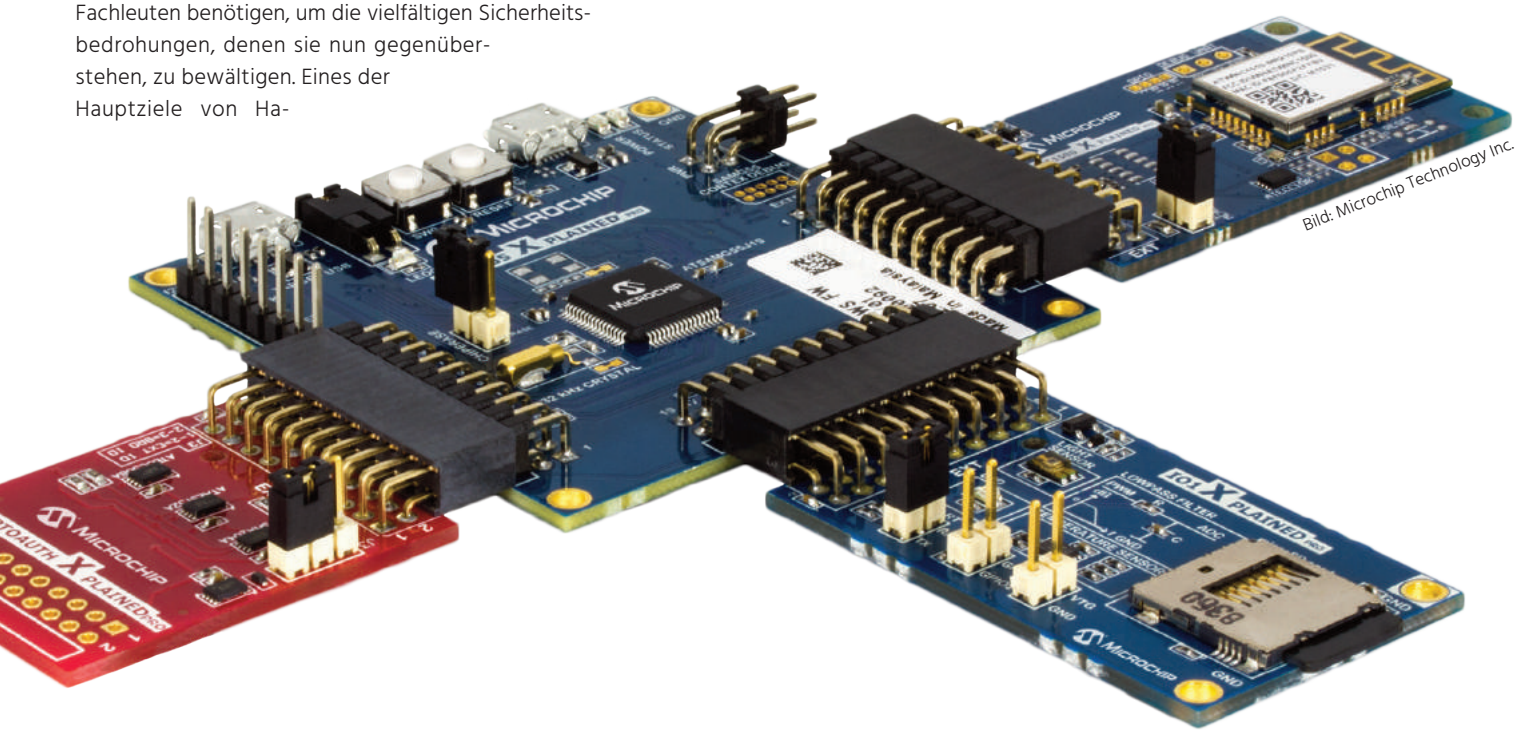


Bild: Microchip Technology Inc.

Authentifizierung

Das wichtigste Teil des Sicherheitspuzzles ist die Authentifizierung. Ein Systementwickler muss mit der Konzeption beginnen, dass alle an ein Netzwerk angeschlossenen Netzwerkknoten eine eindeutige, geschützte und vertrauenswürdige Identität haben. Zu wissen, ob jemand, der sich im Netzwerk befindet, auch derjenige ist, für den er sich ausgibt und ob er vertrauenswürdig ist, ist von höchster Wichtigkeit. Um dies zu realisieren, muss die übliche Verwendung des Verschlüsselungsprotokolls TLS 1.2 und die gegenseitige Authentifizierung zwischen einem Server und einem IoT-Endknoten stattfinden. Dabei werden Informationen verwendet, denen beide Seiten vertrauen – eine Zertifizierungsstelle. Jedoch funktioniert dies nur, wenn das vertrauenswürdige Zertifikat, das von der Zertifizierungsstelle ausgestellt wurde, ständig geschützt ist, vom Projektstart angefangen, über die Fertigung und sobald das System in der intelligenten Fabrik eingesetzt wird. Der private Schlüssel, der zur Bestätigung der Authentizität des IoT-Endknotens verwendet wird, muss sicher und geschützt sein. Ein schwaches aber verbreitetes Implementierungsverfahren, das dafür angewendet wird, ist die unverschlüsselte Speicherung des privaten Schlüssels in einem Flash-Speicher innerhalb eines Mikrocontrollers, wo er eventuell Softwaremanipulationen ausgesetzt ist. Allerdings kann jeder auf diesen Speicherbereich zugreifen und ihn einsehen, steuern und so in den Besitz des privaten Schlüssels gelangen. Dies ist eine mangelhafte Umsetzung, die Netzwerkdesignern ein falsches Gefühl von Sicherheit gibt. An dieser Stelle kommt es zu Schäden und großen Problemen.

Sicheres Element

Um eine sichere Lösung zu gewährleisten, müssen der Schlüssel und andere wichtige Anmeldeinformationen nicht nur vom Mikrocontroller entfernt, sondern auch vom Mikrocontroller entkoppelt werden und dürfen in keiner Weise mit der Software in Verbindung geraten. Hier setzt das Konzept eines sicheren Elements an. Die Idee hinter dem sicheren Element besteht darin, im Wesentlichen einen sicheren Hafen zur Verfügung zu stellen, wo der Schlüssel gespeichert und geschützt ist und niemand auf ihn zugreifen kann. Befehle von der CryptoAuthLib-Bibliothek ermöglichen es dem Schlüssel, die entsprechenden Aufforderungen/Antworten vom Mikrocontroller an das sichere Element zu senden, um die Authentifizierung zu validieren. Zu keinem Zeitpunkt des Produktentwicklungsprozesses und des Lebenszyklus wird der private Schlüssel freigelegt oder verlässt er das sichere Element. So kann eine durchgängige Vertrauenskette aufgebaut werden. Die sicheren Elemente sind autonome integrierte Schaltkreise (ICs) des Typs CryptoAuthentication, die als Tresore, in denen Unternehmen ihre Geheimnisse lagern, angesehen werden können. In diesem Fall beinhalten sie die für die IoT-Authentifizierung benötigten privaten Schlüssel.

Schlüssel bereitstellen

Ein zweites wichtiges Konzept besteht darin, wie die privaten Schlüssel und andere Anmeldeinformationen vom Kunden in das CryptoAuthentication-Gerät übermittelt werden. Zu diesem Zweck bietet Microchip eine Plattform, über die der Kunde während der Fertigung der integrierten Schaltkreise die Programmierung seiner geheimen Daten erstellen und sicher organisieren kann, ohne dass jemand an sie gelangt – auch nicht die Mitarbeiter von Microchip. Microchip fertigt dann das sichere Element an seinen gesicherten und nach einheitlichen Kriterien zertifizierten Fertigungsstandorten. Erst kurz bevor das sichere Element dem Endanwender bereitgestellt und an diesen versandt wird, verlässt es diesen gesicherten und nach einheitlichen Kriterien zertifizierten Fertigungsstandort. Wenn Kunden AWS-IoT-Accounts eröffnen, bringen sie die Kundenzertifikate mit, die Microchip in ihrem Auftrag mit der Use Your Own Certificate-Funktion von AWS ausgestellt hat. Anschließend nutzen sie die IoT-Funktion von AWS, die Just-In-Time-Registrierung (JITR) genannt wird, um einen Massen-Upload der auf Gerätezertifikate durchzuführen, die für das Konto des AWS-IoT-Anwenders im sicheren Element gespeichert und bereitgestellt werden. Das Zertifikat auf Kundenebene kann nun das Zertifikat auf Geräteebene verifizieren, und die Vertrauenskette ist somit vollständig. Durch diese Funktion wird – mit Blick auf die Sicherheit – echte Unternehmens-IoT-Skalierbarkeit ermöglicht. Es gibt möglicherweise viele tausend Zertifikate, die unter Anwendung des Just-In-Time-Registrierungsverfahrens (JITR) verarbeitet werden können. Sie können ohne Eingreifen des Anwenders in der Masse verarbeitet werden, anstatt nacheinander. Anstatt Zertifikate manuell von den verknüpften Geräten in ein Cloud-Konto laden zu müssen und diese Dritten zugänglich zu machen, können die Anwender jetzt veranlassen, dass neue Gerätezertifikate sich automatisch als Bestandteil der Ausgangskommunikation zwischen dem Gerät und dem AWS-IoT registrieren, ohne dass die Sicherheit jemals gefährdet ist.

Erste Schritte

Das vorkonfigurierte Zero-Touch-Bereitstellungskit (siehe Abbildung) ist im Crypto-Authentifizierungsgerät ATECC508AMAHAW enthalten. Damit lässt sich das Authentifizierungsverfahren gegenüber dem AWS-IoT-Konto durchführen. Der erste Schritt besteht darin zu erfahren, was eine Vertrauenskette ist. Dazu werden die neuen Python-Scripts angewendet. Weiterhin erfährt man etwas zum Bereitstellungsprozess, der in den Fabriken von Microchip während der Bereitstellungsphase stattfindet. Der Bausatz zeigt, wie die Prinzipien des Herstellungsprozesses in gewissem Umfang funktionieren. Außerdem weist das Gerät eine hohe Widerstandsfähigkeit gegen physische Manipulation auf und ist mit Vorkehrungen zur Abwehr von Angriffen von der Seite ausgestattet. Darüber hinaus verfügt es über einen hochwertigen Federal Information Processing Standard (FIPS) konformen Zufallszahlengenerator und über einen energiesparenden Verschlüsselungsbeschleuniger für die Kompatibilität mit einer breiten Palette von ressourcenbegrenzten IoT-Geräten. Außerdem besitzt das Gerät die Fähigkeit, unterschiedliche Fertigungsabläufe kosteneffizient nahtlos anzupassen. Um die Kluft zwischen Embedded-Ingenieuren und IT-Profis zu überbrücken, wird der Bausatz, zusätzlich zur Python-Script-Eingliederung, mit dem CloudFormation-Script ausgeliefert, das die Einrichtung des AWS-Kontos zu beschleunigt und die Cloud-Anbindung einfacher macht. Mit Hilfe eines CloudFormation-Scripts kann der Anwender in Minutenschelle eine Anwenderschnittstelle (UI) innerhalb der AWS-Umgebung definieren.

Fazit

Die Kombination der Just-In-Time-Registrierung (JITR) von AWS-IoT, in Verbindung mit dem CryptoAuthentication-Gerät ATECC508MAHAW und dem sicheren Bereitstellungsprozesses in der Fertigung von Microchip bietet IoT-Sicherheit. Diese echte Ende-zu-Ende-IoT-Sicherheitslösung ermöglicht den Erfolg der Industrie 4.0-Sicherheit in für sicheres und effizientes Wachstum. *www.microchip.com* ■

Was brauche ich?

SLC (Single Level Cell) ist die **langlebigste** Technologie bei **NAND-Flash-Speichern**. Entsprechend sind SLC-Flash-Speicher nach wie vor die **beste Wahl** für die **industrielle Automation** - aber auch die **teuerste**. Wo **lohnt sich die Investition in SLC?** Und welche Anwender können auf MLC- oder neu auf pSLC-Speicher ausweichen?

PATRIK HELLMÜLLER, SYSLOGIC GMBH

NAND-Flash-Speicher sind im Gegensatz zu Harddisks unempfindlich gegen Schocks und Vibrationen. Dadurch eignen sie sich für Industrieanwendungen. Nachteilig sind hingegen die beschränkten Schreib- und Lesezyklen von NAND-Speichern. Trotzdem eignen sie sich für Anwendungen, die eine lange Lebensdauer verlangen. Vorausgesetzt die Speicher werden bedarfsgerecht evaluiert.

SLC-Speicher: Ideal für die Industrie

SLC-NAND-Speicher (Single Level Cell) haben die höchste Lebensdauer. Diese Grundregel hat nach wie vor Bestand. SLC-NAND-Speicher lassen mit Abstand am meisten Schreib- und Löschzyklen zu und haben dadurch die höchste Lebensdauer. Die von Syslogic vertriebenen SLC-Speicher von Cactus Technologies verfügen über A-Grad-Flash-Zellen (NAND) von Toshiba mit 43 oder 32nm-Technologie. Dabei handelt es sich um die größten erhältlichen NAND-Shrinks. Die SLC-Speicher von Cactus gehören zu den langlebigsten Flash-Speichern auf dem Markt. Sie erlauben 100000, respektive 80000 Schreib- und Löschzyklen. Entsprechend müssen sie lange nicht ersetzt werden.

Einzige Nachteile von SLC-Speichern sind der höhere Preis gegenüber MLC-Speichern (Multi Level Cell) sowie die beschränkten Speicherkapazitäten. Syslogic empfiehlt für alle Anwendungen, bei denen eine lange Lebensdauer wichtig ist und bei denen die benötigte Speicherkapazität 16GB nicht übersteigt, in SLC-Speicher zu investieren. Auch bei hoher thermischer Belastung lohnt sich die Investition in SLC-Speicher, da diese unter extremen Temperaturen wesentlich zuverlässiger funktionieren als MLC-Speicher.

Bild: Syslogic GmbH

Die Single-Level-Cell-Speicher von Cactus gehören zu den langlebigsten Flash-Speichern auf dem Markt. Erreicht wird das durch hochwertige NAND-Zellen, durch clevere Firmware und durch ein ausgeklügeltes Testverfahren.

pSLC-Speicher: das Beste, was man aus MLC-Flash machen kann

Eine Innovation bei industriellen Flash-Speichern ist die pSLC-Technologie (Pseudo Single Level Cell). Diese baut zwar auf MLC-NAND (Multi Level Cell) auf, die NAND-Zellen werden aber wie ein SLC-Speicher betrieben. Anstelle von zwei Bits, wie bei MLC üblich, wird nur ein Bit pro NAND-Zelle gespeichert. Zudem sind die Unterschiede zwischen den Spannungsniveaus wesentlich größer als bei herkömmlich betriebenen MLC-NAND. Dadurch erreichen pSLC-Speicher sechsmal mehr Schreib- und Löschzyklen als herkömmliche MLC-Speicher. Bei Industrieanwendungen mit hohem Speicherbedarf, die trotzdem hohe Anforderungen an die Lebensdauer und Funktionssicherheit stellen, können pSLC-Speicher eine attraktive Alternative sein. Dass pSLC-Speicher allerdings an SLC-Speicher heranreichen, ist ein Irrglaube. Echte SLC-Speicher haben eine bis zu fünfmal höhere Lebensdauer (Endurance) als pSLC-Speicher.

MLC-Speicher: für sehr große Speicherkapazitäten

MLC-Speicher waren in der Industrie lange verpönt. Mittlerweile gibt es aber Speicherhersteller, die mit cleverer Firmware die Langlebigkeit und Zuverlässigkeit von MLC-Flash-Speichern verlängern. Gleichwohl erreichen MLC-NAND bis zu dreißigmal weniger Schreib- und Lesezugriffe als SLC-Speicher. Entsprechend empfiehlt Syslogic MLC-Speicher nur für Anwendungen, bei denen entweder die Langlebigkeit nicht zentral ist, oder bei denen sehr große Speicherkapazitäten benötigt werden. Wenn man sich für MLC-Speicher entscheidet, lohnt es sich, auf einen Hersteller mit Industrieerfahrung zurückzugreifen. Zudem lässt sich die Haltbarkeit von MLC-Speichern verlängern, indem man große Speicherkapazitäten einsetzt. Dadurch werden die Schreib- und Lesezugriffe auf mehr NAND-Zellen verteilt.

Product Grade Selector

Product Grade	Industrial	OEM	Commercial
NAND Types	SLC Single Level Cell	pSLC Pseudo SLC	MLC Multi Level Cell
Bit/Cell	1	1	2
Endurance Cycles	100K / 80K / 50K	20K	3K
Reliability	●●●●●	●◖	●
Data Retention	●●●●●	●◖	●
Life Cycle	●●●●●	●●	●●
Locked-BOM	✔	✔	✔
Cost	$$$$	$$$	$$

Bild: Syslogic GmbH

Cactus Technologies bietet ausschließlich Speicher für die Industrie. Im Angebot hat der Hersteller Flash-Speicher mit SLC-, pSLC- oder MLC-NAND-Technologie.

Mit bedarfsgerechter Evaluation lässt sich Ärger vermeiden

Flash-Speicher erfüllen die Ansprüche der Industrie betreffend Langlebigkeit und Zuverlässigkeit ideal. Voraussetzung dafür ist, dass eine gewissenhafte und bedarfsgerechte Evaluation gemacht wird. So wird sichergestellt, dass Unternehmen in die richtige Flash-Technologie investieren. Syslogic vertreibt die Flash-Speicher von Cactus Technologies. Cactus bietet Flash-Speicher in allen gängigen Formfaktoren. Es sind sowohl SLC-, pSCL- als auch MLC-Produktlinien erhältlich. Diese decken unterschiedliche Bedürfnisse ab. Allen gemein ist, dass sie von Cactus ausschließlich für industrielle Anwendungen entwickelt wurden. Besondere Merkmale der Cactus Speicher sind hochwertige NAND-Zellen von Toshiba (A-Grade), eine ausgeklügelte Firmware und eine lange Verfügbarkeit. Dadurch gehören die Cactus Speicher zu den langlebigsten und zuverlässigsten Flash-Speichern auf dem Markt. Außerdem bietet Cactus für all seine Speicher eine Fixed BOM (Bill of Material), also eine feste Stückliste. Dadurch werden Kompatibilitätsprobleme vermieden.

www.syslogic.de ■

Halle 7
Stand 193

Intelligent steuern

Bild: Kontron S&T AG

Die KBox C-Serie ist leistungsstark, skalierbar und kommt mit wartungsfreiem Design

In nahezu allen **Digitaldruckmaschinen** der Heidelberg Druckmaschinen AG ist ein **IPC** von Kontron aus der KBox C-Serie implementiert. Mit Kontrons KBox **als zentralem Rechenknoten** hat das Unternehmen einen **neuen Hochleistungsleitstand** entwickelt, der neue Maßstäbe setzt hinsichtlich Leistungsstärke, Produktionssicherheit und Bedienkomfort von Druckprozessen.

SANDRA KORSINEK, Kontron S&T AG

Die Heidelberger Druckmaschinen AG (Heidelberg) ist seit vielen Jahren Anbieter und Partner für die globale Druckindustrie. Sie sorgt für effiziente und zuverlässige Produktionsprozesse und den reibungslosen Zugang zu allen benötigten Materialien. Das Geschäftsmodell basiert auf drei Säulen: Equipment, Service und Verbrauchsmaterialien.

Schnelligkeit und Effizienz

In Druckereien selbst zählen vor allem Schnelligkeit und Effizienz. Die Druckmaschinen werden deshalb im industriellen Betrieb per Touchscreen gesteuert. Bei großen Geräten erfolgt dies in eigens entwickelten Hochleistungsleitständen, voll digitalisierte Steuerzentralen wie dem Prinect Press Center 2. Das schafft Voraussetzungen für eine effiziente Produktion.

Ultra-HD im produktiven Einsatz

Auf dem Prinect Press Center 2 überwachen die Anlagenbetreiber den Druckvorgang an einem riesigen 65Zoll großen Wallscreen. Dieser verfügt über eine im industriellen Bereich sehr seltene 4k-, Ultra-HD-Auflösung. Das ist wichtig, denn nur so lassen sich im produktiven Einsatz alle wichtigen Kennzahlen zu komplexen Druckvorgängen auf einen Blick erfassen. Die Rüstzeit, also der Zeitraum, der benötigt wird, um einen Auftrag auf der Druckmaschine einzurichten, verkürzt sich dank des modernen Leitstandmonitors erheblich. Zum Ultra-HD-Leitstand war es allerdings ein langer Weg. Schon 2014 hatten die Ingenieure von Heidelberg mit der Entwicklung der Steuerzentrale begonnen. Dabei war es für sie eine Herausforderung, die hohe Auflösung des Wallscreens umzusetzen, denn sie stellt hohe Anforderungen an den Leitstandrechner. Hubert Blüm, verantwortlich für den Einkauf elektronischer Automatisierungskomponenten bei Heidelberg: „Ultra-HD-Technologie gibt es heute in jedem gut sortierten Elektronikfachmarkt, doch im industriellen Umfeld ist das nicht selbstverständlich. Dort sind die Komponenten einer viel stärkeren Belastung ausgesetzt. 'Industrietaugliches Ultra HD', das kann nicht jeder."

Zuverlässige Komponenten

„Wir erwarten hohe Zuverlässigkeit von unseren Komponenten. Unsere Druckmaschinen laufen 24 Stunden am Tag, 7 Tage die Woche. Sie sind als Investitionsgut nicht selten 15 bis 20 Jahre im Einsatz. Lange Wartungsintervalle sind dabei das A und O", sagt Frank Reitter, Entwicklungsingenieur im Bereich Elektronikkomponenten bei Heidelberg. Zusätzlich zur Bildschirmauflösung verlangen auch die aufwändigen, in die Druckmaschinen integrierten Farb- und Qualitäts-Messsysteme Rechenpower. Insbesondere die Inline-Messsysteme setzen eine hohe Leistungsfähigkeit der verbauten

Computerhardware voraus. Sie erfassen in Sekundenbruchteilen Farbgenauigkeit und andere Erscheinungsmerkmale der Druckerzeugnisse und regeln sie bei eventuellen Abweichungen selbständig aus - ein rechenintensives Verfahren.

