SPECIAL ISSUE
Internet-of-Things

EXTENDING THE BATTERY LIFE OF
WEARABLE DEVICES

By Mouser Electronics
THE WORLD’S LARGEST SELECTION OF ELECTRONIC COMPONENTS AVAILABLE FOR IMMEDIATE SHIPMENT!

OPEN ACCOUNTS AVAILABLE FOR QUALIFYING CUSTOMERS

FREE SHIPPING ON ORDERS OVER €65*

LOCAL SALES & TECHNICAL SUPPORT

FIND CONTACT AND ORDERING INFORMATION FOR YOUR REGION AT DIGIKEY.COM/EUROPE

1,000,000+ PRODUCTS IN STOCK | 650+ INDUSTRY-LEADING SUPPLIERS | 3.9 MILLION PARTS ONLINE

*Shipping charge of €18.00 (£12.00) will be billed on all orders of less than €95.00 (£60.00). All orders are shipped via UPS for delivery within 1-3 days (dependent on final destination). No handling fees. All prices are in euro and British pound sterling. If excessive weight or unique circumstances require deviation from this charge, customers will be contacted prior to shipping order. Digi-Key is an authorized distributor for all supplier partners. New product added daily. © 2013 Digi-Key Electronics, 791 Brooks Ave. South, Thief River Falls, MN 56701, USA.
Dear Readers,

There is now doubt - a new emerging Megatrend called the Internet of Things (IoT) is going propelling the entire electronics industry. According to the definition of Wikipedia “The Internet of Things is the network of physical objects or things embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.” The Internet of Things is by another definition “a group of physical objects with embedded sensor technology that communicates an internal state or external environments to a network”.

According to Gartner, there will be nearly 26 billion devices on the Internet of Things by 2020. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of Things (Internet of Everything) by 2020. As per a recent survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing will have widespread and beneficial effects by 2025. It is, as such clear that the IoT will consist of a very large number of devices being connected to the Internet. What also means that IoT will create nearly endless growth opportunities for companies in the electronics, IT, and software industries. The embedded computing nature of many IoT devices means that low-cost computing platforms are likely to be used.

Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist firefighters in search and rescue. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include smart thermostat systems and washer/dryers that utilize Wi-Fi for remote monitoring.

Besides the plethora of new application areas for Internet connected automation to expand into, IoT is also expected to generate large amounts of data from diverse locations that is aggregated very quickly, thereby increasing the need to better index, store and process such data. What also implies that the IoT goes far beyond the traditional embedded technology. The Internet of Things has already evolved due to a convergence of multiple technologies, ranging from wireless communication to the Internet and from embedded systems to micro-electromechanical systems (MEMS). This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of Things. To keep you up to date with the challenges but also possibilities of the IoT we decided to focus this issue upon this topic.

Yours Sincerely

Wolfgang Patelay
Editor
CONTENTS

Viewpoint 3

Internet-Of-Things – Applications
Extending the battery life of wearable devices 6
IoT global cellular networks – one step closer to 5G 10
Five Senses of Sensors - Part 1: smell, taste, and hearing 12

Internet-Of-Things – Systems Design
Designing robust electronics for the Internet of Things 15
Simulating IoT designs: will large-scale deployment work in practice? 22
Virtualization in broadband gateway creates value-added service platform 24

Internet-Of-Things – Security
Security requirements of the Internet-of-Things 27
Security squared: system board featuring encryption technology 30
In automotive software security is the new guard dog 32

Internet-Of-Things – Smart Industry
Embedded systems best suited for the Industry 4.0 project 34
Brilliant machines enable the industrial Internet of Things 36

Embedded Computing
On the way to significantly boost market share 38
Long-term partnership ensures safe and secure robot control 41

Product News 43-47

Cover Story: Extending the battery life of wearable devices 6
This article gives just a small look at low power management technology and how products can work together to create the ultra-low power systems to drive the emerging wearables market and other applications where conserving battery life and/or conserving harvested energy is critical.

Five Senses of Sensors - Part 1: smell, taste, and hearing 12
This article is the first of a two-part series on the “Five Senses of Sensors”. The discussion looks at advances in sensor technology that mimic and mirror human smell, taste, and hearing. The focus is on changes in the underlying sensors and how applications have grown, particularly in the light of the Internet of Things (IoT). Part 2 will examine touch and vision sensors.

Designing robust electronics for the Internet of Things 15
Since the earliest days of the high-tech revolution, simulation-driven product development has been critical for satisfying consumers’ increasing demand for device functionality, speed, bandwidth, aesthetics and other characteristics. As before, the winners in the IoT economy are adopting typical best practices outlined in this article.

Security requirements of the Internet-of-Things 27
This article explains the security requirements of the IoT, and introduces a starter kit comprising all necessary components to rapidly develop a prototype to test IoT technology as simply as possible.

Embedded systems best suited for the Industry 4.0 project 34
This article describes how Kontron, together with technology partners like Intel, Wind River, Telekom and Salesforce, is already working on solutions that are founded on a standard base of embedded systems, which can be connected to the Internet of Things (IoT), and which also offer cloud solution approaches.
SECURING THE INTERNET OF THINGS

SAFE, RELIABLE, SECURE.

For more than 30 years the world’s leading companies have trusted Green Hills Software’s secure and reliable high performance software for safety-critical applications.

For the connected car, consumer and medical devices, industrial telemetry, smart grid, telecoms hubs and more, our software and services deliver proven secure, reliable underpinning technology for the Internet of Things.

To develop devices for the Internet of Things with the highest levels of security and reliability, visit www.ghs.com/secureIoT

Copyright © 2015 Green Hills Software. Green Hills Software and the Green Hills logo are registered trademarks of Green Hills Software. All other product names are trademarks of their respective holders.
Extending the battery life of wearable devices

By Landa Culbertson, Mouser Electronics

To gain market acceptance and meet the projected 380 million units in use worldwide by 2018, extending battery life in wearable devices is critical. Energy harvesting, wireless charging, battery management, power management and low power solutions are all considerations. Energy harvested from the body (heat or movement), or from the environment (ambient light), yields insufficient power for something like a smartwatch. Texas Instruments Ultra Low Power Power Management IC with Boost Charger bq25570, can take 300 to 400 millivolts collected by energy harvesters and boost it to 3 to 5 volts - enough to charge a battery. Although insufficient to power a smartwatch, it could extend its runtime and also includes a highly efficient nano-power buck converter to provide the option of a second power rail to the system.

The new TI bq25100 single-cell Li-ion charger provides a tiny solution for traditional battery charging via a USB port or adapter. Half the size of existing charger solutions, it supports low cost unregulated adapters which may be used in the cost-sensitive wearables market. Maxim’s highly integrated MAX14676/76A Wearable Charge Management Solution ICs provide another option for battery charge management in wearable applications. They include not only a linear battery charger, but also numerous low-power power management peripherals to save system board space while extending battery life. Wireless charging via a charging base is popular and convenient for consumers. Qi is an international standard for interoperability of wirelessly charged device - any Qi certified wireless power receiving device, such as the Moto 360 smartwatch, can work with any Qi certified charging base. Wireless charging solution reference design from TI, TIDA-00318, suits 135mA charge current applications and is just 5x15mm2. Any wearable implementing the TIDA-00318 design should be able to gain Qi certification and work with any Qi charging base. For an even smaller wireless charging receiver solution capable of delivering up to 2W of power, TIDA-00329 reference design is only 5.23mm x 5.48mm. On the wireless power transmitter or charging-base side, TIDA-00334 reference design is a low power design laid out in a 30mm area that matches the diameter of the round Wurth coil 760308101103 - slightly larger than a 2 Euro coin.

Ultra-low power conversion is critical to achieving optimal battery life in wearable devices. Some of the latest low power products or highly efficient dc-dc converter products currently available include: TI TPS727xx series of 250mA LDOs with ultra-low Iq of just 7.9µA, very low dropout, high PSRR of 70dB at 1kHz for quiet performance in RF applications, and TI TPS82740A and TPS82740B 200mA step-down converter modules with 95% conversion efficiency, 360mA Iq during active operation and 70µA during standby. Step-up or boost conversion is generally not as efficient as step-down conversion, so stepping up from the battery voltage is often necessary to power various circuits in the system, especially displays. New Maxim 1A step-up converter, MAX8627, generates a boosted output voltage from 3V to 5V from a single-cell Li-ion battery, with up to 95% efficiency and consumes just 20µA Iq. Silicon Labs TS33x step-up converters have Iq as low as 150µA and step up input voltage from 0.9V to 3.6V to eight selectable output voltages ranging from 1.8V to 5V.

Higher power consuming functions such as processing and displaying can be offloaded to a smartphone, tablet, or PC. Bluetooth Smart or Bluetooth Low Energy now automatically built into most new smartphones is the de facto wireless communication standard for wearables. Optimized for low power operation, TI Bluetooth Wearable Watch Development System TI Meta Watch enables rapid development of connected watch applications and includes a watch with a display, a 3 ATM water resistant stainless steel case, leather strap, a mineral glass crystal, vibrating motor, three-axis accelerometer and an ambient light sensor.
Hermes

Efficient Metering Bus Networking

Hermes is a high performance M-Buss slave transceiver optimised for minimum power consumption in metering communications. The device is housed in a space-saving QFN-20 package and is compliant with the EN 13757-2 and EN 1434-3 standards. It has very low quiescent current, supports low bus voltage operation and features optimised low power modes ideal to interface with Wireless modules. It can be powered from the bus or from an external power supply and can even drive six M-Bus loads.

For all information, design know-how and application support please contact your local partner of EBV Elektronik, the leading specialist in EMEA semiconductor distribution, or check under ebv.com/hermes.
MCU choice is important for power management of wearables: efficient MCUs process data quickly and save power in sleep mode. As 32-bit MCUs have become cost-competitive with 16-bit MCUs, designers now have a wide choice. ARM Cortex-M series of 32-bit processor cores is optimized for cost and power sensitivity and MCUs based on the series are available from many different suppliers, including Texas Instruments, and STMicroelectronics (STM32 L1 and L0 Ultra-Low-Power MCUs). Improvements in sensor technology are one of the developments fueling the wearables market but sensor power management needs consideration. Peripheral circuitry for sensors shouldn’t be overlooked - STMicro OA4NP quad, low power op amp consumes just 580nA per channel (at 1.8V power supply).

For further information visit the Applications & Technologies section of mouser.com

**Product News**

**Eurotech and WebRatio extend their technological collaboration for the IoT**

Eurotech announced that they have reinforced their technological collaboration with WebRatio. After a year of cooperation, during which Eurotech and WebRatio showed together proof-of-concepts at Shop.org in Seattle in 2014, and again at the 2014 Red Hat Open Source Day in Rome, the two companies decided to extend their technological collaboration.

*News ID 2912*

**IAR: Embedded Workbench supports RX71M MCUs targeting the IoT**

IAR Systems has released version 2.70 of its development toolchain IAR Embedded Workbench for Renesas RX family of MCUs. In addition to new features including position-independent code and data, version 2.70 adds updated device support and example projects for the latest Renesas devices. The support includes the new RX71M group with advanced security features for the industrial Internet of Things.

*News ID 2840*

**Dialog Semiconductor: Bluetooth Smart SoC family with application-optimised versions**

Dialog Semiconductor announces three additions to its SmartBond family of ultra-low power, Bluetooth Smart SoC integrated circuits. The devices, aimed at high volume, high growth consumer markets, are the smallest and lowest power wireless connectivity solutions for the Internet-of-Things. Versions optimised for wireless charging and remote control units address markets that will ship over 1.5 billion units per annum within 4 years.

*News ID 2852*

**IOLITE and Lantiq: standard- and device independent open smart home platform**

Lantiq and IOLITE, a spin-off of DAI-Labor (Technical University of Berlin), present the innovative smart home platform IOLITE. The platform is designed as an open and fully interoperable ecosystem. It allows devices of all standards and kinds, e.g. sensors, actuators, or cameras to be integrated in a home environment and used in a range of innovative applications. The computing power for the IOLITE platform is provided by Lantiq’s high-performance GRX 300 network processor family.

*News ID 2905*

**Infineon and Fraunhofer: security solution for PLC-based industrial automation systems**

The digitalization and increasing networking of production require significantly higher security standards in industrial automation than has it previously been. Digital threats based on malware, incorrect firmware updates, and counterfeit components can bring entire production lines to a standstill and cause significant costs. Infineon Technologies and the Fraunhofer Institute for Applied and Integrated Security (AISEC) have developed a solution that protects PLC based industrial automation systems from unauthorized access and manipulation.

*News ID 2917*

**Rutronik: Embedded WISE-Node and gateway devices from Advantech**

Advantech offers a new integrated IoT solution – WISE (Wireless IoT Solution Embedded). With WISE-cloud IoT software built-in, it provides remote device management, reliable data acquisition and security protection for many IoT applications. The WISE-Node and -Gateway devices for System Integrators to build their own IoT environment is available at distributor Rutronik as of now.

*News ID 2936*

**Silicon Labs: Wireless M-Bus platform solution for smart metering**

Silicon Labs introduced the industry’s first complete Wireless M-Bus platform solution designed to simplify the development of wirelessly connected smart meters for electricity, gas, water and heat resources in the European market. Silicon Labs’ comprehensive smart metering solution includes the Wireless M-Bus software stack and wireless starter kits to speed time to market. The Wireless M-Bus solution is portable across Silicon Labs’ wide array of energy-friendly ARM-based microcontrollers and sub-GHz wireless ICs, and it supports all modes for smart metering in Europe including the popular 169 MHz N modes.

*News ID 2898*
Build Your Internet of Things with ADLINK

We provide comprehensive Building Blocks for IoT enabled by SEMA Cloud Solution embedded boards and gateways to networking platform

- **cExpress-BL**
  Compact COM Express® Type 6 Module with 5th Generation Intel® Core™ i7/i5/i3 System-on-Chip

- **MXE-200i**
  Intel® Atom™ Processor-Based Embedded IoT Gateway Platform

- **IMT-BT**
  10.1" Industrial Mobile Tablet with Intel® Celeron® N2807 and Windows Embedded 8.1/7

Member of m2m alliance
IoT global cellular networks
– one step closer to 5G

By Guillaume Crinon, Avnet Memec

Together with Telecom Design as the historical Sigfox modem provider, Semtech, Silicon Labs, and Avnet Memec have committed to help develop the business of IoT networks in Europe and beyond, whatever the technology, thus paving the way for what 5G will bring to the Internet-of-Things: ubiquitous low-cost and low-power Internet connectivity for all our “things”.

What if the IoT big numbers were not too far-fetched? What if expanding the market of the connectable “things” was simply crunching the cost of connecting them? What if we had the technology and business-model available? What if IoT telecom operators were already offering new global cellular services in the unlicensed industrial scientific medical (ISM) bands?

Twenty years ago, massive investment was made by major telecom operators around the globe in order to seamlessly connect people to one another: Mobile Network Operators were born. At the same time, the Internet reached every single neighborhood and home: optimism and enthusiasm in the “new economy” fueled the growth of the first telecom revolution and dotcom bubble. Twenty years and two economic crises later, everyone agrees that it has been a success: half the world’s population owns a cell phone or a smart phone, has fixed or mobile Internet access, and is now accustomed to spending monthly on a voice and data plan for services which have truly become vital needs.

In order for the Mobile Network Operators (MNO) and Mobile Virtual Network Operators (MVNO) to maintain their average revenue per User (ARPU), the service delivered to the end-user has no other choice than to improve, compensating for the data plan natural price erosion. This is the reason why 2G, 2.5G, 2.75G, 3G and 4G have taken over one another for the past twenty years, always promising more bandwidth, higher mobility, denser coverage, better quality of service.

With more SIM cards than inhabitants in most developed countries, the market has reached saturation. MNOs and MVNOs have therefore been trying hard to develop a Machine-to-Machine (M2M) market for the past ten years. Given the cost of connectivity, the cost of the modem, the inadequacy of the technology with long-life low-cost battery-operated systems, this M2M market relying on legacy cellular networks is limited to a few verticals (automotive, tracking, vending machines, point-of-sales, security, etc), which can accommodate these constraints. This nevertheless leaves the vast majority of objects or “things” we live and work with unconnected. Connecting them is the challenge of the IoT, either indirectly through a gateway, be it a smart-phone or an Internet box, or directly under a dedicated cellular network.

Looking at the way the 5G Public-Private Partnership and mobile and wireless communications enablers for the Twenty-twenty Information Society (METIS) are defining the needs for making our cellular networks evolve by 2020, it has become obvious that different technologies will coexist in order to best address the needs: “amazingly fast” calls for more bandwidth and bit rate, “great service in a crowd” could be served by repetitive broadcast schemes, “best experience follows you” will require sophisticated signal processing and network architecture, and “ubiquitous things communicating” calls for a simple, low-power, low-cost technology “thing” coupled to an agile easy-to-deploy network infrastructure. This latter item is the one we will explore.

Among the verticals not easily served by legacy networks are: metering (water and gas meters), industrial logistics (pallets), extended fleet management (bicycles, trailers), security (smoke detector, leak detection, anti-tampering), environmental (waste containers, weather stations), agriculture (irrigation, sensors), health (pill box, social alarm), and many more where battery life and connection cost is a deterrent. For all these applications, a WiFi or Bluetooth smart router may not be available behind each and every device to service a connection to the Internet, while a 2G/3G connection will hinder the profitability with higher costs of connectivity and battery replacement. Nonetheless, all these applications have the following in common:
1) they are required to report only a few bytes of data per hour or per day,
2) they tolerate network latency in the order of magnitude of the second,
3) the objects under the network need neither
be connected nor synchronized to the network since they sleep most of the time,
4) the objects do not need to talk to one another in peer-to-peer mode,
5) the objects mostly need to upload data to the network, and
6) they can tolerate missed packets here and there.

