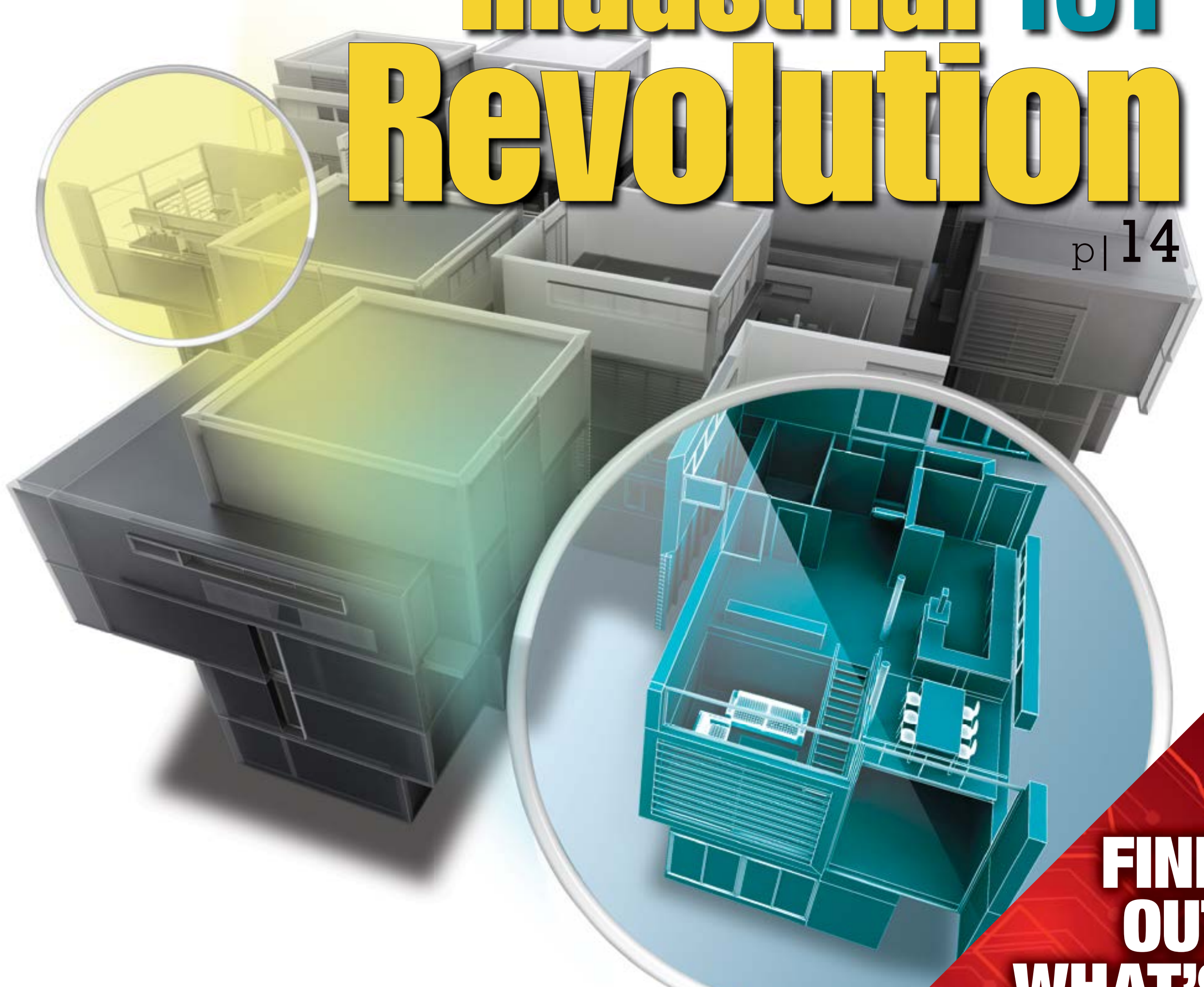
electronic design

THE AUTHORITY ON
EMERGING TECHNOLOGIES
FOR DESIGN SOLUTIONS

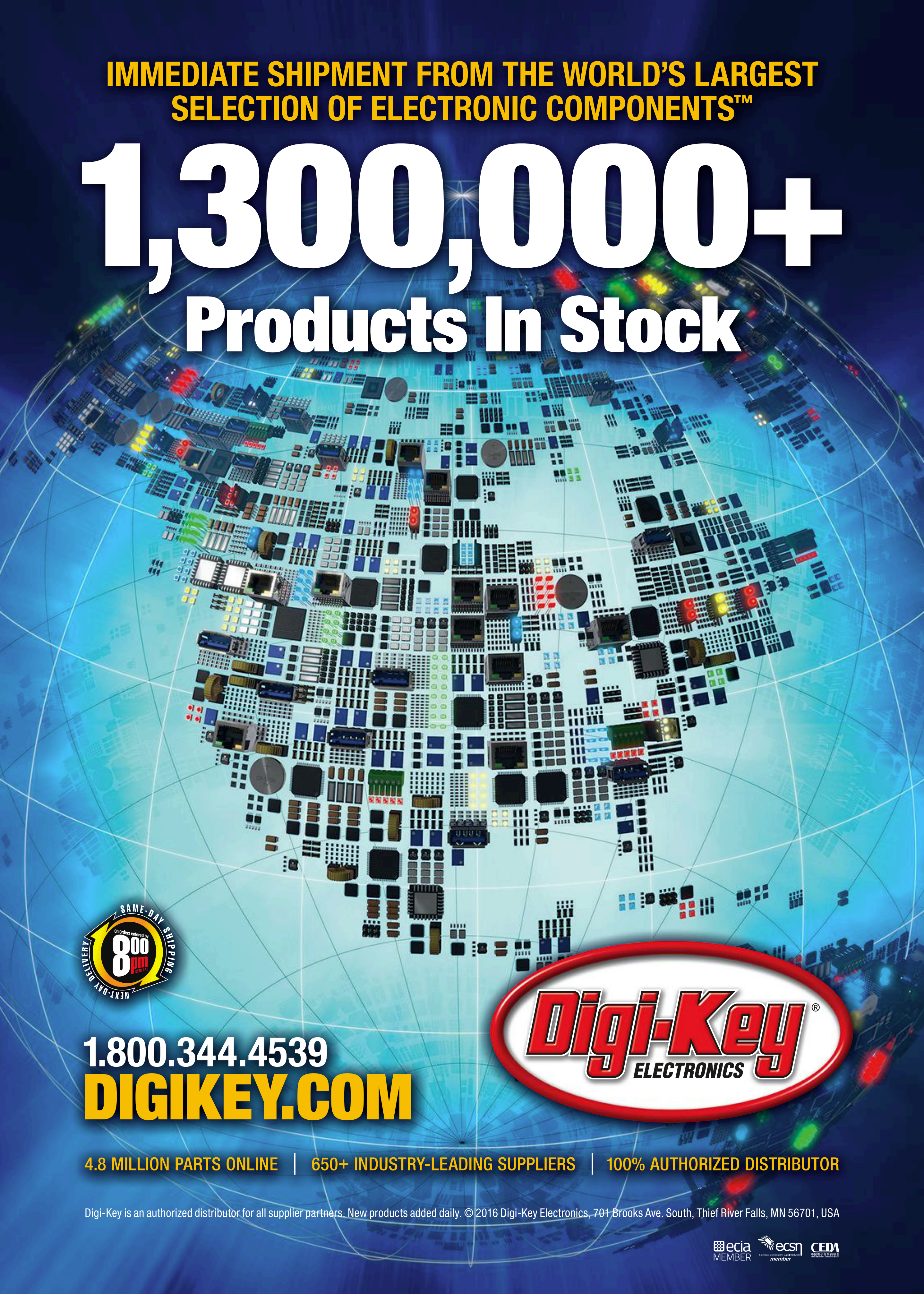
June 2016 electronicdesign.com

Industrial IoT Revolution

p| 14



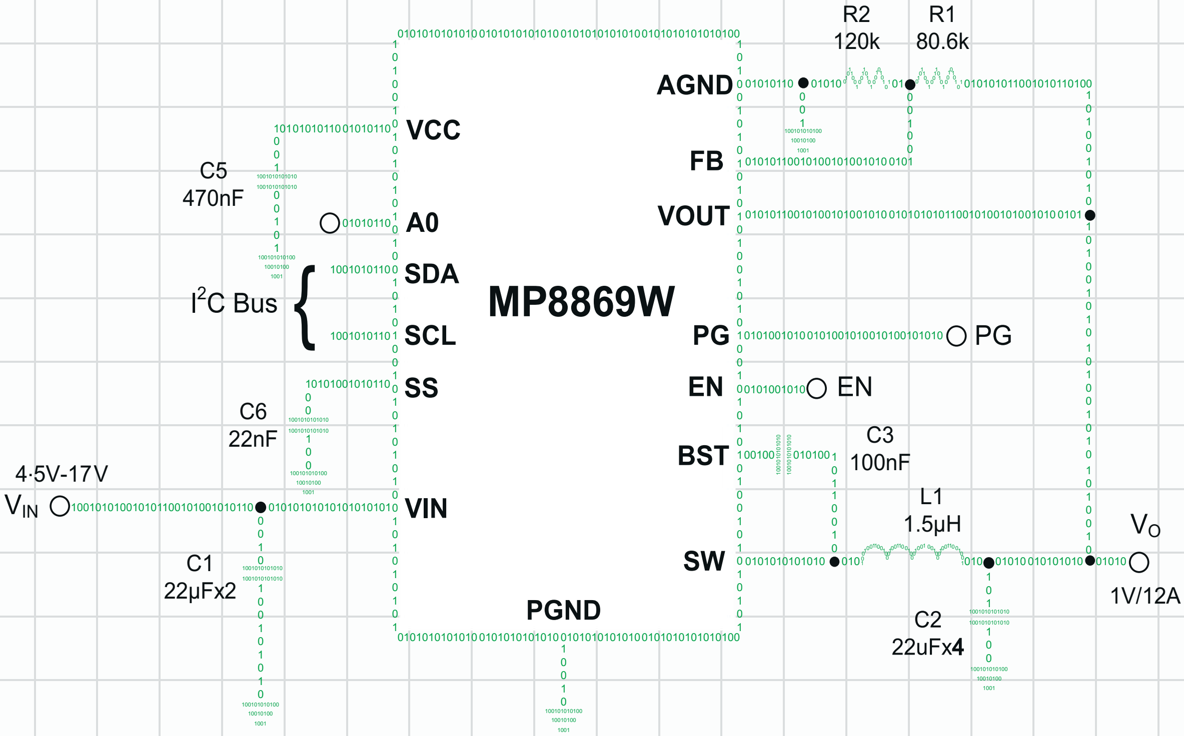
$10.00 Powered by Penton


IMMEDIATE SHIPMENT FROM THE WORLD'S LARGEST SELECTION OF ELECTRONIC COMPONENTS™
1,300,000+
Products In Stock
SAME-DAY SHIPPING
on orders entered by
8:00 pm
CENTRAL
NEXT-DAY DELIVERY
1.800.344.4539
DIGIKEY.COM
Digi-Key®
ELECTRONICS
4.8 MILLION PARTS ONLINE | 650+ INDUSTRY-LEADING SUPPLIERS | 100% AUTHORIZED DISTRIBUTOR
Digi-Key is an authorized distributor for all supplier partners. New products added daily. © 2016 Digi-Key Electronics, 701 Brooks Ave. South, Thief River Falls, MN 56701, USA
ecia MEMBER
ecsn member
CEDA

Simple, Easy Solutions

Design Like You Mean It

Wide Input 3-18V, 12A, Synchronous Step-Down Converter with Integrated Telemetry via I²C Interface



Key Highlights

- 5% Accuracy Output Voltage and Output Current Monitoring
- Programmable Current Limit
- Programmable Frequency
- Selectable PWM/PFM Mode
- 1% Internal Reference Accuracy
- I²C Programmable Output Range from 0.6V

Applications

- Enterprise SSD's
- Networking
- Gaming Systems

www.monolithicpower.com

Follow us on:

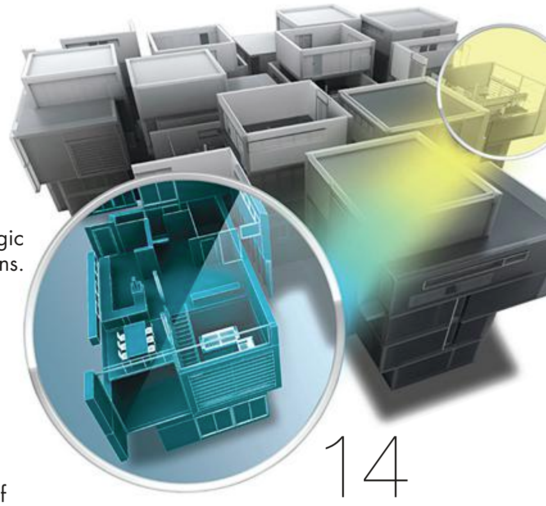
In This Issue

FEATURES

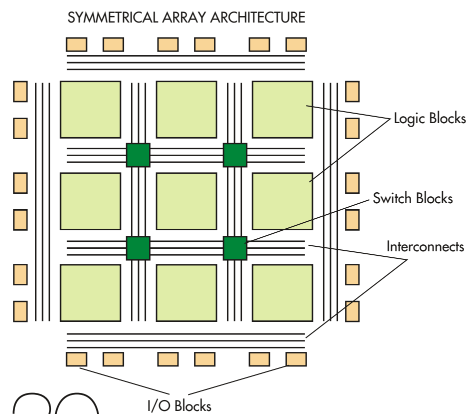
NEWS & ANALYSIS

IDEAS FOR DESIGN

COLUMNS & DEPARTMENTS



14



20

24

EDITORIAL MISSION:
To provide the most current, accurate, and in-depth technical coverage of the key emerging technologies that engineers need to design tomorrow's products today.