Anforderungen

Die Anforderungen an den neuen Industrie-PC waren leistungsstark, robust und langlebig. Fündig wurde der Druckmaschinen-Hersteller bei Kontron. „Wir pflegen seit Jahren eine vertrauensvolle Zusammenarbeit und kennen Kontron als kompetenten Partner im Bereich der industriellen Computer“, so Reitter. Viele Kunden von Kontron stammen aus der Luft- und Raumfahrtindustrie, aus der Transport- und Verteidigungsbranche. Während die Ingenieure bei Heidelberg an einem neuen Leitstand arbeiten, beschäftigen sich die Kontron-Entwickler mit einem neuen Produkt: der KBox C-Serie. Ziel ist es, die Industriecomputer der KBox-Reihe in zwei Punkten zu verbessern: Der Kunde soll die Systeme individuell nach seinen Bedürfnissen konfigurieren können und dabei die Wahl zwischen verschiedenen Leistungsstufen haben: Lüfterlose, wartungsfreie Rechensysteme und hochgradig robuste Hochleistungsrechner - beides soll möglich sein. Als das Team in Heidelberg von der neuen Rechnerserie erfährt, ist klar: die KBox ist die geeignete Rechnerplattform für ihre Zwecke. Die Entwicklung von Leitstand und KBox läuft fortan parallel.

Parallel entwickeln

In regelmäßigen Projektreviews tauschen sich die Experten beider Firmen aus. Heidelberg erwartet etwa eine Vielzahl von Schnittstellen, ohne dass Erweiterungskarten notwendig sind. Das lässt Kontron direkt in die Optionen der Konfiguration bei der KBox einfließen. Frank Reitter: „Die Skalierbarkeit des Systems hat uns überzeugt. Gerade im Entwicklungsprozess ist es ein großer Vorteil, wenn man Systeme entsprechend anpassen kann, sobald es notwendig wird.“ Seit 2016 ist in allen Bogenoffset-Druckmaschinen und nahezu allen Digitaldruckmaschinen von Heidelberg mindestens eine Kontron KBox implementiert. Sie dienen als Steuerzentrale zur Bedienung der Druckmaschine, Farbmessung und Qualitätskontrolle, zur Analyse der Predictive-Maintenance-Daten und dazu, Auftragsdaten für die Verbesserung von Druckereiabläufen auszuwerten. Als zentraler Rechenknoten sammelt und wertet sie alle Daten aus, die von den Druckmaschinen geliefert werden. Auch die Visualisierung aller Daten in Ultra-HD ist kein Problem mehr. „Durch die 4k-Auflösung können wir viel mehr Informationen an zentraler Stelle abbilden und damit die Bedienung ganz anders gestalten. Der Anwender wird viel besser unterstützt und kann noch produktiver agieren“, erläutert Frank Reitter.

www.kontron.de ■

Prinect Press Center XL 2: Moderne Technologie, intelligente Automatismen und Datenmanagement schaffen die Voraussetzungen für eine dauerhaft effiziente Produktion und bieten die Investitionssicherheit, die Druckbetriebe heute und in Zukunft brauchen. Die neue Leitstandgeneration nutzt konsequent alle Potenziale, um den Zeitaufwand pro Druckauftrag zu reduzieren.

Bild: Heidelberger Druckmaschinen AG

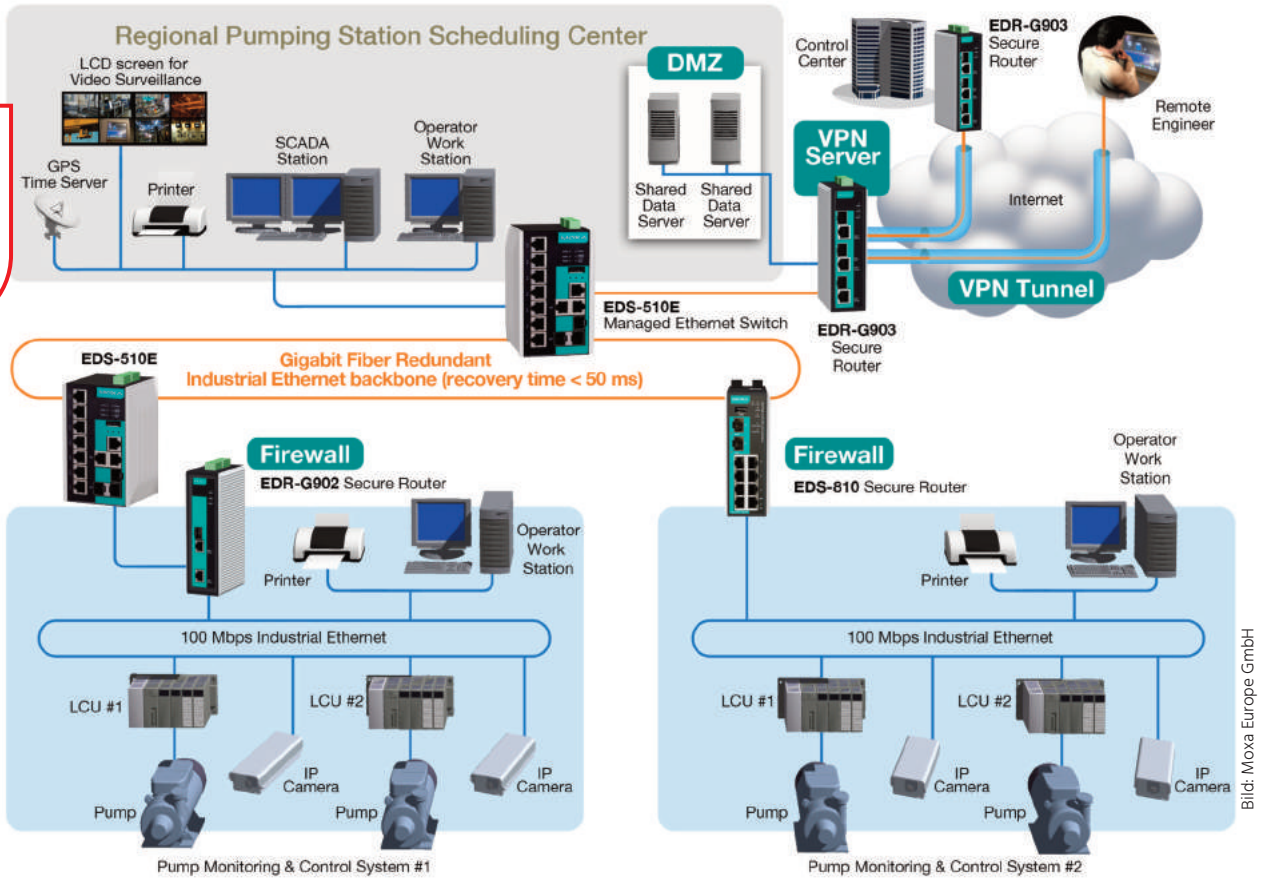


Bild: Moxa Europe GmbH

Sicherheitslücken schließen

Fernzugriff ist für viele betriebskritische **industrielle Automatisierungssysteme** notwendig. Netzwerkbetreiber müssen das Thema **Cybersecurity** berücksichtigen. **VPNs** können die wichtigsten **Sicherheitslücken in Wasserpumpenstationen** schließen.

ALVIS CHEN, Moxa Europe GmbH

Die Konvergenz von IT- und OT-Netzwerken hat neue Sicherheitslücken erzeugt, die Hackern mehr Möglichkeiten zur Infiltration eröffnen. Als Konsequenz des IIoT-Trends mussten Netzwerkbetreiber ihre industrielle Netzwerksicherheit neu durchdenken. In Industrienetzen verteilte SPSen und RTUs wurden nicht dafür hergestellt, Firewalls und Anti-Virus-Software ähnlich derer in IT-Netzwerken zu unterstützen. Und obwohl viele Firmen Leitfäden für die Hardware-Nutzung herausgeben, nutzen Mitarbeiter oder Dritte ihre Firmen-Laptops oftmals außerhalb des Firmennetzwerks, wo möglicherweise keine angemessenen Sicherheitsmaßnahmen vorhanden sind. Schnell ist da ein Virus heruntergeladen. Werden dieselben Laptops wieder ans Firmennetz angeschlossen, ist es passiert: die Firewalls, die das Herunterladen verhindern sollten, greifen nicht mehr. Auch über USB-Geräte, Smartphones oder Tablets sind Viren schnell eingeschleppt oder über das Herunterladen von Anhängen in Emails.

Sicherer Fernzugriff

Pumpenstationen sind oft über große Distanzen verteilt und müssen aus einer Zentrale heraus verwaltet werden. Die Fernüberwachung, -wartung und -diagnose überwinden die Grenzen der industriellen Herstellung und reduzieren die Betriebskosten erheblich. Netzwerkbetreiber können die Sicherheitsrisiken folgendermaßen reduzieren:

- LAN-Sicherheit: Die erste Verteidigungslinie, um nicht autorisierten Netzwerkzugriff zu verhindern. Setzt voraus, dass die gesamte Firmware auf

dem neuesten Stand ist, dass die installierten Geräte Datenverschlüsselung unterstützen und dass das Netzwerk physisch abgesichert ist.

- VPNs: Sie erleichtern den sicheren Fernzugriff auf ein privates Netzwerk für Nutzer, die sich aus einem öffentlichen Netzwerk einloggen
- Firewalls: Filtern den Netzwerkverkehr, um auf Basis einiger vorab definierter Sicherheitsregeln sicher zu stellen, dass keine Sicherheitsrisiken das private Netzwerk erreichen.

Das Netzwerk im Überblick

Die Aufgaben von Pumpenstationen umfassen die Extraktion von Frischwasser aus Bodenquellen, Abwasserhebeanlagen, die das Abwasser zu den Kläranlagen transportieren, und extensive Drainage-Anlagen, die zurückgewonnenes Land trocken halten. Üblicherweise wurden Pumpenstationen mit Hilfe von Scada-Systemen überwacht und gesteuert. Mittlerweile hat Ethernet weitgehend Einzug gehalten, was den Netzwerkbetreibern das Fernwirken und -warten ermöglicht. Auch wenn der Zugriff aus der Ferne vieles erleichtert, bleibt noch die Angreifbarkeit der Scada-Systeme, die in privaten Netzwerken weder Authentifizierung noch Verschlüsselung nutzen können. Die Local Control Units (LCUs) im Steuerungssystem sind angreifbar, da keine angemessenen Sicherheitsmaßnahmen vorhanden sind.

Sicherheits-Herausforderungen

Fernzugriff: Pumpenstationen sind meist weit voneinander entfernt - Fernzugriff ist erforderlich. Die nötigen Sicherheitsanforderungen sollten vollumfänglich erfüllt werden, müssen aber gleichzeitig finanziell erschwinglich bleiben. Wenn die Fernsteuerung und -überwachung über Ethernet-Netzwerke erfolgt, muss die Datenübertragung verschlüsselt erfolgen, um Angriffe von außen erfolgreich abzuwehren. Erlangen Hacker Zugriff auf das Netzwerk, können sie jegliche Datenpakete, die sie abfangen, dazu nutzen, die Netzwerktopologie zu interpretieren und volle Kontrolle über das Netzwerk zu ergreifen. Um dieses Risiko zu bekämpfen, lassen sich zwischen den Pumpenstationen und der Leitstelle VPNs installieren, die durch hohe Verschlüsselungsstandards nicht einfach gehackt werden können. Solche Standards, wie AES256, haben sehr lange Schlüssel, die nur mit extrem hohem Aufwand geknackt werden können. Auch wenn es Publikationen darüber gibt, wie man sie knackt, ist dies sehr kompliziert und zeitintensiv, sodass es sich kaum lohnt.

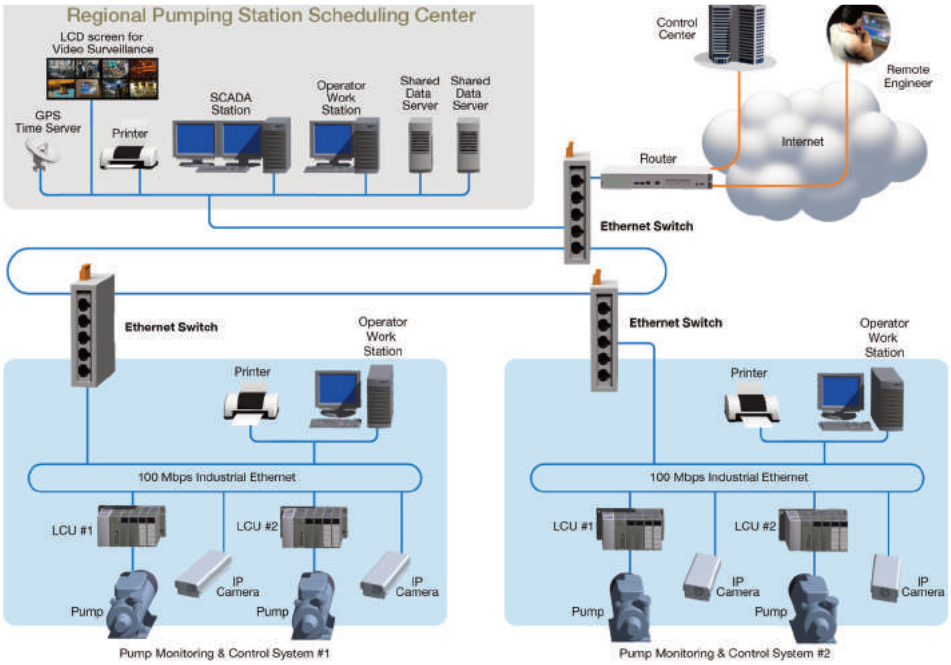


Bild: Moxa Europe GmbH

Die Local Control Units (LCUs) im Steuerungssystem sind angreifbar, da keine angemessenen Sicherheitsmaßnahmen vorhanden sind.

Videoüberwachung: Es ist wichtig, dass industrielle Ethernet-Automatisierungsnetzwerke keine Verzögerungen bei der Datenverarbeitung erleben. Daher sollten die Sicherheitsmaßnahmen keine Leistungseinbußen mit sich bringen, während überprüft und verschlüsselt wird oder Datenpakete gekapselt werden. Alle Geräte im Netzwerk sollten ausreichend Verarbeitungsleistung haben, um die Sicherheitsfunktionen über den gesamten Lebenszyklus hinweg durchzuführen. Das gilt ebenfalls für Videoüberwachungsanwendungen, bei denen Verzögerungen aufs absolute Minimum beschränkt werden müssen. Videodaten müssen vom Moment, in dem sie die Kamera verlassen, bis zum Erreichen der Leitstelle abgesichert sein. Um das zu gewährleisten, nutzen Netzwerkbetreiber nahezu immer VPNs. Da Videopakete verzögerungsfrei geliefert werden müssen, darf dieser Vorgang durch die Sicherheitsmaßnahmen nicht verzögert werden. Software-Verschlüsselung erfüllt die hohen Anforderungen von Video-Streams mit großen Bandbreiten nicht, daher ist es notwendig, die Übertragung der Videodaten zur Leitstelle über sichere VN-Tunnel mit sicherer Hardware-Verschlüsselung zu schützen. Die meisten Netzwerkbetreiber setzen dazu Stand-alone-Geräte ein. Diese dürfen weder den legitimierten Zugriff aufs Netzwerk verhindern, noch betriebskritische Pakete stoppen - denn beides könnte zum Systemausfall führen.

Netzwerkredundanz: Pumpenstationen sind betriebskritische Teile der kommunalen Infrastruktur. Sie erfordern zuverlässige Verbindungen für das Fernwirken und -warten. Experten sind sich einig, dass die Installation eines Netzwerks ohne Back-up oder redundante Konnektivität nicht ratsam ist. Um Redundanz zu unterstützen, müssen die Geräte, welche als Steuerungs- und Überwachungs-Gateways zu einer Pumpenstation fungieren, duale Konnektivität vorhalten. Netzwerkbetreiber sollten Geräte installieren, die duale, redundante WAN-Schnittstellen haben, da diese die Wahrscheinlichkeit des Konnektivitäts-Verlusts zwischen Pumpenstation und Leitstellen reduzieren.

Betrieb in rauer Umgebung: Pumpenstationen sind in der Regel unbemannt und haben weder Heizung noch Klimaanlage. Daher muss jegliche Hardware robust genug sein, um Temperaturschwankungen und Feuchtigkeit zu widerstehen. Robuste Geräte reduzieren die Notwendigkeit für Service-Besuche für Wartung oder Geräteersatz und die Ausfallmöglichkeit aufgrund von Gerätefehlern. *www.moxa.com* ■

Im zweiten Teil des Beitrags, der in der Ausgabe 1/2018 erscheint, erfahren Sie wie VPN-Lösungen die Sicherheit in Pumpenstationen aufrecht erhalten und den Fernzugriff erleichtern.

Wissen ist Macht

Die digitale Zukunft, besonders im Zusammenhang mit dem **Internet der Dinge und Industrie 4.0**, ist **ohne vernetzte Produkte als Datenquellen nicht vorstellbar**. In Zukunft werden **zusätzlich Daten und Informationen** benötigt, **um international wettbewerbsfähig** zu bleiben.

KLAUS-DIETER WALTER, SSV Software Systems GmbH

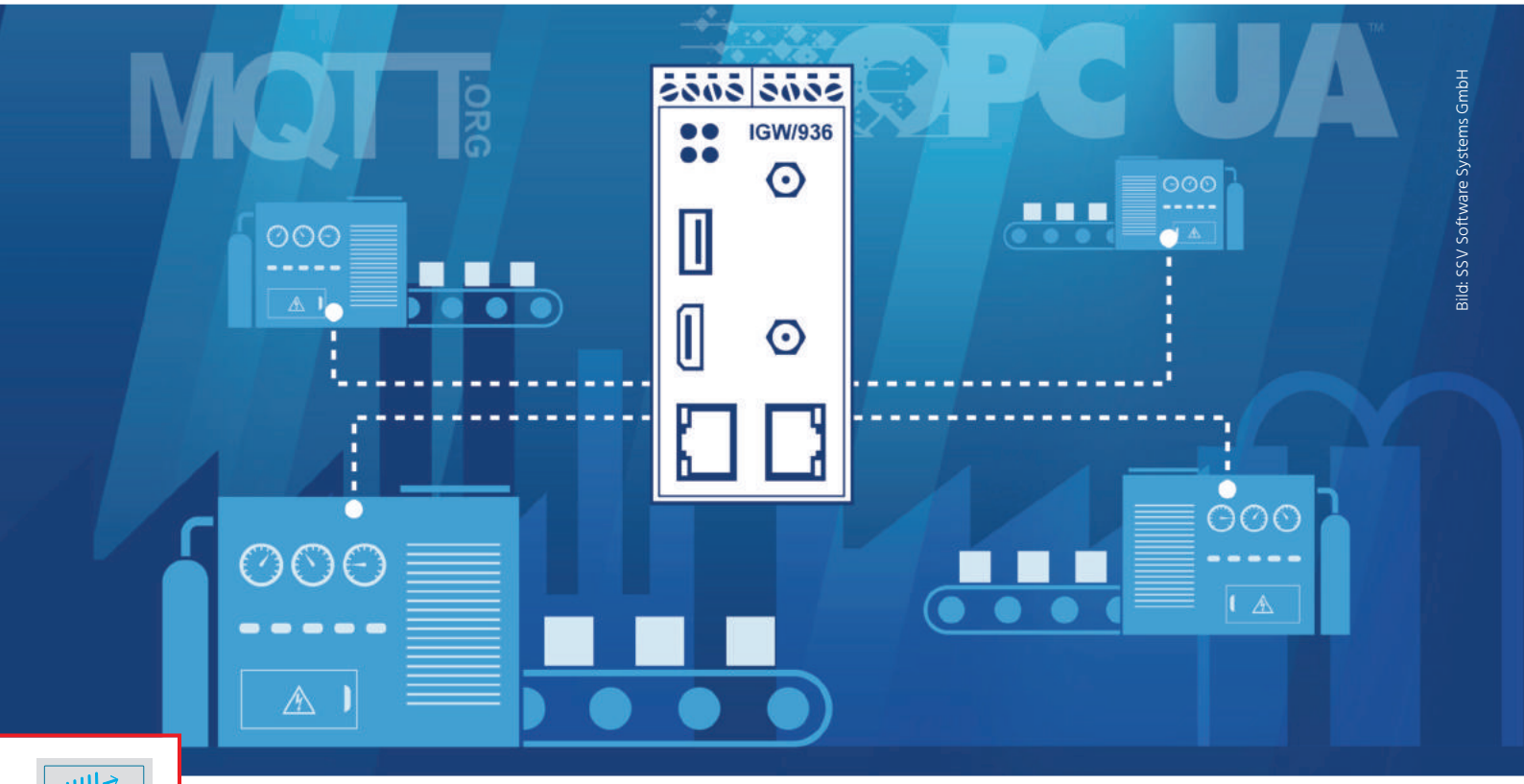


Bild: SSV Software Systems GmbH

Halle 6
Stand 140Q

Einige Maschinenbauer praktizieren immer noch das alt bewährte 'Deliver & Forget'-Prinzip: Man verkauft dem Kunden eine Maschine und freut sich, wenn man danach nicht mehr allzu viel vom Kunden hört. Schließlich haben Kunden, die sich nicht melden, auch nichts zu reklamieren. Die tatsächliche Kundenzufriedenheit bekommt der Anbieter allerdings nicht mit. Im IoT-Zeitalter ist dieses Verhalten gefährlich. In Zukunft werden nur die Maschinenbauer ihre Wettbewerbsfähigkeiten steigern können, die am schnellsten auf sich verändernde Kundenanforderungen reagieren können. Da hilft es auf jeden Fall weiter, möglichst viel darüber zu wissen, wie Kunden die jeweiligen Produkte nutzen. Die meisten Maschinenbauunternehmen besitzen komplexe Wertschöpfungsketten mit unterschiedlichen Schichten und Instanzen. Innerhalb dieser Strukturen gibt es zahlreiche Interessengruppen, für deren tägliche Arbeit die Produktnutzungsdaten und daraus abgeleitete Informationen einen erheblichen Wert hätten. Hierzu drei Beispiele:

- **Service:** Die Hauptaufgabe einer Servicemannschaft ist es, die optimale Kundenzufriedenheit für die gesamte Produktnutzungsdauer zu gewährleisten. Dieses Ziel lässt sich in erster Linie über eine wirkungsvolle Unterstützung beim Vermeiden ungeplanter Maschinenstillstände, schnelle Reaktionszeiten im Servicefall und möglichst kurze Lieferzeiten für Ersatzteile erreichen. Dabei helfen der Serviceleitung zeitnahe Informationen zur Nutzungsintensität (Betriebsstunden, Auslastung), die aktuellen Umgebungsbedingungen (Druck, Spannung, Frequenz, Temperatur), Infos zum Vibrationsverhalten sowie Fehler- und Störungsmeldungen.
- **Marketing und Verkauf:** Vom Marketing und dem dazugehörenden Produktmanagement erwartet man detaillierte Vorgaben zur Weiterentwicklung bestehender Produkte. Dazu benötigt man erfahrungsgemäß u.a. Nutzungsinformationen hinsichtlich der einzelnen Produktmerkmale (Fragestellung: Welche Produkteigenschaften werden wie oft genutzt?). Ein Vertrieb sollte über geeignete Informationen mitbekommen, ob der Kunde irgendwelche Erweiterungen gebrauchen könnte und wann es Sinn hat, den Nachfolger für die aktuell genutzte Maschine anzubieten. Mit entsprechenden Nutzungsdaten und den daraus ableitbaren Informationen lassen sich auch proaktive Serviceprodukte verkaufen.