Considering all these properties, it becomes possible to build a very
light network infrastructure. Taking advantage of 1) and 2), the phys-
ical layer can operate at a very low bit rate (a few kilobits per second
or less), yielding a higher link budget and a longer communication
range between the object and a base-station, translating into wider
cells, lighter infrastructure to deploy, lower CAPEX and OPEX for
the operator, lower cost of communication for the object. Number
2) offers the possibility of managing Medium Access Control from
the Cloud, and potentially in future deployments even the physical
layer itself with enhanced diversity. Numbers 3) and 4) mean that the
objects can operate asynchronously with one another and that the
network base-stations essentially continuously listen to the objects
broadcasting randomly. Number 5) allows deploying a very effec-
tive network where base-stations operate in half-duplex mode, with
uplink and downlink bands sitting next to one another in a license-
free ISM band. Last but not least, number 6) helps validate the proof
of concept with reasonable investment, both on the network and
application side.

A few radio technologies can already support such networks: nar-
row-band FSK/MSK with WmBUS metering private networks, LoRa by Semtech based on Chirp Sequence Spread Spectrum, Ran-
dom-Phase-Multiple-Access by On-Ramp-Wireless, and alternative
Direct-Sequence-Spread-Spectrum layers to be standardized by Sili-
con Labs and others at the IEEE. In Europe, several utility companies
are deploying their private networks dedicated to metering based on
WmBUS. Others, such as Actility relying on the LoRa technology, are
installing private networks for the smart grid and the smart city.

But only one company has taken the step to actually raise funds to
deploy and operate a truly global and general purpose IoT network
on the basis of their Ultra-Narrow-Band Phase-Shift-Keying: Sigfox.
There is little doubt that other telecom operators relying on competing
technologies will also deploy their solutions in the years to come. There
is also little doubt that as soon as a few hundred million connections
are sold yearly worldwide, legacy cellular operators will consider allo-
cating a few hundreds of kHz of their expensive spectrum to a similar
technology, giving birth to 5G.

Product News

- Toshiba: ARM Cortex-A9 based processors for IoT applications
  Toshiba Electronics Europe has expanded its selection of ApP
  Lite processors with the launch of the TZS010XBG, TZS011XBG,
  TZS012XBG and TZS023XBG. Designed for Internet of Things
  applications, these new ARM Cortex-A9 based processors reduce
  power consumption.
  News ID 2918

- EnSilica: processor cores targeted at IoT sensing
  nodes and always-on applications
  EnSilica has added to its family of eSi-RISC processor cores with the
  launch of the eSi-3260 targeted at IoT sensing nodes and always-on
  applications. The eSi-3260 combines advanced DSP functionality
  with the characteristic eSi-RISC small footprint and extremely low
  power consumption.
  News ID 2921
An artificial olfaction device, an electromechanical or e-nose, is an array of chemical gas sensors, a sampling system, and a pattern-classification algorithm to recognize, identify, and compare gases, vapors, or odors. These devices mimic the human olfactory system and have been successfully used in a wide variety of applications including detection of food quality, wastewater management, measurement, and detection of air and water pollution, in health care, and in warfare. One of their strengths is that the data gathered can be interpreted without bias.

In food safety, the most common use is to determine the quality of tea, milk, alcoholic beverages, fruits, meats and fish, cheese, and other dairy products. Gas sensors include methane, ethanol, toluene, o-xylene (an aromatic hydrocarbon based on benzene), CO2, and CH4. For medical applications, e-nose devices are being explored for the detection of the cancer biomarkers necessary for early diagnosis and fast treatment. For example, researchers at the University of Tampere in Finland have used a device that conducts molecular analysis of the air above urine samples, testing it for the volatile organic compounds associated with prostate cancer. In a study, published last year, the scientists claimed the method had a detection rate of 78 percent.

The use of nano-materials in e-nose applications is gaining ground along with the capability of creating sensors with ultra-high sensitivities and fast response (due in part to a smaller structure). The smaller sensor size also promotes integration into a larger number of devices. An attractive class of materials for functional nano-devices is metal-oxide semiconductors. They offer simple operation, ease of fabrication and the potential for compatibility with microelectronic processing, as well as low cost and low power consumption. There are still many challenges to be overcome, including fully understanding the nano-material growth mechanism to assure sufficient quality. Aligning nano-materials between predefined electrodes and forming proper contacts that directly influence device performance is also not an easy feat.

There have been recent sensor breakthroughs with devices that could give smartphones a sense of smell. Developed by Honeywell ACS Labs, the new device utilizes a new type of MEMS vacuum pump, hundreds of times smaller than previously available. In human olfaction, lungs bring odor to the olfactory epithelium layer inside the nose, while the e-nose uses a pump. The Honeywell devices promise to initially provide an add-on sense of smell for spectrometers, but it may also end up in smartphones that can sense everything from toxic chemicals to pollen to general air quality.

The classes of e-noses include those with conductive polymer, surface acoustic wave, calorimetric, and polymer composite. Often there are several types or classes of sensors used in these applications, including optical-sensor systems, mass and ion mobility spectrometry, gas chromatography, infrared spectrometry, and chemical sensors. An example of a gas sensor used for CO2 detection is Amphenol’s Telaire 6613 CO2 module (figure 1). The small, compact module is designed to integrate into existing controls and equipment to meet the volume, cost, and delivery expectations of OEMs. All units are factory calibrated to measure concentration levels to 2000 and 5000 ppm. Dual-channel sensors are also available for higher concentrations. The affordable, reliable, flexible sensor platform is designed to interact with other MPU devices.

The electronic tongue (e-tongue) uses an array of liquid sensors that mimic the human sense of taste, without the intrusion of other senses such as human vision and olfaction that often interfere with taste perception. Within a few years, researchers anticipate that a machine that experiences flavor will determine the precise chemical structure of food and why people like it. Digital taste-buds also will help
Free Your Creativity
with Core Independent Peripherals

PIC® microcontrollers with Core Independent Peripherals take 8-bit MCU performance to a new level. With a number of on-board modules designed to increase capability in any control system, these MCUs represent the best value in embedded design.

Core Independent Peripherals are designed to handle their tasks with no code or intervention from the CPU to maintain operation. As a result, they both simplify the implementation and boost the performance of complex control systems while giving designers the flexibility to innovate.

Flexible Functional Building Blocks

- Power conversion
- Motor drive
- Signal generation
- Sensor interface

www.microchip.com/get/eucip

The Microchip name and logo, the Microchip logo, and PIC are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries. All other trademarks are the property of their respective owners. © 2015 Microchip Technology Inc. All rights reserved. DS000017488. MRC206/Eng03.15
E-tongues /or/ ten are used in liquid environments to discriminate between samples. Most e-tongue measurements to classify the contents of the liquid, based on the human palate. There are five basic types of tastes: sweet, bitter, salty, sour, and umami (a Japanese word that can be translated as deliciousness or pleasant, savory taste). To mimic the human tongue, sensors are used in multiplexed arrays containing multiple taste receptors. E-tongues are used in liquid environments to classify the contents of the liquid, based on the human palate. There are five basic types of tastes: sweet, bitter, salty, sour, and umami (a Japanese word that can be translated as deliciousness or pleasant, savory taste). To mimic the human tongue, sensors are used in multiplexed arrays containing multiple taste receptors.

While e-tongue technology has advanced past several years, it is taste accuracy that has become a priority. For example, in 2014 researchers managed to distinguish between different varieties of beer using an electronic tongue with an accuracy of approximately 82 percent, while other e-tongue prototypes have demonstrated ability to successfully distinguish between wines.

Hearing systems are increasingly being trained by listening to sounds, detecting patterns and building models to decompose sounds. One of the most common applications for sensors in this segment is in hearing aids. Digital advances have made hearing aids today smaller, smarter and, fortunately, easier to use. The most advanced hearing aids are now interacting with other devices, such as smartphones and digital music players, to deliver sounds directly and wirelessly to the listener. Recent improvements are based on better microprocessors and noise-reduction software so that the hearing aid can be selective about the types of sound it amplifies, muffles, or suppresses.

The focus of current research is on directionality and speech enhancement. Sound systems can employ digital signal processing to automatically shift between two different types of microphones in order to pick up either a single speaker voice or sound coming from all around. Digital-speech enhancement can now increase the intensity and audibility of some segments of human speech. Research projects are underway to reduce the size and cost of hearing aids, improve their directional capabilities, and identify and amplify desired sounds such as a human voice while muting background noise. Researchers are also working hard to extend battery life through the use of tiny microphones mounted on MEMS chips. These chips enable multiple microphones to be placed inside a device small enough to fit in a user ear without rapidly draining the batteries.

For example, while flies ordinarily have no sense of hearing at all, one subset, the Ormia ochracea, a parasitic fly, can determine the direction of a sound to within two degrees, which seems impossible given the tiny size of the fly. Cornell scientists are studying the extremely tiny insect parasite as the basis of an effort to develop a man-made directional-listening system based on the auditory apparatus of the fly, naturally small enough to fit inside a hearing aid.

Sensors that detect sound or hear are essentially microphones with sophisticated signal-processing capability. In robotics, sound sensors are used in a myriad of applications. One sensor particularly well-suited for sound-based application is the Parallax Sound Impact Sensor (figure 2) that provides noise control to a project and responds to loud noises such as a clap of the hands. Through the on-board microphone, this sensor detects changes in decibel level, which triggers a high pulse to be sent through the signal pin of the sensor. This change can be read by an I/O pin of any Parallax microcontroller. An on-board potentiometer provides an adjustable range of detection of up to 3 meters away.

Targeting speech recognition, the STMicroelectronics MP34DB01MEMS audio sensor digital microphone (timing waveforms are presented in figure 3) is an ultra-compact, low-power, omnidirectional, digital MEMS microphone built with a capacitive sensing element and an IC interface with stereo-operation capability. The IC interface is manufactured using a CMOS process and features a single supply voltage, low power consumption, and omni-directional sensitivity. The MP34DB01 has an acoustic overload point of 120 dB SPL with a 62.6 dB signal-to-noise ratio and -26 dBFS sensitivity. It is available in a bottom-port, SMD-compliant, EMI-shielded package and is guaranteed by the supplier to operate over an extended temperature range from -40 °C to +85 °C. In summary, in the near future there will be more developments in the smell-, taste-, and hearing-based sensor technology used a variety of applications.
Designing robust electronics for the Internet of Things

By Sudir Sharma, Ansys

Since the earliest days of the high-tech revolution, simulation-driven product development has been critical for satisfying consumers’ increasing demand for device functionality, speed, bandwidth, aesthetics and other characteristics. As before, the winners in the IoT economy are adopting typical best practices outlined in this article.

Today we live in a world based on connectivity and communication, in which a burgeoning network of electronic systems and devices helps us navigate our days. Smartphones, tablets and GPS systems are the most obvious examples. In addition increasingly sophisticated electronics in cars, homes, hotels and offices keep us secure and comfortable, and medical implants and prosthetics are relied upon every day by many to maintain health and quality of life. When we visit theme parks or attend concerts, wristbands or smartphones may be scanned for admittance. Wearable wristbands and activity trackers can monitor our physical movements, vital signs and sleep patterns. Today, high-tech devices are inescapable. This proliferation of connected devices and systems is being called the “Internet of Things” or IoT. By 2020, over 200 billion devices will be connected to the Internet, delivering over $7.1 billion in economic value.

This rapid growth brings significant challenges. As devices proliferate, consumer expectations for connectivity, energy efficiency, reliability, ease of use and structural strength will only increase. Electronics must be not only innovative and high-performing, but must also be attractive. And, of course, all this functionality and beauty must be delivered at a low price. How can high-tech engineering teams manage these pressures? Since the inception of the industry, market leaders have relied on simulation-driven product development to launch their devices quickly, cost-effectively and with a high degree of confidence that they will perform as expected in the real world. Designing robust systems for IoT will require engineers to improve communication speed, maximize energy efficiency, optimize antenna performance, and improve structural and thermal integrity. The following sections provide greater insight into these challenges as well as some technical examples.

As mobile devices proliferate, more and more data is being transmitted and received, driving the need for faster communications networks. Video streaming, interactive gaming and high-speed web service are pushing the limits of not only mobile devices, but also servers, routers and switches. Improving speed and bandwidth is an industry imperative, but design complexity poses significant challenges. For example, designing printed circuit boards (PCBs) for high-speed, double-data rate (DDR) memory buses or serial communication channels requires extreme care. High data rates combined with low operating voltages can cause signal and power

Figure 1. Design automation tools like ANSYS PowerArtist can identify the key RTL changes with the greatest power-saving potential

Figure 2. Design of sensor antennas for a smart watch
To squeeze every bit of performance, product development teams need to use coupled multiphysics software, which can analyze the trade-offs among speed, bandwidth, signal integrity, power integrity, thermal performance and EMI/EMC. For example, maximizing data throughput in a smartphone may require system engineers to focus on electromagnetic, structural, and thermal performance of the RF shielding.

Power efficiency can be discussed from two perspectives: power delivery and power consumption. The first one is delivering power efficiently and safely. As an example, consider an implanted medical device. It needs a power source, which can be charged wirelessly, without damaging living tissue. So, wireless power transfer, energy harvesting, and regulatory compliance are key considerations for IoT devices. On the power consumption side, engineers need to fully model integrated circuits, IC packaging and printed circuit boards. Low-power IC design begins with optimization of Verilog and VHDL (RTL) code. Clock gating, memory-access optimization, and turning off unutilized logic are simple improvements that can make a big difference in lowering power consumption. Design automation tools like Ansys PowerArtist can identify the key RTL changes with the greatest power-saving potential. Power efficiency isn’t limited to the design of ICs.

To achieve best power efficiency, engineers need to consider the whole system, including antenna and wireless systems. An optimized antenna system can provide a better user experience, including increased talk time. For example, simulation allows engineers to model the performance of antennas in free-space, within device enclosure, and then next to the human head. Properly designed antennas can provide 2.25 times more talk time. The proliferation of wireless devices creates new performance demands for antennas and radio systems, which need to deliver uninterrupted connectivity. As previously noted, antenna system designers must consider the comprehensive characteristics of the environment in which the antenna will operate. This can include modeling effects such as plastic covering over the antenna, the interaction of a mobile handset with the human hand, or the way an antenna is installed in an automobile. With so many complex wireless systems operating in close proximity, electromagnetic interference can become a big issue. Consider the design of antennas and sensors for a smart watch. The watch band contains a biometric sensor antenna, operating at 400MHz, and a Bluetooth antenna, operating at 2.4GHz. Each frequency band excites a different part of the antenna requiring additional sophisticated engineering analysis. Using finite element (FEM) domain decomposition, 3-D method of moment (MoM) and hybrid FEM–MoM enables antenna engineers to quickly solve electrically large and complex, full-wave electromagnetic models. To get a complete picture, engineers need to examine the behavior and scattering of radiation across time and space using transient analysis.

Today, high-tech companies turn to advanced lightweight, yet strong, materials to create flexible mobile and wearable electronics. However, a range of complex issues must be considered when evaluating new materials – including electrical conduction properties, structural strength, and dimensional stability over time and resistance to thermal build-up. Design for manufacturability is also an important consideration. For example, even when a smart watch has been designed with the strongest practical materials, the device may be damaged due to impact. To achieve the right trade-offs between material strength, cost and design elements, engineers can turn to simulation tools for structural and explicit dynamics analysis to model physical impact and drop-tests.

Manufacturing robust modern electronics products is complicated by their complex shapes and functions. In the smart watch example, the electronics within the watch are under stress due to the curvature of the wristband. Understanding this issue beforehand can help the device last longer and deliver better user experience. In this case, the curvature of the wristband was adjusted to reduce the stress on the antenna.
Internet-of-Things Conference

The Internet of Things is chance and challenge. It might be one of the biggest changes ever, as more and more standalone embedded systems evolve into massive and powerful networks of devices.

The future will see an Internet of Things where billions of devices are connected to each other, all sharing data via the Internet.

Conference Focus

This 1-day conference focuses on Embedded Systems Design for the Internet of Things and will provide

- System Designers
- Hardware Engineers
- Software Developers

with first-hand information about visions, trends, technologies and implementations in application areas like

- Smart Manufacturing/Industry 4.0
- Smart City, Smart Energy
- Smart Buildings, Smart Homes

A major topic of the conference will be Security, because Security is paramount for the safe and secure operation of IoT devices in all above mentioned application areas.

Exhibition

There will be a table-top exhibition running parallel to the conference.

The exhibition provides a communication platform where the conference delegates and the exhibition visitors can talk to leading suppliers of IoT solutions.

The table-top stands will be manned with technical specialists thus this exhibition provides a unique opportunity for discussions with the major players in the IoT arena.

Delegates Registration

The Conference will take place on on May 19, 2015 in Munich in the RAMADA Hotel, Konrad-Zuse-Platz 14, 81829 München

Conference Fee:
EUR 79.- (plus 19% VAT)
This includes lunch, coffee and softdrinks.

Silver Sponsors

http://www.iot-design.com
# Conference Programme

The Conference Programme runs from 10h00 to 17h30 and consists of 3 parallel streams with 20-minutes technical presentations about technologies, solutions & applications.

The programme will be structured into different Sessions covering topics like Security for the Internet-of-Things, Smart Manufacturing, 4.0, Smart Cities, Buildings & Home, Smart Energy, Smart Medical, Wearable Devices,.....

