Embedded COMPUTING DESIGN

Connecting Silicon, Software, and Strategies for Intelligent Systems

JUNE 2015
VOLUME 13
#4

EMBEDDED-COMPUTING.COM

INNOVATIVE PRODUCTS NOMINATIONS PG. 27

TOP EMBEDDED INNOVATORS

PG. 21

T.J. Rodgers
Cypress Semiconductor Corp.

Dr. Stan Schneider
Real-Time Innovations (RTI)

Jean Labrosse
Micrium

+ PLUS

DIY CORNER
A DEVELOPMENT PLATFORM FOR ALL MAKERS
PG. 9

STRATEGIES
MEDICAL DEVICE 3D GRAPHICS CHALLENGES
PG. 18

Annapolis Micro Systems

The FPGA Systems Performance Leader

WILDSTAR OpenVPX Ecosystem

FPGA Processing Boards
1 to 3
Altera Stratix V or
Xilinx Virtex 6 or 7
FPGAs per Slot

Input/Output Modules Include:
Quad 130 MSps thru Quad 550 MSps A/D
1.5 GSps thru 5.0 GSps A/D
Quad 600 MSps D/A
Dual 1.5 GSps thru 4.0 GSps D/A

1 to 40 Gbit Ethernet
SDR to FDR Infiniband

Open VPX Storage
Up to 8 TBytes Per Slot
4 - 8 GBytes Per Second

GEOINT, Ground Stations, SDR, Radar, Sigint, COMINT, ELINT, DSP, Network Analysis, Encryption, Image Processing, Pattern Matching, Oil & Gas Exploration, Financial and Genomic Algorithms,

Open VPX Switch
1 to 40 Gbit Ethernet
SDR to FDR Infiniband

Chassis
4, 6 or 12 Slot
Up to 14G

Annapolis Micro Systems

High Performance Signal and Data Processing in Scalable COTS FPGA Computing Fabric

190 Admiral Cochrane Drive, Suite 130, Annapolis, Maryland USA 21401
wfinfo@annapmicro.com USA (410) 841-2514 www.annapmicro.com

ISO 9001:2008 & AS9100C CERTIFIED

ITAR REGISTERED

VECTOR
ELECTRONICS & TECHNOLOGY, INC.
A FINE TECHNOLOGY GROUP

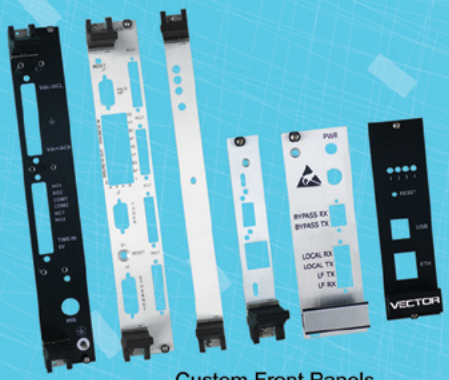
Since 1947

MADE IN THE USA

VME / VXS / cPCI ®

Chassis, Backplanes & Accessories

Chassis and Rack Accessories

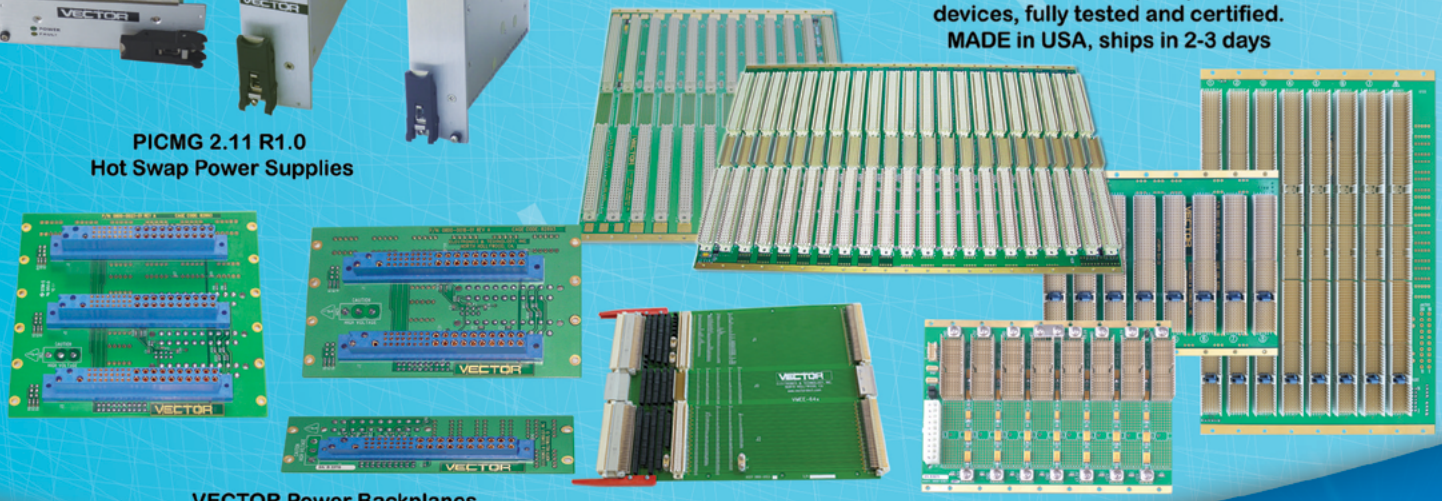


Custom Front Panels

PICMG 2.11 R1.0
Hot Swap Power Supplies

Mil-1-46058-C Conformal Coating Available for all VECTOR backplanes

Hi-speed VITA ANSI/VITA 1.1-1997 monolithic backplanes (Hi Current VITA 1.7 compliant) with Electronic Bus-Grant (EBG), Surface mount devices, fully tested and certified. MADE in USA, ships in 2-3 days



VECTOR Power Backplanes
PICMG 2.11 R1.0 Specification

(800)423-5659

WWW.VECTORELECT.COM

MADE IN U.S.A.

Embedded COMPUTING DESIGN

JUNE 2015
VOLUME 13
#4

embedded-computing.com | @embedded_comp | opsy.st/ECDLinkedIn

TOP EMBEDDED INNOVATORS 21

Departments

Silicon

Software

Strategies

Events

» **IoT Evolution Developers Conference, August 17-20**
opsy.st/IoTDevCon2015

Special Features

APP EXTRAS

Download the Embedded Computing Design app:
iTunes: itun.es/iS67MQ
Kindle Fire: opsy.st/kindlefireamaz

Related Publications

» **Automotive E-mag**
url.opensystemsmedia.com/auto2

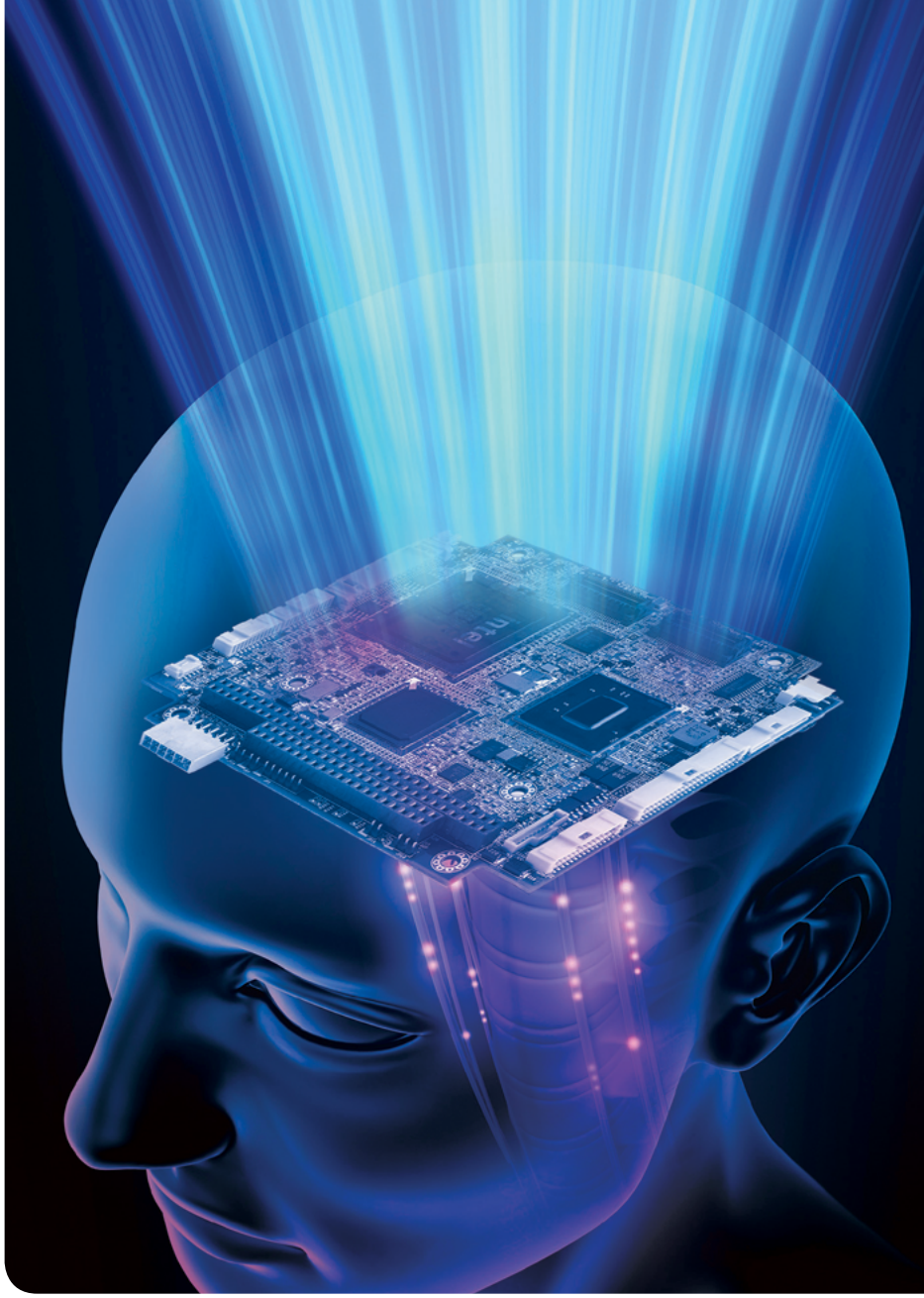
» **Industrial Embedded Systems Resource Guide**
industrial.embedded-computing.com/emag

EPIC Single Board Computers
Rugged, Stackable Form Factor
Fanless -40° to +85°C Operation

Small Form Factor Computers
Intel® Atom™ E3800 and i.MX6 CPUs
Fanless -40° to +85°C Operation

PC/104 Single Board Computers
Rugged, Stackable Form Factor
I/O Modules and Power Supplies

Single Board Computers
COM Express Solutions
Power Supplies
I/O Modules
Panel PCs



Thinking beyond the board

Sometimes our off the shelf products are not the perfect fit. Our application engineers and in house design talent are ready to develop customized solutions for your system requirements. Our stock products are accessible to use as building blocks for your next project. Calling WinSystems connects you directly with an Application Engineer who is ready to discuss customization options for firmware, operating systems, configurations and complete designs.

Team your engineers with ours to move your product from concept to reality faster.

715 Stadium Drive | Arlington, Texas 76011
Phone: 817-274-7553 | Fax: 817-548-1358
info@winsystems.com

Call 817-274-7553 or visit www.winsystems.com.
Ask about our product evaluation!

Take a peek at our NEW Website!