• **Technologie-Entwicklung:** In der Entwicklung liegt die Verantwortung, dass die technischen Daten einer Maschine im Praxiseinsatz beim Kunden auch wirklich geliefert werden. Insofern existiert hier ein großes Interesse an Betriebsdaten und Informationen, aus denen hervorgeht, dass die verkauften Merkmale auch zur Verfügung stehen. Darüber hinaus sind Informationen zu den Umgebungsbedingungen, dem Vibrationsverhalten sowie Fehler- und Störungsmeldungen auch für die Mitarbeiter in der Entwicklung von erheblicher Bedeutung.

nicht nur Zustandsdaten an den Maschinenbauer liefern. Sie müssen auch für den Maschinenbetreiber einen echten Mehrwert bieten, beispielsweise Informationen zur Produktionsleistung und zum Energiebedarf einer Maschine innerhalb einer Produktionslinie. Technisch sollte eine Daten-Retrofit-Lösung möglichst unabhängig von der Maschinensteuerung (SPS) und den in der Maschine bereits verbauten und mit der SPS verbundenen Sensoren sein. Mit anderen Worten: Ein Eingriff in die zeitkritische 'Control-Loop' aus Sensoren, SPS und Aktoren ist möglichst zu vermeiden. Dadurch lassen sich auch zusätzliche IT-Security-Risiken vermeiden. Für ein Daten-Retrofit werden daher aufgabenbezogene Sensoren, ein geeignetes I4.0-/IIoT-Gateway plus die Softwarekomponenten zur Informationsgewinnung benötigt. Vor der Auswahl der Sensoren muss allerdings weitestgehend feststehen, welche Informationen am Ende benötigt werden. Der Markt bietet zwar für nahezu jede Messgröße eine Vielzahl in Frage kommender Sensoren an. Um aber aus den Sensorrohdaten werthaltige Informationen zu gewinnen, sind zahlreiche Zwischenschritte erforderlich. Dazu gehört zunächst einmal die Auswahl eines geeigneten messtechnischen Verfahrens inklusive Kalibrierung für jeden einzelnen Sensor, um die zur Messgröße passenden Daten zu erzeugen. Dafür ist ein umfangreiches Spezialwissen erforderlich. Liegen die Messgrößen-bezogenen Daten im Gateway vor, werden mit Hilfe eines geeigneten Algorithmus die benötigten Informationen gewonnen. Für den Entwurf und die Implementierung eines derartigen Informationsgewinnungs-Algorithmus wird ein breites Datenanalyse-Knowhow benötigt. Dabei ist zu berücksichtigen, dass zur Informationsgewinnung verschiedene Sensordaten einer Maschine miteinander verknüpft werden. Um zum Beispiel einen Maschinenschaden eindeutig vom Überlastungsfall unterscheiden zu können, kann es vorkommen, dass der Algorithmus die Daten einer Strom- und Spannungsmessung mit den Ausgaben eines bildgebenden Sensors zur Objekterkennung verknüpfen muss.

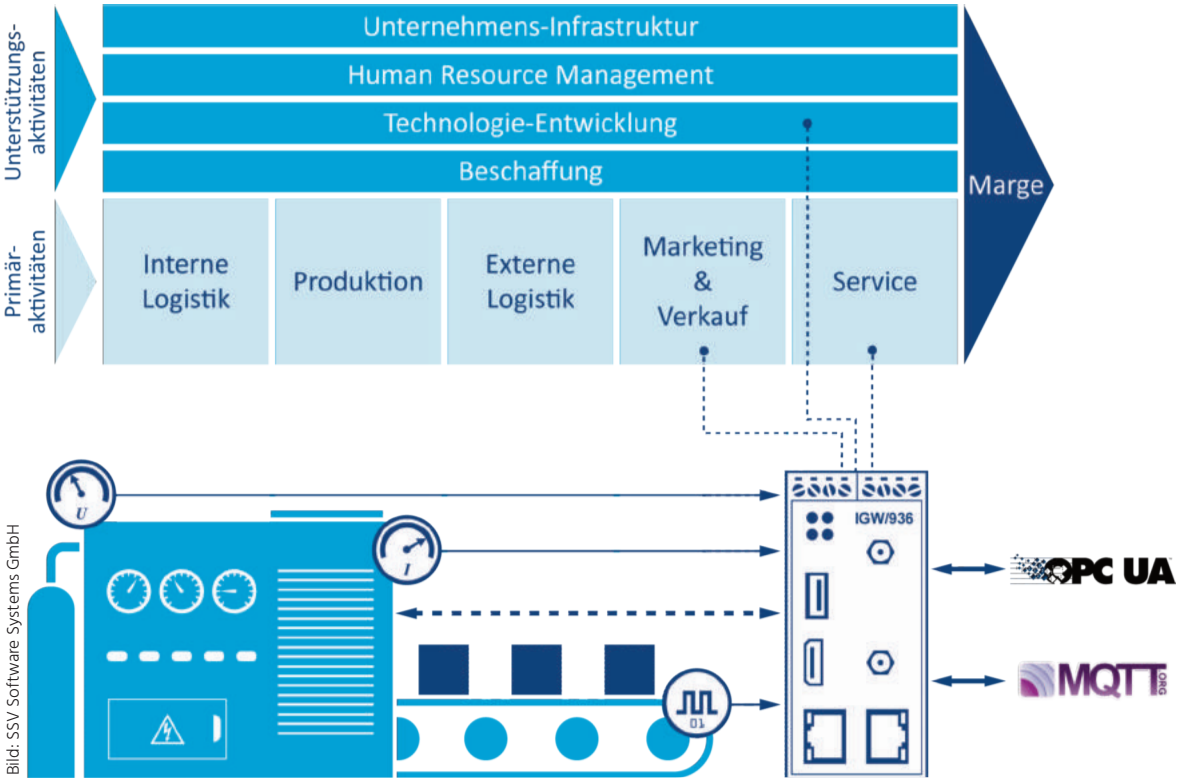


Bild: SSV Software Systems GmbH

Jede Maschine oder Anlage lässt sich im Nachhinein durch ein Daten-Retrofit-Kit modernisieren, um wertvolle Informationen für die unterschiedlichen Interessengruppen innerhalb der Wertschöpfungsketten des Maschinenbauers und -betreibers zu gewinnen. Dafür werden unterschiedliche Sensoren, ein Gateway und ein aufgabenbezogener Informationsgewinnungs-Algorithmus benötigt.

Wie kommt man an den Datenschatz?

Zukünftige Maschinen, die von Grund auf neu entwickelt werden, um als Industrie-4.0-konforme Produkte vermarktet zu werden, bieten vermutlich bereits ab Werk verschiedene Möglichkeiten des Datenzugriffs für Hersteller und Betreiber. Vielleicht werden diese Maschinen dann auch nicht mehr verkauft, sondern in erster Linie als Service angeboten. Schließlich will etwa ein Bierbrauer lediglich sein Bier in Flaschen und Fässer füllen, aber nicht unbedingt eine Abfüllanlage kaufen und betreiben. Bis dahin sind zunächst einmal Retrofit-Lösungen gefragt, mit denen der im Feld installierte Maschinen- und Anlagenbestand nachgerüstet bzw. modernisiert werden kann. Solche Nachrüst-Angebote dürfen aber

Zweifache Kommunikationsfähigkeit

Bedingt durch die Anforderung, sowohl den Maschinenbetreiber vor Ort als auch den Maschinenbauer in der Ferne mit Daten und Informationen versorgen zu müssen, benötigt die Gateway-Baugruppe einer Daten-Retrofit-Lösung zwei unterschiedliche Kommunikationsschnittstellen: Betreiberseitig steht ein Informationsmodell per OPC UA zur Verfügung. Zwischen Maschine und Hersteller kommt ein Cloud-Service zum Einsatz, der per MQTT mit Daten versorgt wird.

www.ssv-embedded.de ■

Bild: © adam121 / Fotolia.com

Auf Nummer sicher gehen

Sicherheit sorgt einerseits dafür, dass die Betriebssicherheit (**safety**) erhalten bleibt, andererseits versteht man darunter die Gesamtheit der Maßnahmen, um ein System nach außen zu schützen (**security**). Das unterstreicht sowohl die Abgrenzung dieser Begriffe, zeigt aber auch, **wie eng sie zusammenhängen**.

MARCUS GÖSSLER, MicroConsult GmbH

„Die Security ist der Schutz vor gezieltem und höchstwahrscheinlich auch böswilligem Handeln, mit dem Ziel, Vertraulichkeit, Integrität, Authentizität etc. zu erreichen." Diese pragmatische Definition des Begriffs, formuliert von Prof. Dr.-Ing. Hans-Joachim Hof (Hochschule München) zeigt den umfassenden Anspruch deutlich. Das kann sich in der Realität aber als schwierig erweisen, da zum Zeitpunkt der Projektierung unbekannt ist, welcher Art von Angriff ein System irgendwann ausgesetzt sein wird. Die einschlägigen Normen für funktionale Sicherheit sehen daher vor, potenzielle Angriffe in die Gefahren- und Risikoanalyse der funktionalen Sicherheit aufzunehmen und bei absehbarer Bedrohung der Security eine explizite Security-Analyse durchzuführen. Frappierendes Beispiel hierfür ist der Computerwurm Stuxnet, der 2010 für große Unruhe und Schäden verantwortlich war. Stuxnet war in einer Weise aktiv, die bis dahin als nicht möglich galt:

- Der Wurm konnte Grenzen physikalisch getrennter Netze überspringen
- Stuxnet konnte in Embedded-Plattformen Schäden anrichten, die dem Hacker vorher nicht bekannt gewesen sein konnten. Der Wurm war so 'gewitzt', dass die mangelnde Vertrautheit mit einem System kein Hinderungsgrund war.
- Stuxnet gelang eine weitere 'Unmöglichkeit', er infiltrierte eine Atomaufbereitungsanlage. Damit drückte Stuxnet den aktuellen Möglichkeiten des technisch Machbaren seinen eigenen Stempel auf. Eine optimierte Betriebssicherheit wurde mangels Security zum Sicherheitsrisiko.

Mit Hackern kommen Herausforderungen

Aufgrund der zunehmenden Vernetzung von Embedded-Systemen fallen mechanische Barrieren zwischen ihnen immer mehr weg. Dennoch beruht Sicherheit häufig auf physikalischer Sicherheit und weniger auf Cybersecurity oder Informationssicherheit. Und das, obwohl es gerade in Infrastrukturnetzen (z.B. intelligente Stromzähler - Smart Meter) von großer Bedeutung ist, dass die vernetzten Komponenten autonom, ohne Benutzereingaben und vor unbefugten Zugriff geschützt miteinander kommunizieren können. „Aufgrund der Verarbeitung und Zusammenführung personenbezogener Verbrauchsdaten in Messsystemen sowie möglicher negativer Rückwirkungen auf die Energieversorgung ergeben sich hohe Anforderungen an den Datenschutz und die Datensicherheit. Bekannt gewordene Hackerangriffe auf Smart Metering Systeme in den USA und Gefährdungen wie die Schadsoftware Stuxnet haben gezeigt, dass in Deutschland ein akuter Handlungsbedarf für Rahmenbedingungen einer sicheren Lösung im Bereich Smart Metering besteht." (Zitat von der Website des Bundesamts für Sicherheit in der Informationstechnologie). Was könnte die Lösung sein? Denkbar wäre eine Hardware-basierte IT-Sicherheitsarchitektur für Embedded-Systeme mit einem Security Controller oder einem Trusted-Platform-Modul im Zentrum - ein sicherer Speicher für digitale Schlüssel. Der wiederum könnte ein Zentrum für kryptografische Operationen bilden, und dieses müsste an den lokalen Computer gebunden sein und nicht an einen bestimmten Benutzer. Sodann wäre es unmöglich, das Trusted-Platform-Modul entgegen den Interessen des Eigentümers zu nutzen, sofern der Beschränkungen festgelegt hat: eine Basis für die sichere Kommunikation der Netzteilnehmer.

Einfallstor Strommarkt

Nochmal zu den Smart Grids: Diese benötigen für die Ermittlung des individuellen Strombedarfs und die korrekte Abrechnung die Verwendung entsprechender Verbrauchszähler (Smart Meter). Szenarien, die böswilliges Eindringen und Betrügen ermöglichen, sind hier leicht denkbar. Die Liberalisierung des Strommarktes mit zahlreichen Klein- und Kleinst-Stromlieferanten aus Wasserkraft oder Photovoltaikanlagen kann Hackern weitere Einfallstore für mögliche Angriffe zum Zweck der kriminell motivierten Manipulation bieten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet daher gemeinsam mit Industriepartnern für Smart Meter ein neuartiges Schutzprofil. Das neue Schutzprofil /3/ definiert ein anhand gemeinsamer Kriterien festgelegtes 'Security Modul' für alle kryptografischen Operationen.

Algorithmen und Methoden nutzen

Bei der Entwicklung von Embedded-Systemen können durch die Anwendung kryptologischer Verfahren viele Prozesse sicher oder zumindest sicherer gemacht werden. Leider passieren nämlich immer wieder die gleichen Fehler bei der Implementierung von Kryptologie. Eindringlinge haben es dadurch unnötig leicht. Softwareentwickler gehen häufig davon aus, dass die von ihnen entwickelten Algorithmen niemand knacken kann, doch das Gegenteil ist der Fall. Ein gängiges Mittel ist das Schreiben unklaren oder scheinbar verworrenen Codes. Doch gerade bei der heutigen Vernetzung wird jedes Verfahren früher oder später bekannt. Zum Beispiel führt der Selbsttest eines eigenentwickelten Algorithmus möglicherweise zu dem Ergebnis, dass es nicht einmal dem Autor selbst gelingt, ihn zu knacken. Das gilt dann als besonders sicher. Das Kerckhoffs'sche Prinzip oder Kerckhoffs' Maxime ist ein 1883 von Auguste Kerckhoffs formulierter Grundsatz der modernen Kryptographie, welcher besagt, dass die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus. Dem Kerckhoffs'schen Prinzip wird oft die sogenannte „Security by Obscurity" gegenübergestellt: Sicherheit durch Geheimhaltung des (Verschlüsselungs-)Algorithmus, möglicherweise zusätzlich zur Geheimhaltung des Schlüssels. (Wikipedia) Aber: „Jeder kann einen Algorithmus entwickeln, den er selbst nicht brechen kann, aber es geht darum, dass ihn andere nicht brechen können" (B. Schneier) - eine interessante Erkenntnis. Letztlich sieht man es einem Algorithmus nicht an, ob er nun sicher ist oder nicht. Daher gilt die Empfehlung, konservativ zu entwickeln und dabei bekannte und altbewährte Algorithmen und Methoden zu nutzen. Doch auch einer perfekt implementierten Kryptologie sind Grenzen gesetzt, wie z.B. Denial-of-Service-Attacken oder der immer Erfolg versprechende Versuch, stets das schwächste Element eines Walls von Maßnahmen für die Sicherheit zu instrumentalisieren: den User selbst. So gilt letztlich, dass gesunder Menschenverstand niemals hinter Formalismen verschwinden darf.

Kein „verbauen und vergessen" mehr

Für die Realisierung von Sicherheit gilt immer, dass etwas Sicherheit besser ist als gar keine. Angesichts des rasanten Fortschritts, der von zunehmendem Zeit-, Konkurrenz- und Erfolgsdruck zuverlässig begleitet wird, besteht die zentrale Herausforderung darin, neben Qualitätsforderungen auch ein angemessenes Sicherheitsniveau zu realisieren. Die Anforderungen Offenheit (Vernetzbarkeit mit anderen Systemen), Änderungsfreundlichkeit und Sicherheit sinnvoll unter einen Hut zu bringen stellt extrem hohe Ansprüche an das Software-Engineering. Dies führt beispielsweise zu folgender paradoxen Situation: Gerade bei Embedded-Software kann eine Verbesserung der Zugangssicherheit über Software- Updates erfolgen. Dies wiederum erfordert die Zugänglichkeit des Systems über Schnittstellen, z.B. zum Internet. So führt die Anforderung, die Sicherheit der Software durch Updates zu verbessern, zwangsläufig dazu, dass das System nicht vollständig gegen unbefugten Zugriff schützbar ist. Daraus ergeben sich gleichermaßen Aufgaben für die Entwicklung von Soft- und Hardware. In punkto Hardware werden dafür nämlich sichere Interfaces und Übertragungsprozeduren benötigt. Und die Software muss so aufgebaut sein, dass sie autorisiert korrigiert, aber nicht ohne Autorisierung manipuliert werden kann. Das Motto „Verbauen und Vergessen" gehört damit der Vergangenheit an.

www.microconsult.de ■

Angriffe abwehren

Das Industrial Internet Consortium (IIC) und die Working Group for Industry 4.0 haben mit der Industrial Internet Reference Architecture (**IIRA**), beziehungsweise dem Reference Architectural Model for Industry 4.0 (**RAMI 4.0**), **Richtlinien und Empfehlungen gegen Cyber-Attacken** erarbeitet. Einen Schutz vor Cyber-Angriffen bietet die **Separation-Kernel-Technologie**. Sie ermöglicht es, anfällige Schnittstellen streng zu kontrollieren, um Angriffe schon im frühen Stadium zu unterbinden.

ARUN SUBBARAO, Lynx Software Technologies

Das RAMI 4.0-Modell (Abb.1) ist eine dreidimensionale Matrix aus Schichten, einem Life Cycle & Value Stream und Hierarchieebenen. Dies ähnelt auffällig den 'Functional Domains' und 'Viewpoints' des IIC IIRA Modells (Abb. 2). Angesichts der zentralen Rolle der Angriffssicherheit (Security) für alle Architekturen im industriellen Internet, hat das Industrial Internet Consortium (IIC) das Industrial Internet Security Framework (IISF) veröffentlicht. IISF ist ein Schutzkonzept, mit dem sich gleich mehrere Gefahrenquellen des IIoT abwehren lassen.

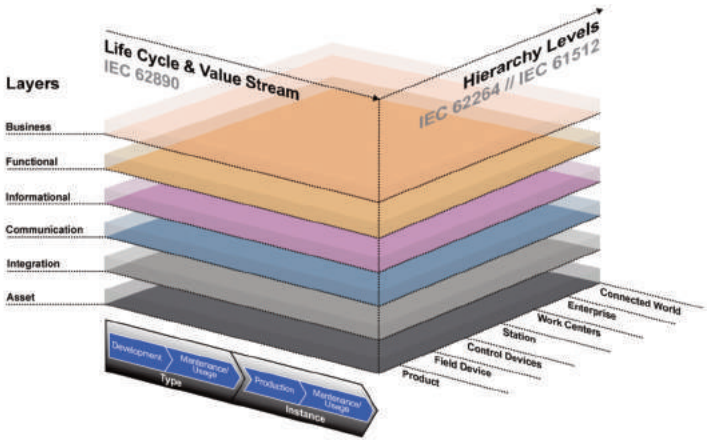


Bild: Lynx Software Technologies

Referenzarchitekturmodell für Industry 4.0 (RAMI 4.0)

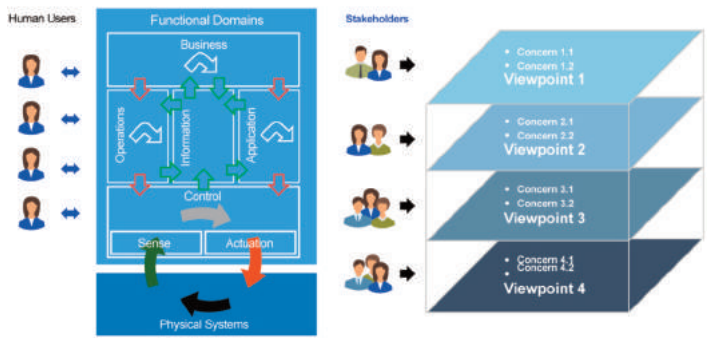


Bild: Lynx Software Technologies

Darstellung der IIC Functional Domains und Viewpoints

Das Industrial Internet Security Framework (IISF)

Das IISF deckt fünf Merkmale ab, die die Vertrauenswürdigkeit in der Informationstechnologie (IT) und bei operativen Prozessen (OT) ausmachen: Schutz, Datenschutz, Belastbarkeit, Verfügbarkeit und Sicherheit. Mit den Risikoanalysen, Gefahren- und Leistungsindikatoren des IISF können Manager und IT-Verantwortliche ihre Unternehmen schützen. Man sollte sich vergegenwärtigen, dass beide Abstrahierungen zwei bislang meist getrennte Welten einander annähern: die Informations- (IT) und die Operationstechnologie (OT). Die Aussichten und die Versprechen des IoT lassen sich nur realisieren, wenn diese heterogenen Systeme miteinander verbunden werden, was die OT jedoch neuen Sicherheitsbedrohungen aussetzt, denen zu begegnen sie aber nie ausgelegt war. Das geeignete Paradigma für ein IT-OT-Szenario ist, die Domänen voneinander zu isolieren, gleichzeitig aber einen kontrollierten Informationsfluss zwischen diesen beiden Domänen aufrechtzuhalten. Eine Industrie 4.0-sichere zugrundeliegende Software-Basis muss einerseits dafür sorgen, dass die OT ihr bestehendes Niveau hinsichtlich Betriebssicherheit, Belastbarkeit und Zuverlässigkeit beibehält, andererseits aber auch den Grad an Datenschutz und Datensicherheit erhöht, um die IT-Komponente zu schützen. Umgekehrt wird die IT-Seite - zusätzlich zu ihrer vorbildlichen Leistung in Sachen Datenschutz, Datensicherheit und Zuverlässigkeit - für eine bessere Belastbarkeit und Betriebssicherheit sorgen müssen. Idealerweise würden diese miteinander verbundenen IT-OT-Systeme von Anfang an in Hinblick auf Konnektivität konzipiert. Eine empfohlene Technik der IISF ist der Einsatz eines Separation Kernels, um das erforderlichen Isolierungsniveau zwischen unterschiedlichen Domänen zu bewahren und dennoch einen kontrollierten Informationsfluss zu erlauben. Eine passende Umsetzung, um diesen Grad an Isolierung zu erreichen, erfordert eine sichere, nicht umgehbare Basis, sollen die übergeordneten Schichten mit der notwendigen Zuverlässigkeit und Sicherheit operieren.