## Timetable

<table>
<thead>
<tr>
<th>From</th>
<th>Keynotes</th>
<th>Industry 4.0, Smart Buildings, Smart Home &amp; more (Track 1)</th>
<th>Industry 4.0, Smart Buildings, Smart Home &amp; more (Track 2)</th>
</tr>
</thead>
</table>
| 10h00  | **The Internet-of-Things: chance and challenge**  
*Speaker: Eric Schneider, Chairman M2M Alliance*                                                                 |                                                                                                                                 |                                                                                                                                 |
| 10h40  | **IoT - It's all about Security**  
*Speaker: Colin Walls, Embedded Software Technologist with Mentor Graphics*                                                  |                                                                                                                                 |                                                                                                                                 |
| 11h10  | Coffee Break                                                                                 |                                                                                                                                 |                                                                                                                                 |
| 11h40  | **Verifiable security for the embedded Internet of Things**                                   | **Intel-based Embedded Platforms for IoT**                                                                                | **Long range, low power IoT networks for the Smart City**                                                                   |
| 12h05  | **Security by Separation**                                                                    | **New business models for IoT and Industry 4.0 with Advantech Webaccess Framework**                                      | **Smart Sensor platform for home & building automation**                                                                    |
| 12h30  | Lunch                                                                                        |                                                                                                                                 |                                                                                                                                 |
| 13h45  | **Secure Element – the cornerstone for a safe connected object**                             | **IoT in mobility and harsh environment**                                                                                  | **Comparison of all in one and modular hardware for IoT**                                                                   |
| 14h10  | **Root of trust brings trust!**                                                               | **IoT in industrial automation - challenges and solutions**                                                               | **Ease interoperability challenges for the Internet of Things**                                                             |
| 14h35  | Coffee Break                                                                                 |                                                                                                                                 |                                                                                                                                 |
| 15h00  | **How to come around the IoT data security challenges**                                      | **Bringing Intelligence into the cloud**                                                                                  | **Realizing the Big Data potential - from data to business intelligence**                                                   |
| 15h25  | **Security aspects for COM-based IoT systems**                                               | **Smart cloud solutions for Industry 4.0 applications**                                                                    | **From Sensor to gateway, the way to an IoT device**                                                                      |
| 15h50  | Coffee Break                                                                                 |                                                                                                                                 |                                                                                                                                 |
| 16h20  | **Storage and Security - a perfect chance for system security**                              | **IoT in building management and environmental monitoring**                                                                | **Universal platform for building automation solutions**                                                                  |
| 16h45  | TBD                                                                           | **TBD**                                                                    | **TBD**                                                                    |
| 17h10  | Wrap-up and Prize Draw                                                                        |                                                                                                                                 |                                                                                                                                 |

## Date & Location:

May 19, 2015 in Munich in the RAMADA Hotel  
(Konrad-Zuse-Platz 14 81829 München)  

http://www.iot-design.com
Security for the IoT

- **11h40 - 12h05**
  **Verifiable security for the embedded Internet of Things**
  **Speaker:** Dave Hughes, HGC-embedded
  In this paper, Dave Hughes will discuss how rigorous software development processes are becoming critical for protecting connected devices in the Internet of Things. The IoT is dragging embedded developers into the network security debate. As embedded devices become increasingly networked, there is a growing risk that poor software quality can affect the quality of the final product and the security of customers data. A recent spate of high profile network security breaches with devices using software such as OpenSSL has highlighted serious risks companies may be exposing themselves and their customers to. Many of the defects discovered appear to have occurred as a consequence of a lack of rigor in the software development life cycle process. The issue of process must be addressed if application developers want to demonstrate they are serious about network security.

- **12h05 - 12h30**
  **Security by Separation**
  **Speaker:** Mehmet Özer, SYSGO
  To fundamentally secure connected device a new approach is needed. Separating sensitive devices physically from the network is for sure secure, but not in the sense of the inventor. A separation kernel offers a logical and efficient separation by its design, and has proven its safety and security in aerospace, transportation and automotive applications for many years. SYSGO’s PikeOS Real-Time Hypervisor uses the separation kernel architecture to isolate partitions, and thus separate secure and non-secure applications and data. The main security paradigms of PikeOS are separation of data, controlled information flow and white list policy. By cooperating with Kaspersky Lab, SYSGO brings a next level of security into the IoT market place. The Kaspersky Security System (KSS) controls the security policy of communication between isolated PikeOS partitions and thus mitigates the undesirable impact of security attacks.

- **13h45 - 14h10**
  **Secure Element – the cornerstone for a safe connected object**
  **Speaker:** Guillaume Crinon, Avnet Memec
  Although cryptography is a mature science offering robust algorithms and protocols for authentication, encryption, non-repudiation, identification, their implementation is too often misunderstood and flawed with mistakes, backdoors and bugs that hackers take advantage of. With the promise of connecting wirelessly tens of billions of yet unconnected machines, objects, tools and sensors by the end of the decade, our industry and society are facing an important security challenge: reaching a security level equivalent to the SIM and payment cards at such an affordable cost that the business-models are not impacted. Avnet-Memec believes that the answer lays in the Secure Element, the missing piece of inexpensive silicon at the heart of every single connected object for a safe Internet-of-Things.

- **14h10 - 14h35**
  **Root of trust brings trust!**
  **Speaker:** Christophe Tremlet, Maxim Integrated
  Whether they are used for consumer, industrial or medical applications we need trust in connected objects. The highest level of security is reached when the security chain is built on a root of trust. Learn how to implement the root of trust in your design and master IoT security.

- **15h00 - 15h25**
  **How to come around the IoT data security challenges**
  **Speaker:** Christian Eder, cong tec
  IoT will require smart embedded computers. The embedded hardware platforms like Qseven, COM Express and Mini-ITX are available. But how to implement the required security levels on a system base? Pre-integrated soft/hardware combinations of Intel Atom boards or module together with software package „Intel® Gateway Solution for IoT“ (from Intel, WIND RIVER and McAfee; Intel code name „Moon Island“) solves the reliability, connectivity, manageability and security challenges. The presentation provides an comprehensive overview about use cases and functionalities of certified embedded hard- and software combinations.

- **15h25 - 15h55**
  **Security aspects for COM-based IoT systems**
  **Speaker:** Peter Eckelmann, MSC Technologies
  For IoT systems built with Computer-on-Modules, there are various built-in security features which will contribute greatly to the overall security properties of the networked system. For x86-based processor boards, some well-known security aspects come from the utilization of security-centric hardware features while others are built into the Operating Systems. But even for ARM-based hardware there are very efficient tools and features to augment security to the desired level.

- **16h20 - 16h45**
  **Storage and Security - a perfect chance for system security**
  **Speaker:** Hubertus Grobbel, Swissbit
  The presentation will provide a status update of the industry in terms of currently available and commercially viable methods to protect device firmware and know-how, data and system integrity checks and enable strong authentication and encryption for embedded and industrial computing applications. It will also strive to compare and contrast various security strategies and propose a new approach for system security by combination of storage and security in one form factor.
Industry 4.0, Smart Buildings, Smart Home & more (Track 1)

- **11h40 - 12h05**
  **Intel-based Embedded Platforms for IoT**  
  **Speaker:** Wolfgang Heinz-Fischer, TQ-Group
  IoT is more than connected intelligent devices and cloud solutions. Every type of connected device and gateway has its own requirements regarding feature set, performance and software preferences. Different types of Intel based Embedded Modules and Platforms are available to meet these requirements. Unique and well known CPU architecture and pre-validated IoT software solutions with integrated management and security options help to reduce NRE and Time-to-Market. System partners can also benefit from custom specific hardware solutions Made-in-Germany to make IoT products more reliable and best optimized for their end-to-end solution.

- **12h05 - 12h30**
  **New business models for IoT and Industry 4.0 with Advantech Webaccess Framework**  
  **Speaker:** Tineke Borgen, Advantech
  Advantech WebAccess is a web browser-based software package for human-machine interfaces (HMI) and supervisory control and data acquisition (SCADA). All the features found in conventional HMI and SCADA software including Animated Graphics Displays, Real-time Data, Control, Trends, Alarms and Logs, are available in an standard web browser. WebAccess is built around the latest internet technologies.

- **13h45 - 14h10**
  **IoT in mobility and harsh environment**  
  **Speaker:** Mario Banganga, AAEON
  In this presentation AAEON introduces IoT Application Ready Platform (ARP) solutions in Mobility and Intelligent Gateways for Harsh Environment. Several intelligent gateway devices will be introduced for Transportation, Automation and Smart Metering market, connecting devices to cloud and data accessible anywhere with Rugged Tablet solution. In cooperation with ASUS cloud expertise, AAEON are able to offer secure and robust Application Ready Platform solutions.

- **14h10 - 14h35**
  **IoT in industrial automation - challenges and solutions**  
  **Speaker:** Markus Grebing, ADLINK
  Industry 4.0 is currently on of the hottest topics in the IoT ecosystem. What are the challenges, chances and most secure and reliable ways to transmit collected data? Learn more about this and which building blocks - modules, gateways, systems, software and a sophisticated security solution - of the broad ADLINK portfolio are best fit to make your application IoT-ready.

- **15h00 - 15h25**
  **Bringing Intelligence into the cloud**  
  **Speaker:** Michael Gaulitz, Wind River
  This talk will give a short introduction into the Internet of Things. Discusses what is required on the technical side to securely and reliably connect devices. Furthermore attendees will learn how to efficiently connect to a cloud and utilize big data analytics to transfer data into information. Nowadays the challenge is to leverage the tremendous set of new technical and business opportunities by enabling intelligent interconnection of devices and facilitating cloud connection offers. Security is a must and a strategy must cover all levels, including network, application, user, and data security to protect both data at rest and data in motion.

- **15h25 - 15h55**
  **Smart cloud solutions for Industry 4.0 applications**  
  **Speaker:** Johann Mühbauer, home2net
  Industry 4.0 will be the critical factor for tomorrow’s industry. Particular for Central Europe’s industry with its SME-based culture a quick and smooth transition to Industry 4.0 is vital. Differentiation and value creation have to exceed development and processing of mechanics and electronics – software is the key differentiation factor now. Smarter machines will be dependent not only from local data and sensors but also from global interconnecting. Interworking and linking to private and public clouds will enable new opportunities and new options for value creation. This will change organisation and work flow at production sites radically. Smart Cloud Solutions by home2net enables customers to adapt their infrastructure safely and quickly to industry 4.0’s demands to be ready for tomorrow’s challenges.

- **16h20 - 16h45**
  **IoT in building management and environmental monitoring**  
  **Speaker:** Mario Banganga, AAEON
  AAEON and its eco-partners introduce innovative Industrial IoT Application Ready Platform (ARP) solutions for Smart Building Management and Environmental Monitoring. Thanks to the support of the most important wireless and wired protocol, machine to machine connection, data exchange and monitoring will not be any more a barrier for Industrial Internet of Things (IIoT) revolution.

---

http://www.iot-design.com
Industry 4.0, Smart Buildings, Smart Home & more (Track 2)

• 11h40 - 12h05
Long range, low power IoT networks for the Smart City
presented by Jonathan Pearce, Microchip, in cooperation with Mouser Electronics
Significant numbers of IoT applications only require occasional and low-data-rate transmissions yet the same applications could be dispersed across major conurbations / regions and may rely on battery power / energy harvesting techniques. This presentation discusses the challenges of addressing increasing demands on end-nodes for long range connectivity, low power for battery operation and low cost for volume deployment and it will introduce the LoRa technology which enables low-data-rate wireless networking standard IoT and M2M wireless communication with a range of more than 10 miles (suburban), a battery life of greater than 10 years, and the ability to connect millions of wireless sensor nodes to LoRa technology gateways.

• 12h05 - 12h20
Smart Sensor platform for home & building automation
Speaker: Uwe Hirsch, Avnet Memec
The Avnet Memec IoTtoolbox is a comprehensive Cloud-ready ecosystem, helping to have a fast entry in the IoT market. It combines the “best of all” technologies for Sensors, MCU and Wireless Communication. On the Sensor side you will find typical sensors (RH/T, Light, Proximity / Gesture, Sound, Current, Accelerometer) for the home and building automation area. The sensor uses standard wireless communication to talk to an embedded low-power Gateway, which combines all wireless sensors and links to the cloud.

• 13h45 - 14h10
Comparison of all in one and modular hardware for IoT
Speaker: Wolfgang Lex, Conrad Business Supplies
IoT is not any more just a dream. Emerging from PLC based M2M solution to clever one board microcontroller: 3 different clever hardware-products for your IoT solution show how close technology is meanwhile to the future. Developers do not have to invent the wheel a second time. The long way has become shorter now. Select your favorite solution depending on where you would like to start and where you want to go. Different aspects are reflected in this comparison of a tiny industrial proven web-server and clever, but open all-in-one microcontroller board, based on latest chip technology.

• 14h10 - 14h35
Ease interoperability challenges for the Internet of Things presented by Sylvain Gardet, Freescale, in cooperation with Mouser Electronics
The IoT is ever evolving and extending the landscape of new devices that use data and control automation to solve real-time problems in a specific context. While the processing and communication capabilities for these new devices increases, ease of use with software development and also communication interoperability are challenged to keep pace. The connected home environment is a very good example where multiple devices are deployed but not necessarily capable of exchanging data together. That’s the reason why Freescale is contributing to and supporting the Thread initiative. Thanks to Thread, all these IoT devices in the home can work together to form a cohesive mesh network.

• 15h00 - 15h25
Realizing the Big Data potential - from data to business intelligence
Speaker: Dominikus Hirsch, Telt
The next wave of business productivity will come from the ability of information systems to look at Big Data stores fed by connected devices everywhere. Trends which are today seen as information elements looking into weeks and months into the future, will evolve to provide immediate future trends, looking into the next few hours or even minutes. This opens up opportunities for entirely new business models for example in traffic jam avoidance routing and even collision avoidance. Along with micro trends, Big Data enables new business models based on uniqueness of the analysis of data and the ability to make key predictions for businesses on markets, products, competition. At the heart of this exciting new world is the wireless module and the chain of services that enable it to connect and integrate Big Data. In this session Telt will describe this revolution engine in detail and how it contributes to the expansion of Big Data and analytics and the enablement of business models.

• 15h25 - 15h55
From Sensor to gateway, the way to an IoT device
This paper is presented by Advantech
Details will follow soon

• 16h20 - 16h45
Universal platform for building automation solutions
Speaker: Wolfgang Heinz-Fischer, TQ-Group
The building automation market has lots of standards, such as KNX, DALI, SMX and others and it will be difficult, to combine different standards in a complete building automation solutions. Missing all over all standards is a blocking point, to speed up the building automation market. A new approach is offered by TQ-Systems with B-control, a universal building automation platform, which allow to connect all devices from the market with a high integrated controller and Multi I/O box. The solution is driven by one software tool from planning to executing, object oriented and following open Standard IEC 61499.
Simulating IoT designs: will large-scale deployment work in practice?

By Jakob Engblom, Wind River

This article highlights the problem of developing and testing big IoT applications, and comes to the result that simulation is a practical solution.

Developing and testing Internet of Things applications and systems are big challenges, simply because the systems are big – they contain a lot of units. It is difficult to get hundreds of nodes into the software development lab for testing, and it is also difficult to provide all those nodes with interesting and realistic inputs. When developing software that will run on hundreds or even thousands of IoT nodes, just how do you test that software in a practical manner? Simulation is a very good answer.

The IoT systems that are being built today often follow a three-tiered architecture as shown in figure 1. There are many small nodes that connect to each other and to gateways using wireless mesh networks, and the gateways then connect to a management server or the cloud. The small nodes can be sensors like temperature sensors, electricity meters, cameras, light switches, or actuators like thermostats, lights, and door locks. The gateways or concentrators handle the connection to the outside world, and ensure security. The back-end server, which is often in the Cloud, deals with the business and control aspects of the IoT system.

To test this type of system, you want to have the wireless nodes spread out over a large area so that not all are in contact with each other, which requires using entire buildings or campuses as the lab. Setting up and maintaining such a network is a significant amount of work, with labour costs quickly dwarfing the cost of the nodes themselves. In a simulator, as shown in figure 1, setting up a large network is really easy. You just write a program to virtually deploy and spread out the nodes over the virtual space you need, and then model the wireless reachability between the nodes. Instead of manually handling hundreds of physical items, you manage a single script or program. Using a simulation solution like Wind River Simics to build this simulation, we simulate the hardware of each node, with processors, memory, timers, LEDs, wireless radio, and everything else that is needed. The different types of nodes are faithfully simulated, and run within the same simulation setup.

Simulating the entire IoT system in this fashion allows you to test all aspects of the software, including things such as the wireless communications stack and how it deals with network problems, the sensing and actuator code and how it works with the environment, and the sleep modes and wake-up intervals on the nodes and how well they conserve power. Other software functions that could be tested also include the reporting function from sensors to gateways and on to server, the middleware that manages network nodes and updates software on the nodes including OTA updates, along with the security of the gateways and the nodes and the scalability of the data management system as the number of nodes goes up.

One particular aspect of an IoT system test that is a very good fit for simulation is testing system and software behaviour as the system is scaled up. As shown in figure 2, simulation provides the ability to build systems of any size – from quite small to very large. This means that the behaviour of the system can be tested on a whole range of scales, from small unit tests or subsystem tests, all the way up to the largest setups imaginable. Often, each system scale will reveal different issues in the system. It is not just about the very largest setups, but also about making sure things work efficiently at intermediate system sizes too.

Figure 1 also shows simulation of the environment that the IoT system operates in. Each sensor node will typically interface to a simulation of the world surrounding it – so that it has some data to send back to the gateway and server. An IoT node without a world around it is not all that useful. System testing
INTERNET-OF-THINGS – SYSTEMS DESIGN

will involve varying the simulated radio network conditions. In a simulator, it is trivial to impose particular signal strengths between any pair of nodes, and to implement rules that randomly drop packets as signal strength goes down. The configuration can be varied during a test, to check how nodes behave when conditions change, such as when a train passes across the line of sight between two nodes and interrupts radio communications for a short while. Best of all, such tests are precisely controllable and repeatable, unlike in the real world where trying to impose radio conditions is difficult at best. Testing can also scale out horizontally, as shown in figure 3. It is easy to build many variants of networks to test the software with different ways to deploy the same number of nodes. Different balances between gateways and sensor nodes can be tested, as well as different network topologies. Figure 3 also shows how simulation lets you run many different tests in parallel, which makes the total time to run a set of tests much lower than if they had to be run serially on hardware.

But can it really work in practice to simulate hundreds or thousands of nodes on a single host computer? The answer is yes. IoT sensor nodes typically have a very low duty cycle. The sensors do not sense the world continuously, but rather, wake up regularly to take a sample and report it. Each sample run might take a second or just a few milliseconds, and then the system can be idle for minutes or even hours. This saves power, and makes it possible to have nodes deployed in the real world for extended periods of time without having to service them to change batteries.