WinSystems®
The Embedded Systems Authority

ADVERTISER INDEX

Get your free digital edition at embedded-computing.com/emag

Subscriptions
embedded-computing.com/subscribe
subscriptions@opensystemsmedia.com
opensystemsmedia.com/subscriptions

OpenSystems media®

ISSN: Print 1542-6408, Online: 1542-6459

Embedded COMPUTING DESIGN — OpenSystems media®

Embedded Computing Design Editorial/Creative Staff

Rich Nass, Brand Director
rnass@opensystemsmedia.com

Curt Schwaderer, Editorial Director
cschwaderer@opensystemsmedia.com

Monique DeVoe, Managing Editor
mdevoe@opensystemsmedia.com

Brandon Lewis, Assistant Managing Editor
blewis@opensystemsmedia.com

Rory Dear, Technical Contributor
rdear@opensystemsmedia.com

David Diomede, Creative Services Director
ddiomede@opensystemsmedia.com

Konrad Witte, Senior Web Developer
kwitte@opensystemsmedia.com

Chris Rassiccia, Graphic Designer
crassiccia@opensystemsmedia.com

Sales Group

Tom Varcie, Sales Manager
tvarcie@opensystemsmedia.com
(586) 415-6500

Rebecca Barker, Strategic Account Manager
rbarker@opensystemsmedia.com
(281) 724-8021

Eric Henry, Strategic Account Manager
ehenry@opensystemsmedia.com
(541) 760-5361

Kathleen Wackowski, Strategic Account Manager
kwackowski@opensystemsmedia.com
(978) 888-7367

Asia-Pacific Sales
Elvi Lee, Account Manager
elvi@aceforum.com.tw

Regional Sales Managers
Barbara Quinlan, Southwest
bquinlan@opensystemsmedia.com
(480) 236-8818

Denis Seger, Southern California
dseger@opensystemsmedia.com
(760) 518-5222

Sydele Starr, Northern California
sstarr@opensystemsmedia.com
(775) 299-4148

Reprints and PDFs

republish@opensystemsmedia.com

EMEA

Rory Dear, Technical Contributor
rdear@opensystemsmedia.com

James Rhoades-Brown – Europe
james.rhoadesbrown@husonmedia.com

Christian Hoelscher, Account Manager – Europe
christian.hoelscher@husonmedia.com

Gerry Rhoades-Brown, Account Manager – Europe
gerry.rhoadesbrown@husonmedia.com

OpenSystems Media Editorial/Creative Staff

Embedded COMPUTING DESIGN | Military EMBEDDED SYSTEMS | SIGNAL PROCESSING DESIGN | INDUSTRIAL EMBEDDED SYSTEMS | PC/104 small form factors | PICMG SYSTEMS & TECHNOLOGY | VITA TECHNOLOGIES

John McHale, Group Editorial Director
Military Embedded Systems
PC/104 and Small Form Factors
PICMG Systems & Technology
VITA Technologies
Signal Processing Design
jmchale@opensystemsmedia.com

Joe Pavlat, Editorial Director
PICMG Systems & Technology
jpavlat@opensystemsmedia.com

Jerry Gipper, Editorial Director
VITA Technologies
jgipper@opensystemsmedia.com

Steph Sweet, Creative Director

Joann Toth, Senior Designer

Lisa Daigle, Assistant Managing Editor
Military Embedded Systems
PC/104 and Small Form Factors
ldaigle@opensystemsmedia.com

Sally Cole, Senior Editor
Military Embedded Systems
scole@opensystemsmedia.com

Brandon Lewis, Assistant Managing Editor
Industrial Embedded Systems
PICMG Systems & Technology
Signal Processing Design
blewis@opensystemsmedia.com

Jennifer Hesse, Managing Editor
VITA Technologies

Joy Gilmore, E-cast Manager
jgilmore@opensystemsmedia.com

Mariana Iriarte, Associate Editor
Military Embedded Systems
miriarte@opensystemsmedia.com

Corporate — opensystemsmedia.com

Patrick Hopper, Publisher
phopper@opensystemsmedia.com

Rosemary Kristoff, President
rkristoff@opensystemsmedia.com

John McHale, Executive Vice President
jmchale@opensystemsmedia.com

Rich Nass, Executive Vice President
rnass@opensystemsmedia.com

Wayne Kristoff, CTO

Emily Verhoeks, Financial Assistant

Headquarters – ARIZONA:
16626 E. Avenue of the Fountains, Ste. 201
Fountain Hills, AZ 85268
Tel: (480) 967-5581

MICHIGAN:
30233 Jefferson, St. Clair Shores, MI 48082
Tel: (586) 415-6500

Internet of (enchanted?) Things

By Rory Dear, Technical Contributor *rdear@opensystemsmedia.com*

Emerging claims suggest that the next thing after the Internet of Things will be "Enchanted Objects", but is there really a distinction between the two?

I aspire to be considered a "thought-leader" in the embedded industry, though when considering the possibilities of emerging technology, one invariably treads a thin line between thought-leading and sensationalistic speculation. Driven by this aspiration, I regularly ponder: What comes after IoT? The trending answer appears to be "Enchanted Objects", I suspect soon to be acronymised "IoET".

The self-proclaimed primary thought-leader of Enchanted Objects is David Rose, published author of this subject in 2014. He defines enchanted objects as "Ordinary things enhanced by just a little bit of technology to vastly expand their usefulness and interactivity" – hold on, isn't this essentially just IoT?

The claimed difference in an enchanted object is it's not something entirely new, i.e., a wearable device and the driving intelligence is subtle, rather than the key selling point. Rose believes the ubiquitous front end of a "slim slab of black glass" as the human machine interface must disappear and that current technology demands too much from the user in terms of search terms, Internet addresses, etc. Logical – but if asked to imagine a typical IoT device, I would invariably imagine a headless device, as I'm sure most others posed the same question would.

Rose of course had to tread the same thin line as I presented above. I worry that a motivation to publicize one's ideas as unique and revolutionary became a motivator. The definition of "Internet of Things" is naturally broad and I've not yet seen evidence that sufficient deviation from that definition exists to warrant an entirely new term. What Rose presents appears to be purely a distinction between connected devices that employ a front end user interface, such as a display, or do not thus operate "autonomously".

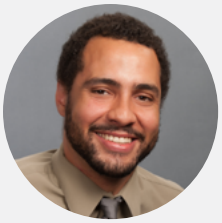
To draw any meaningful conclusion we must look beyond one man's vision and review others striving to popularize the term and their proffered examples. Cedric Hutchings, CEO of Withings leads the embedded industry down an unfamiliar path, to the fashion industry. Hutchings believes "The smart devices of the future would be integrated into 'dumb' objects we already take for granted: Wearables need not be 'dropables'. We have to fix the shortcomings of these devices to appeal to more people". This view is shared by Stephane Marceau, CEO of Omsignal who is a pioneer in smart fitness tracking clothing and has recently partnered with Ralph Lauren to integrate sensor technology into fashion.

What particularly caught my eye is an "Enchanted Mirror", soon to be deployed at Neiman Marcus. All very "Snow White", the social Internet enabled mirror instantaneously links consumers with their remote peers for approval. I read this technology beautifully summarized as "The answer to the perennial question 'Does my a** look good in this dress?' can now be crowd-sourced."

Whilst the fashion industry is one of the last that would leap out of most embedded visionaries' minds, is that wherein lies the answer? Should the current IoT movement be considered to be connecting all existing electronic products to the cloud and there is room for a term covering making smart "manual" items?

Now to a more familiar industry to us, medical technology, Vitality's intelligent medication control solution, Glowcaps, is being vaunted as part of "enchanted things". Actually at Embedded World 2015 I covered a not dissimilar solution to the issue of ensuring patients take prescribed medicines very much under the remit of IoT, the SMARTpack. Both employ the cloud and local Internet enabled pill dispensary devices to alert patients (or relatives) if medication is not consumed as prescribed. There are financial benefits as well as lives to be saved here; the Boston Globe estimated "The U.S. economy loses $100 billion annually because of patients who don't take prescribed drugs."

Having evaluated the current evidence, I remain unconvinced that anything currently paraded as an "enchanted thing" justifies that label and in fact should be considered at the more innovative end of the IoT spectrum. I tried tirelessly to identify a true differential, though none held up real credibility when evaluated against suggested examples. Of course we should always ponder "What's next?", but in an industry littered with often ambiguous buzzwords, we must be careful not to needlessly spawn even more. ECD



10 sensors, 3 protocols, 3 minutes, 1 dev kit for cloud-connected IoT apps

By Brandon Lewis, Assistant Managing Editor *blewis@opensystemsmedia.com*

It should come as no surprise that since the release of the original Arduino, BeagleBoard, and Raspberry Pi platforms only a few short years ago that quick-start development boards have become all the rage. The value proposition is obvious for the developer community and vendors alike, as the low-cost dev kits reduce barriers to entry for those looking to prototype Internet of Things (IoT) designs, and also enable semiconductor companies to market their offerings to a much wider audience than ever before.

However, while sub-$50 development platforms have greatly expanded the reach of embedded hardware and software tools to engineers of all experience levels, their price point also limits the capabilities a single off-the-shelf kit can provide designers that are serious about bringing IoT projects to market. This has lead to the evolution of various "cape" ecosystems wherein additional sensors, connectivity, or other functionality can be obtained through hardware peripherals available at nominal price points. But if you are trying to decide between Bluetooth Smart or 6LoWPAN for a wearable device, or whether adding a temperature or proximity sensor will really help push your smart home monitor over the top, the development time and cost of integrating additional capes can add up quickly, particularly when trying to move from the drawing board to a cloud-connected proof of concept in the fast-paced world of IoT.

So, how do you reconcile the low cost of DIY development boards with the functionality of a full-blown embedded development platform? If you ask Jarle Boe, System Applications Manager at Texas Instruments, the answer comes from kits that add as many faculties as possible "because they can."

SimpleLink SensorTag: More hardware options, quick cloud access

In a May media briefing, Boe and his team out of Oslo, Norway unveiled TI's new SimpleLink SensorTag platforms, a suite that includes development packs (a Debug DevPack, Display DevPack, and LED Audio DevPack) for engineers looking to get a head start on IoT designs (Figure 1). Out of the box each kit contains 10 low-power sensors, which may seem like overkill on the surface, but as Boe points out, "it's much easier for anyone using our design as a starting point to remove sensors than to add new ones."

Figure 1 Based on the SimpleLink CC2650 wireless MCU that targets Bluetooth Smart, ZigBee, and 6LoWPAN applications, the Texas Instruments SensorTag development kit provides 10 sensors and quick-connect cloud access for rapid IoT prototyping and development.

More importantly, though, is multiprotocol wireless support permitted by the onboard CC2650 wireless MCU with an integrated Bluetooth Smart, ZigBee, and 6LoWPAN radio. Since most IoT products begin as a simple sensor application, the support for multiple 2.4 GHz wireless standards allows developers to easily test and switch between connectivity solutions with a simple software download as application requirements evolve – where the process of reading, downloading, and patching to get Linux-based gateways off the ground can sometimes be days long, this capability can significantly reduce development time and cost.

The SimpleLink SensorTags also include access to the IBM Bluemix IoT Foundation, which facilitates cloud access in matter of moments using the IBM Quickstart cloud. From there, all that's needed to connect your sensor and start developing cloud-based applications is to download the SensorTag app, turn on the sensortag, and wait about 90 seconds for the sensors to start advertising their data. According to Boe, the process shouldn't take more than three minutes.

Open season for IoT

Originally labeled as tinker toys for hobbyists, open hardware and software platforms have carved out a space in the embedded market as the starting point for many high-volume product deployments. They represent one of the few areas where business models permit collaborative synergies between the tech establishment and grassroots organizations. If only in an effort to help grow the pie, the resulting innovation will yield new applications and services that benefit industry as a whole. This is IoT.

To view a video demonstration of the new SensorTag platform, visit opsy.st/SensorTagDemo. ECD

A development platform for all kinds of makers

By Monique DeVoe, Managing Editor *mdevoe@opensystemsmedia.com*

The number and variety of DIY boards available today is quite amazing. There's a board for every level of maker from beginner students to advanced professionals, but no matter the level they all seem to have a steep learning curve to get to your first blinking LED. For those new to electronics and programming this perceived barrier to entry can be a deterrent to getting started. Jason Gouw, electrical engineer, lifelong maker, and Co-founder of Qfusion Labs (www.qfusionlabs.com), saw an opportunity to bridge this gap and make DIY electronics more accessible.

The inspiration

As an engineer for ferryboat services, Gouw often used industrial automation programmable logic controllers (PLCs) on the job.

"PLCs are a very modular system so it's very easy to add on modular blocks for controlling motors, lights, whatever, and programming them uses ladder logic, which is a fairly easy way to create programs other than coding," Gouw says. "I took that concept and thought why don't we have this for a consumer that's a little bit more cost-effective and friendly to use?"

With this approach in mind, Gouw, along with his software engineer brother Marvin Gouw and some friends, built the Cubit Controller and Workshop visual programming tool.

The platform

The 1.6" x 1.6" x 0.4" Cubit Controller hardware consists of a 32-bit MCU, built-in Bluetooth, a multicolor LED, a programmable button, and six Smartports which all can be used to power Cubit and to connect Smartware add-on modules. The Smartwares – the 20 of which so far cover the basics like servos, sensors, buttons, LEDs, and a custom connector – have embedded chips that do all of the handshaking in the background so users don't have to know how to wire or configure the electronic components. Through Bluetooth the Cubit Controller wirelessly pairs with a computer for programming through Workshop and loading the program back to the Cubit Controller.