Prinzipien eines Separation Kernels

Auch wenn der Separation Kernel auf Prinzipien beruht, die dem industriellen Sektor vielleicht neu sein mögen - andernorts werden sie längst erfolgreich eingesetzt, um sensible Daten zu schützen. Das Konzept eines Separation Kernels wurde erstmals 1981 von John Rushby diskutiert, der

eine Kombination aus Hardware und Software vorschlug, welche die Ausführung mehrerer Funktionen auf einer gemeinsamen physischen Plattform erlaubt, ohne sich gegenseitig zu behindern. Ebenfalls führten Saltzer und Schroeder aus, dass „jedes Programm und jeder Benutzer nur die Rechte erhält, die zur Erfüllung der jeweiligen Aufgaben absolut erforderlich sind." Dieser simple Ansatz der geringstmöglichen Privilegien oder Rechte wird dringend notwendig, wenn Anwendungen unterschiedlicher Kritikalität in unmittelbarer Nähe zueinander ausgeführt werden. Die Konzepte von Separation Kernel und Least Privilege konzentrieren sich beide auf die Vorzüge der Modularisierung, wobei ersterer auf die Ressourcen und letzterer auf die Systemfunktionen gerichtet ist. Abbildung 4 zeigt die 'Subjects' (aktive, ausführbare Einheiten) mit den wenigsten/ geringsten Rechten und 'Ressources', die über die Separation Kernel Blocks gelegt sind. Wo der Separation Kernel die Granularität der Flusskontrolle je Subjekt und je Ressource unterstützt, werden weit weniger unerwünschte Kontrollflüsse zugelassen, als wenn die Flusskontrolle jeweils per Block verwaltet würde. Infolgedessen ermöglichen die oben genannten Schlüsselelemente einen isolierten und kontrollierten Informationsfluß zwischen mehreren Domänen unterschiedlicher Kritikalität, was direkt der Forderung nach einer IT-OT-Isolierung nachkommt, um IIoT-Designs mit einem hohen Niveau an Sicherheit, Schutz und Zuverlässigkeit zu schaffen.

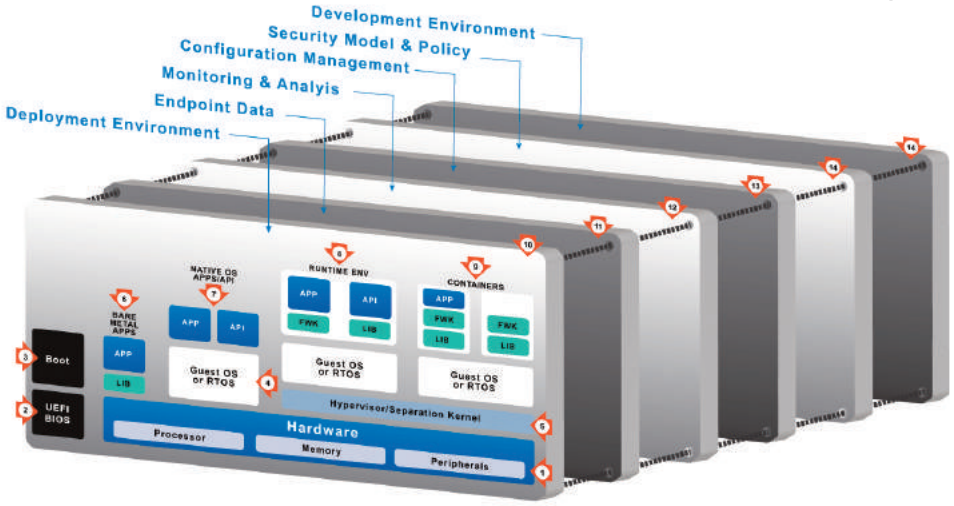
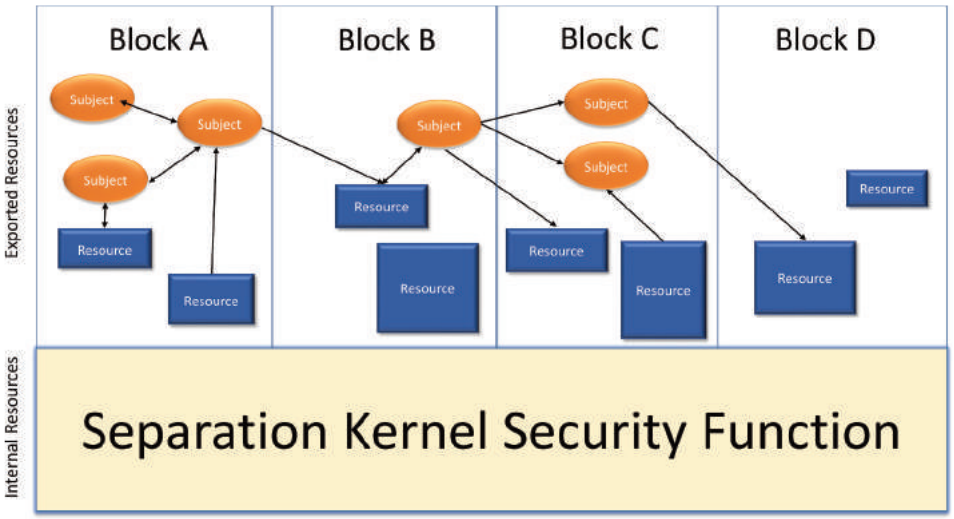


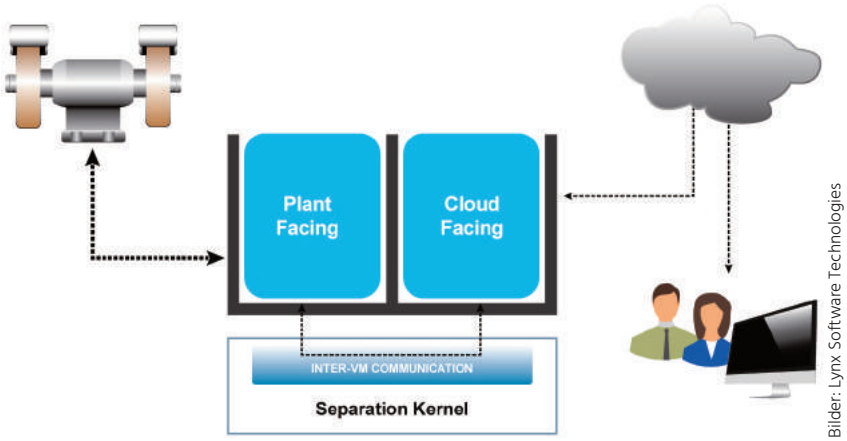
Bild: Lynx Software Technologies

Bedrohungen und Verwundbarkeiten von IoT-Endpunkten gemäß IISF



Bilder: Lynx Software Technologies

Die Überlagerung der Separation Kernel-Blöcke durch Least Privilege-Prinzipien ergibt eine feinere Granularität pro Subjekt durch die Steuerung des Ressourcenflusses.



Bilder: Lynx Software Technologies

Vereinfachtes Schema einer praktischen Separation Kernel- Anwendung

Praxistauglich

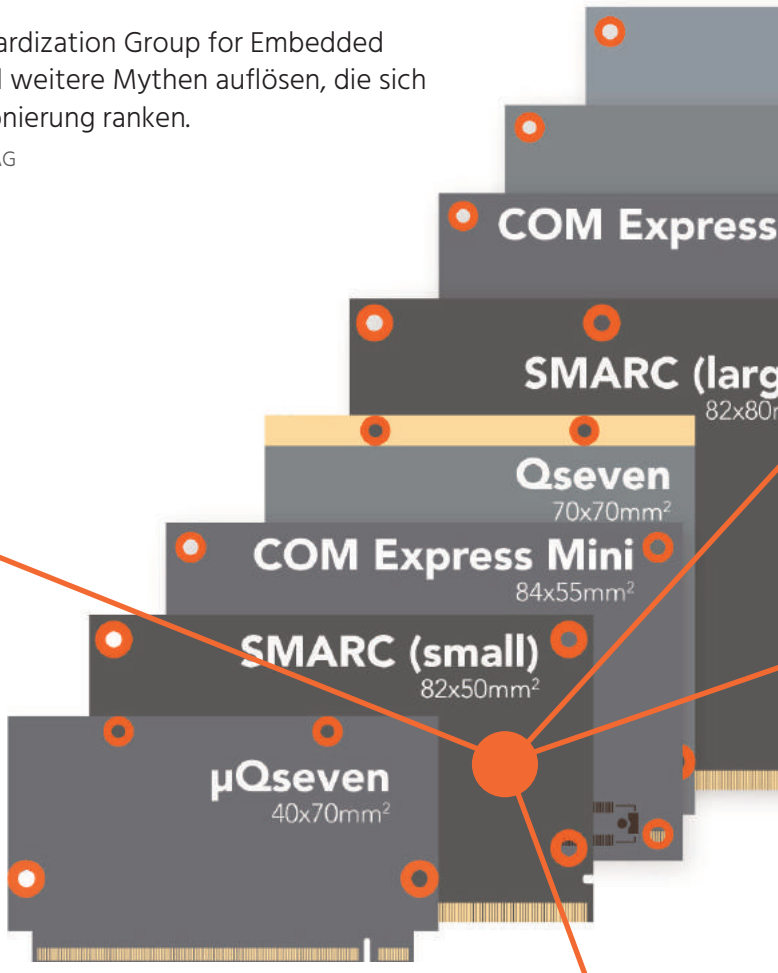
Ein praktisches Beispiel wäre etwa eine Drehmaschine, die Produktionsdaten generiert (Abb. 5). Diese Daten sollen aber über die Cloud geteilt werden, etwa auf Abruf durch einen Betriebsingenieur. Die der Cloud zugewandte Komponente in diesem Beispiel könnte ein Allzweckbetriebssystem wie Windows oder Linux sein, das anfällig für einen Angriff durch ist. Wichtig ist, dass böswillige Hacker nicht auf die Komponente zugreifen kann, die der Fabrik zugewandt ist, selbst wenn das in Richtung Cloud gerichtete Subjekt beeinträchtigt wird. Ein Separation Kernel, im Einklang mit Least Privilege-Prinzipien implementiert, wird folgende Schlüsseleigenschaften aufweisen, die für ein solches Szenario optimal sind:

- Sicher: Statische Konfiguration sorgt dafür, dass der Separation Kernel, einmal entwickelt und implementiert, unveränderlich ist und über eine kleinstmögliche Angriffsoberfläche verfügt.
- Schnell: Um fast native Performance zu erreichen, darf der Separation Kernel so wenig Overhead wie möglich mit sich bringen und sollte so effizient wie möglich auf die hardwareunterstützten Virtualisierungsfunktionen zurückgreifen.
- Klein: Wenn Betriebssystemfunktionen wie Treiber, Ein-/Ausgänge sowie Prozessverwaltung durch die Subjekte gehandhabt werden, wird der Separation Kernel selbst sehr viel kleiner ausfallen und dadurch weniger Angriffsfläche bieten.
- Praktisch: Der Separation Kernel unterstützt die Wiederverwendung bestehender Software, indem er ein 'virtuelles Motherboard' präsentiert, auf dem sich die einzelnen Subjects installieren und ausführen lassen, als befänden sie sich in einer nativen Installation. *www.lynx.com* ■

Mythen über Smarc 2.0

Smarc 2.0 ist die Formfaktor-Spezifikation der Standardization Group for Embedded Technologies (SGET). Dieser zweite Teil des Beitrags soll weitere Mythen auflösen, die sich um Smarc 2.0 und seine Marktpositionierung ranken.

ZELJKO LONCARIC, Congatec AG



Mythos 8: Smarc 2.0 nutzt das kostenintensive HDMI

Auch das ist so nicht korrekt, obwohl es eine der Optionen ist. Smarc 2.0 unterstützt 2x 24 Bit LVDS / eDP / MIPI DSI sowie HDMI/DP++ und DP++. Die zwei dual-mode DisplayPorts sind dabei sehr flexibel. Systeme, die DP++ für externe Displays unterstützen, können darüber sowohl DisplayPort, HDMI oder sogar VGA-Signale übertragen. Welche Signale genutzt werden wird einzig über die verwendeten Kabel definiert, von denen einige aktive Komponenten nutzen. Ein weiterer Vorteil ist, dass in diesem Fall keine Lizenzgebühren anfallen. Bei HDMI können sich diese für Systemhersteller auf bis zu 10.000US$ jährlich belaufen. Die neueste DisplayPort-Version ist 1.4, die am 1. März 2016 veröffentlich wurde und Bildschirmauflösungen von bis zu 7680x4320 Bildpunkten unterstützt. Auch die Steuerung interner Displays ist bei Smarc 2.0 sehr flexibel und zukunftsorientiert gelöst. Aktuell ist LVDS die am häufigsten genutzte Schnittstelle. Über sie lassen sich bei zwei 24bit-Datenkanälen hochauflösende Displays ansteuern. Neben den Bildschirmsignalen bietet LVDS auch einen kompletten Satz an Hilfssignalen, sodass die Konfigurationsdaten für die Grafik über den I2C Bus übermittelt werden können. Darüber hinaus ist es auch möglich, die Stromversorgung über zwei separate Signalleitungen zu steuern (VDD_EN). Die Helligkeit der Hintergrundbeleuchtung kann über die Enable-Signale für die Backlight-Beleuchtung (BKLT_EN) und ein Pulsweiten-Signal (BKLT_PWM) für zwei Bildschirme separat erfolgen.

Mythos 9: Upgrades von Smarc 1.1 gestalten sich schwierig

Um den Technologiesprung von Smarc 1.1 auf die Revision 2.0 umzusetzen, wurden 105 der insgesamt 314 Signalpins umgewidmet. Das sind ungefähr ein Drittel aller Signale. Trotzdem stellt die Spezifikation sicher, dass ein neues Modul in einem älteren Carrierboard zu keinerlei Beschädigungen führen wird. Ob sich dasselbe Maß an Funktionalität ohne jegliche Entwicklungsaufwendungen erreichen lässt, hängt allerdings vollständig von der individuellen Applikation ab und erfordert eine Einzelfallprüfung. Congatec bietet deshalb im Rahmen seines persönlichen Integrationssupports freie Revisionsprüfungen und berät bei nötigen Anpassungen existierender Carrierboards. Die Tabelle zeigt, was sich genau geändert hat:

Mythos 10: Carrierboards sind Geheimsache der OEMs

Für dedizierte, kundenspezifische Carrierboards trifft das durchaus zu. Aber die meisten OEMs benötigen keine kundenspezifischen Carrierboards oder halten es für vorteilhaft, eigene Designs komplett selber zu entwickeln. Deshalb gibt es Startersets mit voll ausgestatteten Carrierboards und viele Modulhersteller bieten ihren Kunden Beispiel-Layouts, die das Layout angepasster Carrierboards vereinfachen. Designguides von der SGET und den Modulherstellern vervollständigen das Supportangebot. Die Zusammenarbeit mit Modulherstellern, die einen persönlichen Integrationssupport bieten, vereinfacht den Einsatz dieser Embedded-Technologie deutlich.

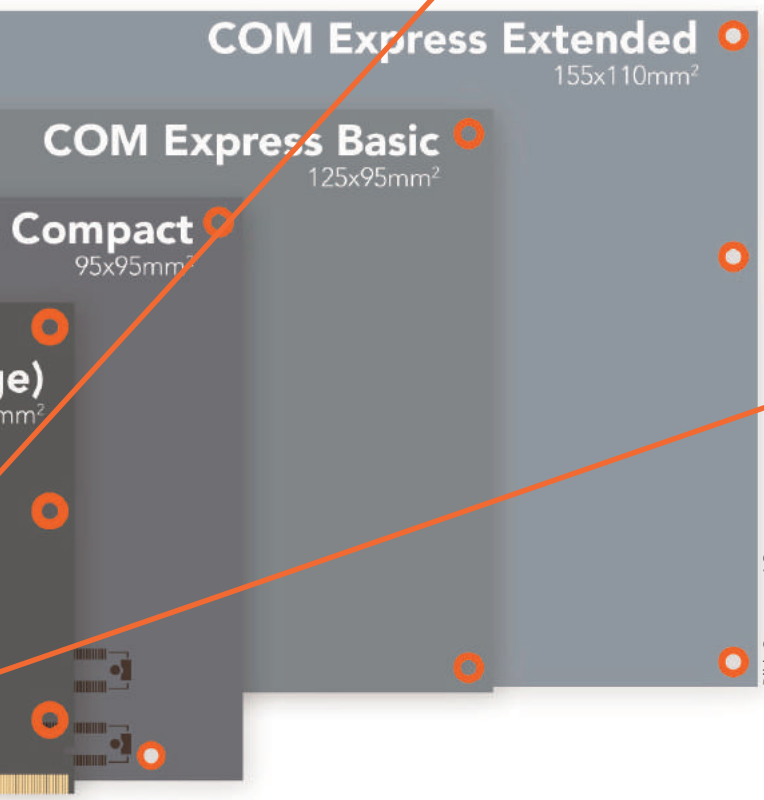


Bild: Congatec AG

Mythos 11: Interessenten mussten länger auf Smarc-2.0-Module warten

Das stimmt nicht. Erste Module wurden bereits am 25. Oktober 2016 präsentiert, parallel zum Launch der neuen Intel Atom-, Celeron- und Pentium-Prozessoren (Codename Apollo Lake). Diese Prozessoren sind eine geeignete Bestückung für Low-Power-Designs und Small-Formfaktor-Systeme. Die neuen Intel-Atom-Produkte unterstützen sogar den erweiterten Temperaturbereich von -40 bis +85°C, was sie für viele Outdoor-Projekte prädestiniert, wie Smart Cities, Smart Grids und viele andere intelligente IoT- und Automatisierungs-Projekte. Die kreditkartengroßen conga-SA5 Smarc-2.0-Module sind entweder mit den Intel Atom-Prozessoren x5-E3930, x5-E3940 und x7-E3950 für den erweiterten Temperaturbereich von -40 bis +85°C erhältlich oder mit den Intel Celeron N3350- oder Intel Pentium N4200-Quadcore-Prozessoren.

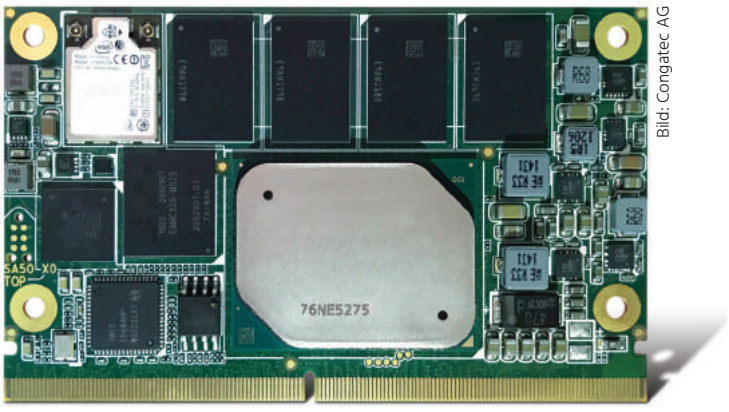


Bild: Congatec AG

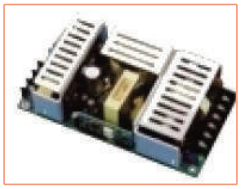
Die kreditkartengroßen conga-SA5 Smarc-2.0-Module sind entweder mit den Intel Atom-Prozessoren x5-E3930, x5-E3940 und x7-E3950 für den erweiterten Temperaturbereich von -40°C bis +85°C erhältlich oder mit den Intel Celeron N3350- oder Intel Pentium N4200-Quadcore-Prozessoren.

SMARC 2.0	SMARC 1.1
2x Gigabit Ethernet	1x Gigabit Ethernet
eSPI	
SATA 0	SATA 0 / eMMC
MIPI CSI 0-1	Parallel Camera
HDA / I2S 0-1	I2S 0-2 / SPDIF
USB 2.0 0-5 / USB 3.0 0-1	USB 2.0 0-2
HDMI & DP++	HDMI
PCIe 0-3	PCIe 0-2
GPIO 0-11 / SDIO	GPIO 0-11 / SDIO
LVDS 2x24 / eDP / MIPI DSI	Parallel Display
SER 0-3 / CAN	SER 0-3 / CAN
SPI / I2C	SPI / I2C / AFB
Power	Power

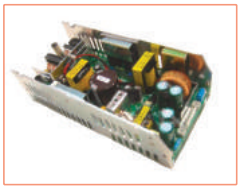
Stromversorgung

Werden Stromversorgungen in Embedded-Systemen untergebracht, sind die Open-Frame-Varianten besonders praktikabel. Aber folgende Punkte sollten beachtet werden.