Thus, there is a large amount of idle time in the system, idle time that can be exploited to accelerate the simulation by using hyper simulation. Rather than playing out idle time cycle by cycle, a simulation solution like Simics jumps straight to the next interesting event that would wake up a sleeping node. That means that a system that is mostly idle can be simulated many times faster than real time, which is a property that is exploited in large IoT simulations. I actually did this myself a decade ago, when we ran 1000 IoT nodes on a single-core Windows XP 32-bit host faster than they would have in the real world. At the time, that seemed insane, but today it sounds like business as usual.

In the end, physical labs are needed to perform final testing on your system. You have to test what you ship and ship what you test. However, using simulation to augment the physical test lab to cover more test cases and run more test variants is necessary to ensure that quality is maintained and that the system is robust across a wide variety of situations. With simulation, you will be able to build a better IoT system in a better way.

**Product News**

- **GreenPeak: Smart PIR sensor for smart home applications**
  GreenPeak Technologies announced a new addition to its Smart Home portfolio with the launch of a reference design for a low cost Passive Infra-Red (PIR) sensor with outstanding performance. The reference design of the PIR motion detector can enable application developers to quickly build a ZigBee enabled motion sensor that is ready to be produced with GreenPeak’s qualified ODMs and can be integrated in Smart Home applications like home monitoring, senior lifestyle, smart HVAC or smart lighting.
  News ID 2856

- **Imagination: Ensigma Whisper cores for wearables and IoT**
  Imagination Technologies announces the first members of its Ensigma Whisper flexible connectivity IP family, designed specifically to enable the integration of ultra-low power communications in SoCs targeting wearables, IoT and other connected devices that require extended battery life and low cost points. With the new Ensigma Whisper radio processing units, customers can choose to integrate Wi-Fi 802.11n, Bluetooth Smart, or a combination of the two standards, depending on their specific application.
  News ID 2934
Virtualization in broadband gateway creates value-added service platform

By Stephan Pruecklmayer and Ananta Vedantam, Lantiq

The broadband gateway can be turned into a powerful network hub for the smart home, instead of a simple network pipe. Virtualization, based on a powerful new class of network processor, is the key to dramatic improvements in the capabilities of the gateway that will allow carriers to serve as a central provider of smart home services.

Today, telecom and cable companies (carriers) provide residential broadband access to nearly 700 million customers worldwide. While the number of customers for these services is forecast to grow at single digit percentage rates through the decade, the emergence of the smart home offers a new opportunity to market intelligent electronic devices and services to consumers. However, wireline carriers are not the only resellers targeting the smart home. Broadband customers can choose from a growing number of third-party providers for equipment and value-added services. This can lead consumers to view broadband service as a commodity that is purchased based on price alone, driving carriers to compete for a shrinking share of residential customer spending.

The advantage a carrier has is the currently installed broadband customer premise equipment (CPE). With the proliferation of tablets and portable devices used to stream content in homes, recent improvements to the CPE have focused on optimizing distribution of multiple media streams. Smart home services – such as climate control and home energy management, security and room-to-room monitoring, and home automation – offer an incremental market opportunity for carriers that could be worth $10 billion or more in new service revenue by 2017. To win that revenue, carriers and their equipment suppliers need to turn the CPE into the central server of the smart home. This requires a system with the flexibility to effectively support core broadband access service, media streaming, and new smart home service requirements.

Equipment providers need to deliver platforms that can stream content seamlessly to multiple client devices, provide robust device, offer greater security levels with more efficient processor usage and application management capability, and achieve exceptional system stability while handling a large, heterogeneous application load. A key capability for this new generation gateway is virtualization, which serves as the basis for true multi-application operation. Virtualization is a process of running multiple operating systems and applications on a single, shared hardware resource while maintaining isolation and security between them. While it is possible to execute virtualization in a system using software only, this approach faces limitations in terms of resource allocation (which can affect performance) and security. With its newest home gateway network processor, Lantiq delivers the hardware basis for secure, stable and high performance virtualization. Hardware-based virtualization creates two or more virtual machines (VMs) that act as physically separate central processing units (CPUs) or even CPU clusters. To achieve this, the underlying hardware must control access to system memory and peripherals. A virtualized, smart home capable gateway addresses a broad set of requirements: Isolation between applications/services that protects each service such that a crash of software running on one CPU does not disrupt other services; data security and integrity between the different services; prioritization of resources between the virtual entities; ability to securely deliver and turn on/off add-on services from a remote location; remote trouble shooting to reduce the help desk traffic; and flexibility for the user to choose applications from third party suppliers, e.g., an app store.

Hardware virtualization in CPE is implemented by creating different partitions with separated access rights and different operating systems. At minimum, the partition must support one OS for the broadband access and other telecom operations of a gateway with a focus on stability and security. Then a second area, or even multiple, independent areas can be defined for smart home functionality. An important aspect of one or more of the independent area(s) is that they be designed to accommodate applications (provided by either the carrier or delivered as third-party apps) that have much faster update cycles than the core gateway functionality. Critical functional characteristics of hardware-
enabled virtualization include Platform Security, Data Security and Data Isolation, and Resource Control. The home gateway processor requires a hardware root of trust that allows designated VMs to run only code that is authenticated. Combined with secure debugging and secure storage, this establishes platform security.

Data security and data isolation based on hardware controls that isolate the software code (both instructions and data) of each separate VM to prevent unauthorized access and risk of corruption between VMs. Resource control based on automatic hardware limitations to protect on-chip resources and access to peripherals so that the core broadband gateway functions and performance are not impaired by smart home tasks. Importantly, the hardware-enforced VM approach also supports the different life cycles of smart home gateway applications. The requirements of core gateway functionality (broadband access) entail rigorous test cycles to assure stability and assurance that any future field upgrades can be executed with absolute security. Add-on functions, fast changing services and third-party apps that will likely be updated or changed frequently by the end customer benefit from executing on a separate VM.
Virtualization solely at the software level can be executed with the use of specialized Hypervisor software to define virtual processing entities (VPEs) operating in a symmetric multi-processing cluster. This can limit the overall robustness and performance of the gateway, as it is possible that demands of any application or service affect the performance of a critical service. Alternatively, a smart home service container can be bound to a specific VPE and constrained by hardware to use only specified resources to assure that overall performance is not threatened.

The latest generation Lantiq gateway processor integrates multiple Imagination Technology InterAptiv processor cores, an independent trusted execution processor, and multiple dedicated processing engines designed by Lantiq to implement a powerful and flexible System-on-Chip that supports TrueVirtualization. This approach to virtualization uses dedicated on-chip hardware to manage system resources and adds hardware-controlled platform security and data isolation. The trusted execution processor acts as a root of trust to enforce secure boot and secure storage in the CPE environment, achieving best-in-class platform security. By design, smart home software running on the system cannot access the code or data associated with broadband gateway or home network control. Integrated hardware watchdogs also ensure correct operation and, if necessary, force reboot of smart home software without disturbing gateway functionality. Broadband carriers are well positioned to deliver value-added services to residential customers. To succeed in the new smart home market, the carrier point of entry into the home must become more robust, more flexible and more secure. For carriers, hardware-based virtualization results in a platform that is simpler to develop and maintain than a service package that combines separate systems.

Robust functionality is achieved through the combination of hardware-based virtualization and platform security. Support for new and evolving services on a single platform gives a carrier flexibility, potentially improved customer acceptance and faster time-to-revenue. In short, the gateway becomes a powerful delivery mechanism for both traditional broadband access and new smart home applications.

**Product News**

**u-blox: tiny surface-mount GNSS global positioning module supports all satellites**
u-blox announces the CAM-M8C, a small, low profile GNSS positioning module with an integrated wideband chip antenna for reception across the entire L1 band. The module offers simultaneous GNSS operation for GPS/GLONASS, GPS/BeiDou, or GLONASS/BeiDou flavours. TRACE32 allows easy development and reliable positioning anywhere in the world. Featuring industry-leading sensitivity, the CAM-M8C integrates a u-blox M8 satellite receiver, crystal oscillator, SAW filter and low-noise amplifier.

News ID 2942

**PRQA: RT-RK adopts QA·C for automotive software defect detection**
RT-RK and PRQA announce that QA-C has been made mandatory on all RT-RK projects for the automotive industry. The use of QA-C has been imposed by TTTech, the technology leader in robust networked safety controls for automotive, aerospace and other safety related markets. TTTech is based in Vienna, Austria, and uses RT-RK as NSDC (Near Shore Development Center), providing a vital link in their development process, which generates the highest quality code for safety-critical systems.

News ID 2821

**Apacer: PCIe SSDs go far beyond SATAIII in transmission efficiency**
Since the PCIe SSD was adopted by Apple as a standard accessory in MacBook Air in 2013, its excellent flash storage performance featuring high-speed transmission has led the competition to follow, including the fully PCIe SSD-supported Microsoft Windows 8.1 operating system and the new generation Intel CPU chip. According to a survey conducted by the global market research firm TrendForce, the transmission speed of PCIe Gen 2 (PCIe Generation 2.0) surpassed that of SATA III SSD in 2014.  

News ID 2880
Security requirements of the Internet-of-Things

By Christian Eder, congatec

This article explains the security requirements of the IoT, and introduces a starter kit comprising all necessary components to rapidly develop a prototype to test IoT technology as simply as possible.

The fourth industrial revolution (Industry 4.0) is becoming a reality. Driven by the immense possibilities of the Internet, real and virtual worlds are growing closer together, merging in the Internet of Things. The biggest opportunities of Industry 4.0 lie in greater customization enabled by highly flexible production, closer integration of clients into value-added processes and the coupling of production and services. However, tighter connectivity and the associated exchange of large amounts of data also lead to increased security demands. Next to operational safety, which ensures that manufacturing systems and products pose no risk to humans and the environment, a second aspect, namely security, is gaining hugely in significance. Facilities and products, as well as data and know-how, must be reliably protected against unauthorized access and misuse.

Since 2010 – the year the Stuxnet computer worm was discovered – the number of connected automation systems has grown dramatically. Measures to increase the security of such systems have been implemented, but not at the same rate. It is a likely assumption that potential attackers were able to copy from the Stuxnet worm to optimize any future attacks. In 2012, the Carna botnet infected around 420,000 devices that themselves collected information on global IP addresses - even behind firewalls. In 2013, the TRENDnet web camera attack gave unauthorized access to numerous surveillance cameras, including many in the private sector. In 2014, the Linux Dariloz worm infected more than 40,000 routers and set-top boxes based on the Intel x86, ARM, MIPS and PowerPC architectures to steal digital currencies. A greater hacking success of 2014 was Thingbots which infected more than 100,000 smart devices – from routers to TV sets and fridges – and used them as a platform from which to send spam emails. With the increasing number of connected devices, their attraction as a target for attacks is growing. It is therefore high time to give more attention to the issue of security, especially since several billion IoT systems are expected to be in operation by 2020 worldwide. The figures differ widely from one analyst to the next, but are consistently quoted to lie in an impressive single to double-digit billion range.

While most companies have already put in place good security measures for their servers and workstations, IoT devices tend to get forgotten. But even a connected thermostat can become a danger if it is not adequately protected. In the hands of a cyber-criminal, the device can become one of many soldiers for a big attack, or is turned into a silent spy who collects sensitive data in the background and passes it on. For most application developers, device functionality is their first and foremost concern; few will have specialized in data security. Under those circumstances, a platform that has been optimized and tested by security experts is required. But what should such a platform look like if it is to benefit a wide variety of applications? There are four fundamental aspects that need to be considered: reliability, connectivity, manageability and security. Reliability is strongly determined by the hardware. A design must be durable because - unlike classic office PCs - IoT devices don’t have an 8-hour day. Any IoT
A TPM can generate true random numbers, and that is extremely important for any encryption. Software-generated random numbers are created on the basis of an algorithm that is to some degree predictable and hence less secure. The TPM is therefore also a good place to store algorithm keys securely. Many modern computers are already equipped with a TPM, but unfortunately this functionality is rarely used. This may have something to do with the fact that programming requires some depth of encryption expertise. If the platform itself uses TPM, the application developer does not need to go into deep details.

The next billion of IoT devices also need to be managed safely. Remote access and maintenance have to be performed via secure data links. They are also needed to ensure that devices are clearly identified. TPM can help authenticate devices; when there are only a few IoT devices it is quite easy to keep the software up-to-date and apply all necessary security and feature updates. To do the same for millions of devices, special manageability features are required. Technologies from the telecommunications sector can help: TR-069 is a protocol for exchanging data between the server of a communications provider and an associated customer device. This protocol is used, for example, for secure remote configuration of DSL routers. OMA DM is used in mobile phones for initialization and configuration, upgrades and fault management. This protocol is also perfect for IoT applications.

Unlike standard PCs, IoT devices have a clearly defined set of functionalities. This allows white-listing software so that only permitted and desired software can actually run; malware cannot possibly be activated. To implement the diverse demands on IoT devices quickly, easily and securely, Intel has worked with Wind River and McAfee to develop a software package that is tailored to the specific requirements of the IoT. The suitable hardware platform for the Intel Gateway Solution for IoT is tested by Intel. Thanks to the validated combination of hardware and software, the developer of an IoT application is free to focus on device functionality, safe in the knowledge that most security aspects are already covered.

In order to test this technology as simply as possible, congatec has put together a starter kit comprising all necessary components to rapidly develop a prototype. The kit contains a Qseven module based on the Intel Atom E38xx with a footprint of 70x70mm the module can be integrated into almost any IoT application. In addition, the kit includes everything from cables to display and carrier board to test the Intel Gateway Solution for IoT directly on a certified hardware. This starter kit, a successful combination of technologies from Intel, Wind River, McAfee and congatec, makes both current and future IoT challenges easier to handle, especially as far as increasingly important security aspects are concerned.

The congatec IoT kit provides a complete set for the rapid prototyping of embedded IoT applications. In addition to a Qseven Computer-on-Module (COM) based on the latest Intel Atom processor technology, a compact IoT carrier board and a 7” LVDS single touch display with LED backlight, the starter kit contains an extensive set of accessories including AC power supply and 802.11 WLAN antenna with IoT Wind River Linux image on USB stick. With the provided set of cables, developing an IoT demo system takes a matter of minutes.

The Qseven module is equipped with the Intel Atom E3827, with 2 cores, 1MB Cache, 1.75 GHz, 8 watt TDP, 2GB onboard DDR3L memory and 4 GB onboard eMMC4 media storage. Compared with the previous model, the integrated graphics is significantly more powerful, supporting DirectX 11, OpenGL 3, OpenCL 1.2 and high-performance, flexible hardware decoding to decode multiple high-resolution full HD videos in parallel. The processor natively supports up to 2,560 x 1,600 pixels via DisplayPort and 1920 x 1200 pixels via HDMI. It is further possible to connect up to two independent display interfaces via 2x 24-bit LVDS. Native USB 3.0 support ensures fast data transmission with low power consumption. A total of five USB 2.0 ports are provided, one of which is designed as USB 3.0 SuperSpeed.

Three PCI Express 2.0 lanes and two SATA ports with up to 6 Gb/s enable fast and flexible system extensions. Use of an Intel I210 Gigabit Ethernet controller promises best software compatibility. A MIPI camera interface, an I2C bus, an LPC bus for easy connection of legacy I/O interfaces and Intel High Definition Audio complete the feature set.
Siemens: Nanobox and Nanopanel PCs concentrate high performance in small space

With the Nanobox PC Simatic IPC227E and Nanopanel PC Simatic IPC277E, Siemens is presenting a new generation of especially compact, rugged devices for industrial use. The Simatic IPC227E Box PC is available with or without a PCIe slot. The Simatic IPC277E is a Panel PC equipped with 7 to 19 inch, wide-format touch displays. Intel dual and quad-core Celeron processors deliver high performance in a compact design. The enclosure of the smallest version of the device has a volume of just one liter.

News ID 2900

Conrad expands range of development and prototyping kits

Conrad Business Supplies announced that a number of new products have been added to its already expansive range of development and prototyping kits. Development kits are essential in simplifying and accelerating the new designs of innovative applications across multiple sectors and technology segments in the electronics industry. Conrad now offers over 5,000 semiconductor development and prototyping products, accessories and tools. New additions to the product range include products from well-known and respected manufacturers such as Microchip Technology, Texas Instruments, Freescale Semiconductor, STMicroelectronics, 4D Systems, Embedded Artists and MikroElektronika.

News ID 2881

COMSOL: Multiphysics v 5.1 supports building and sharing of simulation apps

COMSOL Multiphysics version 5.1 delivers the first integrated software environment that supports the creation of multiphysics models and simulations as well as the building and sharing of easy-to-use simulation apps. COMSOL released COMSOL Multiphysics software version 5.1, an integrated simulation environment for building multiphysics models and for creating and sharing easy-to-use simulation apps.

News ID 2941

IAR: Embedded Workbench enables development for MSP432 MCUs from TI

IAR Systems announce early support for the new ARM Cortex-M4F-based MSP432) from Texas Instruments. The support is available in the development toolchain IAR Embedded Workbench for ARM, which enables developers to take full advantage of the ultra-low-power features of MSP432 MCUs, as proven in recent ULPBench scores.

News ID 2875

powerBridge: GPGPU AMC module provides up to 4 NVIDIA Tegra K1 processors

The new CONCURRENT Technologies GPGPU AMC module has up to 4 NVIDIA Tegra K1 processors. Each Tegra K1 processor consists of a quad-core ARM Cortex-A15 CPU and 192 NVIDIA Kepler CUDA GPU cores which are linked together in the board to create a highly power efficient computing module that easily scales with Fabric Interconnect Networking Software known as FIN-S.

News ID 2826

GOEPFL: testing and programming of ultra-low power processors

GOEPFL electronics extends the VarioTAP processor emulation technology for the Kinetis L series by Freescale. The processor is reconfigured to provide design-integrated test and programming instruments via the SWD port. The user can select the corresponding processor to test and validate the connected hardware as well as program Flash memories.