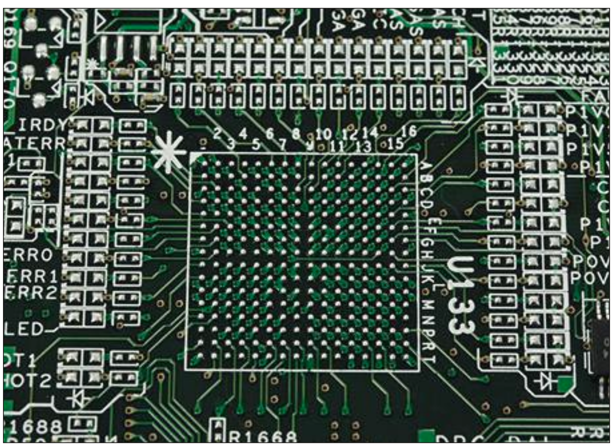
ELECTRONIC DESIGN (ISSN 0013-4872) is published monthly by Penton Media Inc., 9800 Metcalf Ave., Overland Park, KS 66212-2216. Paid rates for a one-year subscription are as follows: $120 U.S., $180 Canada, $240 International. Periodicals postage paid at Kansas City, MO, and additional mailing offices. Editorial and advertising addresses: ELECTRONIC DESIGN, 1166 Avenue of the Americas, New York, NY 10036. Telephone (212) 204-4200. Printed in U.S.A. Title registered in U.S. Patent Office. Copyright ©2016 by Penton Media Inc. All rights reserved. The contents of this publication may not be reproduced in whole or in part without the consent of the copyright owner. For subscriber services or to order single copies, write to Electronic Design, PO Box 2100, Skokie, IL 60076. POSTMASTER: Send change of address to Electronic Design, PO Box 2100, Skokie, IL 60076. Canadian Post Publications Mail agreement No. 40612608. Canada return address: IMEX Global Solutions, P.O. Box 25542, London, ON N6C 6B2.

on electronicdesign.com

JITTER SIMPLIFIED

http://electronicdesign.com/test-measurement/jitter-simplified

Does the word "jitter" strike fear into your heart? It shouldn't. While jitter will always be present in your designs, being able to identify causes and sources of jitter will allow you to confidently design and debug your systems.



5 THINGS TO KNOW ABOUT EMBEDDED JAVA PROGRAMMING

http://electronicdesign.com/dev-tools/5-things-you-need-know-about-embedded-java-programming

Java is a mature development platform, now pushing past 20 years in age. As such, it's ideally suited to developing embedded applications due to its simplicity, ubiquity, and a rich set of both standard and open-source libraries. Read these five key points that you should know when starting to develop embedded Java applications.

UNMANNED VEHICLES FROM XPONENTIAL 2016

http://electronicdesign.com/embedded/gallery-unmanned-vehicles-xponential-2016

XPonential 2016, formally known as AUVSI, brought a host of UAVs and other unmanned platforms and technologies to New Orleans. Tech Editor Bill Wong covers the show and shares a gallery of images of the latest innovations.

2016 TOP ELECTRONICS DISTRIBUTORS

http://electronicdesign.com/another-slow-growth-year-say-top-electronics-distributors

Technology and lackluster growth are shaping leading electronic components distributors' business strategies in 2016. This year's Top Electronic Components Distributors report highlights 27 companies serving customers in North America and around the world, with sales of more than $75 million. It also recognizes a handful of noteworthy U.S.-based firms with sales of less than $75 million, which also serve customers across North America and around the world.

join us online

Follow us on Facebook: http://tinyurl.com/odzo6hc
and Twitter: http://tinyurl.com/k5pum39

electronic design
Powered by Penton
JUNE 2016

EDITORIAL

CONTENT DIRECTOR: **NANCY K. FRIEDRICH** nancy.friedrich@penton.com
CONTENT PRODUCTION DIRECTOR: **MICHAEL BROWNE** michael.browne@penton.com
CONTENT PRODUCTION SPECIALIST: **ROGER ENGELKE** roger.engelke@penton.com
PRODUCTION EDITOR: **JEREMY COHEN** jeremy.cohen@penton.com
DISTRIBUTION: **VICTORIA FRAZA KICKHAM** SourceESBeditor@penton.com
EMBEDDED/SYSTEMS/SOFTWARE: **WILLIAM WONG** bill.wong@penton.com
ANALOG/POWER: **MARIA GUERRA** maria.guerra@penton.com
CONTENT OPTIMIZATION SPECIALIST: **WES SHOCKLEY** wes.shockley@penton.com
ASSOCIATE CONTENT PRODUCER: **LEAH SCULLY** leah.scully@penton.com
ASSOCIATE CONTENT PRODUCER: **JAMES MORRA** james.morra@penton.com
CONTRIBUTING EDITOR: **LOUIS E. FRENZEL** lou.frenzel@penton.com

ART DEPARTMENT

GROUP DESIGN DIRECTOR: **ANTHONY VITOLO** tony.vitolo@penton.com
SENIOR ARTIST: **JIM MILLER** jim.miller@penton.com
CONTRIBUTING ART DIRECTOR: **RANDALL L. RUBENKING** randall.rubenking@penton.com

PRODUCTION

GROUP PRODUCTION MANAGER: **CAREY SWEETEN** carey.sweeten@penton.com
PRODUCTION MANAGER: **FRAN VAUGHN** fran.vaughn@penton.com

AUDIENCE MARKETING

USER MARKETING DIRECTOR: **BRENDA ROODE** brenda.roode@penton.com
USER MARKETING MANAGER: **DEBBIE BRADY** debbie.brady@penton.com
FREE SUBSCRIPTION/STATUS OF SUBSCRIPTION/ADDRESS CHANGE/MISSING BACK ISSUES
T | 866.505.7173 **F** | 847.763.9673 electronicdesign@halldata.com

SALES & MARKETING

MANAGING DIRECTOR: **TRACY SMITH** **T** | 913.967.1324 **F** | 913.514.6881 tracy.smith@penton.com

REGIONAL SALES REPRESENTATIVES

AZ, NM, TX: **GREGORY MONTGOMERY** **T** | 480.254.5540 gregory.montgomery@penton.com
AK, CA, CO, ID, MT, ND, NV, OR, SD, UT, WA, WI, WY, W/CANADA: **JAMIE ALLEN** **T** | 415.608.1959 **F** | 913.514.3667 jamie.allen@penton.com
AL, AR, IA, IL, IN, KS, KY, LA, MI, MN, MO, MS, NE, OH, OK, TN: **PAUL MILNAMOW** **T** | 312.840.8462 paul.milnamow@penton.com
CT, DE, FL, GA, MA, MD, ME, NC, NH, NJ, NY, RI, PA, SC, VA, VT, WV, EASTERN CANADA: **SHANNON ALO-MENDOSA** **T** | 978.501.7303 Shannon.alo-mendosa@penton.com

INTERNATIONAL SALES

GERMANY, AUSTRIA, SWITZERLAND: **CHRISTIAN HOELSCHER** **T** | 011.49.89.95002778 christian.hoelscher@husonmedia.com
BELGIUM, NETHERLANDS, LUXEMBURG UNITED KINGDOM, SCANDINAVIA, FRANCE, SPAIN, PORTUGAL: **JAMES RHOADES-BROWN** **T** | +011 44 1932 564999 **M** | +011 44 1932 564998 james.rhoadesbrown@husonmedia.com
PAN-ASIA: **HELEN LAI** **T** | 886 2-2727 7799 helen@twoway-com.com
PLEASE SEND INSERTION ORDERS TO: orders@penton.com
PENTON REPRINTS: **WRIGHT'S MEDIA** **T** | 877.652.5295 penton@wrightsmedia.com
CIRCULATION: **CUSTOMER SERVICE** **T** | 866.505.7173 **F** | 847.763.9673 electronicdesign@halldata.com
LIST RENTALS:
SMARTREACH CLIENT SERVICES MANAGER: **DAVID SICKLES** **T** | (212) 204 4379 david.sickles@penton.com

ONLINE

PRODUCT DEVELOPMENT DIRECTOR **RYAN MALEC** ryan.malec@penton.com

DESIGN ENGINEERING & SOURCING GROUP

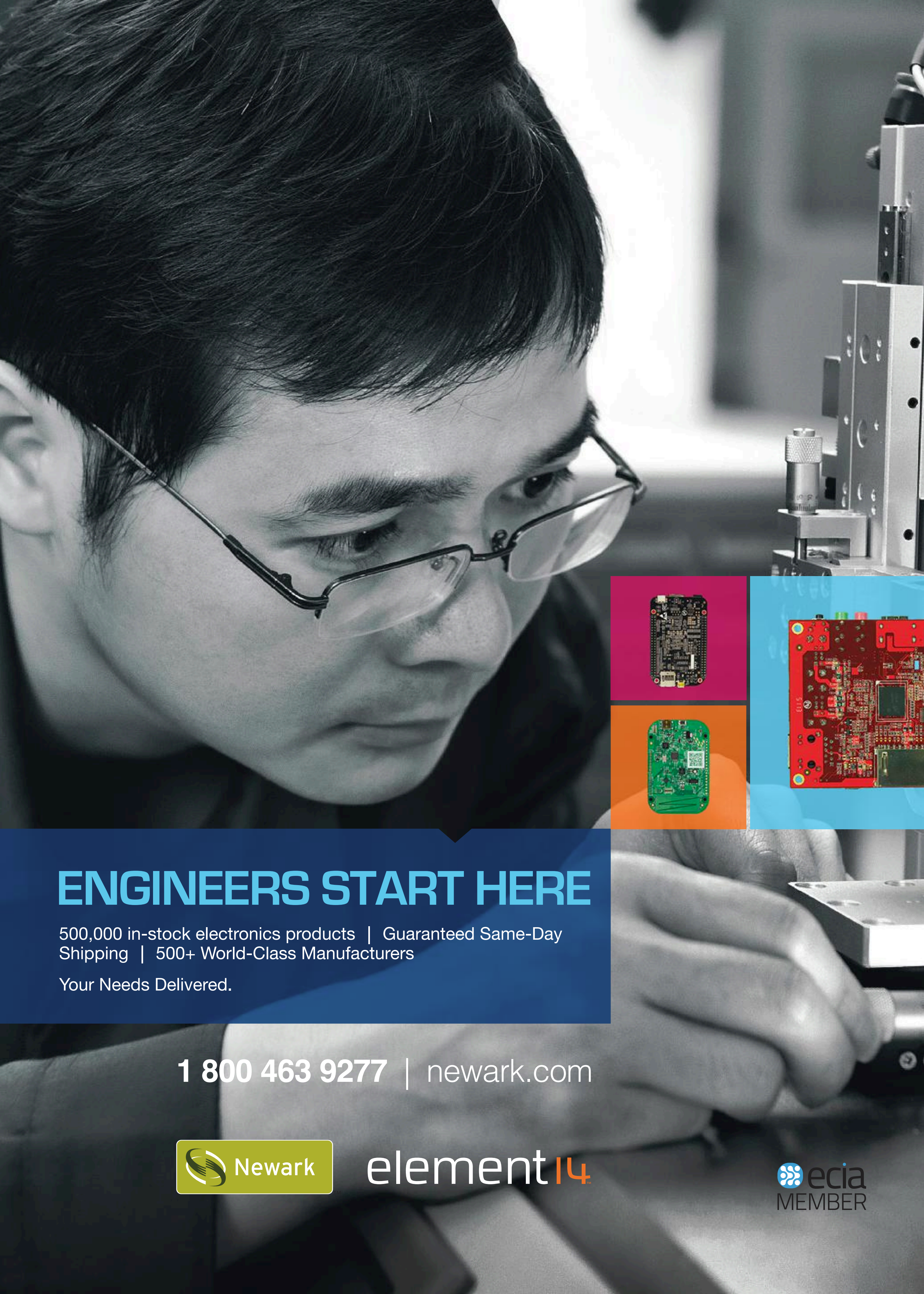
EXECUTIVE DIRECTOR OF CONTENT AND USER ENGAGEMENT: **NANCY K. FRIEDRICH**
GROUP DIRECTOR OF OPERATIONS: **CHRISTINA CAVANO**
GROUP DIRECTOR OF MARKETING: **JANE COOPER**