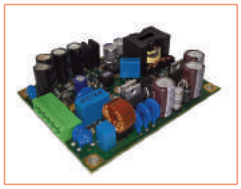
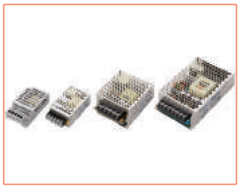
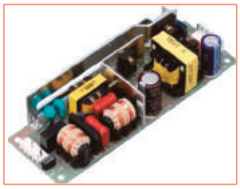
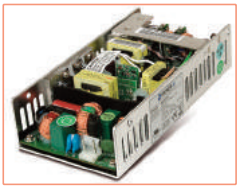
Aufgepasst: Kurzschlüsse lassen sich umgehen in dem man sicherstellt, dass die offene Unterseite der Platine keinen Kontakt zu leitenden Flächen hat. Auch die Kühlung braucht hohe Aufmerksamkeit, damit die Leistung auf Dauer stabil bleibt. Beim Einsatz im lüfterlosen Betrieb stehen wesentlich geringere Ausgangsströme zur Verfügung, so dass manche Hersteller optionale Gehäuseabdeckungen mit integriertem Lüfter anbieten. Ein hoher Wirkungsgrad sogt außerdem für eine geringere Verlustwärme. *(clj)* ■

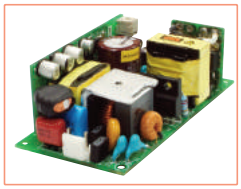
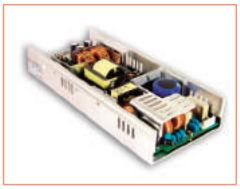


Anbieter	AmpPower GmbH
Kennziffer	**2053**
Ort	Oberursel (Taunus)
Telefon	06171/ 9160139
Internet-Adresse	www.amppower.de
Produktname	PMK150
Produkteinführung	
Länge * Breite * Höhe	139,7* 76,2* 35 mm
Gewicht	630 g
Eingangsspannungsbereich VDC	-
Eingangsspannungsbereich VAC	90 - 264 V
Ausgangsspannungsbereich evtl. Liste fester Stufen	5-48 V
max. Ausgangsleistung	150 W
vorhandene Leistungsklassen	130 / 150 / 225 / 320 / 450 W
Wirkungsgrad	78 - 80%
Restwelligkeit Spitze-Spitze-Wert	100
Betriebstemperaturbereich	- 50°C
PFC Power Factor Correction vorhanden	✓
Einschaltstrombegrenzung / Überlastfest Strombegrenz.	20A (bei 100VAC) 40A (bei 200VAC) / ✓
Leerlauffest	✓
Parallelbetrieb	✓
Redundante Ausführung möglich	✓
Überwachungsmöglichkeiten Power Fail Signal etc.	
CE-Zeichen UL-Zulassung usw.	UL, TUV, CB, CE
Kundenspezifische Lösungen	✓
Lieferzeit in Wochen	4

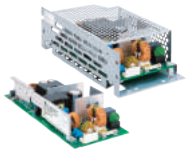


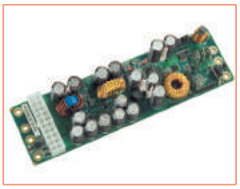
Anbieter	CME CompuMess Elektronik GmbH	Convertec Ltd.	Elektrosil GmbH	ETA-Power Europe Ltd.	ETA-Power Europe Ltd.
Kennziffer	**2237**	**2250**	**2011**	**1775**	**24506**
Ort	Unterschleißheim	Bad Buchau	Hamburg	Steinhausen	Steinhausen
Telefon	089/ 321501-0	07582/ 9318-11	040/ 840001-24	0041/41/ 74701-11	0041/ 41/ 74701-11
Internet-Adresse	www.compumess.de	www.convertec.de	www.elektrosil.com	www.etapower.com	www.etapower.com
Produktname	MINT	OFRI	SNP-Z06x Serie	ETA, PFE-Series,bis 480W Peakload	KMS- für medizinische Geräte
Produkteinführung	2009				
Länge * Breite * Höhe	**	100* 50* 31 mm	101,6* 50,8* 30,4 mm	250* 110* 65 mm	101.6* 50.8* 31.7 mm
Gewicht		600 g	150 g	1200 g	190g
Eingangsspannungsbereich VDC	-	-	-	220 - 340 V	-
Eingangsspannungsbereich VAC	85 - 264 V	90 - 264 V	85 - 264	85 - 264 V	85 - 264 V
Ausgangsspannungsbereich, Liste fester Stufen	3.3; 5; 12; 15; 18; 24; 48 V	3,3V 5V, 12V, 15V, 24V, 48V	3.3,5,12,15,24,48,5/12,5/24,15/5,5/12/-12,3.3/5/12	12,24,36,48 V	12, 24, 48 V
max. Ausgangsleistung	270 W	100 W	90 W	480 W	150 W
vorhandene Leistungsklassen	22, 65, 110, 270 W	100 / 200 W	50 / 65 / 75 / 100 / 200 / 300 W	75 / 120 / 240 W	100, 150, 180 W
Wirkungsgrad	- 90%	89 - 92%	85 - 92%	78 - 86%	90%
Restwelligkeit Spitze-Spitze-Wert	33	100	50	300	
Betriebstemperaturbereich	- 70°C	-25 - 50°C	0 - 50°C	-25 - 75°C	-25 - 55°C
PFC Power Factor Correction vorhanden	✓	✓	✓	✓	✓
Einschaltstrombegrenz. / Überlastfest Strombegr.	✓/✓	/✓	NTC, 40A(115VAC), 70A(230VAC) / ✓	15A bei 230VAC / ✓	/✓
Leerlauffest	✓	✓	✓	✓	✓
Parallelbetrieb	Nein	Nein	Nein	Nein	Nein
Redundante Ausführung möglich	Nein	Nein	Nein	Nein	Nein
Überwachungsmöglichkeiten Power Fail Signal etc.	LED, Power Fail Signal, Power Good Signal				
CE-Zeichen UL-Zulassung usw.	CE, EN, UL	UL/IEC 60950	EN60601-1, UL2610, CSA22.2 No.601.1, EN60950, UL60950CSA22.1 No.234	CE, UL , CSA , EN, VDE, ISO	EN 60601-1, CSA-C22/2, UL 60601-1
Kundenspezifische Lösungen	✓	✓	✓	✓	✓
Lieferzeit in Wochen		4	5-6 Wochen bzw. ab Lager	6-8	8-10

					
Autronic Steuer- und Regeltechnik GmbH **29835** Sachsenheim 07147/ 24 - 0 www.autronic.de	Balluff GmbH **29995** Neuhausen 07158/ 173-0 www.balluff.de	Berger Stromversorgungen GmbH & Co. KG **24555** Achern 07841/ 6 73 04-0 www.berger-stromversorgungen.de	Bicker Elektronik GmbH **16324** Donauwörth 0906/ 70595-0 www.bicker.de	Bicker Elektronik GmbH **24528** Donauwörth 0906/ 70595-37 www.bicker.de	Camtec Power Supplies GmbH **24736** Pfinztal 0721/ 46596-0 www.camtec-gmbh.com
HFC50-W/O 2016	Netzgeräte für Automaten (enclosed) 2014	LFA75F-15 2009	BEO-1500M	BEP-510-B4	OSE01201 2009
100* 80* 27 mm 160 g	* *	150* 50* 33,5 mm 230 g	127 * 76,2 * 26,67 mm 0,27 kg	165 * 83,8 * 40 mm 0,6 kg	94,5* 139,2* 41 mm 510 g
14,4 - 154 V -	120 - 375 V 88 - 264 V	- 85 - 264 V	- 90 - 264 V	- 90 - 264 V	110 - 375 V 85 - 265 V
12 oder 24 V	5V, 12V, 15V, 24V		+12V/+24V/+36V/+48V		12/24/36/48/60/72/110 V
50 W 89 - 92%	160 W 20/35/60/100/150 W 87 - 92%	 versch. Ausgangsspannungen & Gehäuse -	150 W 150 W 90 - 93%	120 W 120 W 80 - 85%	120 W 120W 89 - 91%
1%			1		50
-40 - 85°C	-40 - °C	-10 - 70°C	-20 - 40°C	-10 - 70°C	-20 - 60°C
Nein	✓		✓	✓	Nein
8 A / ✓	/ ✓	/ ✓	max. 110 A (240 VAC) / ✓	/ ✓	NTC 16 A / ✓
✓	✓			✓	✓
Nein	✓		Nein	Nein	✓
Nein	Nein		Nein	Nein	Nein
	Ready Signal, LED grün/rot				Power Good optional
CE Zeichen	CE, cULus, TÜV	CE, RoHS, TÜV Rheinland, cRUus	UL/IEC/EN60601-1 3rd Edition, UL/IEC/EN60950-1, CE	CE, UL60950-1, TÜV: EN60950-1	CE, CSA/UL classified
✓	Nein		✓		✓
8-10 Wochen	ab Lager		Standardprodukte ab Lager lieferbar		4

					
Fortec Elektronik AG **2071** Landsberg 08191/ 91172-0 www.fortecag.de	Heiden power GmbH **21594** Pürgen 08196/ 9988-0 www.heidenpower.com	Huhn-Rohrbacher GmbH & Co. KG **21770** Pforzheim 07231/ 58905-16 www.huhn-rohrbacher.de	ICP Deutschland GmbH **29856** Reutlingen 07121/ 14323-0 www.icp-deutschland.de	IDEC Elektrotechnik GmbH **2324** Hamburg 040/ 253054-0 www.idec.de	M + R Multitronik GmbH **13464** Lübeck 0451/ 609950 www.multitronik.com
SNP-G12 Serie 2011	AC/DC open-Frame Netzgeräte	ACD 3500 BI	ACE-713APM 2007	PS3X 2011	USP350-Serie Mean Well 2005
101,6 * 50,8 * 32 mm 160 g	* *	* * 1.080 g	152,4* 89* 39 mm	62 bis 159 * 28 bis 38 * 51 bis 95 mm 130 g	235,2 * 101,5 * 38 mm 1,1 kg
- 90 - 264 V	- -	400 V 230 V	115 - 230 V -	125 - 375 V 85 - 264 V	127 - 370 V 90 - 264 V
12V, 15V, 18V, 24V, 28V, 36V, 48V		400V DC, 230 AC		5, 12, 24V DC (Poti +/-10%)	3,3V, 5V, 12V, 13,5V, 15V, 24V, 48V
200 W 90 - 91%	 -	3500 W - 97%	130 W - 80%	100 W 15, 25, 50, 75, 100 W 77 - 84%	350,4 W 350 W 78 - 89%
100				300	150
-20 - 45°C	-	-20 - 70°C	-20 - 70°C	-20 - 70°C	-10 - 45°C
✓	✓	✓		✓	✓
/ ✓	/ ✓	✓ / ✓	/	50A (bei 230V AC) bei Kaltstart / ✓	22A/115VAC, 44A/230VAC / ✓
✓	✓	✓		✓	✓
✓	✓	✓		Nein	Nein
Nein		✓		Nein	Nein
		✓		nein	LED grün - Power On
CE, EN60950-1, EN60601-1: 2006		CE gemäß Niederspannungsrichtlinie 2006/95/EG	✓	CE, TÜV, UL, c-UL	CE, EN60950-1, UL60950-1
✓	✓	✓		Nein	
4-6 Wochen		4-16 Wochen		sofort ab Lager	2-3 Wochen

Alle Einträge basieren auf Angaben der jeweiligen Firmen.

					
Anbieter	Neumüller Elektronik GmbH	Neumüller Elektronik GmbH	Pohl Electronic GmbH	Quel GmbH	RSG Electronic Components GmbH
Kennziffer	**21322**	**21333**	**1919**	**24582**	**2139**
Ort	Weisendorf	Weisendorf	Hennigsdorf	Alzenau	Offenbach
Telefon	09135/ 73666-33	09135/ 73666-33	03302/ 559290	06023 9798-11	069/ 984047-0
Internet-Adresse	www.neumueller.com	www.neumueller.com	www.pohl-electronic.de	www.quel.de	www.rsg-electronic.de
Produktname	PJ-12V15W	PJB-24V150W	S8JX-G	HT150	PBA100F
Produkteinführung	2013	2014	2008		2003
Länge * Breite * Höhe	87.5 * 50 * 22 mm	160 * 75 * 37 mm	105-150* 36-150* 92 mm	166* 50,5* 128,4 mm	147* 93* 32 mm
Gewicht	0,06 kg	0,31 kg	370-1800 g	700 g	440 g
Eingangsspannungsbereich VDC	-	-	-	100 - 375 V	120 - 370 V
Eingangsspannungsbereich VAC	85 - 264 V	85 - 264 V	100 - 240 V	90 - 265 V	85 - 264 V
Ausgangsspannungsbereich, Liste fester Stufen	12 V	24 V	+5, +12, +15, +24 V		3.3V, 5V, 9V, 12V, 15V, 24V, 36V, 48V,
max. Ausgangsleistung	15 W	151 W	600 W	150 W	100 W
vorhandene Leistungsklassen	15 / 30 / 50 / 100 / 150 W	100 / 150 W	15, 35, 50, 100, 150, 300, 600 W		75/ 100/ 150/ 300/ 600/ 1000/ 1500 W
Wirkungsgrad	85 - 95%	85 - 95%	75 - 91%	85 - 91%	79 - 86%
Restwelligkeit Spitze-Spitze-Wert			240		160
Betriebstemperaturbereich	-20 - 85°C	-20 - 85°C	-10 - 60°C	0 - 80°C	-10 - 50°C
PFC Power Factor Correction vorhanden	Nein	✓	✓	✓	✓
Einschaltstrombegrenz. / Überlastfest Strombegr.	/ ✓	/ ✓	40A max. bei 200VAC Input / ✓	< 16 A pk / ✓	/ ✓
Leerlauffest	✓	✓	✓	✓	✓
Parallelbetrieb	✓	✓	✓		✓
Redundante Ausführung möglich	✓	✓	Nein		✓
Überwachungsmöglichkeiten Power Fail Signal etc.	LED	LED	LED		Remote ON/OFF
CE-Zeichen UL-Zulassung usw.	✓	✓	UL-, cUL-, UL508-Listung, CE, VDE	CE, EN 60950, EN 61000-3-2	CE, UL60950-1, EN60950-1, C-UL (CSA60950-1), EN50178
Kundenspezifische Lösungen	✓	✓	Nein	✓	✓
Lieferzeit in Wochen	6-8 Wochen für Serienstückzahlen	6-8 Wochen für Serienstückzahlen	ca. 1 Woche	4-6	6-8

					
Anbieter	Spectra GmbH & Co. KG	TDK-Lambda Germany GmbH	TDK-Lambda Germany GmbH	XP Power GmbH	XP Power GmbH
Kennziffer	**13160**	**14752**	**31659**	**2341**	**13264**
Ort	Reutlingen	Achern	Achern	Bremen	Bremen
Telefon	07121/ 14321-00	07841/ 666-215	07841/ 666-333	0421/ 639330	0421/ 639330
Internet-Adresse	www.spectra.de	www.emea.tdk-lambda.com	www.emea.tdk-lambda.com	www.xppower.com	www.xppower.com
Produktname	IDDV-6304140A	ZWS300-BAF - Open Frame-Netzgerät	CUS350M-Medizinnetzteil	ECS25 Serie	ECP150 Serie
Produkteinführung		2013	2016	2011	2011
Länge * Breite * Höhe	160 * 45 mm	180* 84* 42 mm	190* 87* 40 mm	76,20 * 50,80 * 24,10 mm	101,60 * 50,80 * 29,50 mm
Gewicht	118 g	540 g	850 g	100 g	190 g
Eingangsspannungsbereich VDC	6 - 30 V	120 - 370 V	-	120 - 370 V	-
Eingangsspannungsbereich VAC	-	85 - 265 V	85 - 265 V	80 - 264 V	90 - 264 V
Ausgangsspannungsbereich, Liste fester Stufen	3,3V, 5V, +12V-12V, 5VSB	3.3V, 5V, 12V, 15V, 24V, 48V	12, 18, 24, 36, 48 V	12V, 15V, 24V, 48V	12V, 15V, 24V, 28V, 48V
max. Ausgangsleistung	140 W	302 W	417 W	45 W	150 W
vorhandene Leistungsklassen		300 W	30 - 350 W	25 / 100 W	
Wirkungsgrad	- 90%	91%	91 - 94%	86 - 90%	91 - 92%
Restwelligkeit Spitze-Spitze-Wert		300	480	50	1%
Betriebstemperaturbereich	-20 - 85°C	-10 - 50°C	-20 - 40°C	-20 - 50°C	-20 - 50°C
PFC Power Factor Correction vorhanden	✓	✓	✓	✓	✓
Einschaltstrombegrenz. / Überlastfest Strombegr.	/	15A bei 100Vac/30A bei 200Vac / ✓	115/230 VAC 20 A/40 A @ cold start / ✓	40A bei 230VAC / ✓	60A bei 230VAC / ✓
Leerlauffest		✓	✓	✓	✓
Parallelbetrieb		Nein	✓	✓	✓
Redundante Ausführung möglich		Nein	✓	Nein	✓
Überwachungsmöglichkeiten Power Fail Signal etc.			Power Good (optional)		
CE-Zeichen UL-Zulassung usw.	CE, FCC	UL60950-1, CSA60950-1,EN50178, CE	IEC/EN 60601-1, ANSI/AAMI ES 60601-1 und IEC/EN/UL/CSA 60950-1, Geräte tragen CE-Zei.	CE Zeichen, UL - Zulassung, CSA Zulassung	CE Zeichen, UL - Zulassung, CSA Zulassung
Kundenspezifische Lösungen		✓	✓	✓	✓
Lieferzeit in Wochen	2-3	0-7 Wochen		4 - 6 Wochen	4 - 6 Wochen

Vom Nutzen der Modelle

Dieser zweite Teil des Beitrags liefert Ihnen weitere Hinweise, wie Sie anhand grafischer Modellierungssprachen und passender Werkzeuge die **Komplexität von Embedded Systems in den Griff bekommen**.

DR. HORST KARGL, SparxSystems Software GmbH und RÜDIGER MAIER, LieberLieber Software GmbH

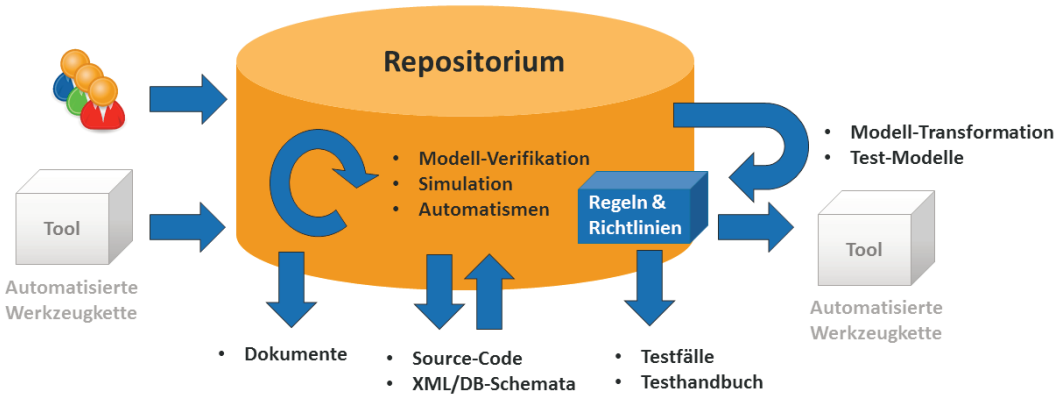


Bild:SparxSystems Software GmbH

Ein gutes Werkzeug erlaubt auch das Einlesen von bereits vorhandenem Code in das Modell und ermöglicht so Roundtrip Engineering. Änderungen sind dann im Code und/oder Modell durchführbar. Es ist auch möglich, den vorhandenen Code lediglich einzulesen, um den aktuellen Implementierungsstand zu dokumentieren, ohne aus dem eingelesenen Modell jemals wieder Code zu generieren bzw. den vorhandenen Code anzupassen. Der Code wird dabei nur im Code-File geändert, das Einlesen ist beliebig oft wiederholbar. Wurde der Code nun als Implementierungsmodell eingelesen, können abstraktere Modelle mit dem Implementierungsmodell verknüpft werden. Damit lässt sich die Nachvollziehbarkeit abstrakterer Modelle zur Implementierung erreichen, um die für den Leser des Modells relevanten Fragen beantworten zu können.

Verifikation der Modelle

Modellierungswerkzeuge bieten in der Regel die Möglichkeit, ein Modell zu überprüfen. Dabei unterscheiden wir die syntaktische Korrektheit der verwendeten Modellierungssprache und zusätzliche Regeln, mit denen das Modell nach eigenen Kriterien überprüft wird. So lässt sich sicherstellen, dass der Inhalt des Modells zumindest den strukturellen Vorgaben eines Referenzmodells entspricht. Werden diese Richtlinien eingehalten, kann man davon ausgehen, dass alles, was aus dem Modell generiert wird, auch korrekt und vollständig ist. Semantische Korrektheit ist natürlich nur bis zu einem gewissen Grad automatisch überprüfbar. Eine semantische Prüfung lässt sich durch aufwendigere Modellierungs-Regeln oder eine Modell-Simulation verifizieren. Die UML/SysML definiert neben der Syntax auch die Semantik, wie Verhaltensmodelle interpretiert werden. Im Werkzeug wird das Modell nach der gegebenen Sprachsemantik interpretiert. Findet sich ein Fehler im Modell, stoppt die Simulation an der Stelle und gibt eine Fehlermeldung aus. Der Aufwand für simulierbare Modelle ist deswegen etwas größer, da man Vorgaben genauer einhalten muss. Der Vorteil dabei ist die Überprüfung der Spezifikation auf beliebiger Abstraktionsebene, was einer semantischen Verifikation entspricht. Die UML/SysML bietet unterschiedliche Sichten zum Beschreiben eines Systems. Je nach Einsatz der Modellierungssprache sind mehr oder weniger manuelle Schritte notwendig, um das gewünschte Modell zu erstellen und synchron zu halten. Ist der manuelle Aufwand zu groß, um Modelle nach gewissen Regeln (dem Referenzmodell/Projekt-Metamodell) zu erstellen, können Automatismen in das Werkzeug eingebaut werden, die die Arbeit erleichtern. Dadurch erreicht man eine höhere Akzeptanz bei denjenigen, die das Modell erstellen und pflegen werden. Die Qualität der Modelle steigt dadurch automatisch, die nochmalige Bearbeitung fehlerhafter Modelle nach der Verifikation reduziert sich auf ein Minimum.