News ID 2873

Ready for OEM applications

As processing performance continues to improve, ECRIN Systems is dedicated to minimize the SWaP envelope of OPALE V2 series. High-end computing performance in a 2U chassis with a depth under 20” (492mm) OPALE V2 Compact fits most any rack space. Distinctively customized oriented thanks to our in-house design team, ECRIN Systems will help to personalize your computer and give you competitive advantage in the industrial world.

- Flexibility with Single XEON performance + ECC Mem or leading edge Core-i7/15/3 Haswell family
- Expandability with 4 full-height and full-length I/O cards into PICMG 1.3 backplane
- PCI Express Rev 3.0 up to 8 Gt/s
- USB 3.0 (500v/s), SATA 3 (600v/s) with RAID 0/1/5/1+0
- High reliability, continuous operation
- High shock and vibration resistant
- Efficient thermal concept to get higher MTBF
- Local I/H/M and Remote Active Management to detect errors before they occur
- Reduced TCO with reporting and Log file for downtime in harsh environments
- Long life: up to 7 years with revision control
Security squared: system board featuring encryption technology

By Harald Maier, TQ-Systems

In the age of the Internet of Things, protecting embedded systems has become more crucial than ever. In response, TQ-Systems has integrated an encryption chip into its new embedded computer boards which provides reliable protection against software manipulation and IP theft.

At present, a vast number of new applications for networked IoT systems are being created for private and professional consumers – be it for smart home or smart factory systems, for digital signage players in shopping malls, for outdoor areas, buses and trains or other networked devices, and for all sorts of machines and equipment. To their users, these applications all open up new realms of experience and deliver the added benefits provided through networking.

The new applications, however, do not necessarily always have to be killer-apps, as often described in cyber-virtual industry 4.0 applications. In most cases, continuous system monitoring often suffices for users and OEMs. This big data on status and usage enables them to improve maintenance cycles and increase availability. License and warranty management can also be planned according to usage times or frequency. For virtually any application with an intelligent embedded system, completely new sales and service concepts are possible.

The advantages of networking, however, also bring risks. Previously, embedded systems in machinery and equipment were basically inaccessible from outside. Potentially, only someone could tap or manipulate the code by connecting locally via proprietary interfaces. Today, IoT connected systems have an IP address, which theoretically can be accessed from anywhere in the world and, consequently, the risks of code piracy or malware implementation are mounting progressively. Increased protection is therefore mandatory.

Various methods of protection are available. Hardware solutions offer a particularly efficient and safe method of protection for software and IP (Intellectual Property). This is why TQ-Systems opted for Gemalto encryption technologies, which are also available as components. This company is one of the leading global suppliers in this field. In the IT world, its solutions protect anything software-operated: from ERP systems on (cloud)-servers to mobile client solutions, right up to ATM machines. The Sentinel HL components are also an ideal protection and licensing solution for embedded system software.

In particular, the Gemalto Sentinel HL chip convinces embedded developers with its Secure Element chip, which presently offers the highest level of protection against malware attacks on hardware and includes, for example, differential power analysis (DPA) and reverse engineering via electron microscopy. In addition, it supports deployment in industrial applications with its temperature range of -25°C to +85°C. Sentinel HL also offers the function AppOnChip which enables a non-separable connection of the application to the hardware key. The code is only available encrypted in the processor cache and, if accessed, is thus useless for IP thieves.

Integrating the AppOnChip into the application is a simple procedure requiring no engineering effort. An automated routine delivers blocks of code to the application functions which are compatible with the AppOnChip feature. These code blocks are encrypted and signed and can only be run on the hardware key. Therefore, without a hardware key, the application cannot be run. The protected code blocks do not occupy any of the hardware key memory so that software manufacturers have maximum memory capacity for license storage. AppOnChip is applicable on x86 Windows-based 32-bit systems.EXE files and further extensions for additional OS and processor platforms are in preparation.

The AppOnChip function makes Gemalto Sentinel one of the most secure solutions available in the market today. Apart from firewalls, VPNs and encrypted communication, the Sentinel HL carries out extremely important core functions to protect IoT-connected intelligent embedded devices. Plus, as it is not even necessary to update the software on the keys deployed in the field parallel to the release of a new version, the solution is suited
INTERNET-OF-THINGS – SECURITY

to long-term available embedded applications with a frozen software status. Further to the high-level protection functions, Gemalto Sentinel also provides extremely granular software licensing and authorization management functions. Function unlocking or system activation is carried out via licenses, which can be enabled or disabled right down to feature level. In this way, defining a device function is an extremely flexible task. Function upgrades are also possible without any hardware having to be exchanged. With the aid of usage reports, OEMs can even monitor the usage of individual features, enabling the implementation of new billing, warranty and service concepts. This big data also contributes valuable information to the future development of applications. Consequently, the added value of security for the Internet of Things in turn delivers OEMs added value for the further development and monetization of their solutions.

The software licensing and authorization management functions can be used on embedded devices, on the cloud server, on-premise as well as on mobile apps. The tiny, fingernail-sized Gemalto chip enables IoT application developers to deploy extremely important additional functions in order to be able to protect the entire IoT application on each participating device from one single source. This significantly reduces the complexity of the IoT security issue for OEMs.

This comprehensive set of features has inspired TQ-Systems to equip their new QSys Board with the new Gemalto Sentinel HL Chip. And, in many other ways, the board is also ideal for embedded IoT applications, as it excels with a variety of security functions, for example, integrated Trusted Platform Modules (TPM) for secure boot function support. To ensure compatibility to TPM 1.2, TQ-Systems equips the board with the Infineon chip SLB9635 or SLB9660, for example. And if the TPM 2.0 standard is required, the QSys Board is also available with the SLB9665. This new, square board boasts an extremely wide range of pre-integrated security functions which offer a significant security bonus compared to other NUC form-factor-based solutions. The QSys platform can also be customized to suit individual requirements. For TQ in-house development and production, ‘Made in Germany’ security and reliability are key issues and this also applies to many OEMs, for whom – next to the integration of the Gemalto chip – in some cases is one of the main security criteria. Incidentally, as the embedded computer board is modeled on the Intel 4x4 inch NUC form factor, users are able to exploit the advantages of the widely spread ecosystem, without having to forego extremely reliable, industrial-grade hardware. And, in order to comply with European metric sizes, the outer dimensions of the board were reduced to 100 mm (3.937 inch), so that the board can be used in both worlds alike - with no compatibility issues.

Figure 2. Gemalto delivers powerful tools for licensing embedded software, which standardizes or automates a variety of processes.

Figure 3. Compact QSys board with its dimensions of just 10 cm x 10 cm allows the fast and inexpensive implementation of powerful and yet passively cooled embedded systems.

www.embedded-news.tv
The Video Portal for the European Embedded Market
Technical Videos, Video Interviews, Demos & more about:
- Chips & Components
- Tools & Software
- Boards & Modules

www.embedded-news.tv
Software development teams across industries and disciplines are under more pressure than ever. Under pressure by consumers to develop new, better bells and whistles quickly. Under pressure from industry and government to ensure their code adheres to critical coding and safety standards. And under pressure from senior management and shareholders to make sure their applications are free of defects that are costly, both financially and to their company reputation. From multimillion pound medical devices with sophisticated software to visualize data, to credit card readers at our local grocery store, to the infotainment systems in our cars that we all take for granted, virtually everything needs software to make it work these days. We've become accustomed to everything we touch being connected and optimized for our convenience.

These days, we call this convenience the Internet of Things (IoT). The term is new but the concept isn't. In fact, we've been trying to get the Internet to do our bidding since way back in 1990 when John Romkey invented a toaster that could be turned on and off over the Internet. We've come a long way since then, but the general idea – and challenge – is just about the same, only now with much higher stakes. The question is, what do manufacturers need to do to ensure the security of their code and ultimately the safety of the consumers of their products? Especially in the automotive industry the Internet of Things intersects with connected cars – automobiles that are largely operated by software.

Code security and product safety rarely intertwine where automobiles are concerned, but the industry is quickly realizing correlations between the two. Software security is any action taken to protect the code from malicious attacks – attacks that can lead to safety issues with the device the code controls - anything from annoying and harmless issues (think spam finding its way into your email inbox) to potentially fatal safety concerns, such as creating a malfunction in a car cruise control system.

This type of car hacking, made possible by security weaknesses in code, may be sensationalized in the media, but is unfortunately becoming a reality. Although automobile hacks have yet to become commonplace, they do happen. Recently in Canada, authorities attributed phantom car break-ins to hacking, and found that a simple program could be written in a matter of hours that jammed the message from the key fob to the car, disabling the locking system. In a more sensational example, BMW recently learned how seemingly small coding errors can become monumental and costly problems for a company. Over two million of the luxury vehicles were identified as at risk in January 2015, six months after the German automobile club ADAC intercepted network traffic from cars to send commands telling them to lower windows or open doors. In many reviews of the issue, the culprit is being identified as the simple difference between using an open HTTP protocol rather than the encrypted and secure HTTPS protocol. A static code analysis and review tool, such as Klocwork static code analysis solution alongside comprehensive threat modeling, is able to mitigate these types of mistakes, although it is important that these fundamental changes to the mindset of development teams are adopted.

The good news is that the automotive industry has some precedent it can lean on rather than inventing secure development processes completely from scratch. Telecom companies faced a similar challenge several years ago when the potential ramifications of their devices being the only thing standing between the consumer and complex, embedded software code became evident. The inherent challenge to this IoT problem is, how do manufacturers ensure that the software, deeply embedded and intertwined with their hardware, is secure, even when there are countless potential consumer environments that their product could
end up in? Clearly, the software development processes of old, one-to-one testing systematically, are not feasible, whether you’re talking about mobile phones or the connected car of today. The amount of testing that would need to take place, when taking every operating system and hardware possibility into consideration, would be virtually impossible.

Telecom managers in the beginning made the choice to take a huge step forward: providing their engineers with processes and tools that addressed security throughout the software development life cycle. This mitigated security risks up front, well before code was deployed. Benefits were not limited to security improvement though; they extended to speedier development processes and simplified adherence to industry and government-imposed standards. This new development era changed everything — for example, the process from fixing security bugs after they already caused problems to finding them before they caused problems in the first place. Automotive is at the right juncture now to take a page from the telecom playbook, to begin standardizing processes and procedures to ensure more secure code development, and hopefully avoiding the BMW recall scenario — or worse.

In another parallel with telecom, automotive manufacturers are learning now that they can’t pass all of the responsibility for security along to the companies that supply the features and related code in their product. In other words, their product is only as strong as their weakest supplier code. In both industries, companies are not only supplying products (cars, phones, etc), they’re now cyber-security managers as well. Seems easy — just make sure everything on the version today of the assembly line (virtual or not) meets security criteria. But just as with the evolution of software development, this is also not your grandfather’s manufacturing. Now, managers at car manufacturers must adjust quickly to development challenges to ensure security within everything that makes up their cars. These same managers are also tasked with quickly adding the latest and greatest features and consumer-demanded innovation in order to stay competitive.

All this technological innovation means compiling pieces and parts of hardware and software into functional end products; the more sophisticated the product, the more lines of code. The more lines of code the more room for security breaches. And with the average high-end car sporting a whopping 100 million lines of code (more, incidentally, than a fighter jet) the fundamental change in products today vs. products of yesteryear creates some chaos. That brings us not only to the evolution of the assembly line, but how software development in and of itself has changed. Once a single developer created code to solve a problem. Now, software developers are like artists, assembling parts from various sources and piecing code together to make a functional end product. The parts that become the product can come from development, from open source code bases, or from commercially available code. All of it has to be secure, whether it was written in-house or not, and how it interacts once it’s pieced together is a consideration as well.

How can companies protect themselves — their reputations, their financial stability, and their customers? They can do it by knowing, understanding, and taking responsibility for all of the code that makes up their product — not just what their own developers have written. The bottom line is that companies need to open the aperture of what they’re securing, and they need to do it before they become the subject of dramatic news headlines. And, those who are part of the supply chain need to tighten processes.

Companies like Rogue Wave continue to lead the curve of software development, providing market-proven solutions, processes, and tools for companies who might not know where to start to ensure security in their code — and ultimately the safety of their automotive products. Putting security first means management committing to three things: companies have to educate their developers and provide policies, processes, and tools that take the guesswork out of security.

The connected car emphasizes the importance of getting security under control as soon as possible. Nowhere is this more evident than in what’s becoming the automotive industry endgame: self-driving cars. Self-driving, or autonomous, cars are the next evolution in transportation and trials are already underway by groups wanting in on the action, from traditional car manufacturers to organizations such as Google and Oxford University. It should come as no surprise that a lot of features in cars today are essentially test beds for future self-driving technology, such as radar-assisted cruise control, adaptive stability control and automated parking.

We must get security right, right now, before more complex systems such as these start changing the lives of people. The car of the future is exciting, and it’s not innovation that needs to slow down. The process of getting products to market simply needs to shift to compensate for new dynamics. Putting in place solid, repeatable processes, along with the right tools and developer education will surely become a priority for companies across the automotive supply chain.

INTERNET-OF-THINGS – SECURITY

Hardware & software for CAN bus applications...

NEW

PCAN-GPS
Programmable sensor module with CAN connection for position and orientation determination. Development package includes the library and programming examples.

NEW

PCAN-USB FD
CAN-FD adapter for USB 2.0 with galvanic isolation, incl. the software PCAN-View for sending, receiving, and recording CAN-FD messages as well as busload measurement.

PCAN-Explorer 5
Universal CAN monitor, symbolic message representation, VBScript interface, integrated data logger, functionality upgrades with add-ins (e.g. Instruments Panel add-in).

www.peak-system.com
Embedded systems best suited for the Industry 4.0 project

By Ingrid Einsiedler, Kontron

This article describes how Kontron, together with technology partners like Intel, Wind River, Telekom and Salesforce, is already working on solutions that are founded on a standard base of embedded systems, which can be connected to the Internet of Things (IoT), and which also offer cloud solution approaches.

In the future, companies will network their machines, storage systems and operating resources globally as Cyber-Physical-Systems (CPS) – according to the implementation recommendations of Acatech in relation to the future project Industry 4.0. To what extent are the technologies for such a task already available today? If we look at manufacturing more closely, then we see that we are dealing with a wide variety of different computer-based components – visualisation units, BV systems, control systems and the like. All of these devices can already be realised nowadays using a standard technological basis. For example, Intel-based COM Express modules, which can be scaled across a broad performance range. The COM Express modules from Kontron cover a wide spectrum of application areas, with performance ranging from the high-end 1.7 GHz Quad-Core Intel Core i7 processor to the cost-optimised Intel Celeron or Intel Atom processors. Based on these COM Express modules, the company launched an IPC switch cabinet for the automation area one year ago as a new member of the KBox IPC product range.

The new IPCs have been designed for industrial control activities and are extremely scalable, from entry level to high-end solutions. All four systems stand out thanks to their industrial design and long-term availability. What’s more, based on individual requirements they can be equipped with industrial I/Os, field busses, industrial Ethernet interfaces and/or wireless or wired communication interfaces via mPCIe or PCIe slots. Thanks to the modular structure, the CPU selection is very flexible and always up to date. Automation providers and OEM customers in the field of mechanical and plant engineering will thus benefit from efficient customisation options on the basis of standardised component groups. And developers in all markets benefit from the tried-and-tested eco-system of the leading PICMG specification for computer-on-modules. Generally, the middleware package standardises access to all Kontron embedded platforms, irrespective of form factor or operating system. And not just for one product category, but for the entire portfolio. Kontron EAPI is compliant with the EAPI of PICMG, but extends its range of functions to include function calls, such as for basic system information (e.g. CPU, RAM, HDD, battery), temperature and voltage meters, CPU performance, and temperature control. What’s more,
the Kontron EAPI also supports different form factors, such as COM Express, SMARC and motherboards, and also allows remote access via the Internet. Developers thus benefit from the security of an independent, standardised programming interface combined with a high degree of convenience and an extended range of functions. Application-ready for the IoT: In June Kontron introduced a box PC based on the SMARC module that supports the Intel Gateway Solutions for the IoT (code name Moon Island). In combination with KEAPI, this application-ready M2M platform (Machine-to-Machine) offers IoT gateway intelligence, which is standardised and easy to use. This allows OEMs to connect their distributed systems seamlessly via wireless networks such as LTE, GSM or WLAN.

Numerous industrial interfaces also support IoT integration for both new as well as existing applications. OEMs and operators benefit from a pre-validated platform based on recognised standards, which can be used to record, evaluate and use all Big Data. The Intel Gateway Solutions for the IoT include Wind River Intelligent Device Platform XT 2.0 as well as McAfee Embedded Control 6, and they enable the development of intelligent gateways, such as the mentioned box PC. Such intelligent gateways are decisive system extensions when it comes to ensuring the ability to connect to the latest intelligent infrastructures. In April 2014 Kontron entered into cooperation with Deutsche Telekom. The objective of this cooperation is to push ahead with the development of M2M solutions. For distributed systems that require a mobile communication connection, the embedded product supplier offers industrial nodes, which are needed to connect end devices to cloud applications in the IoT.