PENTON

CHIEF EXECUTIVE OFFICER: **DAVID KIESELSTEIN** david.kieselstein@penton.com
CHIEF FINANCIAL OFFICER: **NICOLA ALLAIS** nicola.allais@penton.com
INDUSTRY GROUP, PRESIDENT: **PAUL MILLER** paul.miller@penton.com
1166 AVENUE OF THE AMERICAS, 10TH FLOOR
NEW YORK, NY 10036 **T** | 212.204.4200

Penton

Electronic Design | Machine Design | Microwaves & RF | Medical Design | Source ESB | Hydraulics & Pneumatics | Global Purchasing | Distribution Resource | Power Electronics | Defense Electronics | Electronic Design Europe | Engineering TV

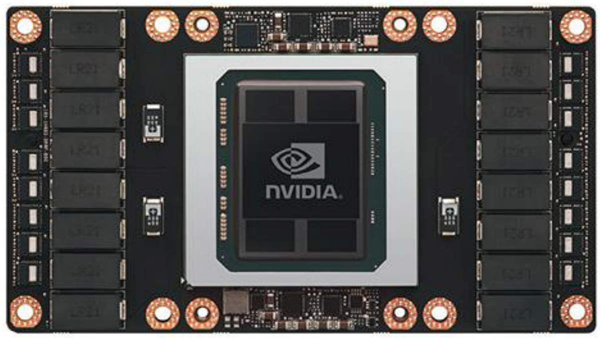

ENGINEERS START HERE
500,000 in-stock electronics products | Guaranteed Same-Day Shipping | 500+ World-Class Manufacturers
Your Needs Delivered.
1 800 463 9277 | newark.com
Newark
element14
ecia MEMBER

BILL WONG | Embedded/Systems/Software Editor
bill.wong@penton.com

GPUs and Deep Learning

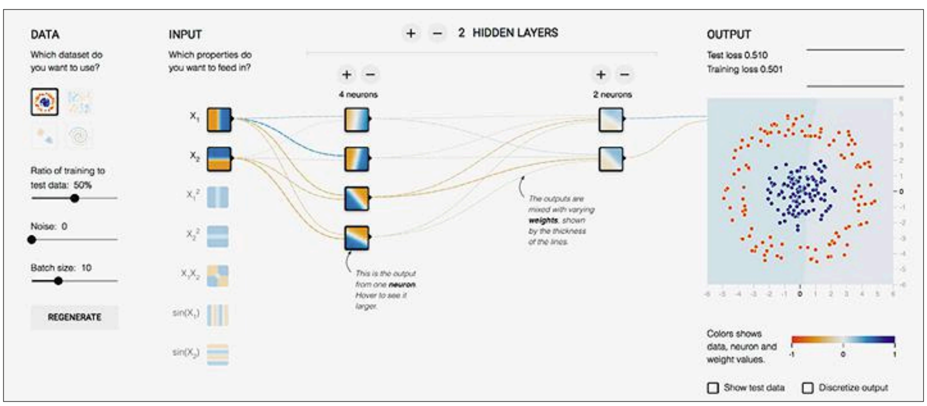
Deep learning, or deep neural nets (DNNs), is the technical craze these days. It is targeting everything from self-driving cars to tagging photos. DNNs are just one of many artificial intelligence (AI) research areas. It has become more popular as processor performance has increased, allowing more complex systems.

DNNs require matrix number-crunching capabilities found in FPGAs and GPUs. GPUs are now the target for a number of DNN platforms. NVidia's Tesla P100 GPU (*Fig. 1*) is designed to tackle applications like deep learning neural nets. The Tesla P100 can deliver 21 TFLOPS of 16-bit floating point that is ideal for DNN applications. It employs CoWoS (Chip-on Wafer-on-Substrate) with HBM2 (high bandwidth memory version 2) technology. AMD used HBM on its Radeon R9 GPU (see *"Best of 2015: High Bandwidth Memory Helps GPU Deliver on Performance"* on electronicdesign.com). The Tesla P100 has four NVLinks allowing multiple chips to be combined into a single compute node.



1. NVidia's Tesla P100 GPU is designed to tackle applications like deep learning neural nets.

NVidia's chip supports the CUDA programming environment. The Cuda DNN (cuDNN) runtime targets DNN frameworks like TensorFlow, an open-source software library for numerical computation. You can check out the TensorFlow Playground (*Fig. 2*) website at http://playground.tensorflow.org to see how TensorFlow and neural networks operate by changing variables such as the number of nodes and layers.



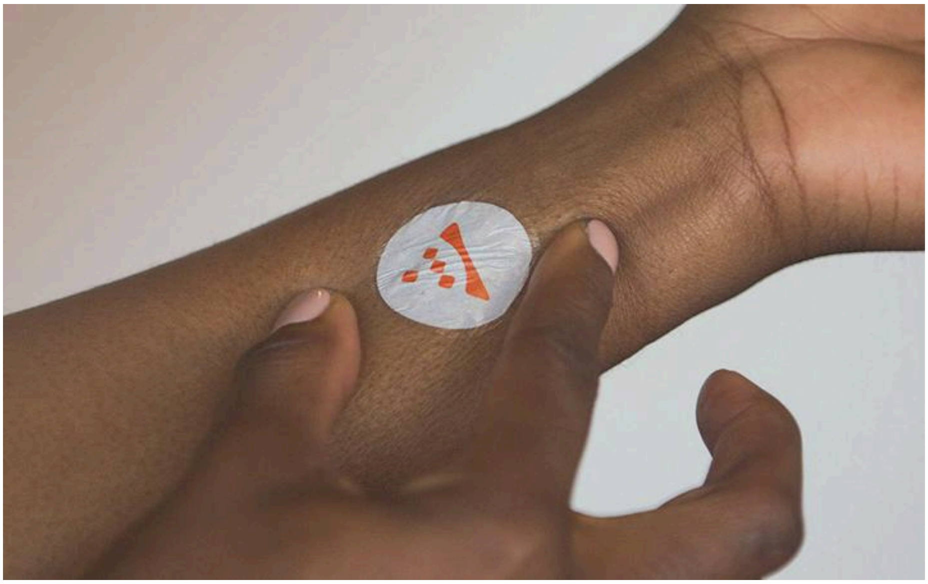
2. The Tensorflow webpage demonstrates different neural net configurations.

DNN will not solve all AI problems and it is not necessarily a magic bullet for applications, but it is a valuable tool that is becoming more practical for general use.

News

ELECTRONIC "TATTOOS" for Healthcare Shift to Gather Business Data

Ben Schlatka maintains that the company he helped found is focused on healthcare. As vice president of corporate development at wearable healthcare startup MC10, he helped supervise the release of the company's first product, BioStamp, an electronic skin patch filled with advanced sensors that record and transmit data about a person's muscle activity and nerve health.



MC10's electronic "tattoos" consist of an antenna and thinned near-field communication chip mounted onto a stretchable adhesive. (Image courtesy of MC10)

But another feature of the electronic patch has enticed industries far outside healthcare. The Massachusetts-based company builds extremely thin and flexible electronics that mimic human skin. These can be glued directly onto the skin and, using a smartphone or other device, transmit data into the cloud. The information is meant to be accessed by doctors and researchers, or analyzed by software programs.

Now, MC10 is turning its healthcare technology over to businesses looking to create new experiences for their customers and exploit new methods for gathering data. The company recently licensed one of its products, an electronic patch that resembles a temporary tattoo, to the manufacturing consulting firm PCH.

The "electronic tattoo" is a combination of advanced polymers and stretchable metal interconnects known as the Wearable Interactive Stamp Platform, or WiSP. No larger than a postage stamp and as thin as a human hair, these devices consist of an antenna and thinned near-field communication chip mounted onto a stretchable adhesive. The device is passive and sends data through NFC-enabled smartphones or readers into the cloud.

In healthcare, WiSP devices are intended to complement more sophisticated medical sensors, storing "a single piece of information that could be read episodically," Schlatka said in a phone interview. The WiSP devices that MC10 has built itself contain sensors that capture electrocardiograms and logged heart rates in real time.

While the Biostamp can be recharged and reused, WiSP devices are low-cost and disposable, Andre Yousefi, co-founder of Lime Lab, the design engineering division of PCH, said in an e-mail. The electronic tattoos could be handed out instead of tickets at a concert or paired with a smartphone to let people make payments with the patch on the back of their hand. PCH is "already in discussions with several major brands in these categories," he added.

Businesses can also build custom sensors into the devices and program the NFC chip to perform different tasks, like give someone backstage access at a concert. "Our partnership with MC10 opens the door for other brands to develop consumer applications using this unique wearable platform. The stamp is highly customizable, allowing brands to create personalized and engaging experiences," Liam Casey, chief executive of PCH, said in a statement.

The possibilities for WiSP underline the increasingly porous boundaries between healthcare, consumer electronics, and businesses now that everything seems ripe for data mining. Most wearables have skirted around healthcare by making devices that collect data on personal fitness. These fitness trackers have inspired a new kinds of smart bracelets, like Disney's MagicBand, which allows guests at Disney World to access parks and make contactless payments.

The first commercial products based on the "smart stamp" were stretchable sensors designed by L'Oreal to monitor exposure to ultraviolet light. The My UV Patch, which was revealed earlier this year at the Consumer Electronics Show, contains dyes that conform to a person's skin tone and react to sunlight. Take a picture of the patch or wave your smartphone over it, and a mobile app determines how badly your skin has been exposed.

PCH has floated other ideas about the technology's potential. Guests at an amusement park, for instance, could wear WiSP devices programmed to allow access to the rides and to other attractions. Credit-card information could also be uploaded to the chip, which provides 32-bit data protection, so that people could buy food or souvenirs by waving the patch over a terminal. The stamps can be glued onto skin for up to two days and when guests leave the park, they peel off the device and it can no longer be read. The amusement park could use the data gathered by WiSP to track the flow of guests and what they used their patches for.

In the meantime, MC10 is keeping its roots in healthcare. John Rogers, a material scientist from the University of Illinois, helped found the company as an outlet for flexible electronics research in 2008. And his research is still focused on healthcare devices such as flexible sensor circuits that can be wrapped around the human heart and pressure sensors that can be implanted in the skull to monitor brain trauma.

While these sensors are not likely to help people get into concerts or make mobile payments, they underline the unique changes in how we interact with electronics. "The goal is really to blur the distinction between man-made electronic systems and biology," Rogers said. *—James Morra*

TOYOTA TURNS ENTIRE CITY into Connected Vehicle Testing Ground

WHILE TECHNOLOGY COMPANIES are fielding small fleets of autonomous vehicles around the United States, Toyota is planning to muster 5,000 vehicles that communicate with each other and infrastructure in a single city. The enormous scale of the tests could help automakers and regulators understand how cars might share information to make driving safer.

The experiment will take place on the streets of Ann Arbor, Mich. with thousands of volunteer drivers, turning the city into a huge testing ground for connected vehicles and infrastructure. Toyota, the world's largest automaker, is partnering with the University of Michigan Transportation Research Institute, which has helped develop similar projects with the Department of Transportation.

Autonomous vehicles will have to be connected to each other and infrastructure like traffic lights before they can reach the masses. By sharing position data with other cars on the road and the surrounding infrastructure, these connected vehicles could avoid accidents with greater sensitivity or prevent distracted drivers from running red lights. These are also connected to the internet, giving drivers access to services that they might expect from a smartphone.

Drivers who agree to participate in the experiment will install a small data-collection device in their trunk, while placing an antenna near the windshield and another antenna on the trunk lid. The device will constantly exchange speed and position data with other

CYPRESS Acquires Broadcom's Wireless IoT Business, Loses Long-Time CEO

CYPRESS SEMICONDUCTORS HAS agreed to buy Broadcom Limited's wireless Internet of Things business for $550 million, further pushing its integrated chipsets into things like wireless sensors, smart home devices, and industrial equipment.

Under the terms of the deal, Cypress will absorb Broadcom's Wi-Fi, Bluetooth, and ZigBee products and intellectual property. The company will also acquire the WICED developer platform, a software development kit for building internet-connected sensors. Cypress is planning to target Broadcom chips mainly at consumer electronics and connected and autonomous vehicles.

T.J. Rodgers, chief executive of Cypress, stressed that the deal would enable the development of end-to-end embedded systems. Along with the announcement, Cypress outlined plans to combine the new wireless chips with its low-power programmable chips and microcontrollers, which are already used in consumer electronics and automobiles.

"With our IoT connectivity products, Cypress will be able to provide the connectivity; the MCU, system-on-chip, module and memory technologies; and the mature developer ecosystem," Stephen DiFranco, Broadcom's IoT general manager, said in a statement.

Broadcom's wireless IoT products were only a drop in the bucket of the company's entire business over the last year. Those products earned only $189 million in revenue during that time, according to the company's financial results. Once the deal has closed, Broadcom will have further trimmed down its encyclopedia of products, formed after the merger with Avago Technologies last year.

Broadcom said in a statement that it would continue making wireless chips for markets unrelated to the Internet of Things, including set-top boxes, wireless equipment, laptops, and smartphones. The deal, which has been approved by both Cypress and Broadcom boards, is expected to close in the third quarter of 2016.