Testfälle automatisch generieren

Ein Modell kann die Struktur und Funktionsweise eines Systems beschreiben. Daher ist es naheliegend, dieses Modell nicht nur zur Erzeugung von Dokumenten, Code und anderen Artefakten zu verwenden, sondern auch zur Erstellung von Testfällen. Bei der Erzeugung von Testfällen kommen oft nicht die konkreten Analyse-, Design- und Implementierungsmodelle zum Einsatz, sondern spezielle Testmodelle. *www.sparxsystems.de* ■

Bonjour, IoT-Ecosystem

Sigfox veranstaltete Ende September in Prag erstmals die **'Sigfox World IoT Expo'**. Das **globlale Funknetzwerk** kann **Objekte** mit **geringem Energiebedarf** drahtlos mit dem Internet verbinden. Wir sprachen mit Aurelius Wosylus, Director Sales bei Sigfox über die zweitägige Expo, LPWAN und die Beudeutung der Sigfox-Partner.

SIGFOX GERMANY GMBH

IoT: Herr Wosylus, die ‚Sigfox World IoT Expo' findet zum ersten Mal statt. Warum so ein Event?
Wosylus: Mit unserem Sigfox Operator in Prag ist die Idee gereift, ein Event abseits der etablierten Messen zu veranstalten – auch um unsere Partner mit ins Boot zu holen.

IoT: Die Messe steht unter dem Motto ‚touch the real IoT', was bedeutet das für Sigfox?
Wosylus: Jeder versucht seine Firma im IoT-Umfeld zu platzieren, es gibt also viele Anwendungen. Wenn ich von 'real IoT' spreche, meine ich vor allem die kleinen vernetzten Applikationen, die Kaffeemaschine, die Wasserflasche, die Feuermelder, die früher nicht vernetzt waren. Die Sigfox-Technologie richtet sich also an lowest-power-Applikationen, die heute erst möglich werden. 80 bis 90 Prozent der IoT-Services brauchen schließlich nur vergleichsweise wenige kleine Datensätze von ihren IoT-Geräten.

„Wir waren schon immer überzeugt, dass IoT weder durch die Cloud-Software noch durch die Device-Hardware entschieden wird – sondern wesentlich dadurch, wie einfach die Anbindung, also der Kommunikationsweg, sein wird. Sigfox ist derzeit ein alternativloses globales Netzwerk, das sowohl günstig bei der Hardware als auch für das Netzwerk ist. Ganz entscheidend ist aber auch der Stromverbrauch: Ein Sigfox Device wie home2net es anbietet wird bereits heute aus einer kleinen Batterie bis zehn Jahre versorgt. Die zwei Tage in Prag haben zahllose Lösungen und Anwendungen basierend auf Sigfox gezeigt, was definitiv den Vorsprung von Sigfox untermauert und dokumentiert."

Hans Mühlbauer, CEO, home2net

IoT: Warum eignen sich LPWAN so gut für das IoT?
Wosylus: LPWAN wie Sigfox übertragen Daten kostengünstig und sind hochverfügbar. Außerdem ist eine durchgängige Datenübertragung gewährleistet. Ein weiterer Vorteil sind Monitoring-Einsichten in Echtzeit.

IoT: Mit welchen Herausforderungen haben Entwickler von IoT Devices zu kämpfen?
Wosylus: Ich sehe die Herausforderungen besonders bei der richtigen Kombination von Technologien, diese auf einem Device zusammenzubringen und das Produkt schließlich auf dem Markt zu platzieren. Wir sind zwar Spezialisten im Funkbereich, aber helfen auch, wenn eine Firma eine Applikation entwickeln möchte und selber keine Designkapazitäten hat. Wir helfen dabei die richtigen Partner zu finden, so dass unter dem Strich auch das Richtige raus kommt, womit der Kunde zufrieden ist.

IoT: Die Expo ist ein Networking-Event für ihre Partnernetzwerk, welche Bedeutung haben diese Partnerschaften?
Wosylus: Mit diesen Partnerschaften bilden wir ein Ecosystem, da wir nicht nur die passende Funktechnologie haben, sondern wir forschen auch nach Lösungen für Konnektivität, Location Services, usw. Aber die einzelnen Applikationen, das heißt die Devices, muss der Kunde selber umsetzen. Die eigentliche Wertschöpfung für denjenigen, der eine Apllikation baut, ist der Device Builder. Derjenige, der die Hardware baut, der das Gehäuse macht, der die Batterien einfügt. Mit denen arbeiten wir sehr eng zusammen, das heißt ohne Halbleiterhersteller, ohne Device Builder, ohne unsere Partner auf der Cloudseite, wäre die Wertschöpfungskette nicht durchgängig. Das macht das Ecosystem so extrem wichtig für uns.

IoT: Wie sieht Ihr Fazit der Veranstaltung aus?
Wosylus: Ich sehe das als extrem erfolgreiches Event an. Wir haben viele Partner und Kunden zusammengebracht, gerade im deutschen Umfeld waren wir sehr aktiv und haben auch sehr kreative Gespräche mit Partnern und Kunden geführt. Von allen haben wir ein sehr positives Feedback erhalten.

www.sigfox.com ■

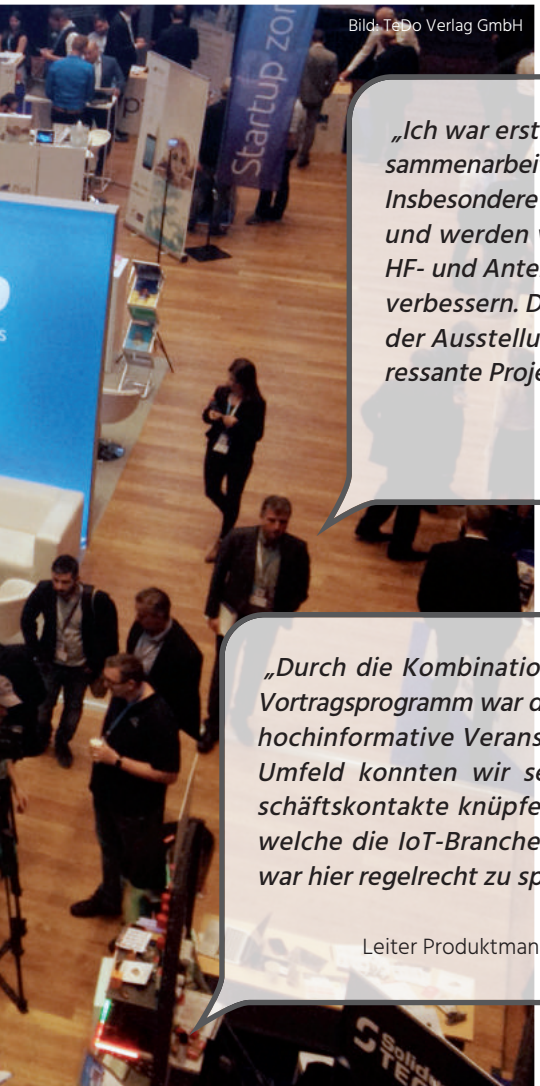


Bild: TeDo Verlag GmbH

„Ich war erstaunt, wie viel Potential für eine Zusammenarbeit auf dem IoT-Markt gerade entsteht. Insbesondere wir als Antennenspezialisten können und werden vielen IoT-Unternehmen helfen, die HF- und Antennen-Performance ihrer Produkte zu verbessern. Diesen Bedarf haben wir deutlich auf der Ausstellung erkannt und freuen uns auf interessante Projekte und neue Herausforderungen."

Dr.-Ing. Sergey Sevskiy,
Geschäftsführer, Sevskiy GmbH

„Durch die Kombination von Messe und Vortragsprogramm war die Sigfox Expo eine hochinformative Veranstaltung. In diesem Umfeld konnten wir sehr gut neue Geschäftskontakte knüpfen. Die Motivation, welche die IoT-Branche derzeit beflügelt, war hier regelrecht zu spüren."

Marko Herold,
Leiter Produktmanagement, IK Elektronik

SIGFOX NEWS

GCT Semiconductor kooperiert mit Sigfox

Der hochintegrierte Single-Chip GDM7243I von GCT Semiconductor wird die LTE-Kategorie M1/ NB1 /EC-GSM neben Sigfox Wireless IoT-Konnektivität auch unterstützen und ist damit eine Hybridlösung, die Konnektivitätsoptionen für IoT-Anwendungen ohne zusätzliche Stückkosten bietet.

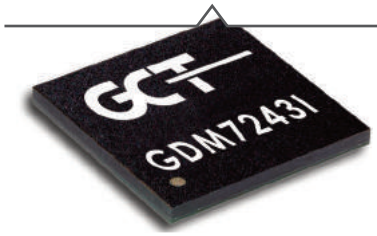


Bild: Sigfox Germany GmbH

Partnerschaft mit Alps Electric Europe

Das Ziel ist bei allgemeinen Kundenprojekten besonders eng zusammenzuarbeiten. Darüber hinaus bevorzugt Alps Electric Europe Sigfox als ihre wichtigste LPWAN-Konnektivitätstechnologie für zukünftige Produktentwicklungen.

Erweiterungsmodul für das Cross Domain Development Kit

Das von Bosch Connected Devices and Solutions und Sigfox entworfene Erweiterungsmodul ermöglicht es IoT-Kunden, besonders schnell Prototypen von neuen sensorbasierten IoT-Geräten und Anwendungen zu entwickeln. Das Sigfox-Erweiterungsmodul wird ab Anfang 2018 im Handel erhältlich sein.

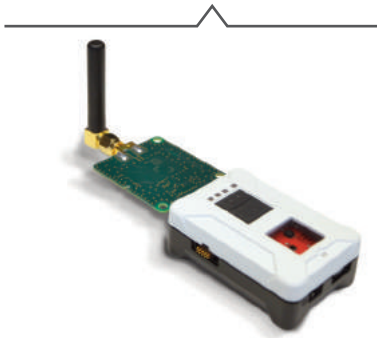


Bild: Sigfox Germany GmbH

Halle 2
Stand 300

CANopen FD in der Cloud

Die **neue CANopen-FD-Spezifikation CiA 1301** ist seit September 2017 verfügbar. Ein Vorzug zum klassischen CAN: es können jetzt **bis zu 64-Datenbyte in einem PDO** übertragen werden. Das neue USDO erlaubt IoT-Gateways dynamisch jeden Datenpunkt zu erreichen.

REINER ZITZMANN, CAN in Automation (CiA) GmbH

Vergleich eines CAN Datentelegramms im klassischen und FD Format

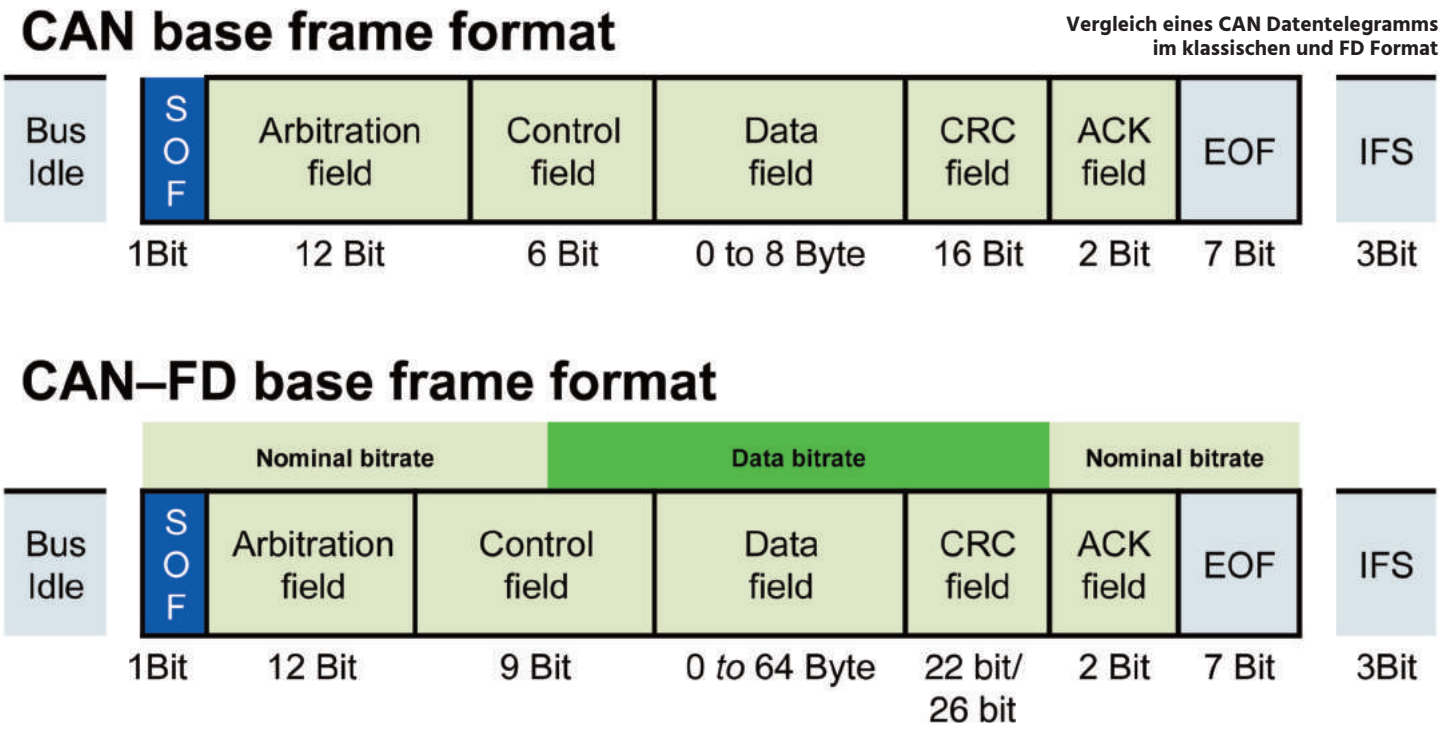


Bild: CAN in Automation (CiA) GmbH

Die von der CiA Arbeitsgruppe 'SIG application layer' vorgenommene Anpassung von CANopen auf CAN FD erfolgte unter der Prämisse, möglichst viel bewährte CANopen-Funktionalität konstant zu halten. Insofern stand am Anfang die Analyse, welcher CANopen-Dienst überhaupt von einer Anpassung auf CAN FD profitieren würden. Dabei kristalisierte sich heraus, dass ausschließlich die Datentransport-orientierten CANopen Dienste SDO und PDO durch das klassische CAN Datentelegramm, in ihrer Effizienz limitiert werden. Somit konnten alle anderen Dienste unverändert übernommen werden; mit Ausnahme des 'EMCY write'-Dienstes. Die SIG application layer hat die Gelegenheit der Überarbeitung von CANopen genutzt, um einen verbesserten Satz an Diagnosedaten, im Rahmen eines erweiterten 'EMCY write'-Dienstes bereitzustellen. Im klassischen CANopen wird ein PDO durch zwei Parametersätze beschrieben; die Kommunikationsparameter und die 'Mapping-Parameter'. Die Kommunikationsparameter beschreiben, welcher CAN-Identifier für das PDO genutzt wird und wann die Steuerdaten zuverlässig kommuniziert werden. Diese Parameter sind unabhängig vom Format des genutzten CAN Telegramms und bedürfen keiner Anpassung. Ähnlich verhält es sich bei den sogenannten 'Mapping-Parametern'. Die 'Mapping-Parameter' beschreiben, als Referenz auf das lokale Objektverzeichnis, welche Daten übertragen werden. Im klassischen CANopen erlauben 64 Einträge das referenzieren von bis zu 64 Informationen aus dem lokalen Objektverzeichnis. Das klassische CAN-Telegramm beschränkt die Datenbreite der insgesamt referenzierten Informationen auf 8Byte. Diese Grenze wird mit CANopen FD auf 64Byte angehoben. Somit ist außer der Anpassung der Summe, der maximal übertragbaren Datenbyte, keine weitere Änderung erforderlich. Die bestehenden, maximal 64 Mappingeinträge sind für den Einsatz von CAN FD ausreichend und können unverändert weiter genutzt werden. Dies gilt vor allem unter der Berücksichtigung, das CANopen FD nur noch Informationen im Objektverzeichnis verwaltet, die auf ein ganzzahliges Vielfaches von einem Byte abgebildet werden.

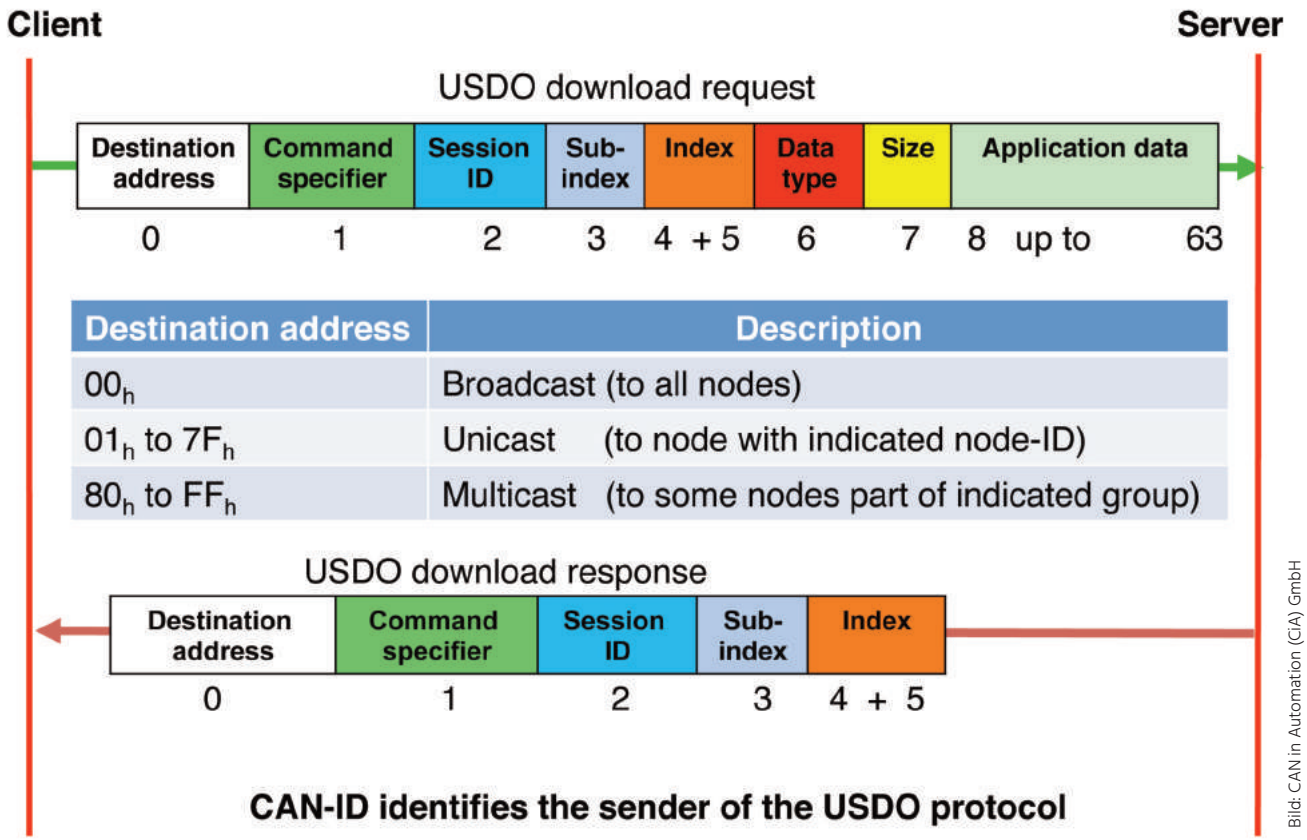


Bild: CAN in Automation (CiA) GmbH

Generelle Struktur des USDO Protokolls

Warum das neue Protokoll

Im Gegensatz zum PDO war es deutlich komplexer, das für Diagnose und Konfiguration genutzte SDO, auf den Einsatz in CAN FD-basierenden Systemen, vorzubereiten. Eine einfache Erweiterung des SDO Protokolls war nicht möglich. An Stelle einer schlecht handhabbaren, umständlichen Erweiterung des ohnehin schon komplexen SDO-Protokolls bevorzugte die SIG application layer einen neuen Dienst einzuführen. Dieser Dienst soll den Anforderungen zukünftiger, in Cloud-Anwendungen integrierter, eingebetteter Netzwerke, Rechnung tragen. Das Ergebnis war das Universal Service Data Object (USDO). Im Gegensatz zum klassischen SDO, ermöglicht das USDO, den dynamischen Aufbau von Kommunikationsquerverbindungen, zur Systemlaufzeit, bei gleichzeitiger Abwesenheit jeglicher Manager-/ Masterfunktionalität. Das USDO erlaubt die Kommunikation in unicast und broadcast und kann dabei jede Datengröße transferieren. Das ermöglicht z. B. einem Telematikmodul, jeden gewünschten Datenpunkt im 'embedded-Netzwerk' zu erreichen, auch wenn ein Systemintegrator bei initialem Systemstart, keine Kommunikationsverbindung zwischen Gateway und Datenquelle eingerichtet hatte. Darüber hinaus ist das USDO inhärent Routing-fähig. Durch das Codieren von Quell- und Zieladresse, kann mittels USDO, in einer auf CANopen FD-Netzwerken basierenden Anwendung, über Netzwerkgrenzen hinweg kommuniziert werden.