Kontron M2M Smart Services Developer Kit is part of the offering for developers of Deutsche Telekom: it offers scalable processor performance, includes all relevant drivers and protocols, and is also flexible with regard to applications and operating systems. The kit also includes a pre-qualified setup for mobile network operators. The system is PTCRB certified and is approved for use in mobile networks. This reduces development time and costs for customers: The approval and certification processes of the network operators, which applications have to pass through before they can be used in their networks, are thus streamlined. For the fast development of applications with local wireless connectivity, the kit supports 802.11a/b/g/n WLAN (Wireless Local Area Network) and 802.15.4 WPAN (Wireless Personal Area Network). Cellular network connections to the cloud applications are also offered through a pre-installed 3G WWAN (Wireless Wide Area Network), which can be extended with a second PCI Express 3G/4G module to provide redundancy. And thanks to the optional smart video and audio module, the system can be extended to provide face-to-face communication. The company Salesforce views itself as the cloud market leader. In February, Kontron announced its cooperation with Salesforce.com at the Embedded World exhibition and conference. The companies are working together on concept studies for the IoT and the Internet of Customers (IoC). The jointly developed concept studies, which are based on Salesforce1, enable developers to implement applications more quickly with minimal technical risk. They also generate inspiration for new designs ideas, in order to drive ahead with the IoT. Virtually all applications that need devices, that need to connect to people and that are found in markets like industry, medicine and Points-of-Sale, can benefit from the IoT and IoC concepts of both companies. These studies simplify development significantly, as they enable developers to concentrate fully on the application level, which means no expert knowledge on computer hardware or software technologies is needed. Kontron assumes that new business models will emerge based on the IoT, which will have a much higher level of development than traditional areas of application of M2M communication. And for a successful IoT implementation, it is no longer so important to collect as much device information as possible. What is more important is to make use of the digital connection, in order to obtain new findings and to connect people with people and devices with people. Together with its technology partners, the company offers a unique range of solutions from a single source, from open, IoT-ready platforms like the compact box IPC, HMIs, rack mounted IPCs and M2M gateways, to the highly-available and compact SYMKLOUD cloud server in connection with the respective software platforms. This enables innovative Industry 4.0 solutions to be implemented economically for both current and future requirements.
As a concept, the Internet of Things embraces an enormous span of commercial, industrial, military and consumer paradigms. In the military, for example, there has long been talk of network-centric warfare and the connected battlefield. These concepts have at their heart the principle of powerful machines – often vehicles – with substantial embedded computing power and equipped with multiple sensors communicating with each other, sharing information – and becoming collectively smarter as they learn from each other. In industry, GE has coined the term Industrial Internet – an application-specific instantiation of the Internet of Things. In today's connected world, machines can communicate and coordinate with each other in ways that were not before possible. These brilliant machines are changing the way businesses work, enabling them to optimize efficiencies, boost productivity, reduce costs, and bring products and services to market faster. There's a major transformation taking place in industry.

What are these brilliant machines? They share numerous characteristics. They are, for example, equipped with processing power that can run to hundreds of GFLOPS – often enabled by GPGPU (general purpose processing on graphics processing units) technology with its massively parallel architecture. Those embedded computing subsystems are small and lightweight, enabling them to be deployed in the most challenging environments. They’re designed to require very little power: the GE mCOM10-K1 rugged COM Express module, for example, delivers 326 GFLOPS of processing power yet consumes 10 watts or less. And, because the Industrial Internet encompasses the harshest, most demanding locations – energy exploration, transportation, heavy industry and so on – they are rugged, able to withstand extremes of temperature, vibration, shock, contaminant ingress, and so on. They are designed to operate right out at the furthest edges of the network. That massive processing power is needed because these brilliant machines are equipped with, or have access to, multiple sensors of different types, collecting enormous amounts of data that needs to be captured, processed, analysed, stored and transmitted.

Powered by the Industrial Internet and with brilliant machines at its heart, this new way of doing business is revolutionizing how decisions are made and generating unprecedented value. Combined with the more recent advances in computing, information and communication systems - in addition to data collection and data sensors - the Industrial Internet delivers the power of data and advanced analytics. With intelligent insights, decision makers can drive smarter design, operations, and proactive maintenance as well as higher quality service and safety. The Industrial Internet is taking place through the convergence of the global industrial system with the power of advanced computing, analytics, low-cost sensing and new levels of connectivity afforded by the Internet. It brings together three key elements: brilliant machines, advanced analytics, and people at work. It drives powerful outcomes and affords new possibilities for industry - enabling businesses to reach never seen before performance levels.

Take, for example, an oil and gas company that can increase asset performance by 10% and more, or improve production uptime by more than 20%, or lower overall total cost of ownership by 15%. These are significant outcomes that companies are achieving today by connecting their machines, data and people and leveraging well-orchestrated analytics. Even a 1% productivity increase in the oil and gas industry from the application of the Industrial Internet could generate approximately $90 billion of value. Or supposing a manufacturer could drive inventory costs down by more than 15%, or improve quality by over 10% or enable labour efficiencies by 30%. These are the real-life results of forward-looking manufacturers that have taken steps to leverage the power of the Industrial Internet. Such numer-
uous improvements at scale - even smaller outcomes such as 1% reduced downtime on critical equipment - can drive big changes in performance and operating margin.

Industrial Internet-enabled solutions are changing the game for industrial companies. They’re enabling businesses to leverage big data to drive performance optimization in their current operations. They’re also enabling predictive analytics so businesses can take a proactive approach to minimize unplanned downtime. By connecting machines and industrial big data, the Industrial Internet enables companies to better understand their operations. They can visualize how their assets and processes are behaving in real time and what events occurred. What’s more, those companies can drive operations to their full potential based on key parameters such as market demand, weather conditions, plant environment, load balancing, and other business objectives.

A mining company, for example, might need better visibility into its complex production processes to achieve optimal control of operations. Solutions powered by the Industrial Internet can, for instance, help monitor processes and control loops. So when a control loop is insufficient, it is possible to quickly identify what has changed and why, and get to the root cause of the issue to gain better insight into process and control problems to minimize deviations outside set parameters. The result: greater consistency, process optimization, and safe production.

What’s more, to capture the full potential of optimization, a company not only needs to understand the current state of its operations, but also have the ability to predict what will happen before it does. While industrial machines have always issued early warnings, it was in an inconsistent way and in a manner where details often crowded out the most critical information. The advent of networked machines with embedded sensors and advanced analytics tools has changed that reality. Now it is possible to leverage advanced analytics in context to predict, providing real-time operational intelligence to the people who need it to make the best decisions. Thus, companies have intelligent foresight to take appropriate action and proactively avoid issues before they occur - a powerful capability that allows for continuous operation.

Let’s go back to that oil and gas company example. A lube oil cooler fails on an offshore oil platform, a pump can fail, or trip offline. An Industrial Internet-enabled solution can provide powerful analysis so a problem can be identified such as high water content in the oil cooler before a failure occurs. And then communicate to the right people in the right place at the right time the need to inspect the pump, avoiding downtime and costly long-term damage to the bearings.

To help companies take the Industrial Internet journey, GE has developed what it calls the Industrial Internet Maturity Model. It is designed to help assess where an organization falls on the spectrum of expected maturity or capabilities within the Industrial Internet and discover the best solution pathway to achieve its business priorities. Based on a series of progressive questions, this model provides a personalized high-level view of an organization current state and recommends a solid solution roadmap. It reveals areas that have not reached their full potential and highlights where an organization aspires to be within the journey. Business priorities are also aligned with the model results, thus targeting the right business solutions in support of achieving that Industrial Internet-inspired vision of a company.

There are five key steps in the model that build on each other to help reach performance optimization. 1) Connect: provides the foundation to connect machines and enables the collection of data from assets and processes as well as management of that data to derive value. 2) Monitor: focuses on helping a company understand the performance of assets and processes, and visualize what events are happening. 3) Analyze: helps determine the root cause of issues based on historical and real-time data to enable an understanding of relationships, correlations, and trends, and to enable effective troubleshooting of problems. 4) Predict: focuses on providing foresight into impending problems so issues can be avoided before they occur and drive greater process consistency and asset uptime. 5) Optimize: maximizes the performance potential of assets and processes to achieve a company’s desired outcomes and leverage the benefits of the Industrial Internet.

The value of the Industrial Internet Maturity Model is that it provides a solid solution path towards optimization. The assessment can be done across various levels - from core assets and adjacent assets, to across a facility and enterprise. A company can understand where its business is today in terms of adopting the Industrial Internet and determine where it wants to be in the future. And hence, that company can align the steps it’s going to take with solutions that help meet the business objectives it has. Ultimately, the Industrial Internet allows organizations to combine brilliant machines with best-in-class analytics to deliver valuable new insights that were never before possible. The results of these powerful analytic insights can be revolutionary, enabling a business to: 1) Avoid unplanned downtime with insight into the equipment function down to the component level with machine sensors and big data analytics, which allow proactive action to be taken for continuous operation. 2) Maximize profitability by managing equipment assets with insights from big data analytics, which enables increased uptime, production, efficiency, and throughput. Using analytics for operational efficiencies can drive even greater profitability for industrial machines. 3) Transform a company’s technology infrastructure by leveraging advances in big data analytics, mobility, data visualization and cloud computing, which changes the operating landscape of today’s industrial companies and creates profit opportunities.

GE believes the Industrial Internet unlocks new possibilities and drives transformation by connecting brilliant machines, advanced analytics, and people at work. With the power of the Industrial Internet at work, we’re already seeing an impact on industry. And without doubt, early adopters will position themselves to reap first-mover competitive advantage. Forward-looking companies have begun to embrace the Industrial Internet to drive new performance highs and generate value like never before. They’re leveraging connectivity and analytics to achieve their business priorities - whether it’s increasing throughput, improving product quality, driving resource efficiency, shortening response times or other valuable outcomes. The Industrial Internet is a journey - one that can lead businesses to a new wave of productivity gains and performance optimization. And it has meaningful implications for us all.

### Product News

**ADLINK: COM Express basic Size Type 6 COM with AMD Embedded R-Series APU**

ADLINK introduced the Express-BE, a COM Express Basic Size Type 6 computer-on-module based on the 2nd generation AMD Embedded R-Series APU (Accelerated Processing Unit, which combines the CPU & GPU on a single System-on-Chip, or SOC) with A77E FCH, delivering power efficiency and high definition visuals to high-performance medical imaging applications. The Express-BE with AMD R-Series APU supports up to four independent displays—at mid-power range (17W~37W) and with resolutions of up to 4K x 2K @ 30 Hz—from a single system driving multiple screens without the need for a discrete graphics card.

News ID 2896
On the way to significantly boost market share

The long-term company goal of ADLINK is to become one of the two global leading vendors in each relevant embedded computing market. To achieve this, the company is investing heavily in Germany and Europe. This article explores the growth potential.

Adlink is a rapidly growing international provider of application-ready intelligent platforms and embedded computing products for enabling the Internet of Things. The company supplies system engineers and architects with embedded computing solutions, high-speed data acquisition cards/modules, ruggedized mobile computers, and a variety of measurement and automation technologies. It also provides design and manufacturing services that enable end users and partners to meet customized requirements for several different industries.

The company has operations in China (Beijing, Shanghai, and Shenzhen), Germany, Japan, Korea, Singapore, and the United States. Growing at a strong compound annual growth rate (CAGR) of approximately 18% through the past decade, it generated revenues of $218M in 2013. The company supports a variety of vertical applications within defense, factory automation, medical, transportation, energy/power, telecommunications, and test and measurement sectors.

Adlink provides embedded computing platforms and building blocks for the creation of modular and scalable IoT product designs spanning end devices, data collection and processing systems, intelligent gateways, and more. The company’s growing OEM/ODM design and manufacturing services will further facilitate engineering efforts across a variety of industry applications. It plans to continue building on its intelligent platforms and integrated solutions with more software and services – which will also include support for more cloud-based services in accordance with the continued proliferation of cloud computing and software-as-a-service business models.

The products have earned their stripes in the field over the past decade with their close relationship to Intel’s platform, as a Silver Windows Embedded partner, and Wind River. As one of only five Premier Partners within Intel Internet of Things Solutions Alliance, formerly the Embedded Solutions Alliance, it is well positioned to remain at the front of new embedded technologies with a faster time-to-market for new designs than most competitors.

While it has a long-standing history within the telecommunication and networking industries supplying ATCA-based solutions equipped with the latest Intel platforms, the company is far from being a typical board supplier from the Asia-Pacific region. The company continues to build support for more of the IoT solution stack (which includes connected hardware, application software, middleware, and cloud services), particularly around software/middleware, to serve as a one-stop-shop for most end users. The traditional data acquisition hardware and software products (and expertise) facilitate one of the major pain points for deploying IoT-driven big data applications – collecting and managing progressively more data from a growing continuum of devices. Further, its software solutions, which at the moment principally enable monitoring control and active management applications, are a starting point to which OEMs can add their own big data analytics or application software on top. The company will offer progressively more flexibility and variety with its embedded software offerings as it plans to integrate and partner with more third-party solutions, with cloud management being a major point of focus.

The Smart Embedded Management Agent (SEMA), which comes supported by the majority of board and system products equipped with a board management controller, enables monitoring and collection of systems performance and status information from the embedded hardware. The SEMA cloud solution pushes system data to the data center server through any kind of TCP/IP connection as a standard.

<table>
<thead>
<tr>
<th>Availability of the SEMA Cloud Management Systems</th>
<th>Protocols</th>
<th>DLMM-ARM 5.2/600</th>
<th>Intel Core-i3/5/7</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBC</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Qseven</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qseven</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XMM-Express</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mini-ITX</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

ADLINK is establishing the SEMA cloud connection as a standard.
connection – ultimately enabling easier access to data and analytics through any commercial cloud portal. Adlink selected Gemalto in May 2014 as its partner to complete the cloud integration, enabling remote system monitoring and real-time maintenance for connected devices using SEMA via a secure web-based dashboard.

The company also offers industrial mobile computing products such as Smart Panels, rugged tablets, and handheld mobile computers supporting Android and Windows operating systems. The COM products span a variety of architectures such as COM Express, SMARC, Qseven, and ETX. By supplying a flexible product portfolio for OEMs to easily augment their designs with a variety of peripherals and functionality, OEMs can focus on differentiating their products and reducing time-to-market. The company also supplies a variety of other embedded computing products such as slot SBCs and carriers, ATCA boards, CompactPCI boards, VPX blades, embedded flash storage, chassis, and more.

Adlink offers a swath of project and design services and support spanning its entire product portfolio and related software packages. The company owns and operates manufacturing facilities in China and Taiwan and maintains complete control of the entire manufacturing process. It is ISO-9001 certified and recently achieved ISO-13485 compliance for medical devices.

The OEM/ODM engineering team is capable of customizing a variety of embedded hardware including system boards, mechanics enclosures, system or carrier boards for modules, and other essential components such as power supplies, DC modules, touch controllers, and more. The growing engineering services business is a product of the company’s rich expertise with single-board design, COM carrier board design and integration, system design and system integration, fanless designs, and extreme temperature and rugged systems (IP65, EN50155, Mil-Std-810G).

Its OEM/ODM engineering team is further supported by rich investments in R&D and test equipment; the company recently spent more than $1 million in pre- and post-route simulation tools and measurement hardware. The company is a market share leader in a variety of embedded hardware markets such as embedded motherboards, SBCs, COMs, and embedded integrated computer systems. Combined with its data acquisition experience, products, and resources, the company is able to satisfy a broad range of IoT requirements while remaining versatile to changes in the embedded hardware market. This versatility, and need to continue building out its product mix, will
Axiomtek has launched PICO840, an ultra-compact PICO-ITX SBC with Bay Trail-I. Axiomtek has launched PICO840, an ultra-small PICO-ITX embedded SBC utilizing the latest quad-core Intel Atom processor (code name: Bay Trail-I) and supporting DDR3L-1066/1333 MHz system memory up to 8 GB. Considering different environments, this industrial grade Pico-ITX mainboard is built to withstand extreme temperature, ranging from -40 to +70°C. Moreover, with superior integration and power efficiency, this compact single board computer enables system developers and OEMs to create smaller, lighter, quieter devices than ever and embrace the new possibilities across POS systems, mobile medical monitor, compact panel PCs as well as multiple embedded computer, system and appliance segments.

Data Modul: 3.5-inch SBC powered by Haswell/Broadwell ULT processors. Data Modul introduces, MS-98F3, a new 3.5” SBC powered by the latest Intel Haswell/Broadwell ULT processors, a system-on-chip with low power consumption and high performance capabilities. The fanless MS-98F3 is equipped with one 204-pin DDR3L SODIMM socket that supports up to 8GB DDR3L 1333/1600 memory. Heating spots like CPU are located at the rear side of the PCB, the passive heatsink is included in the delivery.

Bayer DSP Systeme: PCIe platform with Arria FPGA features dual SFP+ cages. Bayer announced the release of its second low-profile PCIe board based on Altera’s Arria V GZ FPGA - the A5-PCle-S (ASPS). The high-performance, power and cost-efficient Arria V GZ provides a high level of system integration and flexibility for I/O, routing, and processing that enables Bitt-Ware’s ASPS to be a solid platform for network processing, security, broadcast, and various data management to accommodate IoT data streams.

Curtiss-Wright: OpenVPX board features two independent SBCs on a single card. Curtiss-Wright has introduced the industry’s first dual-node Power Architecture OpenVPX single board computer that provides two independent SBC nodes on a single 6U VPX board. The rugged VPX6-195 features dual Freescale 1.5 GHz quad-core T2080 processing nodes, each of which is provided with its own power, I/O, FPGA and XMC expansion site. More information about each news is available on: www.Embedded-Control-Europe.com/magazine
Long-term partnership ensures safe and secure robot control

By Peter Hoser, Fujitsu

This article shows how close cooperation between the main-board supplier and its customer – a robotic company – both located in Augsburg, Germany, results in global market success for the innovative robot products.

In recent years, innovations by KUKA have had a sustained influence on the world of automation, from the Robocoaster safely swinging people through the air at theme parks to the new lightweight robots that can assemble highly sensitive parts and collaborate directly with humans. Yet it was with the introduction of the current KR C4 in particular that KUKA revolutionized robot control. This robot control is based on PCs and open industry standards and was the first robot control in which a complete safety control is integrated as a software function.

As the basis for their controls, KUKA has been using mainboards by Fujitsu for many years, now in the fourth generation. An important reason for this is that the short communication and delivery routes from the Fujitsu mainboard development and production plant in Augsburg, Germany, to KUKA headquarters, also based in Augsburg, are a tremendous advantage over mainboard manufacturers from Asia. Even more important is the synthesis of customer-specific features and economic scale effects.