In Workshop, makers can drag and drop program blocks and connect the "wires" in their project diagram. Behind the scenes, clicking launch causes Workshop to convert the visual blocks into the Lua open source scripting language and loads the code onto Cubit's MCU.

A tool for learning and customization

Workshop doesn't have to be a replacement to learning how to code. The Qfusion Labs team is working on a way to expose the underlying Lua code behind the visual code blocks so users can see the resulting code, make adjustments, and create their own Lua code.

"We want people to be able to understand the visual blocks," Gouw says. "They'll be able to zoom in on the block, expand it, and actually see the underlying code behind the block. It's not up right now on our beta, but we will probably have that available on the first release or on the second run."

But Cubit is not just for beginners. It's designed to expand from a maker's first experience with DIY platforms to those with advanced knowledge. With custom Smartwares, advanced makers can wire in their own sensors, customize code blocks in Workshop, and use a library to control hardware directly; they can use their skills, but they won't have to focus on the simple stuff that's tedious to do by traditional coding. Gouw says it can be a challenge to convey that the platform is for the full spectrum of makers, but he thinks as skilled engineers see what Cubit is capable of they'll see the advantages.

Once you've got a project idea, it's a very quick platform for creating the electronic and code portions of projects.

"With all our projects the electronics have always taken around five minutes to connect because they're all plug and play, and it'll take anywhere from 10 minutes to half an hour to create the programs on the Workshop visual programs. If I were to do that in traditional code it would take me hours," Gouw says. "The most time-consuming part is still the mechanical components like cutting things out of wood, 3D printing things, and designing parts." ECD

For more on the Cubit platform hardware and software features and the next steps for Qfusion Labs read the full article at opsy.st/CubitPlatform.

Connecting devices to the Internet of Things with Wi-Fi

By Nikos Vokas

Developers, vendors, and manufacturers are rushing to join the Internet of Everything, creating new types of products, systems, and devices to make our lives more efficient and comfortable. Many of these are based on Wi-Fi technology to link them together, as well as connecting them to wireless access points that in turn connect to the web and cloud-based intelligence.

As a result, many designers, instead of trying to handle the complexity of developing their own wireless systems for their Internet of Everything products, are instead choosing to use pre-certified fully integrated Wi-Fi connectivity solutions. Created specifically to help designers meet these new challenges, these embedded modules and software provide a cost-effective way for Internet of Everything product makers to get their products to market more quickly with less cost and less risk.

Important features for Wi-Fi connected IoT devices

What Wi-Fi standard does the module support? Depending on the end use, it is often essential that modules support all existing flavors of Wi-Fi, including IEEE 802.11b/g/n standards at data rates of up to 20 Mbps.

In addition to basic 802.11 capabilities, the firmware should also include support for advanced Wi-Fi features such as DLNA, Wi-Fi Direct with P2P-Client, and P2P-GO plus the full range of security options (WPS 2.0, WEP, and the personal and enterprise versions of WPA/WPA2), HTTPS/SSL security stacks, a DHCP Client/Server, a Configurable Web Server, and standard TCP/UDP Sockets to name a few.

To speed up the design process, developers can select Wi-Fi modules that are equipped with internal flash and integrated antenna, and are certified for all agencies. For designers who plan on shipping products worldwide, it is important that the radio section is pre-certified and offer internationally compliant solutions – this can dramatically shorten acceptance cycles and ultimately reduce time to market.

The Wi-Fi modules should incorporate an MCU that supports the 802.11 protocol stack, a full-featured TCP/IP Stack with the accompanied network applications, data security, and also provisioning methods for device configuration. The MCU is also responsible for exchanging data and control signals with the host system via U(S)ART, SPI, I2C, I2S, or SDIO interfaces.

The application software should also include cloud services support to assist in the development of cloud-based applications for use with the IoT. In a similar manner, home entertainment and home automation applications need to be supported via Digital Living Network Alliance's (DLNA/UPnP) protocol stack or alternatives like Apple's Airplay.

A new feature to recently emerge allows Wi-Fi connection settings mass configuration technology to be built into modules for simplified out of the box configuration and rapid registration of devices on existing Wi-Fi networks. Called "ProbMe," it enables device manufacturers, system providers, and end users to simultaneously install, set up, and configure multiple Wi-Fi devices with minimal user input.

It works by utilizing the discovery functionality of Wi-Fi networks. Instead of using the standard 802.11 management frames to interrogate the surrounding networks for their SSID information, the ProbMe method uses these frames as configuration carriers. This enables the Wi-Fi module to recognize when it is receiving configuration information and then utilize that information to configure itself on the network. With multiple devices are ON and awaiting configuration information, all of them can be provided information simultaneously with the same SSID and pass phrase, or SSID and WPS information. This means it is possible to configure 10, 100, or even 1,000 devices all at the same time with one configuration command.

Once the Wi-Fi device is configured with this information, the module by default disables the ability to be reconfigured and requires a physical button be manually pressed on the device in order for the device to be placed back into configuration mode. Various manufacturers could elect to set up secure approaches to access the reset capability through a physical button or software.

Installation/setup challenges

Today, most devices that users connect to a Wi-Fi network need a service set identifier (SSID) and a pass phrase, which is generally longer than a password. Manufacturers of wireless routers initially supplied routers with a default and generic SSID and open settings that required no

pass phrase to join the network. However, most router manufacturers now provide more unique SSIDs and initial unique pass phrases that are printed on a sticker on the Wi-Fi router. This means that when the router is turned on, it comes on in a secure mode with a set SSID and pass phrase. Anyone wanting to join the network then uses the "Join Network" or "Add Network" utility on a smartphone, tablet, laptop, or desktop. A user can easily join and rejoin the network and when moving between locations.

Over the last decade, most of the devices that consumers have been connecting to Wi-Fi wireless routers have had rich computing resources – displays, keyboards, and other abilities – that make entering the information for a secure connection relatively easy.

However, the "things" now being added to homes, offices, commercial spaces, and industrial facilities are quite small and don't have a display or convenient data entry capability to allow users to configure them. Thus, the devices need to be configured by a smarter device that can transmit the necessary configuration information to join the network.

For instance, a consumer buys a Wi-Fi enabled coffee maker. The coffee maker needs to know the SSID and pass phrase so it can connect to the network as a client device to allow the user to turn the coffee maker on and off remotely, change brewing settings, get a signal that the coffee has finished brewing, and possibly connect the coffee maker to the cloud for even more advanced features. Today, there are a couple of options for manufacturers who want to put Wi-Fi capability in a coffee maker.

One option is to use a Wi-Fi protected setup (WPS) button on the coffee maker and assume the user's wireless router has a WPS button as well. This requires the user to press the button on the coffee pot and also press the button on the wireless router.

This approach works well if both devices and their set up buttons are easy to access. However, if the wireless router doesn't have a WPS button or if it isn't easily accessible, this system won't work at all. Also, if both buttons are pressed and the coffee maker doesn't show up on the network, there's no way to troubleshoot. Most importantly, the WPS push-button method has known security flaws.

Another common approach is to have the coffee maker appear as an access point with its own SSID and pass phrase, which is supplied on the manufacturer's quick start card. In this approach, when the coffee maker is plugged in and powered on the SSID of the coffee maker is broadcast so that it is easily identified. A user disconnects from the wireless network, connects wirelessly and directly to the coffee maker, and navigates to an area to enter the SSID and network pass phrase. The device is then configured as a client on the user's network.

The main disadvantage of this method is the required level of technology expertise. Also, the process can be quite time consuming, which is compounded if there are several devices to install, such as light switches, light bulbs, outlets, speakers, cameras, door locks, thermostats, alarms, and so on. Most importantly, this may not be the most

secure approach depending on how the manufacturer decides to handle the start-up scenario. In some cases, consumers may not decide to configure the Wi-Fi feature to their wireless network, and thus, it would remain visible to everyone within broadcast range of the device. A next-door neighbor could find and then take control of another neighbor's coffee maker.

An alternative method

Let's assume that the user has a device on any operating system. Let's assume the user does not have physical access to wireless router. Let's also assume the user is minimally tech-savvy, and able to navigate the basic menus required for getting the device configured on the home's network. And, finally, let's assume that the user doesn't want to announce to the world a coffee maker on the Wi-Fi, nor does the user wish to have an unsecured coffee pot, an easy target for neighborhood shenanigans.

A user would need the coffee pot to power on in a listen-only mode and await configuration. Based on the type of device, it might be desirable to configure in a particular mode or a specific network. And it would be ideal that when multiple devices were turned on out-of-the-box, if all of them could be configured identically with one single entry by the user. Then, after configuration, to keep out the drive-by hackers, it would also be nice for the device to lock itself down from future reconfiguration, assuring it could only be managed by authorized users. This would likely require a user to have access to the device to push a reset button if the device ever needed to be reconfigured.

Now imagine an alternative scenario to the ones described above. In this scenario, the user brings home the coffee maker. After plugging it in, looks at the quick-start card, then using a smartphone enters the proper network SSID and pass phrase, and finally clicks, "Join Network." The smartphone transmits the configuration information and automatically connects all the new ProbMe-enabled devices to the network.

Nikos Vokas is an FAE at Econais.

Econais
www.econais.com
@econais
linkedin.com/company/econais
www.facebook.com/econais
plus.google.com/+Econais/posts
www.youtube.com/user/econaiswifi

The distribution of things: IoT, M2M, and software distribution

By Curt Schwaderer, Editorial Director *cschwaderer@opensystemsmedia.com*

The Internet of Things combines smart devices and sensors with analytics and the cloud. This paradigm shift presents new challenges involving software distribution, updates, and security.

The world is evolving into an "everything as a service" environment and the embedded industry is no different. Internet of Things (IoT) applications make heavy use of the cloud and this new paradigm is essentially what differentiates IoT from traditional networked embedded systems.

Previously I've covered various industry IoT applications and capabilities from the component and functions points of view. However, the proliferation of IoT and M2M applications within the context of the cloud is giving rise to a unique challenge involving how to coordinate and deliver new software features, updates, and/or distributions to these devices.

Software updates are essential

Within the context of IoT and cloud applications, the ability to soft-configure the system is critical and an essential part of the motivation for moving traditional networked embedded systems in this new emerging direction. These kinds of capabilities offer the ability to quickly deploy new features and capabilities at a fraction of the cost. New capabilities promise lower cost and increased revenue. The ability to quickly, securely, and flexibly update any cloud-based service is essential in order to take advantage of the benefits this environment provides.

Further, within the cloud itself, adding new services can adversely affect the security of the existing hosted services. For these reasons, new tools, capabilities, and techniques are emerging to coordinate and synchronize software distribution.

Software distribution and DevOps

JFrog (www.jfrog.com) is a company positioning its products and services to become the de facto standard for software development and distribution for IoT, M2M, and cloud environments.

I discussed software distribution challenges with Fred Simon, Co-founder and Chief Architect at JFrog. His perspective on the software distribution and coordination side of IoT applications reflects JFrog's thought processes behind these challenges. My leading question asked about the software distribution process for IoT.

"I'm not completely sure how to respond to that question," Simon says. "The broad range of IoT services and applications makes that question hard to answer. For higher-end applications involving things with larger storage and compute power like game consoles or smartphones, continuous deployment mechanisms may be involved. For smaller sensor and data driven applications, it's about having a local server that manages pushing firmware into the device. Data driven applications involving sensors also typically have a need for aggregating information into servers that are distributed, but closer to the sensors. The software on these sensor data aggregation servers also needs to be managed and updated."

Software distribution considerations

The software distribution process involves software developers and software users. The developers are creating the software and utilizing a variety of integrated development environments (IDEs), code repositories, automated test, and continuous integration tools. Once the production binaries are created and tested, these binaries need to be controlled, stored, and managed throughout the release. Simon calls these "binary artifacts" and the JFrog Artifactory service bridges the developer tools and remote repositories in the cloud. It's important for binary management solutions to integrate with popular repositories, build tools, and continuous integration servers. Simon mentions Artifactory does this and adds the dimension of management, synchronization, and control of binaries and their distribution to remote repositories.

The other consideration is how developers store, publish, download, and distribute software. The cloud environment adds significant complexity. In many IoT instances, endpoints may be a variety of platforms with end users that may or may not upgrade in a timely manner. These issues complicate the distribution process and the JFrog Bintray solution provides this level of control.