Einfacher in die Cloud

Das CANopen FD PDO, macht den durch CAN FD angebotenen, erhöhten Datendurchsatz, nutzbar. Cloud-basierten Anwendungen kann somit eine größere Datenbasis generiert werden. Das 64-Byte Datenfeld der PDOs, erleichtert das erfüllen von Security-Anforderungen in CAN-basierten Anwendungen erheblich. Das USDO profitiert nicht nur vom CAN FD Datendurchsatz. Die Ausgestaltung des USDOs und der damit einhergehende Funktionsumfang erlauben es, dynamisch Kommunikationsbeziehungen zwischen beliebigen Netzwerkteilnehmern aufzubauen. Somit stellt CANopen FD ein geeignetes Stilmittel für Aufgaben der Fernwartung und –steuerung bereit. Abgeleitet vom Prinzip der Betriebsmittelkennzeichnung hat die CiA Arbeitsgruppe SIG CANopenIoT für CANopen, das Prinzip der Referenzdesignatoren eingeführt. Diese erlauben es in heterogenen Steuerungsarchitekturen, Geräte und -parameter systemweit eindeutig zu kennzeichnen. Diese anwendungsspezifische Kennzeichnung kann wiederum als Adresse für eine logische Adressierung dienen. Im Dokument CiA 309-5, wird diese logische Adressierung für den Zugriff auf CANopen-Netzwerke definiert. Ein weiterer Schritt für CANopen FD wird darin bestehen, das Prinzip der logischen Adressierung im USDO-Protokoll abzubilden. Das Entbinden des Anwenders von tiefer Kenntnis der im 'eingebetteten Netzwerk' verwendeten Technologie, wird die Integration von CANopen FD in 'Cloud-basierte' Anwendungen weiter vereinfachen.

Zusammenfassung

Eine wesentliche Erweiterung gegenüber dem klassischen CANopen ist das USDO Protokoll. Als Multifunktionswerkzeug zukünftiger CANopen FD-Netzwerke unterstützt es unter anderem eine dynamisch aufgebaute Kommunikation in unicast und broadcast; in lokalen oder über Router angebundenen 'Remote-Netzen'. Der Zugriff auf mehrere Sub-indices mittels eines einzigen USDO Lese- oder Schreibzugriff, befindet sich genauso in der Spezifikationsarbeit wie die Umsetzung der Anforderung nach der logischen Adressierung. 'Cloud-basierende' Anwendungen wie 'Condition monitoring' oder 'Predictive maintenance' werden von dem erhöhten Prozessdatendurchsatz profitieren. Die verlängerten CAN FD Datentelegramme ermöglichen das Nutzen von einheitlichen 'Safety'- und 'Security'-Lösungen, welche sich ebenfalls aktuell im CiA in der Erarbeitung befinden. *www.can-cia.org* ■

Zu Ihren Diensten

Um die **neue CANopen-FD-Spezifikation** bestmöglich zu nutzen, braucht es das geeignete Werkzeug. Wir stellen auf die Spezifikation angepasste **Stacks und Toolchain** vor.

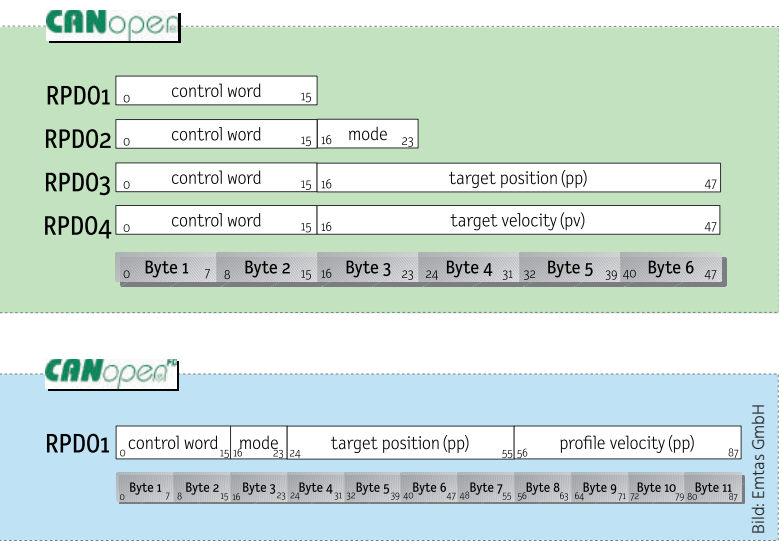
TORSTEN GEDENK, EMTAS GMBH

Um die Vorteile von CAN FD auch außerhalb der Automotive-Welt zu nutzen, wurde das CANopen Kommunikationsprotokoll durch die Mitglieder des CAN in Automation e.V. zu CANopen FD weiterentwickelt und im Dokument CiA 1301 Version 1.0 spezifiziert. Dabei wurden die grundlegenden Prinzipien von CANopen wie das Objektverzeichnis, eine Parameterliste für alle Prozess- und Konfigurationswerte mit jeweils einem 16-bit Index und einem 8-bit Subindex zur Adressierung, beibehalten. Weiterhin gibt es definierte Dienste zur Übertragung von Prozessdaten, Konfigurationsdaten, Alarmnotifikationen sowie zum Netzwerkmanagement. Die maximale Länge der Prozessdatenobjekte (PDO) wurde in CANopen FD auf 64Byte erhöht, so dass nun längere CAN FD-Telegramme mit mehreren Mess- oder Sollwerten zusammen in einem Telegramm gesendet werden können. Neben der Erhöhung des Datendurchsatzes erleichtert dies die Synchronisation zusammengehöriger Daten – beispielsweise in Mehrachs-Controllern. Der bisherige SDO-Dienst zum wahlfreien Zugriff auf alle Parameter und Messwerte im Objektverzeichnis wurde durch den neuen Universal Service Data Object (USDO) Dienst ersetzt. Die USDO-Nachrichten nutzen selbstverständlich auch die volle Länge der CAN-Telegramme. Des Weiteren wurden Mechanismen für Broadcast und zum Routing über mehrere CANopen FD-Netzwerke direkt in das Protokoll integriert. Zudem wurde die Länge der Emergency-Nachrichten erweitert. Darüber hinaus sind die bestehenden CANopen-Dienste auch bei CANopen-FD weiterhin im Einsatz.

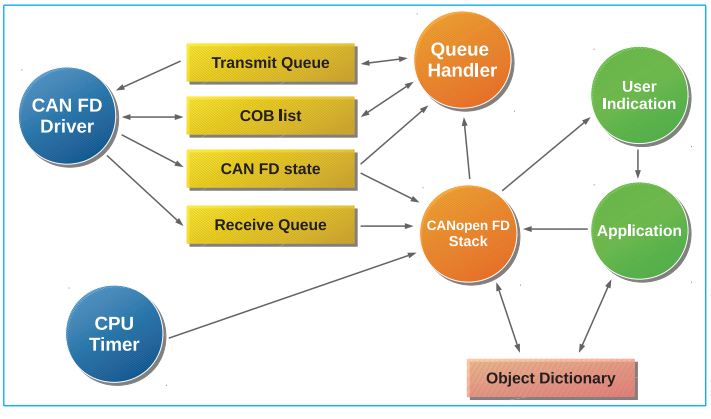
Bestandteile des Stacks

Emtas bietet seit längerem einen CANopen-Stack in verschiedenen Ausbaustufen von Slave, über Master bis hin zur Implementierung eines CANopen-Managers an. Dieser in der Industrie nachgefragte Stack wurde nun entsprechend der aktuellen CANopen FD Spezifikation erweitert und unterstützt je nach Ausbaustufe alle Features von CANopen FD. Der Stack besteht aus einem generischen Teil und einem Hardware-spezifischen Teil zur Anbindung an den jeweiligen Microcontroller bzw. CAN-Controller. Dadurch ist eine einfache Portierung auf weitere CAN FD-fähige Controller zukünftig

PDO mapping für CiA402-Geräte



PDO mapping mit CANopen und CANopen FD



Datenfluss-Modell des CANopen FD Protokoll Stack

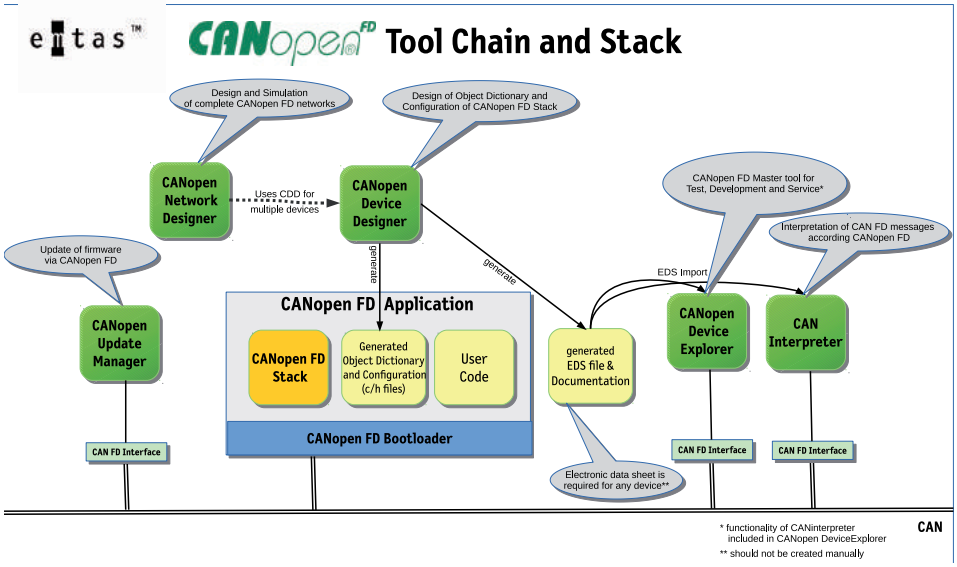


Bild: Emtas GmbH

Die Tool Chain: Konfiguration, Diagnose und Simulation

möglich. Aktuell werden die folgenden Microcontroller unterstützt: STM32H7 von STMicroelectronics, NXP LPC546xx, Microchips Atmel SAMC21 sowie deren Standalone CAN FD Controller MCP2517FD und diverse CAN-USB-Adapter mehrerer Hersteller unter Linux, Windows und Mac OS X. Einer der ersten Einsatzfälle von CANopen FD wird das Firmware-Update für eine End-of-Line-Programierung bei der Fertigung oder direkt im Feld sein. Insbesondere bei diesen größeren Datenmengen kann CANopen FD seine Vorteile ausspielen. Unter Verwendung des USDO-Broadcasts können mehrere Geräte bei der Fertigung parallel geflasht werden. Der CANopen FD Bootloader von Emtas zeichnet sich durch geringen Speicherbedarf aus und besteht aus einer für den Einsatzzweck ausgelegten Version des CANopen FD Stacks. Dabei werden ein Applikationsblock sowie optional mehrere Datenblöcke unterstützt, so dass beispielsweise die Applikation und ein Kalibrationsdatensatz separat aktualisiert werden kann. Möglichkeiten zur Verifikation der Firmware oder zur Integration kundenspezifischer Security-Mechanismen stehen im CANopen FD Bootloader zur Verfügung. Das Firmware-Update kann mit jedem CANopen FD Master oder mit speziellen PC-Tools durchgeführt werden.

Vollständige Toolchain

Emtas bietet einen CANopen FD Master-und-Slave-Stack sowie eine vollständige Toolchain für CANopen FD an. Der CANinterpreter ist ein CAN FD-Analyzer mit CANopen FD-Interpretation, jedoch findet sich die gesamte Funktionalität dieses Tools auch im CANopen FD DeviceExplorer wieder. Der CANopen FD DeviceExplorer ist ein CANopen FD-Master-Tool, das bei der Geräteentwicklung und späteren Diagnose wichtige Dienste leistet. Mit der Möglichkeit der Erstellung eigener Erweiterungen auf Basis von Javascript bietet das Tool vielfältige Einsatzmöglichkeiten. So können zum Beispiel eigene Test- und Serviceapplikationen damit erstellt werden und sich wiederholende Tests automatisiert werden. Für den Entwurf des Objektverzeichnisses ist der CANopen DeviceDesigner im Lieferumfang des CANopen FD Stacks enthalten. Auf der Basis von bestehenden Gerätebeschreibungsdateien oder mitgelieferten Geräteprofilen kann das eigene Objektverzeichnis mit wenigen Klicks erstellt werden. Als Gegenstelle zum Bootloader bietet Emtas mit dem CANopen UpdateManager ein Tool für einfache Firmware-Updates einzelner Geräte oder kompletter Netzwerke. Die Produktpalette rundet der CANopen NetworkDesigner ab, welcher den Entwurf kompletter CANopen FD-Netzwerke erlaubt. Alle Tools des Anbieters sind für Windows, Linux und Mac OS verfügbar und unterstützen aktuell CAN-FD Interfaces von Kvaser und Peak.

www.emtas.de ■

IoT NEWS

Deutsche Bahn startet selbstfahrende Buslinie

Die Deutsche Bahn hat im niederbayerischen Bad Birnbach ein Pilotprojekt mit selbstfahrenden Kleinbussen gestartet. „Gerade sind wir komplett automatisiert in ein neues Verkehrszeitalter gefahren“, sagte Bahnchef Richard Lutz nach der Premierenfahrt Ende Oktober. Damit sei die Bahn das erste Unternehmen in Deutschland, das autonome Fahrzeuge auf die Straße und in den öffentlichen Nahverkehr bringe. „Unser Ziel ist, so Straße und Schiene noch stärker zu vernetzen und damit auch auf dem Land individuelle Mobilität ohne eigenes Auto zu ermöglichen“, sagte Lutz. Das Fahrzeug rollt auf der rund 700m langen Strecke vom Ortszentrum zur Therme über öffentliche Straßen.

Bild: Deutsche Bahn AG / © Uwe Miethe

AMD übertrifft Erwartungen

Der Chiphersteller hat seine Quartalszahlen vorgelegt. Das Unternehmen steigert den Umsatz auf 26 % auf 1,64 Mrd. US$. Für das 4. Quartal rechnet AMD mit einem Umsatzrückgang um zwölf bis 18 % auf 1,34 bis 1,44 Mrd. US$.

ARM-Distributor des Jahres

Hitex ist vom Chipdesigner ARM zum wiederholten Mal als Distributor ausgezeichnet worden. Mit dem Award als 'Most Forward Thinking Distributor in EMEA' würdigt ARM das Unternehmen für das Engagement bei der Erschließung neuer Safety-Märkte für ARM-Produkte.

Bild: Hitex GmbH

Geschäftsführer Jörg Stender (links) und Account Manager Raphael Weiland (rechts) nahmen den Award für Hitex beim ARM Regional Distributor Meeting entgegen.

Bild: Fischer Elektronik GmbH & Co. KG

Wärme ableiten

Die Miniaturisierung von Embedded-Systemen erfordert den Einsatz von Prozessoren mit einer immer höher werdenden Leistungsdichte. **Leistung** bedeutet auch **Abwärme**, umso wichtiger ist die **Auswahl und Anwendung des richtigen Gehäuses um Wärme abzuleiten**.

B.ENG. FATIH SAHIN, FISCHER ELEKTRONIK GMBH & CO. KG

Das Motto der heutigen Systeme ist klar: Maximale Rechenleistung auf engstem Raum durch `downscaling`. Doch die immer leistungsfähigeren Prozessoren wandeln die gesamte elektrische Energie in Wärme um. Fischer Elektronik bietet spezielle Wärmeableitgehäuse aus Aluminiumstrangpressprofilen an. Hauptbestandteil des Gehäuseprofiles ist Aluminium. Da Aluminium allein aber ein weiches Material ist wird beim Strangpressen eine geeignete Knetlegierung eingesetzt. Die europaweit genormte Legierung 'EN AW 6060' hat die Besonderheit bei vergleichsweise geringer Dichte von 2,7g/cm^3 eine dennoch hohe Zugfestigkeit von ~195N/mm^2 und einen für das thermische Management interessanten Wärmeleitwert von ~200W/(mK) aufzuweisen. Des Weiteren lässt sich dieser Werkstoff mechanisch sehr gut bearbeiten und dekorativ gestalten. Profile haben den großen Vorteil, dass nahezu jede beliebige Gehäusekontur erzeugt werden kann.

Gehäusedimensionierung

Wichtig ist dass zur Beginn an eine passende Gehäusegröße ausgesucht wird. Dabei sollten neben der Hauptplatine auch weitere Komponente und mögliche Erweiterungen eingeplant werden. Die Breite und Höhe eines Gehäuses aus einem Strangpressprofil werden von Profilgeometrie festgelegt. Dagegen lässt sich die Tiefe nach Wunsch auslegen.

Thermisches Management

Leistungsstarke Embedded Systeme oder auch Industrie-PCs erfordern ein perfekt ausgelegtes Konzept für das Wärmemanagement. Bereits bei einer Erhöhung der Bauteiltemperatur um 10Kelvin halbiert sich die Le-

bensdauer der Elektronik. Damit es nicht zu Systemausfällen kommt sollte frühzeitig Gedanken über die Entwärmung gemacht werden.

Wärmewiderstand

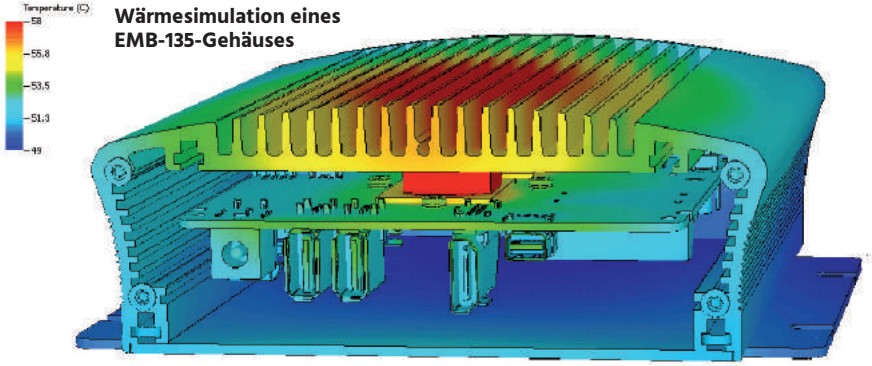
Bei der Auswahl des passenden Wärmeableitgehäuses spielt neben dem Volumen auch der absolute Wärmewiderstand eine wichtige Rolle. Dieser wird in Kelvin/Watt (K/W) angegeben und gibt Information darüber wie viele Kelvin Temperaturdifferenz nötig sind um 1Watt Leistung abzuführen. Kurz gesagt ein Wert der aussagt wie gut die Wärme abgeleitet wird. Umso kleiner der Wärmewiederstand ist desto besser ist der Kühlkörper. Ob das Gehäuse bzw. der Kühlkörper die Anforderungen erfüllt ist erst nach der Bestimmung des erforderlichen Wärmewiederstandes ersichtlich.

Computergestützte Wärmesimulation

Bei komplexen Systemen kommen computergestützte thermische Simulationen zum Einsatz. Eine Wärmesimulation kann bereits in der frühen Entwicklungsphase eingesetzt werden um bereits frühzeitig Erkenntnisse über möglichen Problemzonen zu bekommen. Unter realitätsnahen Bedingungen werden mittels 3D-Daten Baugruppen evaluiert. Hot- Spots und thermisch kritische Bereiche lassen sich so visuell erkennen und einfacher optimieren. Nachträgliche kostenintensive Korrekturmaßnahmen bleiben erspart.

Natürliche oder forcierte Kühlung

Der zukünftige Einsatzort der Elektronik und die abzuführende Leistung sind die Hauptparameter für die Auswahl des Entwärmungskonzeptes. Bei Industrie-PCs die z.B. in rauer Umgebung arbeiten sind geschlossene Gehäuse prädestiniert. Dies hat den Grund, dass Staub oder Wasser ins Gehäuse gelangen und zu Systemausfällen führen können. Geschlossene Systeme verfügen über feste Kühlkörper die für die Entwärmung der Elektronik zuständig sind. In so einem Fall spricht man von einer natürlichen Kühlung bzw. einer passiven Kühlung. Die Vorteile liegen auf



Wärmesimulation eines EMB-135-Gehäuses

Bild: Fischer Elektronik GmbH & Co. KG

IoT NEWS

KI bedroht Überleben der Menschheit

41% der Deutschen befürchten, dass Künstliche Intelligenz tatsächlich das Überleben der Menschheit gefährdet. Das geht aus einer Studie der digitalen Kommunikationsagentur Syzygy hervor. Dabei nutzen trotzdem 38% der Befragten Anwendungen wie Siri und Co. In der Studie wurden jeweils 2.000 Menschen in Deutschland, Großbritannien und den USA zu ihren Einstellungen rund um das Thema KI befragt.

Amazon forscht mit Max-Planck-Gesellschaft an KI

Amazon will sich künftig an der Forschungskooperation beteiligen, die auf Initiative der Max-Planck-Gesellschaft im Dezember 2016 gestartet ist und auf dem Feld der Künstlichen Intelligenz eine der größten Europas ist. Über die Beteiligung am Cyber Valley hinaus wird Amazon in der Nachbarschaft zum Max-Planck-Institut für Intelligente Systeme in Tübingen ein eigenes Forschungszentrum einrichten.

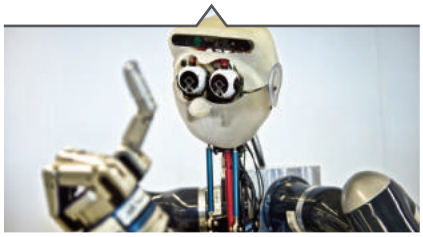


Bild: Max-Planck-Institut/ © Wolfram Scheible

Im Cyber Valley treiben Partner aus Wissenschaft und Wirtschaft die Forschung zur Künstliche Intelligenz voran. Nun will sich Amazon dem Forschungsverbund anschließen.

AR vereinfacht Paketversand bei DHL

Mit Hilfe der DHL Packset App soll es ab sofort für DHL-Kunden einfacher werden, Pakete zu versenden. DHL unterstützt damit die AR-Technologie von Apples iOS 11. Die App scannt eine Oberfläche und fügt automatisch ein virtuelles Packset ein. Nun kann der Kunde den zu versendenden Gegenstand darin platzieren, das passende Packset aus fünf Größen wählen und bei Bedarf eine Versandmarke hinzubuchen.

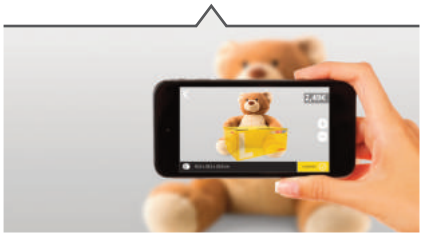


Bild: Deutsche Post DHL Group

der Hand, das System ist wartungsarm und langlebig. Ist die passive Kühlung nicht ausreichend muss auf eine forcierte Kühlung, auch bekannt als aktive Kühlung, ausgewichen werden. Bei der forcierten Kühlung kommen meist Lüfter zum Einsatz. Sie haben die Aufgabe das Gehäuse mit frischer Luft zu versorgen und einen Luftstrom um den internen Kühlkörper zu erzeugen. Durch den Luftstrom vervielfacht sich die Kühlleistung des Kühlkörpers. Größere Mengen Wärme lassen sich so abtransportieren. Ein großer Nachteil der Lüfter ist, dass diese sich bei staubiger Umgebung zusetzen können. Eine Drehzahl- und Temperaturüberwachung der Elektronik ist Pflicht. Außerdem müssen Gehäuse über Lüftungsöffnungen aufweisen die nur eine niedrige Gehäuseschutzklasse erlauben.