The agreement came on the heels of Cypress's first-quarter earnings results. The company reported revenues of $425.2 million on $0.07 earnings per share, a decline of 6.8% from last quarter. In recent months, the company has been running wafer production lines slower than actual demand in an attempt to burn off excess inventory. It has also struggled to integrate several new manufacturing plants acquired from Fujitsu.

Since the company merged with Spansion last year, Cypress has introduced two new 40-nm, ARM-based microcontrollers, one designed for automobiles and the other for cheap, high-volume consumer electronics. Over the last year, the company has introduced 2,472 new products, most of which are automotive and industrial versions of 44 new chip lines.

Coinciding with the Broadcom deal was the announcement that Rodgers would step down as Cypress's chief executive after 34 years in the position. Rodgers, who founded the company in 1982, will remain on Cypress's board of directors and lead several technical projects. The company said it would begin an internal and external search for his replacement.

"I have always planned not to be spending most of my time in the last decade of my career immersed in the details of the operations," he said in a statement. "And, to be completely candid, the board and even the executive staff have urged me to bring new blood into operations."

cars in the experiment and research equipment on certain roads and intersections.

The drivers are not instructed to take specific routes, as the researchers are trying to monitor everyday driving situations. The test results could assist Toyota to develop new technologies like automated braking and lane changes, which make driving safer for human rather than taking their hands off the wheel.

"The current limitation of connected vehicle testing outside of closed circuit test tracks is the lack of connected vehicles," the company said in a statement. "In order to move autonomous driving toward reality, testing requires more cars, more drivers, and more day-to-day miles traveled than any combination of research facilities could support."

Toyota's approach stands in contrast to other forms of testing, like laboratory simulations and driving on closed-circuit tracks. Google X, the division of the search engine's parent Alphabet that develops autonomous cars, pioneered the practice of sending a handful driverless cars into cities around the United States. The company says that its cars have driven almost two million miles without any accidents.

These tests, which seem to preach the quality over quantity of research data, have occasionally been criticized by researchers. Last month, Duke University robotics professor Mary Cummings testified to the Senate that autonomous cars were "absolutely not ready for widespread deployment." She cited the glaring lack of research data—especially on autonomous vehicles driving in snow and rain—and certification programs from government regulators.

Google's "two-million-mile assertion is indicative of a larger problem in robotics, especially in self-driving cars and drones, where demonstrations are substituted for rigorous testing," Cummings said in her testimony.

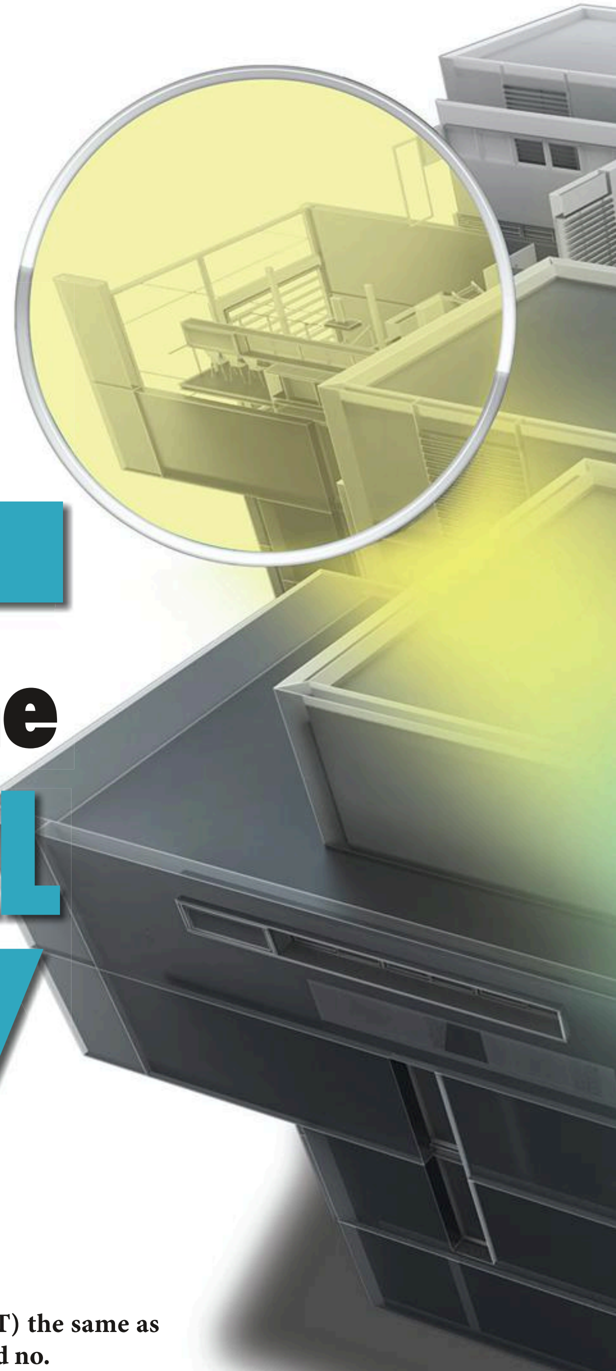
Ann Arbor has slowly become a focal point for more rigorous testing into connected and autonomous vehicles. In 2013, the University of Michigan partnered with the Department of Transportation to connect nearly 3,000 cars and trucks in the Ann Arbor area. Over the next few years, the goal is to equip 6,000 more vehicles, including motorcycles and bicycles—even pedestrians—with wireless equipment.

Toyota's plans were revealed not long after the company announced its third artificial intelligence and robotics center, which will be located in Ann Arbor. The company has already established two other centers, one in Palo Alto, Calif., adjacent to Stanford University, and a second in Cambridge near the Massachusetts Institute of Technology. Last year, Toyota said it would invest $1 billion over the next five years in these research centers.

—James Morra

WILLIAM WONG | Technical Editor

IoT–the INDUSTRIAL WAY



What is Industrial IoT? Find out how it differs from consumer IoT applications and why it is important to industrial applications.

Is the Internet of Things (IoT) the same as Industrial IoT (IIoT)? Yes and no.

Yes, both are such broad terms—like the "cloud" and the "internet"—that they encompass almost any connected device, with IIoT leaning toward industrial applications. The challenge is that many applications destined to be categorized as IIoT will fall exclusively within the realm of industrial deployment, such as factory or warehouse automation. Meanwhile, applications like industrial lighting slip into the consumer or enterprise side, since at least the control applications run on user's smartphones or tablets.

The basic IoT environment links devices (or edge nodes) to the cloud, often through gateways. These days, the cloud typically refers to computation and storage resources connected to the internet. IoT services like analytics and management tools utilize the data in the cloud. The raw and processed information is accessible via user interfaces, from smartphones to PCs.

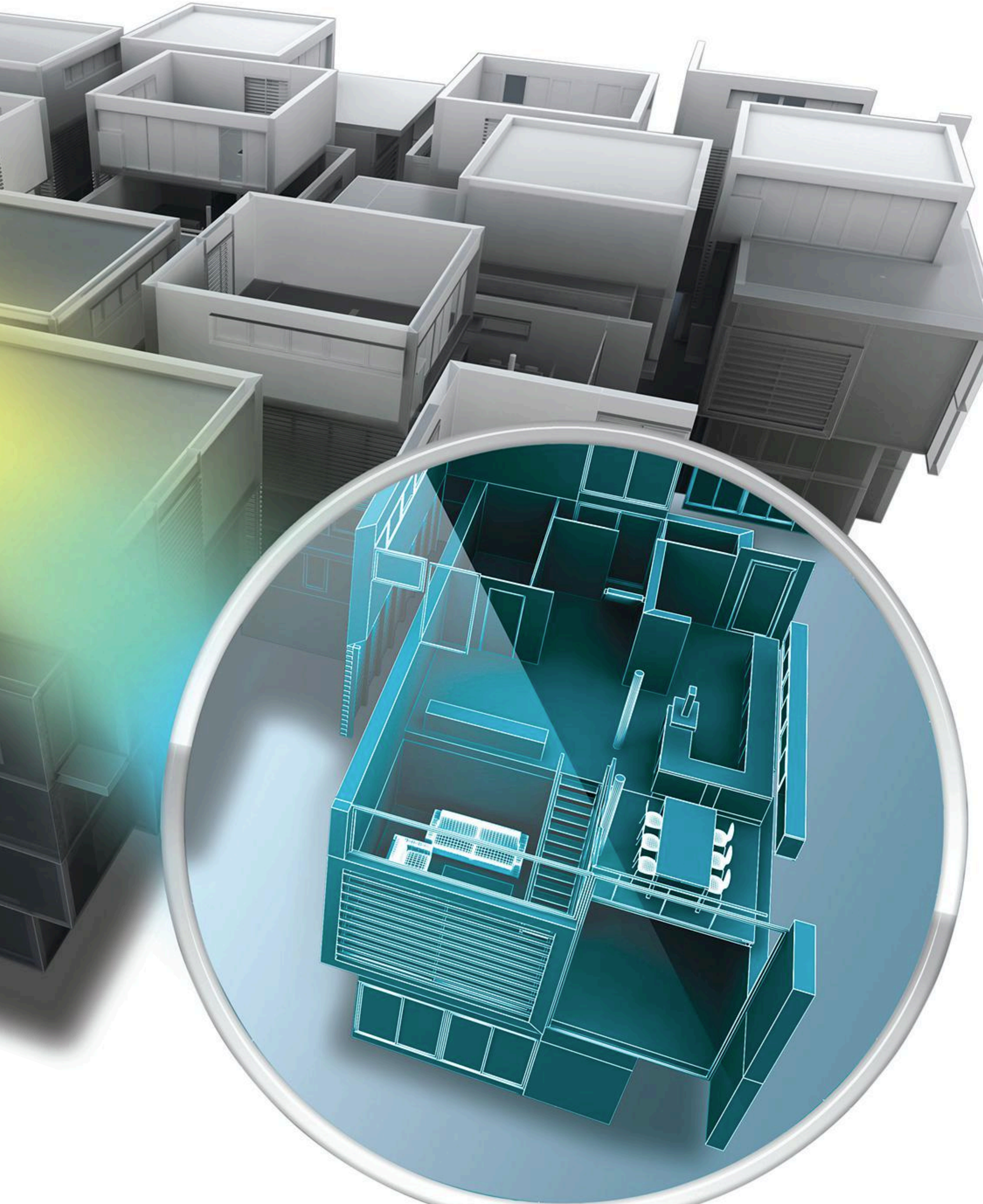
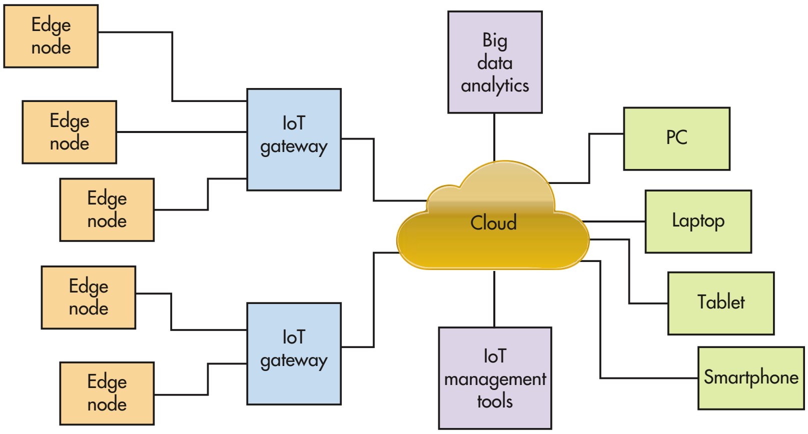


Image Credit: Franck-Boston



1. At a high level, IoT and IIoT have the same architecture using the same protocols. IIoT tends to have a more cooperative device environment, while IoT tends to have devices that are paired with users.

SO WHAT IS IIoT?

Taking the most general view, IIoT is essentially machine-to-machine (M2M) support extended into the cloud. In this sense, IIoT is not really a new idea but, rather, new terminology describing existing systems. The big difference is how existing systems are changing and how available these technologies will be.

For example, large industrial organizations usually have networked control and management of their systems, and this is tied into a corporate server environment that will provide information that can be used to track the system. This can allow predictive analysis to anticipate failures so that maintenance can be done prior to a failure occurring. These systems may be built on lower-level standards like Ethernet, TCP/IP, and SQL, but they were typically developed internally for a company.

The reason IoT and IIoT tend to overlap during any IoT discussion is that the tools and overall architecture for both tend to be the same *(Fig. 1)*. They use higher-level protocols on top of TCP/IP like MQTT and CoAP for data exchange *(see "MQTT and CoAP: Underlying Protocols for the IoT" on electronicdesign.com)*.

The traditional cloud architecture (*Fig. 2*) simply uses embedded software on the Operations Technology (OT) platforms to push data to the cloud where Information Technology (IT) environments can both process it and provide it with users. This tends to be only a slight improvement over non-cloud environments.

Advanced IIoT environments *(Fig. 3)* move more system intelligence from the IT side to the OT side. This provides microcontrollers and embedded platforms with easy access to cloud environments, as well as access to data to authorized devices and users.