Developers can control what versions of binary, software packages, or microservices are to be made available, which end users are allowed to update services, and also incorporates push notifications of new software availability.

Authentication, verification

Given this fully automated management and distribution environment, Simon is fully aware of the security considerations involved.

"Within a networked environment such as this, it's important to have security features that authenticate developers, users, and binary artifacts in order to minimize security risks," Simon says. "We incorporate many signing mechanisms at various levels to ensure security within IoT, M2M, and cloud environments."

Simon admits that there is a need for standardization around different authentication elements within an IoT environment. He mentioned a VMware project called Lightwave – an open source project comprised of standards-based identity and access management services targeted at security, governance, and compliance challenges for cloud-native applications[1].

For the developers, Simon says there is a significant amount of authentication and access permission capabilities in order to authenticate software loads into the cloud environment. For the users, there are a number of rights and permissions features in order to ensure end users get notified or automatically updated with software that is signed, verified, and contains only the features the end user is licensed for.

Corruption and rollbacks

When asked about accidental corruption or non-working components, Simon explained a couple of approaches. First, in order to alleviate complications involved with downloading of incompatible components, it's important to make sure the binary objects are thoroughly tested and ready for release. Second, when managing binaries and software packages you don't modify – you always create a new version. This way you avoid situations where bits and pieces get downloaded that might cause problems. It's important to update packages everywhere and consistently. In case of emergencies, Bintray has the ability to perform rollbacks, but that's to be avoided at all costs.

Facilitating change

Paradigm shifts often usher in new methods and processes designed specifically to support emerging changes. The presence of cloud services coupled with flexibility, reach, and distribution of IoT and M2M end devices and applications requires a new approach to software maintenance, versioning, and distribution. ECD

Reference

[1] Introducing Project Lightwave, VMware, http://blogs.vmware.com/cloudnative/introducing-lightwave/. For more information about JFrog, visit www.jfrog.com.

5 steps to secure embedded software

By Bill Dickenson and Vijayakumar Kabbin

As more and more functionality is embedded into smaller and smaller device footprints, security concerns rise. Often new features crowd out basic security concerns as vendors pack more and more functionality into the package with very little overall systems engineering, and only cursory security testing.

The embedded environment has matured to where security must move to the forefront much the way security did when the PC evolved in the 1990s. With the explosion of the Internet of Things (IoT), there is little doubt that any security flaws will be exploited. IoT devices enable highly useful business cases to come to reality. At the same time, they bring the risk of losing control. Today's embedded systems are far more powerful and vulnerable. If embedded systems are to avoid the pitfalls of the 1990s, protocols and approaches must be in place before they become the entry point for a new generation of hackers.

IT standards groups, like the Consortium for IT Software Quality (CISQ), MITRE Common Weakness Enumeration (CWE), and ISO 9000 and ISO 25000, publish guidelines and software quality standards. CISQ has published automated quality measures for security, reliability, performance efficiency, and maintainability. These measures provide some of the specific attributes that should be used as evidence that embedded systems might need to fulfill their business/mission function. While examining the state of embedded systems, it is apparent that security should be engineered in up front.

Implementing a security strategy

When considering security, most embedded systems engineers immediately focus on the problem of protecting data. Not only should the system protect data (within the application), but should also protect the interfaces from abuse. These five steps represent a reasonable starting point for developing an embedded security policy.

- **No untested programs in the execution space –** No programs other than the programs necessary to execute the functions should exist in a place where they can be executed
- **Data must be private –** Programs should not expose information to each other or to the network unintentionally
- **Confirm data at both ends –** All information must be able to be verified and must be within expected ranges with out-of-bounds information rejected
- **Secure devices –** Devices should have the capability to verify their integrity during boot time; devices should authenticate themselves before transmitting or receiving data
- **Follow the standards –** Look at the Consortium for IT Software Quality (CISQ) quality characteristic measures that can be automated for ongoing security and software quality analysis and mitigation
- **Take action –** If an anomaly occurs, the program must continue to function while handling the issue

No untested programs in the execution space

As embedded vendors strive to differentiate their products, they add programs to their standard distribution. Many of these will not be used and represent a potential security risk. These programs must be eliminated or, even better, never installed at all. Ask for an OS distribution with nothing in it beyond the essentials for the OS to work and install the programs manually. A minimalist strategy is the best for code. If the vendor does not provide stripped down distribution, the OS can restrict access rights for these programs and sensitive APIs, or the unused code can be deleted.

A better way is to provide a sandbox for custom and third-party applications to execute and then push communications through APIs, which provide the necessary isolation.

The hardware itself should be "clean" with no programs installed. It is key that any programs on the device are installed by the developer. Every piece of code must come from a trusted developer and cannot be altered prior to installation.

Data must be private

Programs should not expose information to each other or to the network unintentionally. Tempting as it is to believe that a device cannot be hacked on the Internet, it simply isn't reality. As modules within the program grow, data artifacts tend to grow with them and data tends to become increasingly exposed.

Embedded devices collect sensitive data (e.g., healthcare, enterprise) and there is a strong possibility the data traffic can be rerouted and modified before it reaches its destination. There should be checks to prevent copying and pasting as well as the ability to remotely wipe data if a device falls into the wrong hands.

Developers under pressure to meet deadlines tend to borrow code and routines from themselves and colleagues. Any security flaws will be propagated. Design and build the code right the first time.

Confirm data at both ends

All information must be verified, within expected ranges, and identified clearly. Using the same routines on both ends to validate content is essential. Interfaces should be sensitive to what comes in and be able to take action when the data is not correct. When a device receives bad data from a device that is "trusted," the intrusion is likely a hack. This is also true for direct hardware interfaces.

Like privacy, all connections to the external world need to be treated as suspect. Interfaces should be verified and data examined.

Secure devices

Devices should have the capability to verify their integrity during boot time and should authenticate themselves before transmitting or receiving data. Knowing who is sending the data is important, and one of the simpler hacks is substitution of unverified devices.

When booting up, devices must use cryptographically generated digital signatures. Resource-constrained devices could use unique hardware characteristics instead of compute-intensive algorithms to generate digital signatures for authentication. Devices failing that check should have a planned response.

Each device should have a key and each device should know the acceptable key for its type. When an unidentified key is received, the response should be planned, not simply ignored. If the receipt of the information is critical to the function of the device, receiving an errant ID more than once should be considered an attack. Planning for this fault is essential.

Follow the standards

CISQ has published a security standard that is designed to identify the top 25 known security weaknesses in IT application software as maintained by MITRE in the Common Weakness Enumeration (CWE). The CWEs are a measurable set of items that can be used as evidence for resiliency, security, and safety. Code analyzers such as CAST can pick these out of a complex environment. Developers should stay in constant touch with these important standards.

Take action

If an anomaly occurs, the program must continue to function while handling the issue. Developers normally focus on what happens when good data is received but error handling is typically simplistic. Developer training assumes that bad data is an artifact of programming, and not a hack, which is a policy that needs to be reviewed. Conduct assurance case testing on all key components. Assurance cases support the iterative review and revision of the implementation until the system displays the right behaviors.

In some cases there may be a way for the device to notify another that it is under attack. In other cases it may simply choose to ignore or work around the threat. In either case, communication is a powerful weapon to avoid hacks.

Bill Dickenson is an independent consultant with Strategy On The Web.

Vijayakumar Kabbin is General Manager with Wipro Technologies

Object Management Group

- www.omg.org
- @ObjectMgmtGroup
- www.omg.org/in
- www.omg.org/fb
- www.omg.org/ggl
- www.omg.org/yt

Code Generation – Why and How?

By Cyrille Comar, Co-founder and Managing Director, AdaCore Europe

Programming languages are all about providing human-friendly formalisms to describe what we would like the computer to achieve for us. The original appearance of programming languages such as Fortran, Algol, or C provided a significant expressiveness improvement over assembly languages which were themselves a huge improvement compared to writing programs directly in the binary form that is expected by the hardware.

Unfortunately, increasing automation is ubiquitous these days so that non-computer specialists are finding themselves pushed towards developing the software they need. Having established the fact that general purpose languages are not a fit to their skillset, a new set of languages have emerged, specific to domains, known as Domain Specific Languages (DSLs). In an effort to be friendly to non-programming specialists, they have a tendency to being based on a graphical syntax, as opposed to a textual one, and are often referred to as modeling languages. We are talking here about systems such as Matlab Simulink®, and Stateflow®, used by control theorists to design dynamic reactive systems such as an aircraft flight control system.

The problem with the proliferation of these domain specific languages is that they will have to provide answers to all the problems the software engineering community has been busy solving the past 30 years, such as long term maintainability, portability among hardware and OS platforms, adherence to recognized industry standards, interoperability with other modeling or programming languages, etc.

One way to avoid reinventing the wheel completely is to convert this new approach into terms that are already familiar to the software community. Hence the idea of automatically translating these DSLs into more traditional programming languages. This is what is called "code generation from models."

Current industry standards, especially in regulated industries such as avionics, railway, or automotive, have recently started to recognize the importance of modeling and have started offering guidelines for their usage. The main objectives of these guidelines is to answer two distinct questions:

- If I develop a model, how can I ensure that the generated code will respect the model semantics?
- If I verify the model, how can I ensure that the result of the verification still holds once final code has been generated and run on the target?

QGen

QGen is a technology that has been inspired by the requirements from high integrity industries, such as avionics and railroad. In fact, QGen is built to target TQL-1 qualification for DO-178C, SIL4 certification for EN-50128, and also MISRA requirements for C. In other words, QGen was designed with evidence that the generated code respects the semantics of the input model, and that no safety issue is introduced during the code generation phases.

QGen is integrated with a complete development environment, including a compiler, a structural code coverage tool, a debugger, an emulator... It provides an end-to-end solution, from the model to the binary code, enabling control over the whole production chain. This eases verification of the application after code generation, as well as simplifying the integration with manually written code.

As the president of a company that sells development tools, I am often asked why our teams are working on modeling and code generation. The truth of the matter is that the required skillset matches that of our engineers and technical challenges are very similar to what we are already facing on a day-to-day basis. At the end of the day, model-based development and traditional coding are two synergistic techniques to efficiently create maintainable and reliable software. AdaCore's mission is to help achieve that.

AdaCore | *www.adacore.com*

Medical device 3D graphics challenge systems hardware developers to build with consistency and longevity

By Martin Rudloff

Blending long-life embedded designs with commercial graphics components is a reality facing OEMs and developers. Understanding how to optimize choices for ideal performance and overall cost management is essential – along with collaboration with manufacturing partners for the most strategic long-term stocking programs. New commercial graphics options extend performance life and reduce total cost of ownership.

Enabling embedded graphics performance may be one of the most challenging design issues facing developers today. Even as designers work with some of the most versatile, energy-efficient, and technically advanced x86 processors to date, onboard graphics performance remains a feature that has not kept in step with demand. Certain high-growth embedded markets just require more, driven by a growing reliance on 3D, media-centric embedded applications that are reshaping and improving the end-user experience – illustrated by treatment advances through more detailed imaging in medical systems. Better imaging supports physicians in all areas of treatment from diagnosis to surgery, adding new value to traditional technologies such as X-rays, which lose volumetric data and depict the patient in only two dimensions. In contrast, 3D capabilities maintain the volume of an image, for example adding greater information on the shape, size, and position of a tumor. For developers, this evolution places greater focus on graphics requirements as part of an overall development plan that considers both performance and longevity – assuring a graphics life cycle that meets performance expectations of long-term embedded deployments in medical settings.

What is the ideal option when faced with choosing between less sophisticated onboard graphics or stronger commercial solutions that lack the inherent longevity required for embedded deployment? Sacrificing performance is not an option, and embedded system developers must plan carefully to maintain graphics availability, longevity, and consistency.

Contrasting 2D and 3D requirements

Steady advancements in x86 processors include notable improvements in CPU, graphics and media performance, illustrated by 4th generation Intel Core Processors (formerly codenamed Haswell). While 4th generation Intel Core processors include the HD 4600 GPU to handle advanced graphics processing, its features are optimized for 2D applications, and media functions such as high-resolution imaging or playback of high-definition video.

In contrast, newer graphics cards are intended for 3D graphics performance, functioning almost like a math coprocessor used to supplement performance of the CPU. Without impact on CPU resources, they readily handle the extreme computing

calculations necessary for complex 3D visualization. What side of the object is visible or shaded, where does the brightness fall when light lands on the image, how smoothly does the image turn – these types of movements require intense computational power that must be offloaded from the motherboard or CPU.