Having tested the Fujitsu mainboards over several months before the start of their cooperation, KUKA found the boards met the high standards of industrial robotics in terms of high availability and durability. As the main-board is a central component of the control, it has to fulfill very high requirements: in addition to the guaranteed availability of all individual components, it is indispensable that all systems deliver reliable and extremely stable performance even under rough and demanding conditions in manufacturing environments. The control systems have to reliably meet the challenging safety and security requirements 24 hours a day, 7 days a week at an ambient temperature up to 45°C.

Due to a long-term development partnership, the mainboard supplier already knows the specific needs of the robotic company from previous product generations. Even before they start designing, they involve the robotic manufacturer in the development process of new products. This gives the flexibility to fulfill the customer’s wishes in terms of the board layout, special functionalities, and the BIOS. Instead of costly customized versions especially for this customer, Fujitsu make KUKA’s preferences part of the standard layout of their industrial mainboards. Thus, the boards can be manufactured in very large numbers, which, along with the high degree of automation, enables to produce the boards at competitive conditions despite the high wage level in Germany. For the robotic manufacturer, who delivers some 20,000 robots per year to a highly competitive market, this is an important contribution to optimizing costs. The fact that Fujitsu mainboards are based on a standardized product with a high degree of product maturity proved another point in their favour. The special functionalities KUKA demands from the mainboards are mostly related to functional safety as well as security issues. In robotics it is particularly important to clearly differentiate between safety and security. Subsuming both aspects under the term protection tends to confuse two areas that present control developers with completely different tasks. You can summarize the difference as follows: safety protects humans from machines, security protects machines from humans.

In industrial robotics, there are several main tasks. KR C4 assigns these to various cores of a multi-core processor. Thus, the multi-core processor with its independently operating computing cores enables the integration of safety and other control components within the software, components which previously had to be implemented in the form of external hardware components. Drive control is the fundamental task level. It requires a very high and deterministic real-time clocking frequency. Situated on the level above it is the robot control proper, which determines where the motor power should be directed. A still higher level is occupied by functional safety,
which comprises features such as the operating mode selector, confirmation switch, and emergency stop. The highest level is that of the human-machine interface, which in this case is based on Windows. The developers at KUKA distribute these four tasks among two cores – because redundancy contributes to meeting the safety requirements. This means that two independent cores perform the same safety-related computing operations. If their results match when compared, the system is operating safely.

The integrated safety control not only ensures standard robot safety in accordance with ISO 10218 through emergency stop, operating mode selector, and confirmation switch, but also an extended safety level by monitoring the safeness of operating spaces, speed and acceleration levels, and stopping routines. Safe protocol stacks for FailSafe over EtherCAT, ProSafe over Profinet, and CIP-Safe over Ethernet/IP are supplied entirely on the software level. As a result, only certified, cleared EXEs and DLLs registered with the control system can be configured and unlocked before they can be opened. Other security measures for detecting denial-of-service (DoS) attacks, that is, suspicious access patterns, include Broadcast Storm Denial-of-service (DoS) attacks, that is, suspicious access patterns, include Broadcast Storm

If security is the protection of machines from humans, this usually means protecting machines from unauthorized remote access from outside. In this respect, the current trend towards web-based networking of manufacturing machines tends to open up new potential gateways for intruders. In order to prevent this, KUKA encourages users not to connect robot controls directly to the internet, thus ruling out several risks from the outset. Nevertheless, they offer several lines of defense: a special TCP/IP stack (not Windows) functions as the first touch point with the outside world (KUKA Line Interface). Software-based bridging and Network Address Translation (NAT) ensure that protocols and ports must expressly be configured and unlocked before they can be opened. Other security measures for detecting denial-of-service (DoS) attacks, that is, suspicious access patterns, include Broadcast Storm Denial-of-service (DoS) attacks, that is, suspicious access patterns, include Broadcast Storm Denial-of-service (DoS) attacks, that is, suspicious access patterns, include Broadcast Storm Denial-of-service (DoS) attacks, that is, suspicious access patterns, include Broadcast Storm
Cadence: FreeRTOS now available for Tensilica processors
Cadence Design Systems announced that the FreeRTOS real-time operating system is now available for Cadence Tensilica processors and digital signal processors. FreeRTOS is a popular, scalable, easy-to-use real-time kernel designed specifically for small, low-power embedded systems. According to a 2013 market share study from UBM Tech, FreeRTOS had been selected for 13 percent of embedded projects that utilize an embedded operating system (OS), and is a very popular option for microcontrollers as well as smaller 32-bit processor cores.
News ID 2957

Kithara: real-time Image processing with OpenCV
Kithara Software has successfully finished the real-time support of the open source function library OpenCV within the company's own real-time extension, allowing for an immediate reaction to the processing of image data. The combination of OpenCV 3.0 and the «RealTime Suite» is a significant step, since it incorporates the widespread use of the free program library with the increasing necessity of strict response times for machine vision. This way for instance, AVX2 can be utilized in real-time.
News ID 2895

Maxim: evaluate industrial sensors faster with quad IO-Link master reference design
Designers now have a single platform to develop their own IO-Link master and multiple industrial sensors. The MAXREFDES79# from Maxim Integrated Products, allows manufacturers to bring IO-Link factory automation designs to market faster. As the first ever IO-Link master reference design, MAXREFDES79# reduces the cost and time required to develop and evaluate both IO-Link master and IO-Link sensor systems.
News ID 2919

Micro Digital: SMX RTOS now available for Renesas RZ/A1 ARM Cortex-A9
Micro Digital offers SMX RTOS support for the RZ/A1 group of ARM Cortex-A9 microprocessors from Renesas. This includes immediate availability of the smx real-time multitasking kernel, smxWiFi 802.11a/b/g/i/n wireless stack, smxNS TCP/IP stack, smxNS6 dual IPv4/IPv6 TCP/IP stack, smxUSBH USB host stack, smxUSBD USB device stack, and smxFS FAT file system.
News ID 2860

Microsemi: SmartFusion2 SoC FPGA dual-axis motor control kit
Microsemi announced availability of its SmartFusion2 SoC FPGA dual-axis motor control kit with a modular motor control IP suite and reference design. The kit, which simplifies motor control designs using a single SoC FPGA, accelerates time to market and is scalable across multiple industries such as industrial, aerospace and defense. Typical applications include factory and process automation, robotics, transportation, avionics and defense motor control platforms. The SoC integration of system functions helps to lower total cost of ownership.
News ID 2909

Mouser: rapid prototyping kit for TI’s new MSP432P401R microcontrollers
Mouser Electronics is now stocking the MSP-EXP432P401R LaunchPad Evaluation Kit from Texas Instruments. This new TI LaunchPad is an easy-to-use rapid prototyping kit for TI’s new MSP432P401R microcontrollers featuring 256KBBytes of Flash and 64K of RAM. The new TI MSP432 microcontroller family is based on a low power ARM Cortex M4F and draws as little as 800mA in low power mode, with a run current of 95µA/MHz. The MSP432P401R 32 bit microcontroller supports speeds up to 48MHz and has integrated peripherals for communication, ADC, timers, and AES encryption.
News ID 2933

SEGGER: SmartMSD makes USB file transfer easy
SEGGER’s new Smart Mass Storage Device (SmartMSD) uses the proven MSD standard to easily stream files to and from USB devices. A simple Drag and Drop is all it takes. The active file system technology employed in SmartMSD is unique. Once the USB-device is connected to the host, files can be read or written to the application without the need for dedicated storage memory. The SmartMSD software analyzes what operation is performed by the host and passes this to the application layer of the embedded target, which then performs the appropriate action.
News ID 2940

TI-RTOS 2.12 introduces advanced power management capabilities
Simplifying software development for connected applications has become even more important as the IoT continues to encompass a greater range of everyday products. Texas Instruments announces key updates to its complete real-time operating system, which brings the ease-of-use associated with power management requirements in high-level operating systems, such as Android and Windows, to embedded MCU-based applications. As a result, using TI-RTOS 2.12, developers can easily leverage the power management features built into TI devices to create IoT applications with a longer battery life.
News ID 2909

Mouser: rapid prototyping kit for TI’s new MSP432P401R microcontrollers
Mouser Electronics is now stocking the MSP-EXP432P401R LaunchPad Evaluation Kit from Texas Instruments. This new TI LaunchPad is an easy-to-use rapid prototyping kit for TI’s new MSP432P401R microcontrollers featuring 256KBBytes of Flash and 64K of RAM. The new TI MSP432 microcontroller family is based on a low power ARM Cortex M4F and draws as little as 800mA in low power mode, with a run current of 95µA/MHz. The MSP432P401R 32 bit microcontroller supports speeds up to 48MHz and has integrated peripherals for communication, ADC, timers, and AES encryption.
News ID 2933

SEGGER: SmartMSD makes USB file transfer easy
SEGGER’s new Smart Mass Storage Device (SmartMSD) uses the proven MSD standard to easily stream files to and from USB devices. A simple Drag and Drop is all it takes. The active file system technology employed in SmartMSD is unique. Once the USB-device is connected to the host, files can be read or written to the application without the need for dedicated storage memory. The SmartMSD software analyzes what operation is performed by the host and passes this to the application layer of the embedded target, which then performs the appropriate action.
News ID 2940

TI-RTOS 2.12 introduces advanced power management capabilities
Simplifying software development for connected applications has become even more important as the IoT continues to encompass a greater range of everyday products. Texas Instruments announces key updates to its complete real-time operating system, which brings the ease-of-use associated with power management requirements in high-level operating systems, such as Android and Windows, to embedded MCU-based applications. As a result, using TI-RTOS 2.12, developers can easily leverage the power management features built into TI devices to create IoT applications with a longer battery life.
News ID 2909

Mouser: rapid prototyping kit for TI’s new MSP432P401R microcontrollers
Mouser Electronics is now stocking the MSP-EXP432P401R LaunchPad Evaluation Kit from Texas Instruments. This new TI LaunchPad is an easy-to-use rapid prototyping kit for TI’s new MSP432P401R microcontrollers featuring 256KBBytes of Flash and 64K of RAM. The new TI MSP432 microcontroller family is based on a low power ARM Cortex M4F and draws as little as 800mA in low power mode, with a run current of 95µA/MHz. The MSP432P401R 32 bit microcontroller supports speeds up to 48MHz and has integrated peripherals for communication, ADC, timers, and AES encryption.
News ID 2933

SEGGER: SmartMSD makes USB file transfer easy
SEGGER’s new Smart Mass Storage Device (SmartMSD) uses the proven MSD standard to easily stream files to and from USB devices. A simple Drag and Drop is all it takes. The active file system technology employed in SmartMSD is unique. Once the USB-device is connected to the host, files can be read or written to the application without the need for dedicated storage memory. The SmartMSD software analyzes what operation is performed by the host and passes this to the application layer of the embedded target, which then performs the appropriate action.
News ID 2940

TI-RTOS 2.12 introduces advanced power management capabilities
Simplifying software development for connected applications has become even more important as the IoT continues to encompass a greater range of everyday products. Texas Instruments announces key updates to its complete real-time operating system, which brings the ease-of-use associated with power management requirements in high-level operating systems, such as Android and Windows, to embedded MCU-based applications. As a result, using TI-RTOS 2.12, developers can easily leverage the power management features built into TI devices to create IoT applications with a longer battery life.
News ID 2909

Mouser: rapid prototyping kit for TI’s new MSP432P401R microcontrollers
Mouser Electronics is now stocking the MSP-EXP432P401R LaunchPad Evaluation Kit from Texas Instruments. This new TI LaunchPad is an easy-to-use rapid prototyping kit for TI’s new MSP432P401R microcontrollers featuring 256KBBytes of Flash and 64K of RAM. The new TI MSP432 microcontroller family is based on a low power ARM Cortex M4F and draws as little as 800mA in low power mode, with a run current of 95µA/MHz. The MSP432P401R 32 bit microcontroller supports speeds up to 48MHz and has integrated peripherals for communication, ADC, timers, and AES encryption.
News ID 2933

SEGGER: SmartMSD makes USB file transfer easy
SEGGER’s new Smart Mass Storage Device (SmartMSD) uses the proven MSD standard to easily stream files to and from USB devices. A simple Drag and Drop is all it takes. The active file system technology employed in SmartMSD is unique. Once the USB-device is connected to the host, files can be read or written to the application without the need for dedicated storage memory. The SmartMSD software analyzes what operation is performed by the host and passes this to the application layer of the embedded target, which then performs the appropriate action.
News ID 2940

TI-RTOS 2.12 introduces advanced power management capabilities
Simplifying software development for connected applications has become even more important as the IoT continues to encompass a greater range of everyday products. Texas Instruments announces key updates to its complete real-time operating system, which brings the ease-of-use associated with power management requirements in high-level operating systems, such as Android and Windows, to embedded MCU-based applications. As a result, using TI-RTOS 2.12, developers can easily leverage the power management features built into TI devices to create IoT applications with a longer battery life.
News ID 2909
At the Aviation Electronics Europe event, 18th 2015 in Munich, Germany. With the focus on the consortium EMCC2015 consisting of the Wind River Open Virtualization, Security Wind River has delivered enhancements to TEM and Timing-Architects, do hold an June 2015 event in Munich, Germany.

**Wind River: Linux profiles updated with latest kernel/ toolchain from Yocto Project 1.7 release**

Wind River has delivered enhancements to Wind River Open Virtualization, Security Profile for Wind River Linux, and Carrier Grade Profile for Wind River Linux. These profiles provide developers with key capabilities to create the safe, secure, and reliable intelligent systems that will harness the power of the Internet of Things. Open Virtualization, Security Profile, and Carrier Grade Profile have been updated with the latest Linux kernel, toolchain, and user space from the Yocto Project 1.7 release.

News ID 2844

**SYSGO and Curtiss-Wright present safety-critical Avionics platform**

At the Aviation Electronics Europe event, SYSGO and Curtiss-Wright Defense Solutions will demonstrate a joint platform for avionics systems that combines SYSGO’s DO-178C/B certified hypervisor PikeOS with Curtiss-Wright’s VPX3-1701 Freescale LS1020A dual ARM Cortex-A7 processor-based single board computer. The demo will feature CoreAV1 safety-critical OpenGL ES/SC graphics drivers running on Curtiss-Wright’s XMC-715 E4690 GPU-based graphics module. At SYSGO’s booth, visitors can learn about the new safety-tested platform.

News ID 2862

**iSYSTEM : embedded Multi-Core conference in Munich**

The consortium EMCC2015 consisting of the partner companies Elektrobe, Infineon, iSYSTEM and Timing-Architects, do hold an Embedded Multi-core conference June 16th to 18th 2015 in Munich, Germany. With the focus on “Best Practice Multi-Core Embedded Development and Test”, the four partner companies will bring together multi-core experts to meet the challenges of this technology and to present, discuss and exchange experiences and solutions.

News ID 2867

**Microchip: 5 GHz power amplifier module for IEEE 802.11ac Wi-Fi standard**

Microchip announces its new SST11CP22 5 GHz Power Amplifier Module for the IEEE 802.11ac ultra-high data-rate Wi-Fi standard. This PAM delivers 19 dBm linear output power at 1.8% dynamic Error Vector Magnitude with MCS9 80 MHz bandwidth modulation. Additionally, the SST11CP22 delivers 20 dBm linear power at 3% EVM for 802.11a/n applications, is spectrum mask compliant up to 24 dBm for 802.11a communication, and has less than -45 dBm/MHz RF harmonic output at this output power, making it easier for the system board to meet FCC regulations.

News ID 2838

**Renesas: development environment for RL78 family**

Renesas Electronics announced the availability of the CC-RL 12 compiler, a development environment for the RL78 Family 16-bit MCUs widely used in the home appliances, industrial, and automotive systems. Recently, increased diversity and performance of functions provided by systems that include motors, such as home appliances or industrial equipment, have become strongly desired. This has resulted in demand for increased processing speed in the MCUs used.

News ID 2938

**Vector introduces Covered by Analysis capability in VectorCAST 6.3 suite**

Vector Software announces the availability of VectorCAST/CBA (Covered By Analysis) which allows users in regulated industries to augment measured coverage with manual analysis to achieve the mandated 100% code coverage. VectorCAST/CBA is available as an add-on for all VectorCAST products, and provides an intuitive editor which allows users to provide analysis for statements, branch outcomes, or MC/DC pairs depending on the coverage level.

News ID 2839

**Atmel: lowest power ARM Cortex-M based solution extends battery life**

Atmel is sampling the industry’s lowest power ARM Cortex-M based solution with power consumption down to 35µA/MHz in active mode and 200µA in sleep mode. The ultra-low power SAM L family broadens the Atmel SMART 32-bit ARM-based MCU portfolio and extends battery life from years to decades, reducing the number of times batteries need to be changed in devices such as fire alarms, healthcare, medical, wearable, and devices placed in rural, agriculture, offshore and other remote areas.

News ID 2874

**Cadence and ARM announce strategic IP interoperability agreement**

Cadence Design Systems and ARM announce the signing of a broad Intellectual Property Interoperability Agreement. This multiyear agreement provides reciprocal access to relevant IP portfolios from the Cadence IP Group and ARM. Additionally, the agreement grants both companies rights to manufacture test chips containing Cadence IP and ARM IP and to provide development platforms to customers.

News ID 2834

**Ti introduces ultra-low-power 32-bit MSP432 MCUs**

TI’s new MSP432 MCUs are the latest advance in the company’s ultra-low-power innovation, delivering a best-in-class ULPBench score of 167.4 – outperforming all other Cortex-M3 and -M4F MCUs on the market. This ultra-low power benchmark from the Embedded Microprocessor Benchmark Consortium (EEMBC) provides a standard way to compare power performance on any MCU, independent of architecture.

News ID 2857

**Toshiba: ARM Cortex-M4F-based MCUs for secure communications control**

Toshiba Electronics Europe has announced a new ARM Cortex-M4F based microcontroller for use in secure systems control. The TMPM46BF10FG expands Toshiba’s existing TX04 range and adds a selection of enhanced security features, ideally suited to applications in Internet of Things devices, energy management systems, sensor technology and industrial equipment.