Chip Downing, senior director for Wind River's Aerospace and Defense division, notes, "Advanced sensor-to-cloud architectures enable systems intelligence along the entire path of business intelligence so decisions can be made autonomously on the OT side, on the side of running the day-to-day operations, enabling business intelligence in the IT side to focus more on business analysis, strategy, and the optimized flow of required assets and money."

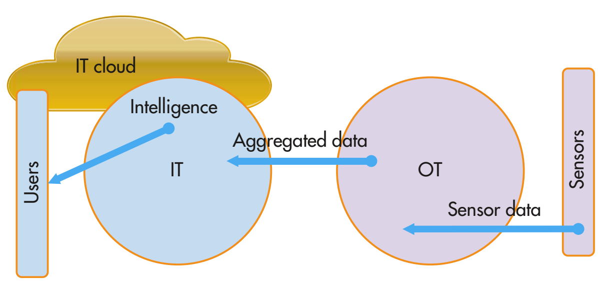
These more advanced IIoT environments are targeting a range of application areas from smart factories to smart cities. The idea is to provide more information throughout the environment, and to allow more dynamic distribution of data and applications.

In general, IIoT tends to have a more structured connectivity environment because the system is more mission-critical than typical IoT applications. Response time tends to be an issue, whereas an IoT application like a fitness tracker can often store data until a wireless link is available. IIoT also tends to target existing equipment and standards, while consumer IoT devices are often new products.

IIoT STANDARDS

IoT environments span a wider range of communication and services than previous models. This means there is a wider range of companies involved. It is also why IoT development and deployment tend to be more complicated and expensive, although in theory, the resulting system should be more efficient, more flexible, and ultimately reduce costs while providing more functionality.

A number of visions and consortiums have arisen around IoT and IIoT. For example, Platform Industrie4.0, or Industry 4.0, is the vision behind the 4th Industrial Revolution that has been associated with the smart factory. The four primary char-



2. The traditional cloud architecture has data moving from the right to the left, from sensors to embedded platform aggregation to an IT system, then pushed to a cloud environment, and then finally to the user. This is only a slight improvement over non-cloud environments. *(Courtesy: Wind River)*

PROVEN
40
YEAR
OPERATING
LIFE*

And keep them running until 2056.

The battery of the future is here today. Tadiran bobbin-type lithium thionyl chloride ($LiSOCL_2$) batteries feature an annual self-discharge rate of just 0.7% per year: so energy efficient that they allow low power consuming wireless devices to operate for up to 40 years on a single battery. No one else even comes close. Tadiran lithium batteries also feature the highest capacity, highest energy density, and widest temperature range of any lithium cell, plus a glass-to-metal hermetic seal for added ruggedness and reliability in extreme environments.

For a battery that lasts as long as your device, run with Tadiran.

TADIRAN
BATTERIES

Tadiran Batteries
2001 Marcus Ave.
Suite 125E
Lake Success,
NY 11042
1-800-537-1368
516-621-4980

www.tadiranbat.com

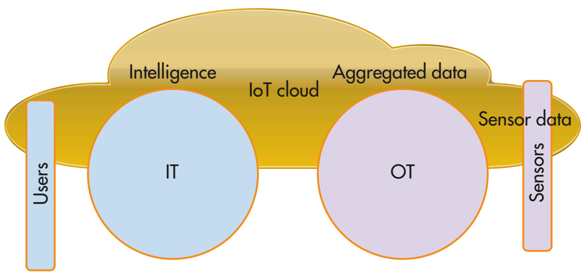
* Tadiran LiSOCL2 batteries feature the lowest annual self-discharge rate of any competitive battery, less than 1% per year, enabling these batteries to operate over 40 years depending on device operating usage. However, this is not an expressed or implied warranty, as each application differs in terms of annual energy consumption and/or operating environment.

> "One of the big challenges for IIoT is safety and security, since IIoT often links devices and services to the cloud that used to be much more isolated."

acteristics of Industry 4.0 include vertical integration of smart systems, horizontal integration of global value chain networks, integrated product life cycle management, and incorporation of new and existing technologies.

Industry 4.0 has six design principles: interoperability, virtualization, decentralization, real time support, service orientation, and modularity.

A host of consortia has arisen to address different IIoT aspects. For example, the Open Connectivity Foundation (OCF) incorporated the Open Interconnect Consortium (OIC) specifications, and the IoTivity open-source IoT framework. It highlights the difficulty of working with IIoT because of the range of alternatives available. For example, IoTivity is one of many IoT frameworks.



3. IIoT is a more integrated architecture that blends IT, OT, and the cloud so that aggregated data and computation are not focused on one side or the other. (Courtesy: Wind River)

There are also other groups that address aspects of IoT and IIoT, such as the AllSeen Alliance and the Thread Group *(see "Gallery: Threading FTF 2015" on electronicdesign.com)*. These target specific aspects of IoT and IIoT, and their standards are often referenced by other organizations as part of a higher-level IoT/IIoT standard. The AllSeen Alliance provides services that enable connecting IoT devices together, while the Thread Group defines a wireless ecosystem for the OT device side of things.

The Industrial Internet Consortium (IIC) is part of the Object Management Group. IIC is focusing on IIoT, or Industrial Internet Systems (IIS) in IIC terminology, at a systems level rather than specifics like OCF's IoTivity. IIS is divided into five domains: control, operations, information, application, and business. IIS is discussed in IIC's Industrial Internet Reference Architecture, which is more oriented toward system models that can utilize different underlying technologies like Thread or IoTivity.

The challenge with IIoT systems is that they require high-level specifications like IIC's because IIoT systems tend to be large and complex, incorporating end-to-end process control and management. Specifications for each level of functionality or communication are also required, so isolating them to specific areas such as Thread and local wireless communication allows the standards to be both manageable and understandable.

IIoT SAFETY AND SECURITY

One of the big challenges for IIoT is safety and security, since IIoT often links devices and services to the cloud that used to be much more isolated. In many cases there was an "air gap" between an unconnected device and a corporate network or the internet. Providing a network link allows real-time communication and often brings data to the cloud that was not obtainable in the past.

Most IoT frameworks or protocols incorporate one or more aspects of security such as encryption of communication links to authentication of data or commands. Some even include support for security policies and other security and safety management. The problem is that an IIoT environment may incorporate a range of frameworks and protocols that have differing security features and management methods, leading to complexity and possible configuration errors that would allow security breaches.

Features like secure boot, security operating systems, and secure communications are the basis for a secure IoT environment, but even with all these in place it is possible to have security problems that can crop up due to errors in applications, operating systems, or device drivers.

This is why a layered security environment is important for IIoT applications and why security needs to be of paramount importance when designing and implementing the system. It cannot be just the utilization of underlying security features or adding features like encrypted communication after the fact.

IIoT is the trend, but it will be challenging to incorporate existing networked systems into an overarching IIoT environment. There is no one IIoT standard, and a single one is unlikely given the plethora of conflicting and existing products and services that vendors have already.

Still, there will be a continued push to implement IIoT because of the availability of more information for big data analysis, as well as more real time information that will allow more just-in-time (JIT) features—such as product and raw material delivery, preventative maintenance, and real-time information about the overall process in smart factory or smart city environments. ed

MARIA GUERRA | Technical Editor

The Principles of FPGAs

Field programmable gate arrays (FPGAs) were introduced more than three decades ago, and since then they have evolved, giving way to new generations of FPGAs with better logic density and performance that can be used in a broader range of applications.

The first FPGA was invented by Ross Freeman (cofounder of Xilinx) in 1985 and since then their logic capacity has enhanced greatly and they have become a popular choice because FPGA systems can be reprogrammed after manufacturing to implement the user's final desired application. Some FPGAs can be reprogrammed infinite times and some limited times.

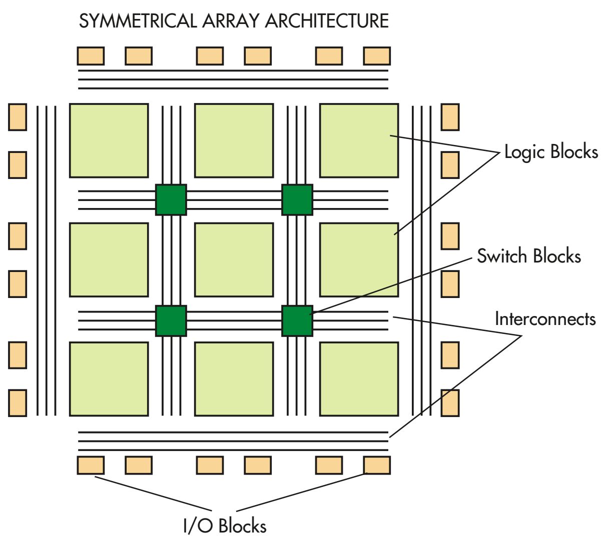
In general terms, FPGAs are programmable silicone chips with a collection of programmable logic blocks surrounded by Input/Output blocks that are put together through programmable interconnect resources to become any kind of digital circuit or system. FPGAs developed from programmable read-only memory (PROM) and programmable logic devices (PLDs).

Unlike processors, FPGAs are truly parallel in nature. Each independent processing task is assigned to a dedicated section of the chip. Therefore, the performance of one part of the application is not affected when more processing tasks are added.

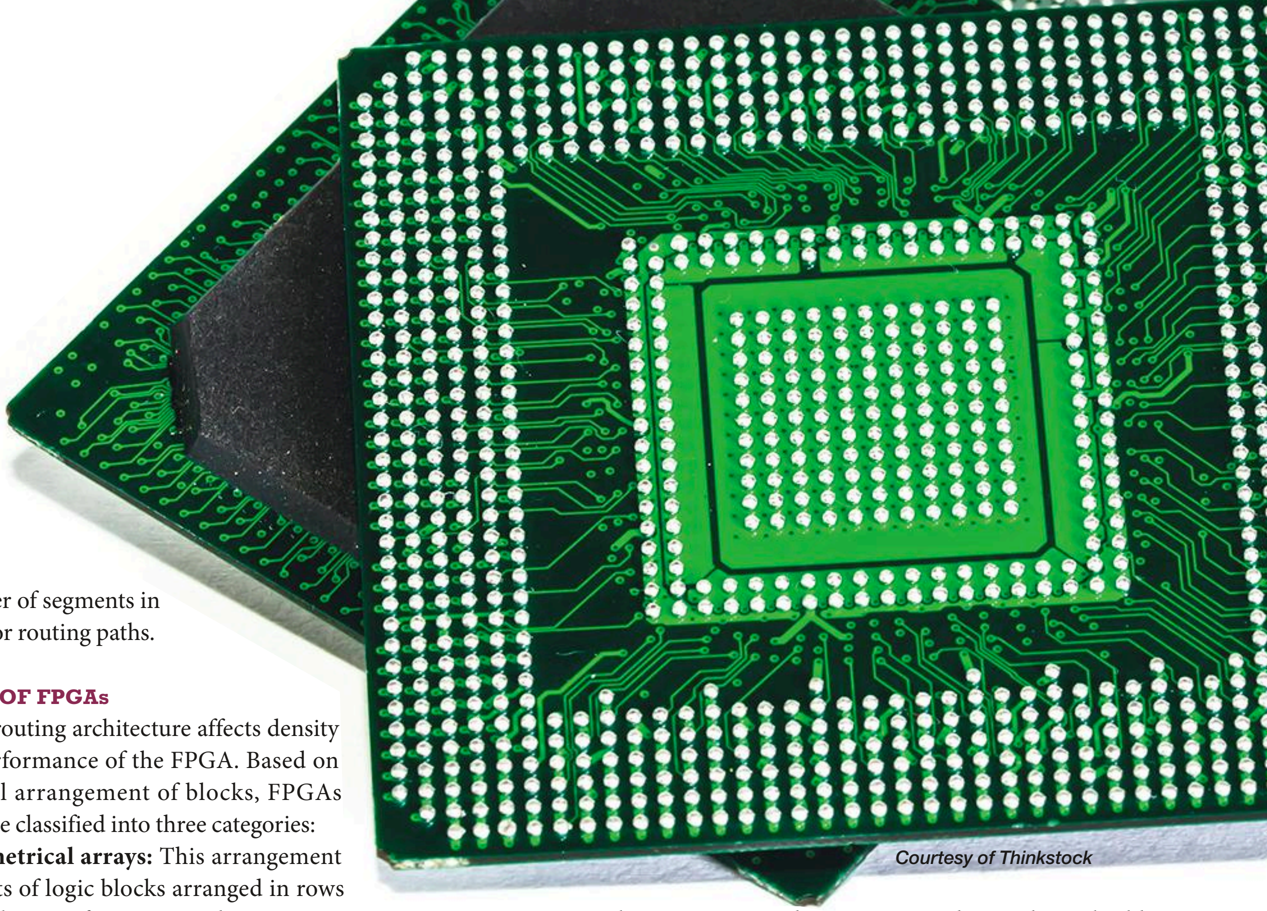
FPGA ARCHITECTURE

A precise architecture of an FPGA varies from manufacturer to manufacturer. Here, we present a generic FPGA structure that contains the following elements:

- **Programmable logic blocks:** Logic blocks can be formed from thousands of transistors to millions of transistors. They implement the logic functions required by the design and consist of logic components such as transistor pairs, look-up tables (LUTs), and Carry and Control Logic (flip flops and multiplexers).
- **Programmable I/O blocks:** They connect logic blocks with external components via interfacing pins.
- **Programmable interconnect resources:** They are electrically programmable interconnections (pre-laid vertically and horizontally) that provide the routing path for the programmable logic blocks. Routing paths contain wire segments of varying lengths that can be interconnected via electrically programmable switches. The FPGA density depends of the



1. Symmetrical arrays consist of a two-dimensional array of logic modules interconnected by vertical and horizontal programmable interconnect resources. *(Courtesy of rfwireless-world)*



Courtesy of Thinkstock

number of segments in used for routing paths.