Addressing a graphics processing gap

The divide between x86 and card-based graphics performance appears to be a permanent issue, as 3D capabilities are not called out in Intel's embedded roadmap. The onboard HD 4600 GPU is a strong, proven option designed to accommodate an end-user's audio-video experience, and is not intended to handle the heavy processing requirements of 3D applications; cost would be prohibitive to change this model. For example, current graphics cards have more transistors than the 4th generation Intel Core CPU itself, making it unlikely that onboard video is going to compare favorably to a discrete graphics processing option. (Nvidia's Kepler generation of GPU products contain 7 billion transistors.) Graphics technology players like Nvidia have only to focus on improving graphics performance, while each x86 advancement incorporates improvements to every facet of the chip.

Yet embedded developers in markets such as medical imaging must consistently address demand for 3D graphics. Diagnostics have advanced far past flat screen images and instead rely on real-time images that demonstrate volume and size; a surgical suite might have a 4K monitor to guide a procedure with the best possible imagery. These are realms that really must rely on long-life commercial cards for 3D graphics capabilities – mandating a design strategy that thinks outside of onboard x86 options.

Not all graphics cards are created equal

Graphics cards are available in different flavors, which may add some options for consideration by embedded designers. Commercial cards, originally intended for the gamer or maker market, deliver some of the strongest graphics performance available – however their average one-year life cycle is often untenable in the grand scheme of materials management for medical systems. It's not impossible, but a card of this type adds a significant amount of advance planning to maintain system performance for a multi-year, extended deployment, ultimately causing significant sustaining engineering costs.

Long-life commercial cards are an alternative, although "long life" means something different when compared to a component on a traditional embedded roadmap. Long life in terms of graphics cards is defined as perhaps three years, accompanied by much higher costs when compared to a regular commercial card. This is a new option, and may not be familiar to embedded designers. Cost may be a factor initially, yet should be evaluated carefully as these cards reduce operating costs over the long term. New software specifications, tools, or compilers may be needed to accommodate a new card; software re-certification could be required, and is often more challenging and costly than hardware certification processes. With a three-year life cycle, system operators face this less often and have fewer re-certifications, system tests, or driver changes that add complexity and cost to maintaining graphics performance. For medical OEMs and developers, this adds crucial value in minimizing additional FDA re-certifications.

Committing to card-based graphics

Nvidia is a recognized primary supplier of chips for graphics cards, including the commercial-grade GeForce and the long-life Quadro families. The company is also the originator of the CUDA core, used for compute-intensive applications such as animation or simulation and very popular among 3D design environments.

Nvidia's cards execute graphics functions using proprietary technology called PhysX, a scalable multi-platform solution purpose-built to meet the unique requirements of physics algorithms. Accelerated by its CUDA core, PhysX enables simulation-driven effects and represents a computing environment that's much different than a general purpose CPU – its primary focus is determining how objects

move and react to the environment around them. Other graphics solutions rely on OpenCL technology, an open standard used to provide a heterogeneous computing platform for parallel processing and high-performance graphics processing. Many 3D applications, such as medical imaging, industrial vision, or training and simulation, incorporate support only for the proprietary PhysX architecture. Once a system is based on PhysX, a move to OpenCL is very complex as it would require new development and an additional skillset in developing an OpenCL integration.

Building in longevity

Committing to card-based graphics drives developers to plan for obsolescence as a strategic consideration early in the design phase. Collaborating with a manufacturing partner in the initial steps of development assures the greatest number of flexible options, which vary according to OEM needs, volumes, and requirements. Stocking programs may include purchasing parts based on OEM forecasts; bonded programs source components and then stock and hold them based on the OEM's purchase order and forecast. Some designs require more secure partner stocking programs optimized to manage shorter life cycles, illustrated by Corvalent's purchase order-based, non-cancellable procurements for long-term, consistent stocking of components.

Given the unique design challenges of 3D performance, OEMs may not be fully aware of the requirements for creating a long-term bonded product and need to make sure all the right questions are addressed as part of the overall design strategy. Manufacturing relationships add value by working closely with suppliers like Nvidia and Intel, ensuring consistent, advance end-of-life notices for the most effective component management.

Meeting healthcare market expectations with strategic planning

Optimizing long-term performance is a balancing act that adds complexity to an already challenging medical design process. Systems designers often look to the most current and powerful graphics processors available – unaware they are considering components geared to the gaming community and bypassing commercial graphics options that may be more suitable for an embedded design strategy; at the same time, the OEMs that must support the medical system recognize the need to balance this with longer-life components. Risk analysis wins out, and the group typically evaluates immediate cost versus long-term cost of ownership as a deciding factor.

Viewing patient images in 3D is steadily improving treatment options – better data helps in every healthcare setting ranging from surgery, trauma situations, or routine treatment. As graphics-based applications become even more prevalent in clinical decision-making, it is essential to understand options, including the capabilities of x86 onboard processors as well as commercial and long-life graphics cards. New, extended-life graphics cards and their associated costs must be evaluated in terms of an overall system strategy. Greater upfront costs reduce long-term total cost of ownership for medical deployments – providing a more efficient path for replacing or upgrading cards, and delivering on the promise of 3D applications. This design approach requires planning, relying on technical and experienced manufacturer support in ensuring longevity, consistency, and availability for extended embedded deployments.

Martin Rudloff is Chief Technology Officer at Corvalent.

Corvalent
www.corvalent.com
@Corvalent
linkedin.com/company/corvalent
opsy.st/CorvalentFacebookOSM

INNOVATIVE PEOPLE AND PRODUCTS IN EMBEDDED

TOP EMBEDDED INNOVATORS

Embedded Computing Design's Top Embedded Innovators issue is where we showcase the talent of the embedded industry. In our fourth annual Innovator issue we had a great response to our call to nominate exceptional people in the embedded industry. The nominees' roles and contributions covered a wide range, including innovations in new and fast-growing industries like the Internet of Things, fundamentally important areas like security, and examples of their great business sense as market leaders bringing success to their companies and to the growth of the industry as a whole.

With such an impressive group of embedded innovators to choose from, narrowing it down to the top three was difficult for the *Embedded Computing Design* team of Rich Nass, Brand Director, Curt Schwaderer, Editorial Director, Monique DeVoe, Managing Editor, and Brandon Lewis, Assistant Managing Editor. After much deliberation we settled on three winners to represent *Embedded Computing Design*'s three sections, Silicon, Software, and Strategies: T.J. Rodgers of Cypress Semiconductor, Jean Labrosse of Micrium, and Dr. Stan Schneider of Real-Time Innovations (RTI). To read about our 2015 winners and their contributions that stood out to the team, see page 22. Our six honorable mentions can be found on page 23. Read the Q&As with our winners on the challenges they face, the innovative strategies they use to overcome them, and what they see as the next big areas for embedded, starting on page 24.

The innovative people are just one half of *Embedded Computing Design*'s Innovation issue. What innovative people in the embedded industry develop are innovative products. This issue features all the nominations submitted to be one of three Top Innovative Products. The winners will be announced in the August Resource Guide issue. See the nominees beginning on page 27. If you have any experience with these products or know which you think should be the Top Innovative Products for 2015 let us know!

TOP EMBEDDED INNOVATORS

T.J. Rodgers, President and CEO, Cypress Semiconductor

T.J. Rodgers is Founder, President, CEO, and a director of Cypress Semiconductor Corporation. He founded Cypress in 1982 and took it public in 1986. He is a former chairman of the Semiconductor Industry Association (SIA) and SunPower Corp. (solar energy systems), and he currently sits on the boards of directors of high-technology companies, including Agiga Tech (nonvolatile RAMs) and Bloom Energy (fuel cells). He is a Trustee Emeritus of Dartmouth College, his alma mater.

Contributions to embedded computing innovation

T.J. greatly simplified embedded design with Cypress' PSoC programmable system-on-chip and supporting PSoC Creator integrated development environment and PSoC Components. T.J. also drove Cypress' creation of its SONOS (Silicon Oxide Nitride Oxide Silicon) embedded flash memory and the licensing of this IP for MCUs and a broad range of applications.

SILICON

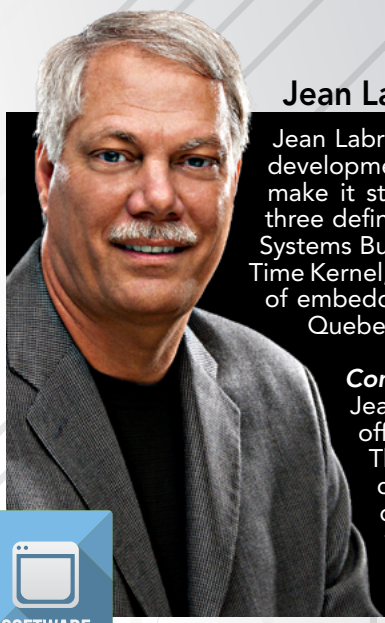
Dr. Stan Schneider, Chief Executive Officer, Real-Time Innovations (RTI)

Stan Schneider is CEO at Real-Time Innovations (RTI), the Industrial Internet of Things connectivity platform company. In 2014, Stan was elected to the Industrial Internet Consortium Steering Committee. Stan has published more than 50 papers in both academic and industry press, and is a seasoned speaker at industry events and conferences. Before RTI, Stan managed a large Stanford robotics laboratory, led an embedded communications software team and built data acquisition systems for automotive impact testing. Stan completed his PhD in Electrical Engineering and Computer Science at Stanford University, and holds a BS and MS from the University of Michigan.

Contributions to embedded computing innovation

Elected by his peers, Stan serves on the Industrial Internet Consortium (IIC) Steering Committee. The role includes fiscal oversight and setting up subcommittees such as research selection, test bed creation, and defining standards requirements and priorities. In addition, Stan has an impressive record of academic and industry published papers and speaking engagements on topics ranging from networked medical devices for patient safety, the future of connected cars, the role of the DDS standard in the IIoT, the evolution of power systems, and understanding the various IoT protocols.

STRATEGIES



Jean Labrosse, Founder, CEO, and President, Micrium

Jean Labrosse founded Micrium in 1999 and continues to maintain an active role in product development, ensuring that the company adheres to the strict policies and standards that make it strong. Labrosse is a regular speaker at industry conferences. He is the author of three definitive books on embedded design: MicroC/OS-II, The Real-Time Kernel; Embedded Systems Building Blocks, Complete and Ready-to-Use Mod-ules in C; and µC/OS-III, The Real-Time Kernel, and has published numerous articles and appeared on industry panels on the subject of embedded design. He holds BSEE and MSEE degrees from the University of Sherbrooke, Quebec, Canada.

Contributions to embedded computing innovation

Jean developed the first RTOS kernel that was published with full source code. µC/OS offered a highly portable RTOS kernel that was easily adaptable to any CPU architecture. This transformed the industry because RTOS vendors then started to provide source code with their products. Jean expanded the embedded engineers toolbox by developing µC/Probe, a program that allows run-time data in an embedded system to be displayed or changed through graphical objects, from a Windows-based PC. The user doesn't need to instrument the code in any way in order for µC/Probe to access target data, revolutionizing ease of use.

SOFTWARE

HONORABLE MENTIONS

Marko Kiiskila,
Principal Engineer,
Ayla Networks
Kiiskila has been a major innovator in the industry's first Agile IoT Platform. He developed an Over the Air (OTA) update process (patent pending) that uses patches with embedded devices. Kiiskila also architected Ayla's Agile IoT Platform to be device agnostic, easy to use, and connect any device to the cloud without writing any device specific code.

Glenn Perry,
Vice President and GM of Mentor Graphics Embedded Systems Division, Mentor Graphics Corporation
Perry helped established the electronic industry's largest embedded software portfolio and ecosystem based on enabling technologies and partnerships to advance embedded development. This includes an automotive software portfolio that spans every aspect of embedded software in the vehicle.

Ween Niu,
General Manager,
USA, Advantech
Since taking the post as GM, Niu has achieved 3,000 percent growth for Advantech. His direction and guidance to realign the organization to have better vertical market support was unique and demonstrated out-of-the-box thinking.

Rose Schooler,
VP, IoT Strategy and Technology, Intel
Schooler helps deliver platforms for networking and storage. She is also responsible for enabling solutions for telecommunications service providers. Schooler joined Intel as a graduate rotation engineer and progressed all the way through the company to her present position.