News ID 2891

**Mouser: keep memory safe with gamma-resistant Wire EEPROM**

Mouser Electronics is now stocking the DS28E801 Wire Gamma Resistant EEPROM from Maxim Integrated. The DS28E801 includes 248 bytes of non volatile memory that utilizes a storage cell technology resistant to 75 kiloGray of gamma radiation. The Maxim Integrated DS28E801 Wire EEPROM, available from Mouser Electronics, has 248 bytes of non-volatile memory organized in 31 blocks of 8 bytes each. Individual blocks can be write-protected to prevent accidental erasure of data. For additional security, each memory block can only be written eight times.

News ID 2923

**Telit: GNSS module enables high-performance position reporting and navigation solutions**

Telit Wireless Solutions released a new GNSS module, the SE868-V3. This positioning module combines GPS, Glonass, Beidou, Galileo, and SBAS which enables the creation of high-performance position reporting and navigation solutions. The SE868-V3 can navigate to -162 dBm and track to -166 dBm, thereby providing improved performance in harsh environments. It is pin-to-pin compatible with the former SE868-V2 as well as the JF2. This advanced GNSS module can track GPS and Glonass or GPS and Beidou constellations simultaneously and it is Galileo ready.

News ID 2935

**MSC: high power LEDs from Cree reduce system costs**

MSC Technologies is offering the new XLamp Extreme High Power (XHP) LEDs from Cree. The first LEDs powered by Cree’s revolutionary XCS Technology Platform, XLamp XHP50 and XHP70 LEDs provide twice the lumen output and improved reliability compared to previous LEDs of the same size.

News ID 2849
FTDI Chip adds graphic toolchain package to EVE offering
Bringing more comprehensive support to its Embedded Video Engine (EVE) product offering, FTDI Chip introduces EVE Screen Designer - which is available to download for free. Suitable for use with Windows operating systems (Windows 7 and above), this highly sophisticated, but easy-to-operate development suite enables the creation of advanced HMIs, via EVE’s innovative object-oriented approach, without any understanding of EVE display lists.
News ID 2850

Infineon: XMC4800 MCUs with EtherCAT support Industry 4.0
On occasion of the Hannover Messe, Infineon announced its new XMC4800 series of 32-bit microcontrollers with on-chip EtherCAT (Ethernet for Control Automation Technology) node. With its outstanding real-time capability the XMC4800 series will drive networked industrial automation and Industry 4.0 applications. Infineon is the first semiconductor company to offer the EtherCAT node integrated on an ARM Cortex-M-based microcontroller with on-chip Flash and analog/mixed signal capability.
News ID 2928

Innodisk: DDR4 memory for industrial applications on upcoming Skylake platform
Innodisk is introducing DDR4 memory modules designed for industrial applications on Intel’s upcoming Skylake platform. The new unbuffered long DIMM and compact SO-DIMM memory offerings will feature significantly lower power consumption and higher performance than comparable DDR3 modules and will have ECC error correction available for industrial and embedded applications. An extra thick 30u gold connector, on-board thermal sensors and conformal coatings make these JEDEC-compliant DDR4 modules especially suited for the next generation of industrial systems.
News ID 2832

EBV Elektronik expands distribution agreement with Cypress
EBV Elektronik announced the extension of the franchise with Cypress Semiconductor. The new agreement is effective immediately. The extended agreement gives EBV Elektronik access to the entire portfolio of Cypress products including the Programmable Systems Division range of products featuring Cypress’ PSoC families of devices. PSoC is the world’s only programmable embedded system-on-chip integrating high-performance analog, PLD-based programmable logic, memory and a microcontroller on a single chip. It is a very flexible microcontroller with re-configurable analog and digital functionality allowing customers very easily to integrate a large amount of analog and digital functionality into the PSoC device saving on both BOM costs and time to market. Overall PSoC comprises 4 families of devices, (PSoC1, PSoC 3, PSoC4, & PSoC5LP) and over 450 individual devices.
News ID 2907

Maxim: highly integrated IO-Link temperature sensor
Designers can save power, cost, and space with the MAXREFDES42# IO-Link temperature sensor reference design from Maxim Integrated Products. The MAXREFDES42# IO-Link joins the company’s portfolio of other IO-Link reference designs for industrial control and automation. This design’s highly integrated analog front end measures temperature, while detecting overvoltage, shorts, and open circuits.
News ID 2861

Microchip: CAN flexible data-rate transceiver family withstands harsh conditions
Microchip announces a new family of CAN FD transceivers, the MCP2561/2FD. As an interface between a CAN protocol controller and the physical two-wire CAN bus, these transceivers can serve both the CAN and CAN FD protocols. This product family not only helps automotive and industrial manufacturers with today’s CAN communication needs, but also provides a path for the newer CAN FD networks that are increasingly in demand.
News ID 2854

MSC: 15.0-inch TFT displays from Mitsubishi with high SXGA+ resolution
Mitsubishi Technologies offers two 15.0-inch TFT displays from Mitsubishi with a high resolution of 1400 x 1050 pixels (SXGA+, 117 pixels per inch). Both displays are designed for use in industrial applications such as image processing, measuring instruments and medical equipment. Furthermore, they are also suitable as display instruments in trains and ships. The operating temperature range of these high-resolution displays is especially wide and ranges from -30 to +80°C.
News ID 2830

A.R. Bayer DSP Systems: PCIe board based on Altera’s Arria 10 FPGA
BittWare announced the availability of its first board based on Altera’s Arria 10 GT/GX FPGA - a low-profile PCIe board called the A10PL4. Integrating the 20nm process technology of the Arria 10 with a wide variety of features, the A10PL4 board supports a range of challenging applications such as network processing and security, compute and storage, instrumentaion, broadcast, and signals intelligence.
News ID 2892
Advantech RISC ultra-low power
Axiomtek: compact fanless Embedded system with Atom E3825
Axiomtek has announced its launch of eBOX530-840-FL. The palm-size embedded system powered by Intel Atom dual core processor E3825 comes with DDR3L memory maximum capacity up to 8 GB and one full-size PCI Express Mini Card with mSATA supported. The eBOX530-840-FL is built of heavy-duty aluminum extrusion with IP40 anti-dust ingress protection giving it a high degree of structural strength. Its fanless design and excellent thermal solution allows it to operate noiseless and properly at temperature ranging from -20 to +60°C in extremely critical environments. The rugged embedded box computer is an ideal fit to various embedded applications such as transportation, POS, kiosk, industrial control automation and medical equipment. News ID 2836

Fastwel: COM Express mini CPU Module with powerful capabilities
The range of Fastwel COM-modules was extended with a new CPC1311 in COM Express mini format (Type 10). This innovative product is designed for OEMs that utilize custom computers in systems designed for mission-critical applications and harsh environments. CPC1311 is based on multicore CPU Intel Atom E3800 with 64-bit architecture. News ID 2845

Axiomtek: low-power COM Express type 2 basic module with Celeron J1900/N2807
Axiomtek has launched CEM841, its new low-power COM Express Type 2 Basic module. The palm size module is based on the ultra-low-power Intel Xeleron processor J1900/N2807 which provides impressive CPU and graphics performance improvements. The CEM841 is equipped with double deck DDR3L SO-DIMM sockets supporting system memory maximum up to 8 GB. News ID 2916

3.5” SBC and Computing Box with TI Sitara processor
Advantech presents two new products powered by the TI Sitara AM3352 Cortex-A8 1GHz high performance processor— RSB-4220 3.5” Single Board Computer, and UBC-FA30 computing box. The low power Sitara AM3352 design uses only 2.8 watts and comes with rich I/O features such as UART, Giga LAN, CANbus and more. RSB-4220 and UBC-FA30 are suited for applications in industrial automation and IoT devices. News ID 2908

MEN: box PC with AMD G-Series APU and real-time Ethernet fieldbuses
The robust BC50F from MEN is another representative of its modular Box and Panel PC family. Offering an APU from the AMD Embedded G-Series, the I/O required in the market, a wide-range PSU with 16 to 36 V input voltage and a robust, maintenance-free enclosure, the BC50F is especially suited for demanding industrial real-time Ethernet applications. Especially developed for industrial applications, e.g. for machine monitoring and control or for use in commercial vehicles and robots, the BC50F impresses with its high performance processor, extreme graphics performance and a huge interface flexibility. News ID 2930

Xilinx: video over IP connectivity solutions enable ‘any media over any network’
Xilinx launched its next generation of Video over IP connectivity solutions to address the industry’s transition to all IP-based networks. These new connectivity solutions enable ‘any media over any network’ transport capabilities to the broadcast and pro a/v markets. Xilinx defines and deploys Video over IP protocols for contribution and distribution networks with the provision of the SMPTE ST 2022-1,2 and SMPTE ST 2022-5.6 IP cores and reference designs. News ID 2887

Wind River and Mathworks integrate Simics and Simulink for advanced model-based design
Wind River is working with MathWorks to integrate Wind River Simics with Simulink for improved model-based design workflows. This collaboration creates smarter system verification by enabling testing and co-simulation of combined design and platform models, and helps drive better designs while removing risk from future development, test, and integration. News ID 2920
Artesyn Embedded Technologies announced the new PCOMnetA5 by F&S Elektronik Systems. The Diamond DSP media engine on a single AdvancedTCA blade. This enables network equipment providers to implement complete solutions such as session border controllers, VoLTE, video optimization or video conferencing with less power consumption. News ID 2827

Diamond: 26-port gigabit Ethernet switch targets rugged networked applications
Diamond Systems unveiled the Epsilon-24000 family of gigabit Ethernet switches. These rugged, managed Layer 2+ Ethernet switch modules offer up to 24 10/100/1000 Mbps copper twisted pair ports plus two small form factor pluggable sockets in the compact PC/104 form factor measuring 96 x 116 mm. News ID 2868

Exploring the world of ARM based embedded computing boards
From just a handful of ARM based board vendors 2 years ago to over 100 today and new ones entering the market there is clearly a new wave of disruption and innovation coming to the world of Embedded Computing Boards. On the ARM Connected Community, you can take a deep dive into the world of ECBs with interviews, videos, blogs, discussion and an interactive guide to available boards. News ID 2914

Artesyn: media processing blade operates in any standard ATCA chassis
Artesyn Embedded Technologies announced the ATCA-8330, which combines a powerful Intel Xeon server with a high density DSP media engine on a single AdvancedTCA blade. This enables network equipment providers to implement complete solutions such as session border controllers, VoLTE, video optimization or video conferencing with less power consumption and therefore less cost. News ID 2886

F&S: SBC with Freescale Vybrid controller
The new PCOMnetA5 by F&S Elektronik Systems is a Single Board Computer consisting of a compact base board and the small and inexpensive F&S module PicoCOMA5 (version PCOMA5-V3-W13 or -LIN). The SBC is based on the Freescale Vybrid controller. News ID 2887

DFI: H81-based Mini-ITX motherboards support 3 independent displays
DFI announced the arrival of HD171-H81 and HD173-H81, two new industrial-grade Mini-ITX motherboards powered by the 4th generation Intel Core with Intel H81 chipset. Intel HD Graphics engine integrated into these 4th generation Intel Core processors provides a seamless visual experience, including superior gaming image quality, vibrant HD video playback, and increased overall speed and performance. News ID 2883

NI: Xeon-based PXI embedded controller and high-bandwidth PXI chassis
NI announced a new Intel Xeon-based PXI Express controller (PXIe-8880) and chassis (PXIe-1085). The combination of the 8-core, server-class processor and full system bandwidth of 24 GB/s delivers breakthrough performance for computationally intensive and highly parallel applications such as RF test, semiconductor test, and 5G prototyping. News ID 2835

PEAK-System: display assembly for visualization of CAN data
For the visualization of CAN data, PEAK-System has developed the PCAN-MiniDisplay. The module to be used for assemblies has an extended operating temperature range of -40 to +85 °C. It provides connections to a High-speed and Single-wire CAN bus. The incoming CAN traffic can be filtered. The graphic representation of the CAN data is configured before using the unit and then is performed on a TFT display with a resolution of 320 x 240 pixels. News ID 2894

IBASE: energy efficient compact SBC with 5th gen Intel Core processors
IBASE has launched its new IB909 series, a 3.5-inch disk size with onboard 5th Generation Intel Core i U-series processors. The IB909 series offers a selection Intel processors manufactured on 14nm process technology namely, the Intel® Core™ i7-5600U running 2.2GHz, the Intel Core i5-5300U processor (1.8GHz) and the Intel Core i3-5010U processor (2.1GHz). News ID 2864

IBASE: energy efficient compact SBC with 5th gen Intel Core processors
IBASE has launched its new IB909 series, a 3.5-inch disk size with onboard 5th Generation Intel Core i U-series processors. The IB909 series offers a selection Intel processors manufactured on 14nm process technology namely, the Intel® Core™ i7-5600U running 2.2GHz, the Intel Core i5-5300U processor (1.8GHz) and the Intel Core i3-5010U processor (2.1GHz). News ID 2864

IBASE: energy efficient compact SBC with 5th gen Intel Core processors
IBASE has launched its new IB909 series, a 3.5-inch disk size with onboard 5th Generation Intel Core i U-series processors. The IB909 series offers a selection Intel processors manufactured on 14nm process technology namely, the Intel® Core™ i7-5600U running 2.2GHz, the Intel Core i5-5300U processor (1.8GHz) and the Intel Core i3-5010U processor (2.1GHz). News ID 2864

VadaTech has released a new 6U MicroTCA “Whisper” cube chassis
VadaTech has released a new 6U MicroTCA embedded computing system platform with quiet fan trays designed to operate at under 55dBa, suitable for office use. The VT989 is a 6-slot cube chassis that is 10.5 inches tall by 10 inches wide by 10.5 inches deep. The “Whisper” chassis features redundant cooling in a push/pull front-to-rear airflow configuration. News ID 2837

IMACS: open source I/O-system for direct sensor/actor adaption
emBRICK is an open-source, modular-plugin I/O/hardware for direct sensor/actor adaption in professional control and measuring applications. By using an efficient and compact open frame construction they are "ready to use" for mounting on so called "patch boards" or DIN hat rails. With this it is a powerful applicable embedded control solution from 1 to more than 1000 I/Os. News ID 2885

Yamaichi: test adapter for SMARC modules
Yamaichi Electronics has developed a new test adapter for the SMARC computer-on-module standard. It realizes the perfect alignment of the contacts and allows for 100% contacting reliability. Due to the use of spring probe pins very high contact cycles can be reached. SMARC stands for Smart Mobility Architecture. It is a specification published by the SGET for computer-on-modules. Its advantage is the low power consumption of the modules due to the implementation of ARM or other low-power processors. News ID 2913

MSI: industrial Mini-ITX board with Haswell/Broadwell solutions
As industrial applications increasingly require higher performance processing now than ever before, MSI released MS-98G5 industrial mainboard with superior processing and graphic capability in response. MS-98G5 is a Mini-ITX board based on Intel® 4th Gen QM87/HM86 architecture that come support with BGA-type Haswell/Broadwell Mobile Core i7/i5/i3/Celeron Processor, multiple display outputs, 1 PCIe(x16), 8 USB 2.0 & 4 USB 3.0 ports, 5 COM ports, SATA 3.0 connector, and 2 mini-PCIe slots. News ID 2879

Pentair: 2-slot Schroff MicroTCA system with integrated eMCH
Smaller MicroTCA systems are used primarily for digital video and image processing, in automation and machine control systems and electronic signal processing. Applications in these areas often require just one or two AdvancedMC modules, but high data rates over the backplane are still necessary. That’s why Pentair has joined forces with N.A.T. to develop a new 2-slot Schroff MicroTCA system. News ID 2871

More information about each news is available on www.Embedded-Control-Europe.com/magazine
You just have to type in the “News ID”. —
THREADX: WHEN IT REALLY COUNTS

When Your Company’s Success, And Your Job, Are On The Line -
You Can Count On Express Logic’s ThreadX® RTOS

Express Logic has completed 17 years of successful business operation, and
our flagship product, ThreadX, has been used in over 2 billion
of electronic devices, and systems ranging from printers to smartphones, from single-chip
SoCs to multiprocessors. Time and time again, when
leading manufacturers put their company on the line,
when their engineering team chooses an RTOS for their
next critical product, they choose ThreadX.

Our ThreadX RTOS is rock-solid, thoroughly field-proven,
and represents not only the safe choice, but the most
cost-effective choice when your company’s product
simply must succeed. Its royalty-free licensing model helps keep your Bill Of
Materials cost low, and its proven dependability helps keep your support costs down as well.
ThreadX repeatedly tops the time-to-market results reported by embedded developers like you. All the while,
Express Logic is there to assist you with enhancements, training,
and responsive telephone support.

Join leading organizations like HP, Apple, Marvell, Philips,
NASA, and many more who have chosen ThreadX for use in
over 2 billion of their products - because their products are too
important to rely on anything but the best. Rely on ThreadX, when
it really counts!

Contact Express Logic to find out more about our ThreadX RTOS, FileX® file system, NetX® Dual IPv4/IPv6 TCP/IP stack,
USBX® USB Host/Device/OTG stack, and our GUIX® graphics toolkit for embedded GUI development. Also ask about
our TraceX® real-time event trace and analysis tool, and StackX®, our patent-pending stack size analysis tool that
makes stack overflows a thing of the past. And if you’re developing safety-critical products for aviation, industrial or
medical applications, ask about our TUV Certification for ThreadX.

expresslogic

For a free evaluation copy, visit www.rtos.com

Germany: info@expresslogic.de • +49 (0) 5143 911304 • UK: info@expresslogic.co.uk • +44 (0) 1527 597007

Copyright © 2015, Express Logic, Inc.
ThreadX, FileX, and TraceX are registered trademarks, and NetX, USBX, GUIX, StackX, and Certification Pack are trademarks of Express Logic, Inc.
All other trademarks are the property of their respective owners.