TYPES OF FPGAs

The routing architecture affects density and performance of the FPGA. Based on internal arrangement of blocks, FPGAs might be classified into three categories:

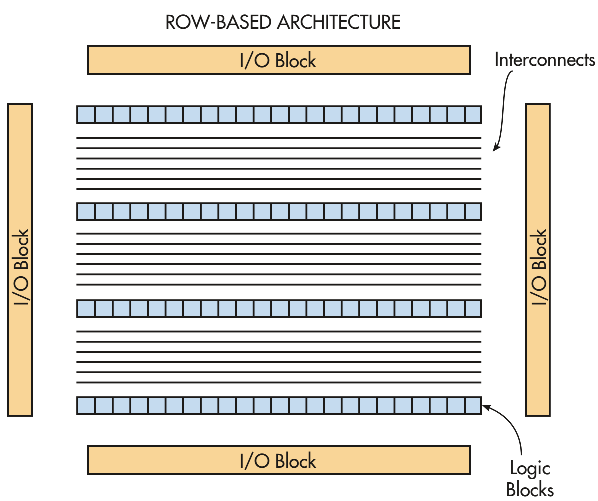
- **Symmetrical arrays:** This arrangement consists of logic blocks arranged in rows and columns of a matrix and interconnect resources between them. This symmetrical matrix is surrounded by I/O blocks that connect it to the outside world (*Fig.1*).
- **Row-based architecture:** It alternates rows of programmable interconnect resources with rows of logic blocks while the Input/Output blocks are located in the periphery of the rows (*Fig. 2*). One row may be connected to adjacent rows via vertical interconnect.
- **Hierarchical PLDs:** These are designed in hierarchical manner with the top level containing only logic blocks and interconnects. Each logic block contains a number of logic modules. And each logic module has combinatorial as well as sequential functional elements (*Fig. 3*).

Based on programming technology type, FPGAs can be classified into three categories:

- **SRAM-based FPGAs:** Static RAM cells control pass-transistor, transmission gates, or multiplexers. They can be reprogrammed as the design evolves, but when the power is off the programming is lost and they need to be configured upon start. Therefore, they need an external memory to store the program.
- **Antifuse-based FPGAs:** They use an antifuse CMOS technology and once the FPGA has been programmed, it cannot be reprogrammed. They retain their program when the power is off.
- **Flash-based FPGAs:** They use floating gate cells as switches that improve area efficiency. They do not lose information when the device is powered down. This technology does not need an external memory to store the program, but they cannot be reprogrammed infinite times due to charge buildup in the oxide.

POWER CONSUMPTION

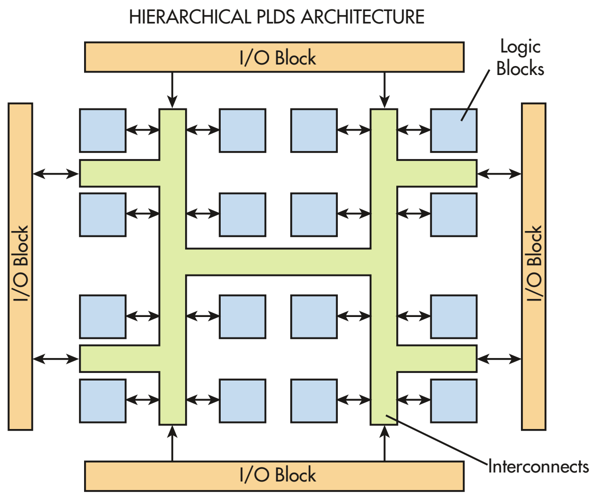
FPGAs consume much more power than ASICs because they have a large number of transistors per logic function in order to program the devices. FPGAs with low power consumption are ideal and they represent a challenge for FPGAs manufacturers. There are three types of power consumption that should be taken into account to design an efficient FPGA:



2. Row-based architecture consists of rows of logic blocks that are separated by programmable interconnect resources. *(Courtesy of tutorial-reports)*

- **Static power:** It is the power consumed by transistor leakage when no signals are toggling.
- **Dynamic power:** It is the power consumed by signal toggling and capacitive load charging and discharging during the operation of the circuit.
- **Input/output power:** I/O power includes the power consumption consumed by I/O blocks, including general-purpose I/Os and high-speed serial transceivers.

There are many power-reduction design techniques used for different FPGA manufacturers. There are many factors that need to be taken into account to analyze and balance to obtain low power consumption, e.g., type of application, programming technology, right architecture, right software power optimization, etc.



3. In a hierarchical PLD, each logic block contains a number of logic modules. *(Courtesy of tutorial-reports)*

APPLICATIONS

Modern FPGAs are used across several markets; some of the latest applications by market include:

- **Energy:** Renewable energy sources (e.g., solar and wind power) are reliable and are found more often as part of a smart grid where standards are still evolving. An optimal control for smart grids requires end-to-end communications and efficient power networks, especially in transmission and distribution (T&D) substations. To support automation, the equipment needs to monitor, control, and secure the grid in real time for more efficient management of peak demand loads.

Altera offers several solutions to enhance smart-grid equipment reliability. For example, the PRP/HSR GbE switch on a Single Cyclone V FPGA supports hardwired, real-time switch performance and reduced latencies. It meets the performance requirements of Gbps Ethernet traffic with PRP/HSR redundancy and evolving PRP/HSR standards.

For easier PRP/HSP implementation, Altera teamed with Flexibilis (a provider of networking equipment and technologies based on industry-standard technologies and protocols for smart-grid substation automation). The Flexibilis Redundant Switch can be easily implemented on an Altera FPGA and is fully compliance tested on the Altera Cyclone family.

- **Automotive:** Microsemi FPGAs enable automotive original equipment manufacturers (OEMs) and suppliers to build innovative safety applications such as adaptive cruise control, collision avoidance, and blind spot warning. Microsemi SmartFusion2 SoC FPGAs and IGLOO2 FPGAs offer security (e.g., information assurance, anti-tamper, hardware security), reliability (through flash, FPGA fabric provides SEU immunity, error-corrected memories) and low power (e.g., industry's lowest static power, low-power modes for on-chip peripherals). Microsemi flash FPGAs offer low static power due to low leakage and can operate in low-power Flash*Freeze mode for low-duty-cycle operations.
- **Aerospace and defense:** Xilinx offers rad-hard and rad-tolerant FPGAs that meet the performance, reliability, and lifecycle demands of extreme environments, while enabling greater flexibility than feasible with traditional ASIC implementations. Xilinx offers two space-grade product families: Virtex-5QV FPGAs and Virtex-4QV FPGAs.

The Virtex-5QV FPGA is a rad-hard reconfigurable FPGA for processing-intensive space systems. The Virtex-4QV FPGAs are SRAM-based FPGAs that are guaranteed for total high-level ionizing dose and single-event latch-up immunity. Extensive single-event upset (SEU) characterization is performed and reported by the Single-Event Effect Consortium.

- **Analog:** FPGAs can be used to perform data-conversion tasks as well. Altera has the MAX 10 FPGA devices that feature up to two integrated analog-to-digital converters (ADCs). You can use the ADCs to monitor many different signals, including on-chip temperature. With 12-bit resolution, it can translate analog quantities to digital data for information processing, computing, data transmission, and control systems.

CONCLUSIONS

Modern FPGAs are very reliable devices with strong advantages: reprogrammability and fast time-to-market concept with no up-front non-recurring expenses (NREs). With their rapid prototype capabilities, a concept can be verified in hardware very fast, while in field-reconfiguration can keep up with future modifications without modifying the board layout. In the past, FPGAs were selected for lower speed and lower volume designs, but today they are still evolving and many can now successfully perform in a wider range of applications. ed

REFERENCES:
1. Altera, "Overcoming Smart Grid Equipment Design Challenges with FPGAs"
2. Xilinx, "Space-Grade Virtex-4QV Family Overview"
3. Altera, "MAX 10 FPGA Device Overview"
4. Microsemi, " Automotive FPGAs & SoC FPGAs"
5. Farooq, Umer, Marrakchi, Zied, Mehrez, Habib, "Tree-based Heterogeneous FPGA Architectures"


THINK™
INTERCONNECT COMPONENTS & HARDWARE
Battery Clips, Contacts & Holders
Fuse Clips & Holders
Terminals and Test Points
Spacers & Standoffs
Plugs & Jacks
Multi-Purpose Hardware
IT'S WHAT'S ON THE INSIDE THAT COUNTS
KEYSTONE®
ELECTRONICS CORP.
www.keyelco.com • (718) 956-8900 • (800) 221-5510

WILLIAM WONG | Technical Editor

NVMe Bids to Win the STORAGE WARS

What's trending in storage? Changes in form factors and interfaces seem to have put the spotlight on NVMe.

A monopoly could well be forming before our eyes in the storage arena, and it's known as NAND flash memory. Storage form factors are changing, as are the interfaces involved with Non-Volatile Memory Express (NMVe)—all of it pushing the performance envelope even further.

A form-factor connector making a splash in this space is U.2 *(Fig. 1)*, formally known as SFF-8639. Available on the 2.5-in. Enterprise Form Factor, it actually supports up to four SAS/SATA interfaces and PCI Express x4, including dual port configurations. In addition, the connector provides power and an SMBus interface, not to mention its support for hot-swapping. The U.2 PCI Express interface is on par with the M.2 PCI Express interface *(see "What's the Difference Between M.2 Modules?" on electronicdesign.com)*.

There are two performance reasons for moving to PCI Express rather than SATA or SAS. The first is scalability: Multiple PCI Express lanes can be used to provide more throughput (for example, x1 and x4 M.2 devices are available). Second, PCI Express lowers overhead and latency, because no additional controllers are needed between the host and the drive.

A drive needn't use all of the interfaces. A motherboard or controller can implement multiple interfaces, allowing it to support different types of drives. For example, a motherboard could support SATA, SAS, and PCIe/NVMe drives. Drives like Intel's 750 Series typically implement a single interface. In this case, the PCI Express x4 interface provides support for NVMe.

Platforms such as Super Microcomputer's (SuperMicro) 2U SSG-2028R-NR48N *(Fig. 2)* and Dell's 2U PowerEdge R820 offer support for NVMe solid-state drives (SSDs), as well as SATA and SATA drives. The PowerEdge R820 features 16 drive slots with up to four Intel E5-4600 processors plus 1.5 TB of DDR3 DRAM. Meanwhile, the SSG-2028R-NR48N packs in two banks of 2.5-in. hot-swap NVMe drives supported by a pair of Intel E5-2600 processors and up to 3 TB of DDR4 DRAM.

PCI Express adapter cards support this type of drive, but most applications instead will utilize PCI Express SSDs. For motherboards with M.2 sockets, Asrock offers a U.2 Kit that plugs into an M.2 socket with Mini-SAS connectors that are linked to a U.2 drive via a cable.

At this point, enterprise applications are pushing NVMe drive support. However, embedded applications such as data logging and video processing will begin to demand the performance and flexibility available with the U.2 form factor. Needless to say, the drive form factor provides a modular implementation that's highly desirable. ed

1. The U.2 connector, formally known as SFF-8639, supports up to four SAS/SATA interfaces and PCI Express x4, including dual port configurations.

2. SuperMicro's SSG-2028R-NR48N squeezes in two sets of 24 banks of 2.5-in. hot-swap NVMe drives.

WILLIAM WONG | Technical Editor

Automated Tools Augment Programmer Efficiency

Style checkers and static-analysis tools are ways to improve code quality. We examine some of the alternatives in this space.

How do you improve the output capability and quality of embedded programmers? One way is to give them better tools such as static-analysis and compliance tools. They tend to be mandatory in embedded arenas such as military and avionics, but—according to the latest Barr Group survey—less prevalent in general *(see "Survey Results Reveal Embedded Safety and Security Trends" on electronicdesign.com)*.

The challenge isn't just getting the tools into developers' hands, but also getting developers to use them. While training definitely helps on the latter front, developers often discount the value of these tools.