Costas Pipilas,
VP of Software Development and Co-Founder, Econais
Pipilas' rethinking of the integration of Wi-Fi modules as native to electric and electronic devices simplifies the upgrading of existing devices into IoT devices. Additionally, ProbMe, a mass configuration capability that ensures improved security and rapid installations for both consumers and installers, allows many devices to be installed configured to the network instantly.

Vegard Wollan,
Vice President and General Manager, Touch Business Unit, Atmel Corporation
Wollan is the co-inventor of the AVR microcontroller architecture. In addition, he saw the need for an MCU-based flash memory, which could be reprogrammed as often as needed, even in-circuit. Wollan also helped to organically develop a community of more than 230,000 members in the AVR Freaks community to discuss technical the AVR architecture.

TOP EMBEDDED INNOVATORS

Q&A

Silicon: T.J. Rodgers, President and CEO, Cypress Semiconductor Corp.

Q What are the largest obstacles to innovation in the embedded realm, and how should those challenges be solved?

Cypress solicits and records customer input in a number of very specific ways. Our customers consistently tell us that the top two challenges to innovation are making products that are easier to use and reducing time-to-market – both ours and theirs.

We address ease of use by creating complete solutions, which include not only our chips but also the software, kits, reference designs, application notes, datasheets, and technical support required for our customers to succeed. Each of these supporting elements must be intuitive to the design engineer and defect-free.

Q How do you stay on the leading edge of innovation, rather than just following the embedded crowd?

Programmable products have been a big differentiator for us. For that reason, we have continued to invest in programmable process technologies and in PSoC. We programmed an off-the-shelf PSoC to quickly jump into the touch business for smartphones. Apple used it to help enable its first iPod scroll wheel interface. PSoC derivatives helped Cypress to become the industry's No. 1 provider of capacitive touch-sensing solutions and enabled us to integrate the transceiver for the new USB Type-C standard into a new, single-chip USB solution in just a matter of weeks. Because the EZ-PD™ CCG1 USB Type-C port controller was first to market, the top-tier PC and cable manufacturers using it now have a leg up in the race to bring their own products to market.

Q How do you recognize when a new technology or application is one your company should invest/innovate in, versus a technology that will experience fast burnout?

At the end of the day, the market determines winners and losers. The market created the demand for touch technology and a new generation of USB connectivity solutions. Programmability simply enabled us to get our solutions to market more quickly.

Beyond that, Cypress is a process- and data-driven company with precise ROI standards for new products and new markets. We evaluate very carefully how our capabilities match up with opportunities. We move worthy opportunities that fall outside our short-term profitability model into our Emerging Technologies Division (ETD). Cypress funds the companies in this division in much the same way that a venture-capital firm bankrolls a startup.

ETD currently includes AgigA Tech, which develops high-density, battery-free non-volatile memories, and Deca Technologies, which has pioneered an approach to wafer-level packaging and interconnect technology. Some ETD businesses wash out, but others are home runs, such as Cypress MicroSystems, which created PSoC, and SunPower Corp., which we spun out in 2008 to deliver a $2.7 billion dividend to Cypress shareholders.

Q In the next 5 years, which embedded technologies, applications, markets, and geographic areas present the most interesting opportunities?

The automotive market represents our single greatest opportunity. The market for automotive chips is growing about 50 percent faster than the broader market. Our merger with Spansion positions Cypress as the No. 3 provider of memories and MCUs to the automotive market with a focus on many of the fastest-growing segments, such as infotainment, advanced driver assistance systems (ADAS), and instrument clusters.

Luxury cars rolling off assembly lines have up to 150 MCUs, but the demand for advanced functionality and the chips to enable it has been moving steadily into the mainstream automotive market. The most advanced automotive systems also require SRAM and NOR flash memories – two categories that Cypress and Spansion, respectively, have dominated for many years.

For more on how Rodgers and Cypress Semiconductor overcome market challenges, see the full Q&A at opsy.st/2015InnovatorsRodgers.

Q&A

TOP EMBEDDED INNOVATORS

Strategies: Dr. Stan Schneider, Chief Executive Officer, Real-Time Innovations (RTI)

Q What are the largest obstacles to innovation in the embedded realm, and how should those challenges be solved?

The "Internet of Things," or IoT will be the next great wave of connectivity after the Internet and the mobile revolution. The IoT, however, is bigger than both combined; there will soon be billions upon billions of devices. This will be the golden age of embedded.

Wearables, home thermostats, and other smart consumer devices will become part of daily life. That said, the big economic impact is not from smarter consumer gadgets. The real value is the opportunity to redesign our most critical infrastructure: transportation, energy, medicine, and manufacturing. These "Industrial IoT" distributed systems can get smarter and be more efficient, safer, and faster. Entire new classes of systems, like autonomous vehicles, smart, connected hospital rooms, and high-performance "microgrids" will fundamentally rewrite the way our world works.

The largest obstacle to this vision is the lack of "systems thinking." Traditional embedded systems, and consumer IoT for the most part, are standalone systems. Designers think of what chip, OS, and perhaps wireless or network connectivity they will need for their device. This is "device" thinking.

The Industrial IoT, on the other hand, is a systems problem. A connected IIoT system will run on many operating systems, networks, and devices. Those become secondary concerns. The systems problem is not about devices, it's about their interactions. The challenges are interoperability, overall systems data management, discovery of data producers and consumers, and scale. There is no way to build these systems with traditional programming techniques. Object orientation, for instance, works well for contained programs. But, exporting "methods" that can vary across a huge system means that every interaction is custom and every interaction is one-to-one. That's unmanageable at scale. Big systems are all about the data; the Industrial IoT embedded systems of the future will need a data-centric interaction approach. Data-centric interaction means modeling the data itself. Data-centric interfaces control data interactions like discovery, rates, reliability, delays, and security.

> "THE NEXT 5 YEARS WILL BE THE MOST TRANSFORMATIONAL IN EMBEDDED HISTORY.

Q How do you recognize when a new technology or application is one your company should invest/innovate in, versus a technology that will experience fast burnout?

We look for leverage due to connectivity. What can a distributed, intelligent system do that's really new and valuable? Another example from the medical industry: hospitals are packed with hundreds of types of devices, from respirators to oximeters to ECG monitors. Today, they are standalone systems. Working alone, devices find worrisome readings for all sorts of reasons. The resulting nuisance alarms are a real problem. As a result, 80 percent of all alarms are turned off. There are whole conferences on alarm fatigue. Patients go unmonitored. And, tens of thousands of people die every year from preventable errors that smarter alarms and smarter distributed connected device systems could easily prevent.

Q In the next 5 years, which embedded technologies, applications, markets, and geographic areas present the most interesting opportunities?

The next 5 years will be the most transformational in embedded history. Every market, from space to mining, from transportation to hospitals, from power to manufacturing faces the opportunity to distribute, connect, and transform. We live in a magic age.

For more on how Dr. Schneider and RTI stay ahead of the embedded curve, see the full Q&A at opsy.st/2015InnovatorsSchneider.

TOP EMBEDDED INNOVATORS

Q&A

Software: Jean Labrosse, Founder, CEO, and President, Micrium

Q What are the largest obstacles to innovation in the embedded realm, and how should those challenges be solved?

Unlike the consumer electronics industry, a good portion of the embedded industry is very conservative and can be fairly slow to adopt major changes. We embedded engineers often learn just enough about our tools to do the work. If something worked well enough in the past then we might not explore new ways or use new tools. Sometimes, we have to break old habits, get out of our comfort zone, and try new and different things if we are to adapt to this ever-evolving world we live in. Engineers should be willing to try new approaches, but also be realistic about when to change course if a project isn't going according to plan. The flip side of the coin is that often it takes years for embedded innovations to be recognized and adopted, and even longer to provide ROI. Engineers must be willing to persevere when they truly believe their innovations have value.

> "...OFTEN IT TAKES YEARS FOR EMBEDDED INNOVATIONS TO BE RECOGNIZED AND ADOPTED, AND EVEN LONGER TO PROVIDE ROI.

Q How do you stay on the leading edge of innovation, rather than just following the embedded crowd?

I am fortunate to be surrounded by people that understand the embedded industry and believe in the same core principles that I do, yet bring their own expertise to bear. At Micrium, we strongly believe in working with our customers, listening to what they are asking for, and anticipating their needs. Maintaining this direct contact with customers and understanding the issues and challenges that they're facing with their next generation products ultimately drives innovation. The µC/OS-II kernel has stood the test of time because it was developed with engineers in mind, to solve their struggles with real-time operating systems (RTOSs). Maintaining this collaborative approach to software development keeps us on the leading edge of innovation.

Q How do you recognize when a new technology or application is one your company should invest/innovate in, versus a technology that will experience fast burnout?

In large part, successfully identifying the technologies or applications that will have staying power comes back to listening to our customers and understanding their needs. Engineers face countless challenges in their jobs to develop new solutions, often using new technologies. I founded Micrium as a company of engineers for engineers and we strive to make their jobs easier and more efficient. This means that generally we invest and innovate in technologies that are closest to our core competencies, but always remain open to reaching outside that realm if necessary to solve our customers' problems.

Q In the next 5 years, which embedded technologies, applications, markets, and geographic areas present the most interesting opportunities?

The embedded industry has a tremendous opportunity right now with the advent of the Internet of Things (IoT), which is becoming a reality. Applications and devices are getting highly interconnected – and often deeply embedded – resulting in ever more complex and interdependent solutions. This creates challenges on many levels: power, performance, reliability and security are just a few. One outcome of this is that there will be even more software oversight to ensure that these devices and applications are safe and secure. This means that anything related to making software safer (static analysis, code reviews, memory protection, etc.) will get attention as well as anything related to security (encryption, secure boot, secure firmware updates, etc.).

TOP INNOVATIVE PRODUCTS NOMINATIONS

28
AdaCore
Aldec, Inc.
Anaren
Ayla Networks
Cavium

29
Cavium
Cypress Semiconductor
Ethertronics
HCC Embedded

30
Icon Labs
Imagination Technologies
Intel
Intersil
Isola Group

31
Mentor Graphics
Mercury Systems
Microchip Technology Inc.
PNI Sensor Corp.
Quantum Leaps, LLC

32
Royal Circuits
STMicroelectronics
Wind River Systems
WITTENSTEIN
Xilinx Inc.

33
Xilinx Inc.

TOP INNOVATIVE PRODUCTS NOMINATIONS

AdaCore — QGen

QGen is a customizable and qualifiable code generator and model verifier for Simulink® and Stateflow® models, producing code in MISRA-C and SPARK/Ada. It is particularly well suited for developing and verifying real-time control systems requiring safety certification, against standards such as DO-178C (avionics), EN 50128 (rail), and ISO 26262 (automotive). Its model verifier detects run-time errors such as integer overflow and division by zero, and it can also find logic errors such as dead execution paths and can verify functional properties through Simulink Assertion blocks. The tool is highly configurable thanks to its open intermediate representation.

www.adacore.com **embedded-computing.com/p372710**

Aldec, Inc. — HES-7™

Aldec first released its innovative HES-7™ backplane-based prototyping architecture with dual Virtex®-7 2000T boards that offered the ability to scale up to eight FPGAs. Today HES-7 is the largest turnkey, off-the-shelf Virtex-7 prototyping board with six FPGAs, scalable up to twenty four, delivering capacity, interconnections and scalability to accommodate the largest SoC projects. Architected to allow for easy implementation and expansion using a non-proprietary backplane connector, HES-7 also offers various peripherals and interfaces via daughter cards including ARM® Cortex™ support with Xilinx® Zynq™. The newest board, boasting six Xilinx Ultrascale®-440 FPGAs on board, will be scalable up to 633 million ASIC gates.