Wärmeleitmaterialien

Der Einsatz von Wärmeleitmaterialien ist unumgänglich. Jede Oberfläche weist eine Unregelmäßigkeit auf. Wenn zwei Flächen aufeinander treffen besteht der Kontakt lediglich an 3 Punkten. In dem entstandenen Zwischenraum wirkt Luft isolierend. Die Aufgabe des Wärmeleitmaterials besteht darin diese Differenz zu füllen bzw. auszugleichen. Strangpressprofile weisen natürliche Durchbiegungen auf. Bei großflächiger Kontaktierung der Kühlfläche ist eine Planfräsung vom Vorteil. Die Auswahl an Wärmeleitmaterialien ist groß und erfordert Sorgfalt bei der Auswahl. Das Sprichwort ‘So viel wie nötig, so wenig wie möglich’ gilt auch in diesem Fall.

EMV-Schutz

Das CE-Kennzeichen ist das europäische Kennzeichen für die Konformität eines Produktes. Nur mit dieser Kennzeichnung darf ein elektrisches Gerät in Europa verkauft werden. Damit ein Gerät die CE-Kennzeichnung tragen darf muss es bestimmte Anforderungen an Sicherheit erfüllen. Darunter fällt auch die Elektromagnetische Verträglichkeit „EMV“ die in der europäischen EMV-Richtlinie 2014/30/EU geregelt wird. Darin geht es um die Fähigkeit von elektrischen Betriebsmitteln, in einer elektromagnetischen Umwelt zufriedenstellen zu arbeiten, ohne dabei selbst Störungen zu verursachen, die für andere Betriebsmittel unannehmbar wären. Hierbei wird zwischen feld- und leitungsgebundenen Störungen unterschieden. Bei einer leitungsgebundener Störung wird die Störgröße, durch die Störquelle, über den elektrischen Leiter zur Störsenke übertragen. Bei feldgebundenen Störungen wird die Störgröße über elektromagnetische Felder übertragen und durch leitende Teile die als Antenne fungieren aufgenommen. Generell werden Aluminiumgehäusen eloxiert. Die Eloxalschicht ist jedoch ein schlechter elektrischer Leiter. Um mit einem Aluminiumgehäuse eine gute Schirmdämpfung zu erreichen müssen alle Gehäuseteile miteinander möglichst großflächig und niederohmig, elektrisch leitend kontaktiert bzw. mit einer gemeinsamen Masse verbunden werden. Durch das Chromatieren von Aluminium wird eine dauerhafte elektrisch leitende Oberfläche auf dem Aluminium erzeugt. Die Oberfläche ist korrosionsbeständig und eignet sich als Haftgrund vor dem lackieren. Spalte die zwischen zwei Gehäuseteilen entstehen sind mit elektrisch leitenden Dichtungen abzudichten.

IP-Schutzklasse

Neben EMV spielt die IP-Schutzklasse bei Gehäusen eine wichtige Rolle. IP bedeutet ‘International Protection’ auch im Englischen als ‘Ingress Protection’ übersetzt. Die europäische Norm DINEN60529 befasst sich mit dem Schutz durch Gehäuse. Darin wir der Schutzgrad eines Gehäuses in Schutzklassen unterteilt und mit einem IP-Code angegeben. Der IP-Code beinhaltet zwei Ziffern, wobei die erste Ziffer für den Berührungs- und Fremdkörperschutz und die zweite Ziffer für den Wasserschutz steht. Zum Abdichten von Gehäusen kommen Flachdichtungen, Dichtungsschnüre, aufgeschäumte Dichtungen oder Dichtmassen zum Einsatz. Die Gehäuseschutzklasse sollte frühzeitig berücksichtig und das Gehäuse entsprechend dem zukünftigen Einsatzort gewählt werden. Nachträgliche Maßnahmen, um die Schutzklasse zu erhöhen, sind oft kostenintensiv und nicht zielführend.

Der Gehäusehersteller

Um bei den ganzen Feinheiten den Überblick nicht zu verlieren ist es ratsam einen Gehäusebauer zeitnah mit ins Boot zu ziehen. Er verfügt über ausreichende Erfahrung und kann mit dem einen oder anderen Tipp nachträgliche Arbeit und Kosten ersparen. Des Weiteren besitzen gut aufgestellte Gehäusehersteller über Simulationssysteme mit denen sich Problemzonen früh erkennen und eliminieren lassen. Auch 3D-Daten von den Gehäusen stehen dem Kunden kostenlos zur Verfügung. Ein Tipp für Sparfüchse: Jeder Gehäusebauer verfügt über fertigungstechnische Stärken. Durch die auf den Gehäusebauer ausgelegte Gehäusebearbeitung lässt sich der eine oder andere Euro sparen.

www.fischerelektronik.de ■

Bild: Fischer Elektronik GmbH & Co. KG

EMV-Materialien mit IP-Dichtungen und Wärmeleitmaterialien

Perfekt ausrichten

Der **Testadapter** für den **Computer-on-Module-Standard Smarc** von Yamaichi Electronics eignet sich auch für die aktuelle Version Smarc 2.0. Der Testadapter realisiert die **geeignete Ausrichtung der Kontakte** und ermöglicht eine **zuverlässige Kontaktierung**. Durch die Verwendung von Federkontaktstiften ist eine hohe Anzahl an Kontaktzyklen erreichbar.

productronica
Halle A1
Stand 217

BERNHARD STOLZ, YAMAICHI ELECTRONICS DEUTSCHLAND GMBH

Bild: Yamaichi Electronics Deutschland GmbH

Smarc ist die Abkürzung für Smart Mobility Architecture, eine von der Standardization Group for Embedded Technologies e.V. (SGET) veröffentlichten Spezifikation für Computer-on-Module (CoMs). Der Vorteil von Smarc gegenüber anderen CoMs liegt im geringen Stromverbrauch, der durch den Einsatz von ARM-Prozessoren oder anderen energiesparenden Prozessoren möglich wird.
Der Smarc-Testadapter von Yamaichi Electronics ist ein impedanzkontrolliertes System, das der SmarcSpezifikation der SGET entspricht. Er ist ein zuverlässiges und langlebiges Kontaktsystem. Da der Adapter zur Prüfung großer Stückzahlen ausgelegt ist, lässt sich der Durchsatz von Prüfmustern steigern. Dies senkt die Kosten pro getestetem Modul. Darüber hinaus ist der Adapter einfach und sicher zu bedienen. Dieser Testdapter der Baureihe YED900 eignet sich für den Einsatz bei:

- Evaluierungstests und
- Zuverlässigkeitstests von -30 bis zu +85°C.

Die Kontaktierung bei diesem Adapter wird mittels Compression Mount Technology (CMT) erreicht, sodass keine Lötarbeiten erforderlich sind. Ausgewählte Werkstoffe wie z. B. luftfahrttaugliches Aluminium, Peek und Peek-Keramik machen den Adapter zu einem robusten Prüfwerkzeug. Der Prüfadapter ist als Plug & Play-fähiges Prüfhilfsmittel einsetzbar.

Zuverlässige Kontaktstift-Technologie

Smarc-Module haben Gold-Pads als Kontaktoberfläche. Die beste Kontakt-Technologie für solche Oberflächenbereiche sind Feinraster-Federkontaktstifte. Die Federkontaktstifte, bekannt aus der Halbleiterprüfung, haben eine sehr lange Lebensdauer. Die Lebensdauer des SMARC-Testadapters ist spezifiziert mit 50.000 mechanischen Zyklen. Zum Kontaktieren der Modul-Pads wird üblicherweise eine konisch geformte ‘Plunger’-Kontaktfederspitze verwendet. Durch diese Kontaktform kann gewährleistet werden, dass am Kontakt-Pad des Moduls nur ein sehr kleiner Abdruck entsteht. Auch Fine-Pitch-Kontaktstifte für Abstände ab 0,3mm sind erhältlich. Ebenfalls Kelvin-Kontaktstifte. *www.yamaichi.de* ■

Kein Löten vonnöten

Leiterplatten und Anschlusskomponenten haben einen hohen Einfluss auf die Leistungs- und Anpassungsfähigkeit elektrischer Geräte. Je **anpassungsfähiger ein Gerät** ist, desto weniger Varianten müssen produziert und vorgehalten werden – und desto **geringer** sind die **Gesamtstückkosten**. Eine **Direktstecktechnik** bringt frischen Wind in die **Leiterplatten-Anschlusstechnik**.

PIA HORSTMANN, Phoenix Contact Deutschland GmbH

Halle 9
Stand 310

Bild: Phoenix Contact Deutschland GmbH

Die Direktstecktechnik SKEDD - schwedisch ‘es ist geschehen’ - ermöglicht direkt steck- und lösbare Leiteranschlüsse an beliebiger Position auf der Leiterplatte. Die SKEDD-Steckverbinder vom Typ SDDC 1,5 und SDC 2,5 von Phoenix Contact benötigen keine Grundleiste mehr - sie können von Hand in verzinnte, durchkontaktierte Bohrlöcher gesteckt werden. Der Vorteil: Bisher mussten die Elektronikhersteller applikationsspezifische Anschlusstechnik wie Leiterplattenklemmen oder Grundleisten in einem irreversiblen Lötprozess mit der Platine verbinden. Damit war die Funktionalität der Leiterplatte und des gesamten Gerätes weitgehend fixiert. Mit der neuen Direktstecktechnik wird dieser Prozess überflüssig; in der Leiterplatten-Fertigung müssen lediglich entsprechende Bohrlöcher vorgesehen werden. So wird die Leiterplatte nicht nochmals thermisch belastet. Aktuell werden viele Leiterplatten im ersten Schritt im SMD-Prozess verarbeitet, und im zweiten Schritt werden Leiterplattenklemmen oder Grundleisten im Wellenlötprozess aufgelötet. Entfällt der zweite Lötprozess, spart der Anwender Prozess- und Bauteilkosten. Außerdem erübrigen sich auch die komplette Logistik sowie die Disposition für die Grundleiste. Im SMD-Lötprozess werden zusätzlich die Rüstkosten und der Feeder-Platz eingespart. Entsprechend spart man beim Verzicht auf die Grundleiste in der SMD-Linie viel Platz für weitere Bauteile. So ist im Idealfall die Fertigung zusätzlicher Baugruppen ohne Umrüstung auf einer Anlage möglich.

Zuverlässige Verbindung

Von dieser Technologie profitieren deshalb sowohl Leiterplatten- als auch Gerätehersteller unmittelbar. Neben der Kostenersparnis können sie nun ein Leiterplatten-Layout für verschiedene Geräteausführungen nutzen - und dennoch flexibel applikationsspezifische Anschlüsse für die Signal-, Daten- oder Leistungsübertragung flexibel umsetzen. Die SKEDD-Kontakte sind eine Weiterentwicklung der Einpresstechnik, sie stellen keine speziellen Anforderungen an die Leiterplatte. Die Kontaktzone besteht aus zwei federnden und leicht nach außen gebogenen Kontaktschenkeln, die sich an die durchkontaktierten Bohrlöcher anpassen. Beim Einstecken des Kontaktes in die Bohrung werden die Kontaktschenkel zusammengedrückt - und sorgen so für eine sichere mechanische und elektrische Verbindung. Seitliche Spreizniete am Steckverbinder erhöhen die mechanische Stabilität zusätzlich. Die Verriegelung ist für Standard-Leiterplatten mit einer Stärke von 1,6 mm ausgelegt, sie erlaubt bis zu 25 Steckzyklen.

Prüfungen nach Bahn- und Hausgerätenorm

Über die geforderten Zulassungs- und Qualifizierungsprüfungen hinaus erfüllen die Direktsteckverbinder erhöhte Anforderungen an die mechanische und elektrische Sicherheit. Die Serien SDDC 1,5 und SDC 2,5 sind beispielsweise nach DIN EN60335-1 (‘Sicherheit elektrischer Geräte für den Hausgebrauch und ähnliche Zwecke’) für spezielle Brandschutzanforderungen qualifiziert. Unter diese Norm fallen Haushaltsgeräte wie Geschirrspüler, Waschmaschinen und tragbare Küchengeräte, Antriebe für Markisen und Jalousien, Heizungen, Klimaanlagen sowie Wärme- und Umwälzpumpen im privaten und gewerblichen Bereich. Zwei Prüfungen weisen die Tauglichkeit der elektrischen Komponenten beziehungsweise des verwendeten Isoliermaterials Polyamid nach. Zunächst wirkt ein Glühdraht mit einer Temperatur von 850°C für 30 Sekunden auf das Material ein. Die Prüfung der Glühdraht-Entflammbarkeitszahl (GWFI - Glow-Wire Flammability Index) gilt als bestanden, wenn die Prüfplatte weniger als 30 Sekunden nach Entfernen des Glühdrahts nachbrennt. Die zweite Prüfung weist die Glühdraht-Entzündungstemperatur (GWIT - Glow-Wire Ignition Temperature) nach. Dazu wird ein Glühdraht mit einer Temperatur von 775°C an die Kunststoff-Prüfplatte gehalten. Das Material darf kurz entflammen, und zwar weniger als 5 Sekunden, sich jedoch nicht entzünden. Die beiden Steckverbinder-Familien sind zudem nach DIN EN61373 (‘Bahnanwendungen – Betriebsmittel von Schienenfahrzeugen – Prüfungen für Schwingungen und Schock’) für Leiterplatten mit chemisch verzinnter und Hot Air Leveling-Oberfläche qualifiziert und freigegeben. Diese Norm stellt hohe Ansprüche an die Schwingungs- und Schocksicherheit der in Zügen eingesetzten Geräte und Komponenten. Die Steckverbinder wurden dazu unter anderem 15 Stunden - je fünf Stunden pro Raumachse - rauschförmigen Schwingungen mit einer Frequenz von 1 bis 150Hz und einer effektiven Beschleunigung von bis zu 5,72m/s^2 ausgesetzt. Die Kontaktunterbrechung darf dabei 1µs nicht überschreiten.

Vielfältige Lösungen

Die normkonformen Prüfungen belegen, wie zuverlässig die Direktstecktechnik auch unter anspruchsvollen Umgebungsbedingungen sowie bei erhöhten Sicherheitsanforderungen funktioniert. SKEDD-Direktsteckverbinder eignen sich damit sowohl für klassische Industrieanwendungen als auch für Applikationen der Gebäudeautomation und Bahntechnik. Mit den Produktserien SDDC 1,5 und SDC 2,5 bietet Phoenix Contact Lösungen für zahlreiche Applikationen wie Klimasteuerungen in Schienenfahrzeugen, Rauch- und Feuermelder oder Haushaltsgroßgeräte. Beide Serien verfügen über den werkzeuglosen Push-in-Federanschluss: Damit lassen sich starre Leiter sowie flexible Leiter mit Aderendhülse ohne Öffnen des Klemmraums anschließen. Die integrierten Prüfabgriffe ermöglichen eine komfortable Funktionskontrolle unter Last. Ausgelegt für Leiterquerschnitte bis 2,5mm^2 eignen sich die einreihigen Direktsteckverbinder SDC 2,5 für Ströme bis 320V. Die doppelreihigen Steckverbinder vom Typ SDDC 1,5 bieten speziell für die oft hohen Signaldichten der Mess-, Steuer- und Regeltechnik eine effiziente Anschlusslösung.

Fazit

Werkzeuglos, zuverlässig, prozesseffizient - die Kombination aus Push-in-Federanschluss und SKEDD-Direktstecktechnik bietet flexible Geräteverdrahtung. Die Steckverbinder benötigen keine Grundleiste und können direkt von Hand in verzinnte, durchkontaktierte Bohrlöcher gesteckt werden. So können Leiterplatten- und Gerätehersteller mit wenigen Leiterplatten-Layouts zahlreiche Geräteausführungen mit applikationsspezifischen Anschlüssen für Signale, Daten und Leistung realisieren.

www.phoenixcontact.de ■

IoT NEWS

Deutsche Auto-Branche meidet Start-ups

Mehr als jeder zweite Automobilhersteller bzw. -zulieferer (56 Prozent) macht einen Bogen um Start-ups und arbeitet nicht mit ihnen zusammen. Nur drei von zehn Unternehmen (29 Prozent) entwickeln mit Start-ups neue Produkte/ Dienstleistungen, 15 Prozent unterstützen Start-ups, etwa durch Förderprogramme. Nur sieben Prozent beziehen Produkte oder Dienstleistungen von Start-ups. Das ist das Ergebnis einer repräsentativen Umfrage im Auftrag von Bitkom unter Vorstandsmitgliedern und Geschäftsführern von Unternehmen der Automobilindustrie mit 20 oder mehr Mitarbeitern. „Wer bei der Digitalisierung auf der Überholspur sein will, der muss mit innovativen, technologiegetriebenen Start-ups zusammenarbeiten“, sagt Bitkom-Präsident Achim Berg.

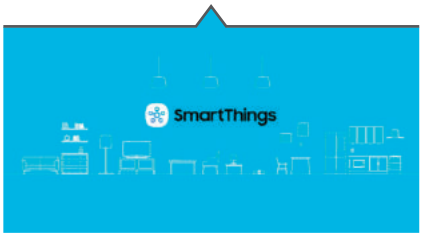
Bild: Bitkom e.V.

Achim Berg, Bitkom-Präsident

Samsung vereint IoT Services

Unter dem Namen ‘Smartthings Cloud’ will Samsung zukünftig all seine IoT-Produkte bündeln. Das Unternehmen betreibt derzeit mit Samsung Connect, Artik, Smartthings und Harman Ignite vier verschiedene IoT-Plattformen. Im Rahmen der hauseigenen Entwicklerkonferenz hat der Konzern angekündigt, diese zukünftig unter dem Namen Smartthings Cloud zusammenzuführen. Die Smartthings Cloud soll als zentraler Knotenpunkt für die Steuerung und Verknüpfung der damit kompatiblen Geräte dienen. Für Entwickler soll das den Vorteil haben, dass sie über eine einzige API alle bislang getrennten Plattformen ansprechen können. Laut den Machern der Artik-Plattform soll die Änderung keinen Einfluss auf bestehende Funktionen haben.

Bild: Samsung Electronics GmbH



Die Smartthings Cloud vereint die vier IoT-Plattformen.

Inserentenverzeichnis

Impressum

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

LIEFERANSCHRIFT
TeDo Verlag GmbH
Zu den Sandbeeten 2
35043 Marburg

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

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

WEITERE MITARBEITER
Inka Bach, Tamara Gerlach, Anja Giesen, Frauke Itzerott, Pascal Jenke, Victoria Kraft, Katharina Kuhl, Kristine Meier, Melanie Novak, Kristina Sirjanow, Marco Steber, Florian Streitenberger, Natalie Weigel

ANZEIGEN
Markus Lehnert, Tel. +49 6421 3086-0
Es gilt die Preisliste der Mediadaten 2017

GRAFIK & SATZ
Anja Beyer, Tobias Götze, Fabienne Hessler, Melissa Hoffmann, Ronja Kaledat, Moritz Klös, Timo Lange, Ann-Christin Lölkes, Nadin Rühl, Verena Vornam, Laura Jasmin Weber

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

ERSCHEINUNGSWEISE
6 Hefte für das Jahr 2017

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

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

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

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

ISSN 1869-8832
Vertriebskennzeichen (ZKZ) 18427

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

Titelbilder: Inasoft GmbH, Fischer Elektronik GmbH & Co. KG, Yamaichi Electronics Deutschland GmbH

Jeder spricht über das IIoT

… wir setzen es einfach um.

sps ipc drives

Nürnberg
28.-30.11.2017
Halle 9, Stand 231

Netzwerke und Computer für eine „smartere“ Industrie.

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

Moxa. Wo Innovation passiert.

www.moxa.com

MOXA®
Reliable Networks ▲ Sincere Service

HMI-PRODUCTS
COMPONENTS & SYSTEMS
ENTWICKLUNG, KONSTRUKTION UND **PRODUKTION** KUNDENSPEZIFISCHER HMI-BEDIENSYSTEME

Kienzle-Gruppe

TOUCH-SENSOREN
... Resistive, Projected-Capacitive, Optical Bonding, EMI-Shilding, Coverglass, Displays, Electronics, ...

FRONTFOLIEN
... mit und ohne Beleuchtung (Nachtdesign), geprägt, PU-Doming, therm. Vakuum-verformung, selektiv strukturiert, vollflächig optisch laminiert, ...

FOLIENTASTATUREN
... in Leitsilber- oder Kupfertechnologie, bestückt mit Metalldomen, Leuchtdioden, Kondensatoren, Widerständen, ...

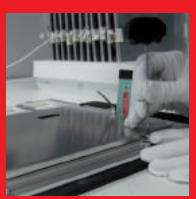
FRONT- UND TRÄGERPLATTEN
... gefräst, gelasert, gestanzt, gestrahlt, eloxiert, pulverbeschichtet, ...

Kienzle-Gruppe
Kienzle Systems
Flach-Eingabe-Systeme

GEHÄUSE
... in Fräs- und Gußtechnologie, eloxiert, lackiert, pulverbeschichtet, ...

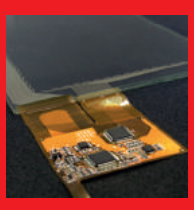
MONTAGE
... kompletter elektromechanischer Baugruppen, Integration von Komponenten, kundenspezifische Prüfungen, ...

Kienzle-Gruppe
Kienzle Components
Keyboard, Touch & Display



Hauptverwaltung: Kienzle-Gruppe
Salinenstraße 26 · D- 74177 Bad Friedrichshall
Telefon 07136/9638-0 · Telefax 07136/9638-38
www.kienzle-gruppe.de · info@kienzle-gruppe.de

Kienzle-Gruppe
Kienzle Mechanics
CNC-Metallbearbeitung



sps ipc drives
28.–30. NOV., HALLE 8, STAND 8-401