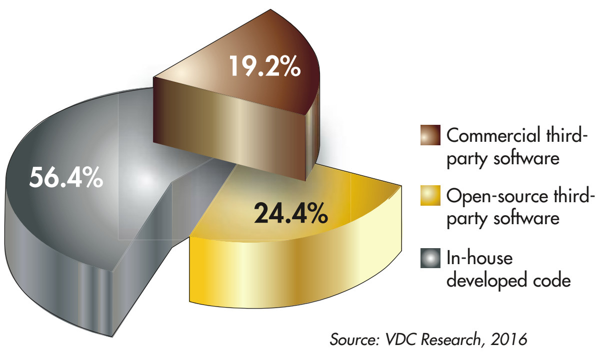
There are a variety of myths about them as well that are easily debunked *(see "11 Myths About Software Qualification and Certification," p. 28)*. For example, these tools are not just for military and avionics applications.

Another myth is that the tools can be expensive to buy and use. That myth has a few more caveats, because most of these tools aren't just simple static-analysis tools. They are often part of a coordinated suite of tools that include things like code coverage analysis, coding standards compliance, requirements traceability, code visualization, and more. Some companies sell their tools unbundled, possibly reducing the initial cost. Some developers may already have similar tools in their toolbox.

The more difficult problems include trying to justify the cost of these tools and incorporate them into the development process. The latter is easier at the start of a project because bad habits are more easily corrected. Adding the tools to the mix of an existing project often generates many new bugs.

The discussion about these types of tools has been ongoing, so why is it more important now? One reason is the rise of the Internet of Things (IoT). The IoT inherently requires a wider range of coding to occur from embedded devices through the cloud, all of which are prone to errors and security issues. The systems tend to be beyond the scope of a single person to implement and execute, making these types of analysis tools more valuable; they provide a more consistent development environment across the IoT platforms, in addition to detecting bugs.

SOURCES OF EMBEDDED CODE



Most embedded code is still developed in-house.

According to VDC Research, most code for embedded applications is developed in-house *(see figure)*. Still, this code may make use of third-party, open- or closed-source libraries and runtime. Good programmers using good programming practices are useful for the code they generate, but what about third-party code? Most developers have access to the source code, so the standard analysis tools can handle it, but code is sometimes available only in binary form. Grammatech's CodeSonar supports a mixed-mode analysis that can analyze binary code, allowing third-party libraries to be checked.

Automated tools like static analysis can pay huge dividends in the long run. They are worth checking out if you are not already using them since they can improve code quality, reduce delivery times, and provide an edge over the competition. The challenge in comparing tools will be the variety of options and variance in features between different vendor products. Features like code coverage and standards compliance tend to be common, but other features may be unique.

Ultimately, deciding on what tools will work best with your current development process can take a good bit of time and effort. It is not something to be done in an afternoon discussion while running through a checklist.

JAY THOMAS | Technical Development Manager, LDRA

11 Myths About Software Qualification and Certification

Common misconceptions about quality-code development practices in the embedded-device and software-development lifecycle create a false sense of safety, security, and quality within the industry.

With software taking on an ever-greater role in embedded systems, companies are realizing that "quality code" requires more than just the developer's claim. Even for systems that don't require formal certification for functional safety or security, software qualification is becoming more common. After all, who really wants to risk expensive field support, product recalls, or even legal action if the software fails? Still, at least 11 myths continue to circulate about software qualification and certification.

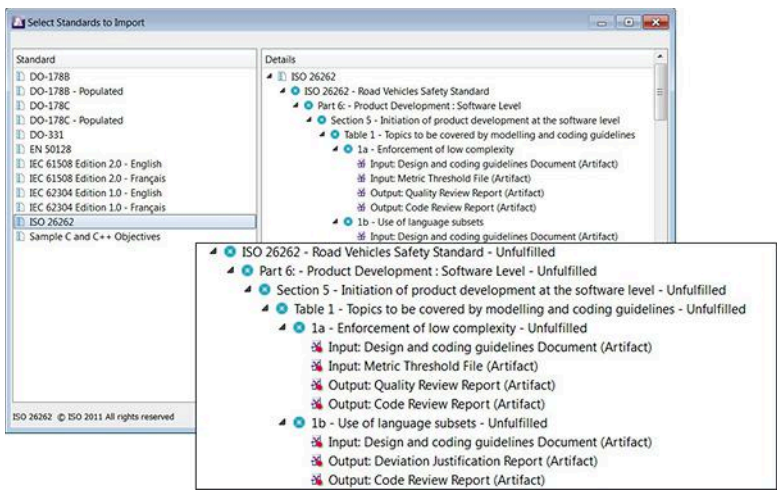
1. Software certification only applies to avionics applications/doesn't apply to my industry/isn't possible.

This myth is often tied up in semantics. For instance, the U.S. aerospace industry requires software to be qualified to specific standards in order to certify systems. And while software isn't required to be certified in other U.S. markets yet (the situation varies by industry and geography), discussions along these lines are underway in many safety-critical industries, including medical, nuclear power, industrial, and automotive. Whether certification is required or not, software developers who can prove compliance to international quality standards can offer confidence to both OEMs and operators that the software in the device will behave as expected.

2. Software certification is only important to government regulators and industry gurus.

As the market pushes for higher-quality software, particularly in safety- and security-critical industries, software certification or qualification is becoming more mainstream. Many software development and verification organizations are being trained on compliance with functional safety and security standards, especially as compliance becomes increasingly important to the supply chain.

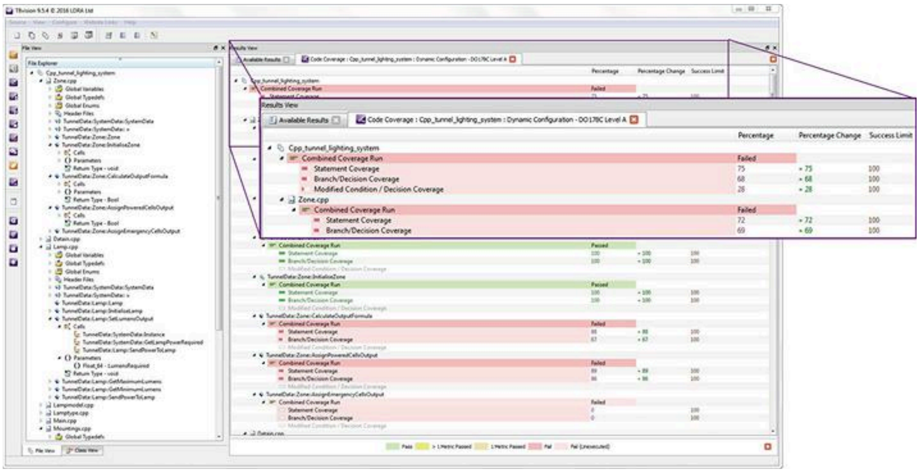
Even if software has yet to be formally regulated, large OEMs may require suppliers to adhere to industry standards such as IEC 61508 (industrial controls), IEC 62034 (medical), ISO 26262 (automotive), IEC 60880 (nuclear energy), and EN 50128 (rail transportation). For instance, GM is now training its software suppliers on formal development processes so that they can provide an audit trail back to GM. Trained developers can gain a competitive advantage by showing that they already follow industry standards and best practices, and developers



1. Artifacts and assets can be linked to objectives to reduce risk and cost during the audit process. *(Photo courtesy of Jane Smith)* who understand these processes can gain a career advantage as well *(Fig. 1)*.

3. Software qualification is too expensive.

This myth is typically based on software qualification that's performed using traditional manual methods. Companies that choose to use non-automated tools, such as Word or Excel, to track processes can become hopelessly bogged down. The process of developing and verifying software needs to be formalized, repeatable, and measurable.



2. Automated code-coverage results are displayed inline with system/file/function name to give you a detailed overview of which aspects of the system meet the expected code-coverage levels or metrics. *(Photo courtesy of Jane Smith)*

By leveraging automation technologies, organizations can greatly reduce the effort and cost of producing high-quality software and—depending on the market and industry standards—certified software. For this to be done cost-effectively, software organizations need to rely on automation technology to perform the menial tasks that often consume large amounts of time and human-resource energy during the software development lifecycle.

4. I can do software certification cheaply without tools and automation.

Software certification is simply not possible in a cost-effective manner without software tools and automation. Without automated tools, developing and providing the evidence required for software certification can be a resource-intensive, time-consuming, and arduous task.

Luckily, many of these manually intensive development and verification tasks can be automated. Some of the manual tasks to consider for automation include requirements traceability and impact analysis, static code analysis, manual code reviews, structural coverage analysis, test-harness generation, test-case generation and execution, regression testing, and documentation generation for compliance and audit trail evidence.

If automating these processes could save your development team three months, for example (potentially 20% to 40% of the overall schedule), it could result in several hundred thousand dollars in reduced man-hour costs. Investing a comparatively small amount into the tools that automatically link requirements to written code, as well as the subsequent tests, and auto-generate documentation can save many times that amount in labor costs and provide first-to-market advantages *(Fig. 2)*.

5. Software qualification isn't worth the cost.

Depending on the market, producing software that's not high-quality, certified, or qualified is simply not a business option. Companies need to perform some level of risk analysis to determine whether the costs involved in addressing market requirements of security and safety are worth it. While formal software certification can be expensive in terms of resources, time, and money, so are product recalls, lawsuits, and brand damage, especially if a software failure results in injury or death. The question to ask is whether you can afford *not* to qualify your software to safety or security standards. We only need to look at the news to see examples such as Baxter's multimillion-dollar infusion pump recall or the Toyota recall of 625,000 hybrid cars—both the result of software flaws.

6. You can rubber-stamp software certification after the fact.

Quality is an ongoing process of design, creation, and testing. If you don't follow the process, you don't get the quality, and there's no post facto rubber stamp that will fix it. Of course, companies continue to try it—we typically read about them in the news (see comments above about Baxter and Toyota). To be performed effectively, software functional safety and security simply must be built into the product from the ground up.

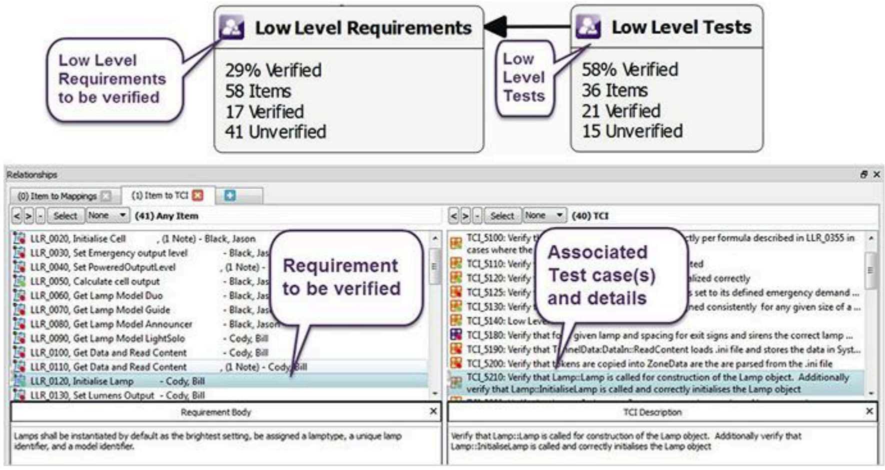
7. Using static analysis is enough to ensure quality code.

Static analysis can lead to higher-quality code by helping ensure that the code is clear, concise, and maintainable, and that it adheres to industry best-practice coding standards. However, it's performed without executing code, so it only addresses one part of the overall software-development lifecycle. Even if code is perfectly written, it's only correct if it meets project requirements. The bottom line? Static analysis is a great enabler, but no panacea on its own.

8. Software certification can be accomplished without a formal development process.

Software certification is about meeting and testing to established software requirements. So while it's possible to accomplish without a prescribed formal development process, doing so is likely cost-prohibitive. Without artifacts, you will essentially have to reverse-engineer your software after the fact in order to document any development and test processes.

This is bound to be error-prone, will take additional resources and developer time, and will delay time-to-market. And if engineers have to be pulled back into the project because they are the only ones familiar enough with the code, then this approach could also impact schedules for other products. A formal development process in which certification is planned from the beginning and managed throughout the development workflow streamlines and shortens verification, making certification much more reasonable in terms of the money and resources required *(Fig. 3)*.

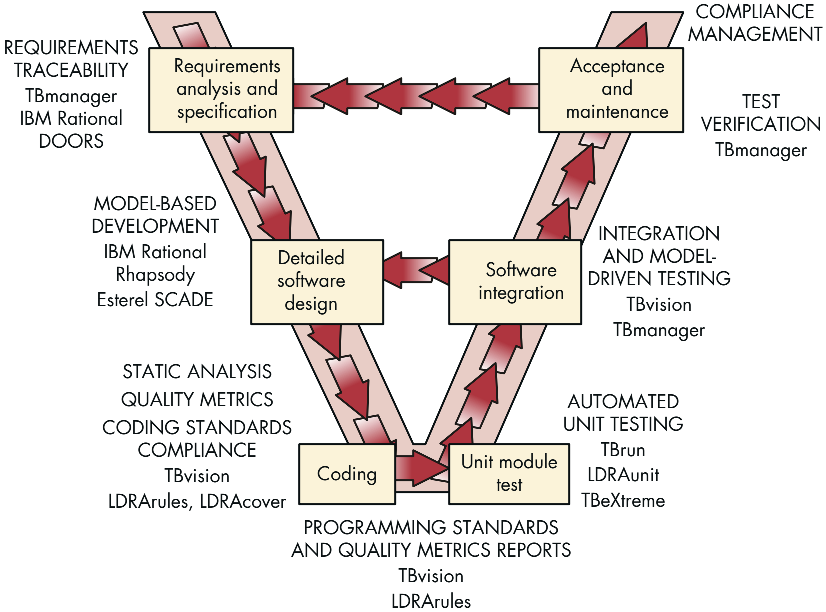


3. Reduce costs of authoring tests, linking to requirements, and performing impact analysis. *(Photo courtesy of Jane Smith)*

9. Software certification is not possible with embedded targets.

In many safety- and security-critical applications, software certification must be done on the actual hardware platform intended to be used for deployment. That said, software testing and verification can often be performed in virtual or simulated environments, and this simulated testing can help keep software development on track during hardware development.