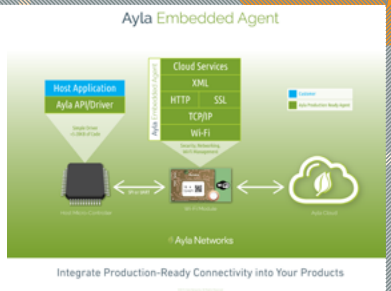
www.aldec.com **embedded-computing.com/p369575**

Anaren — AIR for WICED A20737x

Problem: Manufacturers looking to wirelessly connect their products to the IoT via a Bluetooth® Smart (aka: Bluetooth Low Energy) connection face the formidable challenge creating an embedded-to-wireless link – and developing a mobile "app."
Solution: AIR for WICED Smart modules (A20737x) – based on Broadcom's WICED Smart Bluetooth chip (BCM20737) – are tiny, low-cost radio modules with pre-certified, SMG radios that save non-RF savvy OEM engineers the trouble and cost of developing a radio from scratch. Better still, they are supported by the Anaren Atmosphere tool, which enables development of wireless code and mobile app code in one user-friendly web environment.

atmosphere.anaren.com **embedded-computing.com/p372711**

Ayla Networks — Ayla Embedded Agent



Ayla Enabled Connectivity Modules use leading wireless products, such as the Broadcom BCM 43362, to deliver a plug and play experience to manufacturers developing connected devices. The Ayla Embedded Agent is pre-configured into these modules (for example, the LBWB1ZZYDZ-683 WiFi module by Murata) and includes a fully optimized and production-ready networking stack along with the additional protocols needed to securely connect devices to the Ayla Cloud. This complete solution allows manufacturers to develop their own application on nearly any host micro-controller, while offloading the added complexities created by "must have" features associated with building a connected device.

www.aylanetworks.com **embedded-computing.com/p372713**

Cavium — XPliant™ Ethernet Switch Family

The XPliant™ CNX880xx family of Ethernet switches provide unprecedented flexibility in protocol processing without compromising speed. XPliant Packet Architecture (XPA™) allows programming of every element of switch packet processing. Cavium / XPliant provides a complete set of networking protocols with the switch. However, as new protocols are required, the switch can be updated by software to add support for these new protocols, including changes to parsing, lookups, traffic scheduling, packet modification, scheduling, and traffic monitoring. The CNX880xx with XPA is the first switch that can do this – and it provides industry leading processing at up to 3.2 Terabits per second.

www.cavium.com **embedded-computing.com/p372713**

Cavium

ThunderX™ Workload Optimized Processor Family

The ThunderX™ product family provides the best in class 64-bit ARMv8 Data Center and Cloud processors, offering unprecedented level of integration and industry leading SoC performance. With high performance custom cores, single and dual socket configurations, very high memory bandwidth, large memory capacity, integrated hardware accelerators, fully virtualized core and IO, scalable Ethernet fabric and feature rich I/Os that enable best in class performance per dollar and performance per watt. This family includes multiple Workload Optimized™ SKUs that enable servers and appliances that are optimized for compute, storage, network and secure compute workloads in the cloud.

www.cavium.com **embedded-computing.com/p372714**

Cavium

LiquidSecurity™ Hardware Security Module Family

The LiquidSecurity™ Hardware Security Module (HSM) Family is a complete Hardware Based Transaction Security Solution. LiquidSecurity™ HSM family that provides a FIPS 140-2 level 2 and 3 partitioned, centralized and elastic key management solution with high transaction/sec performance. It addresses high performance security requirements for private key management and administration while also addressing elastic performance per virtual / network domain for cloud environment. It offers a no compromise fully secure and cost efficient solution that addresses the stringent security requirements of SaaS applications, ecommerce payment systems and Enterprise, Banking and Government security applications.

www.cavium.com **embedded-computing.com/p371715**

Cypress Semiconductor

EZ-PD™ CCG1 and EZ-PD™ CCG2

Cypress Semiconductor's new USB Type-C product line includes the industry's first programmable Type-C port controller, EZ-PD™ CCG1, and the industry's smallest one-chip, programmable Type-C cable controller, the EZ-PD CCG2. With these innovative solutions, Cypress is enabling top tier PC makers to integrate USB 3.1 bandwidth in a reversible connector measuring only 2.4-mm in height, the ability to transmit multiple protocols and delivery of 100W of power. Cypress leveraged the programmability of its PSoC® 4 programmable system-on-chip to integrate the transceiver for the Type-C standard in CCG1 in just a few weeks to get to market first.

www.cypress.com **embedded-computing.com/p372716**

Ethertronics

EtherChip EC482

Increasingly, consumers are accessing more movies, television shows, sporting events and other video content via wireless devices. Streaming High Definition video wirelessly to multiple screens has many challenges. EC482 enables Ethertronics' game-changing Active Steering technology for Wi-Fi and other 5 GHz applications by generating multiple radiation patterns from a single antenna structure. Active Steering intuitively 'beam steers' for the best RF signal, achieving ubiquitous coverage regardless of the Access Point's orientation or location to ease installation and improve quality. EC482 maximizes wireless throughput (up to 46% faster downloads) in devices such as set-top boxes, tablets, Wi-Fi access points and more.

www.ethertronics.com **embedded-computing.com/p372717**

HCC Embedded

MISRA Compliant TLS/SSL

HCC's verifiable embedded TLS 1.2 / SSL 3.0 reduces security risk for IoT devices. Many high profile security breaches (e.g. Heartbleed, GnuTLS) have occurred not because of hacked algorithms, but as a result of poor coding. The 'many eyeballs' philosophy hasn't prevented this. HCC Embedded believes security is too serious to be left to chance and has used functional safety processes to create more secure TLS/SSL code. Verifiable development methods have been used in safety-related software for decades and have proven to lower both real costs and defect rates. HCC has used these methods to implement network security and provide extensive supporting life-cycle evidence. With HCC's TLS/SSL implementation, engineers and CEOs can now prove they were diligent in the selection of appropriate security software.

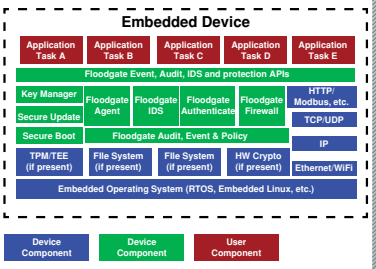
www.hcc-embedded.com/products/tcpip/misra-compliant-tls **embedded-computing.com/p372718**

TOP INNOVATIVE PRODUCTS NOMINATIONS

Icon Labs

Floodgate Security Framework

Floodgate Secure Boot provides a critical security capability for embedded devices by ensuring that only validated code from the device OEM is allowed to run. This prevents attackers from replacing firmware with versions they created to perform malicious operations. Floodgate Intrusion Detection monitors system activity and configuration to detect unauthorized changes to the system. These changes are reported to a security management system. The Floodgate Security Framework also provides management system integration for IT/OT convergence, security capabilities to ensure the device is protected from attack and building blocks for compliance with security standards including NERC-CIP and EDSA.

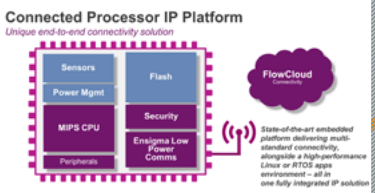


www.iconlabs.com **embedded-computing.com/p372719**

Imagination Technologies

Ensigma Whisper Connectivity IP Family

Imagination's Ensigma Whisper connectivity IP family is purpose-built to enable 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 new Ensigma Whisper radio processing units (RPUs), customers can choose to integrate Wi-Fi 802.11n, Bluetooth Smart, or a combination of the two standards, depending on their specific application. Integrating connectivity onto the main SoC enables companies to reduce power and cost, and the unique Whisper architecture design enables the best connected standby power compared to other connectivity solutions.



imgtec.com/ensigma/whisper-rpu.asp **embedded-computing.com/p372720**

Intel

Intel IoT Platform

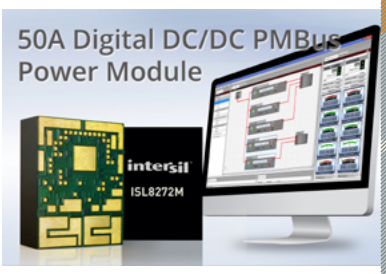
The Intel IoT platform is a family of products from Intel that works with third-party solutions to provide a foundation for seamlessly and securely connecting devices, delivering data to the cloud and value through analytics. The Platform is innovative because its components are secure, interoperable, and scalable, enabling "horizontal" end-to-end IoT deployments across industry sectors. With a secure, horizontal, interoperable platform, Intel enables IoT to scale quickly by creating a repeatable (reusable) foundation that ultimately enables choice in the marketplace. For example, Intel offers businesses that use the Intel IoT Platform the flexibility to use some or all of the technology components from Intel, or interchange them with ecosystem partner components.

www.intel.com **embedded-computing.com/p372721**

Intersil

ISL8272M 50A Digital DC/DC PMBus Power Module

Intersil's ISL8272M is the industry's first fully encapsulated 50A fully encapsulated digital DC/DC PMBus power module. The ISL8272M is a complete step-down power supply that delivers up to 50A of output current from industry standard 12V or 5V input power rails, and four modules can be combined to support up to 200A rails. It provides point-of load conversions for advanced FPGAs, ASICs, processors and memory in space-constrained and power-dense telecom and datacom applications. The device is also well suited for high-end instrumentation, industrial and medical equipment. Used in conjunction with Intersil's PowerNavigator™ graphical user interface (GUI), the ISL8272M simplifies system power conversion and configuration, while speeding design time.



www.intersil.com **embedded-computing.com/p372734**

Isola Group

Tachyon® 100G Laminates and Prepregs for Printed Circuit Board Fabrication

Tachyon 100G materials provide a thermosetting matrix that exhibits dielectric performance on par with PTFE, thermal performance exceeding most high-reliability resin systems, and processing similar to standard FR-4-type products. This enables a broader range of PCB fabricators (versus specialized board shops) to process the materials and enter markets that may have been previously unattainable due to manufacturing and cost limitations. Tachyon 100G laminates and prepregs enable high-layer count, 0.8 mm pitch line cards with heavy 2 oz. copper inner layers that are required to transmit 100 Gigabit Ethernet (100GbE) at data rates in excess of 25 Gb/s per channel. Tachyon 100G materials minimize skew, which limits the bandwidth of these links, adds data-dependent jitter, and limits the possibility of equalizing links to compensate for high-frequency skin effect and dielectric losses.

www.isola-group.com **embedded-computing.com/p372722**

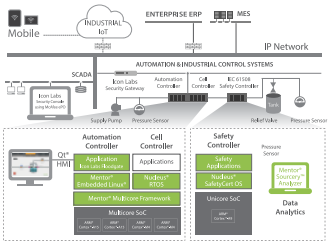
Mentor Graphics

Mentor® Embedded Multi-platform Solution for Industrial Automation

Mentor Graphics announced the embedded systems industry's broadest portfolio for industrial automation (February 2015). In partnership with key industry vendors, Mentor's unique multi-platform approach and robust security architecture enables embedded developers to create feature-rich, power-efficient, safe and secure systems. Its integrated and tested capabilities and features allow equipment manufacturers to focus on strategic competitive differentiation across the spectrum of industrial devices (industrial controllers, process automation controllers, PLCs, data acquisition devices, and motor driver controllers, including motion, vision, and SCADA systems). The convergence of product features and capabilities increase developer profitability by minimizing footprint (floor space), reducing power usage (electricity costs), and decreasing downtime (security vulnerabilities).

www.mentor.com/embedded-software/industries/industrial

embedded-computing.com/p372723



Mercury Systems

Ensemble 8000

Mercury's Ensemble 8000 next-generation secure AdvancedTCA (ATCA) ecosystem is the union of best commercial and embedded processing technologies that bring affordable cloud processing to the tactical edge with system integrity. Expanding upon our extensive ATCA history, these building blocks meet Modular Open System Architecture (MOSA) standards and leverage Mercury's advanced fourth generation server-class thermal management technologies for maximum processing capability and reliable operation. Personalized system integrity solutions integrate Mercury, customer, and third party IP for the highest information assurance. And these building blocks are designed and made in the USA providing a secure, trusted supply chain.

www.mrcy.com/atca

embedded-computing.com/p372724

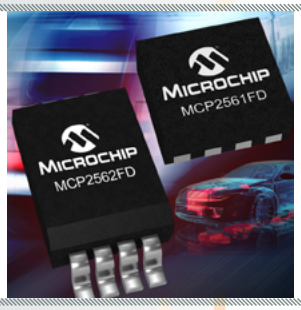
Microchip Technology Inc.

MCP2561/2FD

The MCP2561FD and MCP2562FD CAN Flexible Data Rate (CAN FD) Transceiver Family help CAN systems meet the physical layer requirement for CAN FD systems. The devices are one of only a few CAN FD Transceivers approved by auto OEMs. The device family is the first to support up to 8Mb/s data rate capability and also supports a wide voltage and temperature range helping system migration from CAN to CAN FD.

www.microchip.com

embedded-computing.com/p



PNI Sensor Corp.

SENtrode

SENtrode™, is the only wearable development kit with motion and context algorithms embedded on a sensor-agnostic sensor hub – PNI Sensor's SENtral™. And at just 31.55mm x 37.15mm x 8.28mm with wearable housing in wristband form, it is also the only development kit in the form factor of a wearable. SENtrode also comes with open source software, further speeding development. In addition to PNI's SENtral and sensor fusion algorithms, SENtrode includes a Cortex-M4 programmable processor; JTAG programming board; built-in BLE and open-source BLE protocol for Android and iOS; and a rechargeable battery. Separate housing for IoT devices is also available.

www.pnicorp.com/products/sentrode

embedded-computing.com/p372726

Quantum Leaps, LLC

QP

QP is a family of lightweight software frameworks for building responsive and modular real-time embedded applications as systems of cooperating, event-driven active objects (actors). The QP family consists of QP/C, QP/C++, and QP-nano frameworks, which are all strictly quality controlled, superbly documented, and commercially licensable. The behavior of active objects is specified in QP by means of hierarchical state machines (UML statecharts). The frameworks support manual coding of UML state machines in C or C++ as well as automatic code generation by means of the free QM modeling tool. All QP frameworks can run on bare-metal MCUs, completely replacing a traditional RTOS. QP/C and QP/C++ can also work with a traditional RTOS/OS.

www.state-machine.com

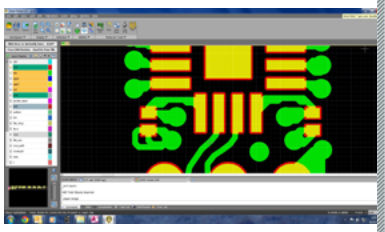
embedded-computing.com/p372727

TOP INNOVATIVE PRODUCTS NOMINATIONS

Royal Circuits

Free Proto

Free Proto is a comprehensive design-for-manufacturing tool with a Gerber viewer. Developed exclusively for Royal Circuit Solutions, this easy-to-use tool helps identify issues that affect manufacturability before they cost money or cause delay. Free Proto allows engineers to run a full DFM check right from the desktop, so they no longer have to conduct DFM checks online and wait for vendor-emailed reports. It also compares Netlists to Gerbers and provides easy-to-read, online views to assist in file verification. All designs verified and ordered with Free Proto are eligible to receive a free extra board.



www.RoyalCircuits.com/FreeProto **embedded-computing.com/p372728**

STMicroelectronics

STM32F7

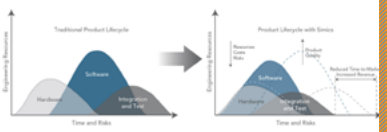
STM32F7 microcontroller series was the first MCU using ARM Cortex-M7 core, ARM's most powerful Cortex-M processor. ST's STM32F7 series delivers, via a seamless upgrade path, ~2x processing and DSP performance as the previous performance champ. It captured "Best in Show" awards at ARM TechCon (from EETimes AND VDC Research) and was named a Product of the Year by German magazine Elektronik. The higher performance of the STM32F7 did not come at the expense of power efficiency. Despite greater functionality, the new series' Run and low-power modes consume current at the same low levels as the STM32F4.

www.st.com/web/en/catalog/mmc/FM141/SC1169/SS1858 **embedded-computing.com/p372729**

Wind River Systems

Wind River Simics

Simulate anything from chip to system. Wind River Simics provides the access, automation and collaboration required for agile development. By simulating the end-target-system, teams can reduce the dependency between software and hardware activities to enable agile practices and continuously deliver better software faster. All developers have unlimited access to virtual hardware, allowing new ways of working, advanced automation and improved collaboration. With Simics, developers can also accelerate every phase of development, while dramatically reducing risks of shipping late, overrunning budget, and sacrificing quality. Additionally, Wind River is delivering new methods to accelerate development with Simics innovations in the cloud.

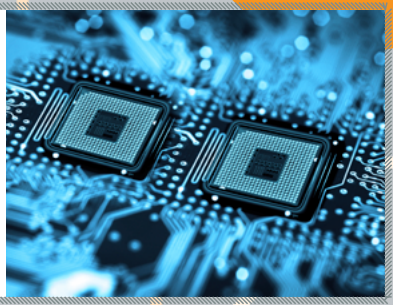


www.windriver.com/products/simics **embedded-computing.com/p372730**

WITTENSTEIN

SafeXchange™ Multi-processor Communication

Our innovative product, SAFEXchange™, allows you to securely share safety critical data between multiple processors and cores across any black channel communication systems. It's certified to IEC 61508, ISO 26262, and IEC 61784-3. SAFEXchange is innovative in that it protects the data shared rather than the communication channel itself, which allows it to be used in conjunction with black channel communication mediums. SAFEXchange is ideal for use in projects working across multiple cores, processors, or in any situation where data integrity must be protected. SAFEXchange is supplied as an add-on component for all RTOS products supplied by WITTENSTEIN high integrity systems.

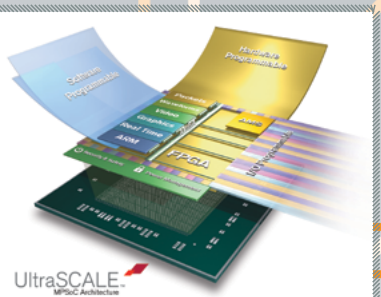


www.highintegritysystems.com **embedded-computing.com/p 372731**

Xilinx Inc.

SDSoC™ Development Environment for All Programmable SoCs and MPSoCs

The SDSoC development environment enables the broader community of embedded software developers to leverage the power of hardware and software 'all programmable' devices. The SDSoC development environment provides a greatly simplified ASSP-like C/C++ programming experience including an easy to use Eclipse IDE and a comprehensive design environment for heterogeneous Zynq® All Programmable SoC and MPSoC deployment. Complete with the industry's first C/C++ full-system optimizing compiler, SDSoC delivers system level profiling, automated software acceleration in programmable logic, automated system connectivity generation, and libraries to speed programming. SDSoC enables end user and 3rd party platform developers to rapidly define, integrate, and verify system level solutions and enable their end customers with a customized programming environment.



www.xilinx.com **embedded-computing.com/p372732**

Xilinx Inc. **Zynq UltraScale+ MPSoC**

The Xilinx Zynq® UltraScale™+ MPSoCs introduces a radically new architecture that provides exponentially higher levels of system integration, intelligence, security and system performance. It is the only heterogeneous multi-processing SoC in the world with the industry's best programmable logic for hardware acceleration. Based on the Xilinx UltraScale MPSoC architecture, the Zynq UltraScale+ MPSoCs enable extensive system level differentiation, integration, and flexibility through hardware, software, and I/O programmability. The Zynq UltraScale+ MPSoC includes ARM's most power efficient 64-bit processors - quad-core 64-bit APU, a dual-core RPU, a graphics processor, and also has H.265 (8K/4K video compression) built in. As well, it includes a host of peripherals, security features and power management, all on one chip.

www.xilinx.com **embedded-computing.com/p372733**

Winners will be announced in the August Resource Guide issue

Medical box PC for OEM applications

The Kontron Clinic-BPC B-101 is a fanless PC specifically designed for medical close-to-patient applications. The system is fanless and incorporates three medically isolated LAN ports and RS-232 ports as well as two external monitor outputs for dual display medical applications. The plastic case also provides long durability and is easy to clean and disinfect.

Kontron | www.kontron.com
embedded-computing.com/p372706

Micrium RTOS for Freescale i.MX 6SoloX applications processor

Micrium's µC/OS-III RTOS has been ported to the Freescale multicore i.MX 6SoloX applications processor containing ARM Cortex-A9 and Cortex-M4 cores. The support extends beyond the RTOS kernel and includes TCP/IP, CAN, USB, and file system support for industrial and automotive applications. A free 30-day evaluation is available for testing and example projects will include µC/OS-III source code. A listing of supported boards can be found on the Micrium web site.

µC/OS-III®
The Real-Time Kernel

Micrium | www.micrium.com
embedded-computing.com/p372708

100G data acquisition and storage system

EDT's WRAP100G is a 100G 9.8 TB system for real-time data acquisition/playback and mass storage. The system includes two 1U units: a SNAP1 to acquire signals up to OTU4, and a WSU1 for mass storage and data transfers reaching 115 Gbps. Each unit runs Linux CentOS on an Intel Core i7 processor with 4 GB of memory. SFP+, QSFP+, and CFP transceivers provide flexible options for data acquisition and transfer.

EDT | www.edt.com
embedded-computing.com/p372709

WHITE PAPER

SIMPLIFYING THE DESIGN OF COMPLEX IMAGING SYSTEMS

By Pleora Technologies

Imaging technologies have revolutionized manufacturing by providing real-time analysis to help automate tasks, guide decisions, and improve efficiencies. Today, imaging products perfected for industrial applications are delivering cost and performance advantages across a widening range of markets.

opsy.st/PleoraImagingWP

BLOG

FLC MEMORY ARCHITECTURE SAVING DOLLARS AND SPACE

By Rich Nass, Embedded Computing Brand Director

I was recently introduced to Marvell's Final-Level Cache (FLC) architecture. It actually solves a problem I wasn't even aware existed. Imagine that. It turns out that, with current operating systems, only a small percentage of application code loaded in main memory is active at any given time.

opsy.st/MarvellFLC

E-CAST

INDUSTRIAL AND M2M EMBEDDED SYSTEM: SILICON, PLATFORMS, AND SOFTWARE

Presented by: Altia, Echelon, Freescale, KORE Telematics

Industrial and related M2M embedded systems include a unique mix of environmental, connectivity, user interface, and security requirements. Silicon and platforms must provide for extended temperature, humidity, and shock & vibration ranges.

ecast.opensystemsmedia.com/554

WHITE PAPER

EOLS HAPPEN: HOW TO OPTIMIZE FOR CHANGES

By Sparton

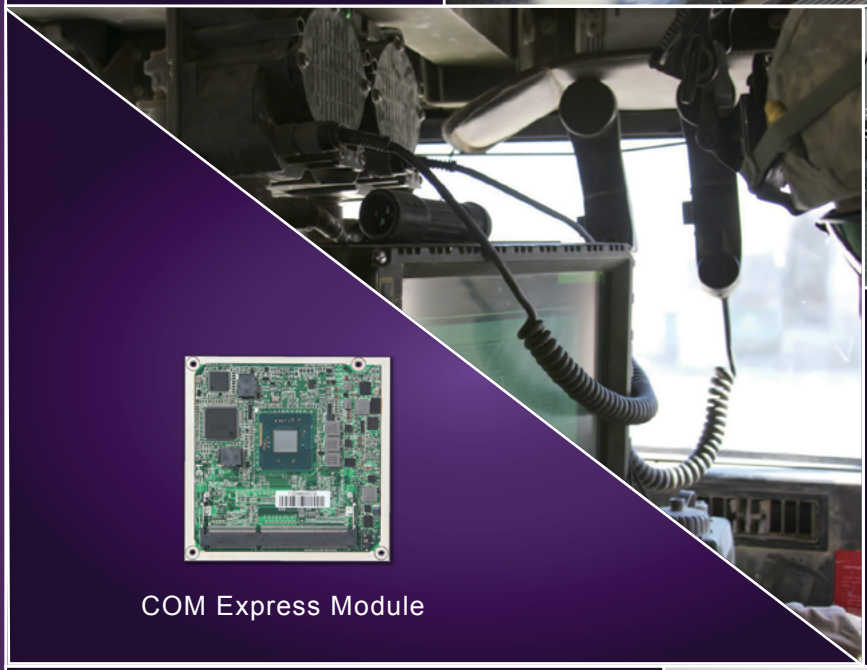
Today, technology is simply changing too fast to wait until the next generation of a product to add new capabilities and to risk losing a competitive edge or, worse yet, to risk the introduction of a new product that is already obsolete. For decades, the general belief was that the replacement of key components during the mid-lifecycle design refresh of complex electromechanical systems was simply too costly and burdensome – and that any changes in product design would simply need to wait until the next generation.

opsy.st/SpartonEOLWP

Portwell Empowers Intelligent Solutions

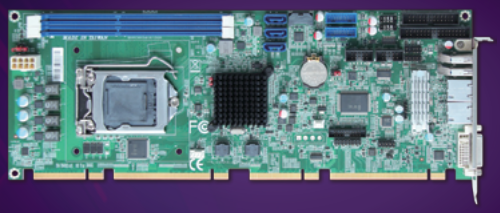
Mini-ITX

Small Form Factor System



COM Express Module

Network Security Appliance



PICMG SBC

www.portwell.com
info@portwell.com
1-877-278-8899

Portwell

intel IoT Solutions Alliance Premier