In those cases, it's incumbent upon the software organization to prove that the software proven in the virtual or simulated environment is the same as the software being deployed in the actual target environment. Tool suites are available, such as those from LDRA, which have probes for embedded hardware. This gives development teams the same test environment for simulated and final hardware test.



4. Build quality into your software development lifecycle. *(Photo courtesy of Jane Smith)*

10. You can build a safe system without security.

In today's connected, Internet of Things world, an insecure system is simply not a safe system. Reports of hacked medical equipment, automobiles, and smart energy devices abound, and systems with low-quality code are simply easier targets for hackers. As a result, safety-critical software must be developed and verified with security in mind from the beginning—this isn't an either/or decision.

11. Software certification is not possible in an agile environment.

For some time, it was believed that only the most formal structured development approaches could produce code that is qualifiable or certifiable. That led to the well-known V model, which moves logically and sequentially from requirements to design to test *(for more, go to http://www.ldra.com/tool-suite)*. Today, agile development environments can be less formal on the surface; developing small pieces of code in short sprints. However, the processes used during sprints can still be automated and documented, resulting in a series of short, less error-prone, and integrated software sprints *(Fig. 4)*. ed

JAY THOMAS is technical development manager for LDRA Technology, San Bruno, Calif.

RICHARD NEWELL | Senior Principal Product Architect
SoC Group, Microsemi Corp. *(www.microemi.com)*

The Biggest Security Threats Facing Embedded Designers

Software security alone is not enough to protect today's networked devices and fielded systems. What's needed is a combination of both software and hardware security.

Embedded-system designers face a number of threats to the applications that they develop for the Internet of Things (IoT). One of the biggest threats comes from subsystems that hackers can access, such as commercial networked HVAC systems, wireless base stations (e.g., small cells), medical devices and their controllers, smart cars and the emerging networked transportation infrastructure, home and industrial-infrastructure network gateway systems, and remote industrial sensors. Factors that make IoT endpoints especially vulnerable to security threats include:

Networked: IoT endpoints may be remotely accessible from nearly anywhere in the world via the internet or other (e.g., phone) networks. Wireless connections, used in many IoT devices, are especially vulnerable.

Fielded: IoT devices are often physically accessible, as well as interconnected. This exposes them to additional hardware attacks that do not usually need to be considered for systems that may be networked but are physically protected by "guns, guards, and gates."

Available: Samples are often easily available through purchase or theft that can be analyzed at the adversary's leisure.

There are definite safety aspects to poor security. An example is the aforementioned connected car, including the Advanced Driver Assistance System (ADAS) that encompasses intelligent, interconnected Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) systems. Since vehicles are fielded systems, they are accessible to people with malicious intentions. There can be serious consequences—up to and including loss of life—if, for instance, ADAS systems cannot ensure that V2V and V2I messages originate from a trustworthy source or are not modified between the sender and receiver.

Connected medical devices such as pacemakers and insulin pumps, and many industrial systems, have obvious safety and even homeland-security implications related to security vulnerabilities. This is why recent revisions of functional safety specifications such as IEC 61508 and the latest avionics standards require good security, too.

With safety implications comes legal liability. Government regulators such as the FDA are becoming more active in mandating strong security to protect consumers from security-related safety, economic, and privacy threats. More and more, companies are being fined or sued over badly implemented security. One of the casualties can be a company's hard-earned reputation; and with a loss of revenue, employee job security.

SECURING THE IoT

Software security, alone, has proven relatively unsatisfactory in protecting networked devices against known and freshly discovered threats (so-called "zero day" vulnerabilities), and is totally inadequate for the additional threats posed to fielded systems. What's needed is a combination of software *and* hardware security. Ideally, the hardware and software solution should combat three types of security: design security, hardware security, and data security.

Design security: This includes IP protection and ensuring that configuration bit streams and firmware are encrypted and protected. Designs need to incorporate a method to ensure that overbuilding or cloning of the design is not possible. Field updates to processor firmware or FPGA configurations need to be authenticated and the payload kept confidential.

Hardware security: Designers also need to certify that user-accessible devices are resistant to physical attacks. For example,

DESIGN NOTES

Ultrathin Triple Output μModule Regulator for DDR, QDR and QDR-IV SRAM Fits 0.5cm^2 Area and Backside of PCB

Design Note 551

Sam Young and Afshin Odabaee

Introduction

Delivering the highest RTR (random transaction rate) of QDR (quad data rate) SRAMs, QDR-IV provides up to 400Gbps data transfer for high bandwidth networking, high performance computing and intensive data processing applications. A key challenge at these faster data rates is maintaining the integrity of the data transferred between the SRAM and devices such as high speed FPGAs and processors.

A good solution is to place the SRAM—QDR-IV, QDR or DDR, for example—very close to the interfaced devices on the PCB's topside. To conserve PCB area and minimize induced PCB parasitic noise on data bus lines, the DC/DC regulator circuit powering the QDR-IV SRAM data bus drivers should be placed nearby. The challenge is finding space for regulators on a densely populated PCB.

Using a complete DC/DC regulator with onboard inductor and MOSFETs housed in a compact package is one solution. But the scarcity of area on the top of the PCB can render even compact solutions insufficient. If the footprint, height and weight of the DC/DC regulator solution can be reduced enough, it can be placed on the backside of the PCB where space is available.

VTT, VDDQ, V_{REF} from $12V_{IN}$ in a Tiny Ultrathin Package

The LTM®4632 is a complete triple output step-down μModule® regulator specifically designed to support all three voltage rails required by the new QDR-IV and older DDR RAMs, housed in a 0.21g miniature ultrathin profile LGA package (6.25mm × 6.25mm × 1.82mm).

Included in the package are the switching controllers, divide-by-2 circuit, power FETs, inductors and support components. Its tiny footprint and low external component count (as low as one resistor and three capacitors) occupies only 0.5cm^2 (dual-sided) or 1cm^2 (single-sided) while its thin profile enables mounting on the PCB bottom side to free up space on the topside for super-compact board designs.

The LTM4632 operates from an input voltage between 3.3V and 15V, providing precision output rail voltages between 0.6V and 2.5V. Its two switching regulator outputs, V_{OUT1} and V_{OUT2}, provide up to 3A for VDDQ and ±3A for VTT bus termination rails, respectively. Its third output provides a low noise buffered 10mA output for the termination reference (VTTR) tracking voltage. Figure 1 shows the LTM4632 circuit in a typical DDR3 application, illustrating its simple solution and small component count.

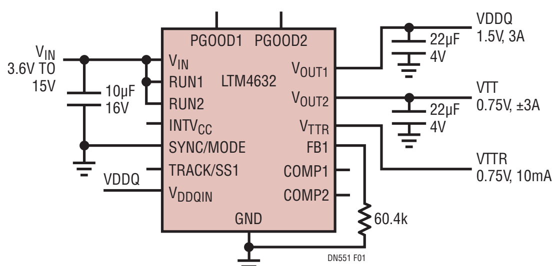


Figure 1. Typical LTM4632 DDR3 Application

Powering More SRAM Modules

The LTM4632's design flexibility enables it to support a broad range of application requirements. For example, its VDDQIN input allows the VTT and V_{REF} rail voltages to be set as either a typical 1/2 × VDDQ voltage or programmed by an external reference voltage for other values. The LTM4632 can be configured as a two phase single output rail for VTT in applications needing more than a ±3A termination

06/16/551

rail current. These features allow the LTM4632 to support voltage requirements for many different SRAMs and increase load current requirements for larger memory arrays.

Figure 2 illustrates the flexibility of the LTM4632. The two switching regulator outputs of the LTM4632 are connected in a PolyPhase® current sharing configuration to provide up ±6A VTT for larger memory banks. For more than 6A VDDQ, the LTM4632 can be combined with other µModule regulators, such as the LTM4630, to provide up to 36A for large SRAM arrays. Efficiency and power loss are shown in Figure 3, with thermal performance for the LTM4632 shown in Figure 4.

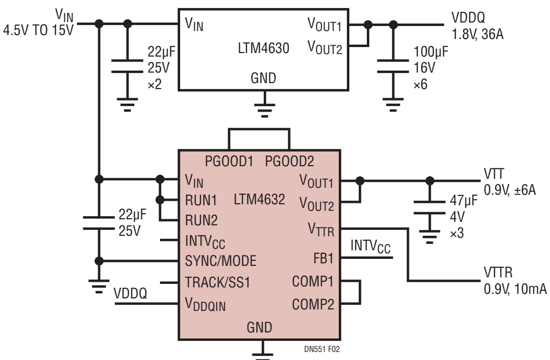


Figure 2. LTM4632 Two Phase Single Output ±6A VTT with 36A LTM4630 VDDQ Supply

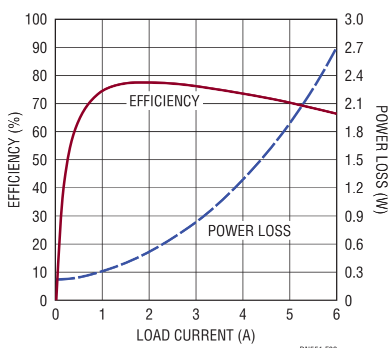


Figure 3. LTM4632 Efficiency and Power Loss. 12V Input. (Figure 2 Design)

Tight Regulation with Fast Transient Response

The LTM4632's unique controlled on-time current mode architecture and internal loop compensation allow for a fast transient with good loop stability

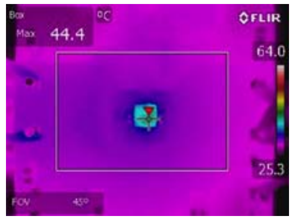


Figure 4. LTM4632 Thermal Performance. 12V Input, 3A. (Figure 2 Design)

over a wide range of operating conditions and output capacitance. Voltage regulation for its switching regulator outputs is precise, with guaranteed low ±1.5% maximum total DC output voltage error over line, load and temperature.

Figures 5 and 6 show the fast transient performance and tight load regulation of the LTM4632 VTT rail of the Figure 2 circuit.

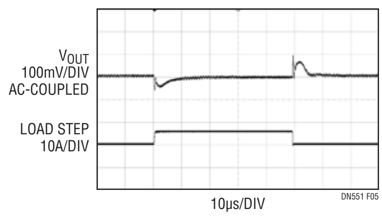


Figure 5. VTT Load Step, –3A to 3A (Figure 2 Design)

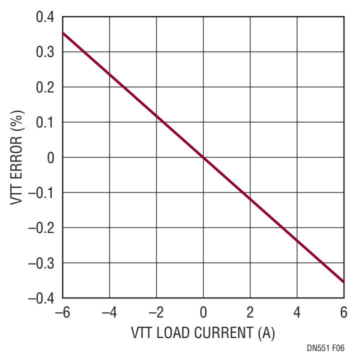


Figure 6. VTT Load Regulation (Figure 2 Design)

Conclusion

The ultrathin LTM4632 provides a complete high performance regulator solution for all three rails required in DDR/QDR RAM applications. Its wide operating range, features and compact solution size make it highly flexible and robust, and capable of fitting into the tightest spaces on the topside and backside of a PCB.

Data Sheet Download

www.linear.com/LTM4632

For applications help,
call (408) 432-1900, Ext. 2463

Linear Technology Corporation
1630 McCarthy Blvd., Milpitas, CA 95035-7417
(408) 432-1900 • FAX: (408) 434-0507 • www.linear.com

dn551f LT/AP 0616 111K • PRINTED IN THE USA

differential-power-analysis (DPA) attacks can extract keys and other vital device information. System boot-up needs to be kept secure, not just from remote network-based attacks, but also where the adversary has physical access.

Data security: This element ensures that communications into and out of the system are authentic and secure, and sensitive data stored in the system cannot easily be extracted.

Embedded-system program managers and development teams must design these types of protections into their products while best leveraging the characteristics of the underlying platform. The result should be a robust protection network with no single point of failure. Key methods for achieving this include:

Risk assessment: Perform a detailed system security evaluation early in the architecture design phase, to assess critical system data/functions, discover vulnerabilities, enumerate threats, and outline the likelihood and consequence of system compromise.

Protection planning: Using risk assessments and any other compiled data, developers should seek to understand protection implementation costs and design options for mitigating identified system vulnerabilities and ensuring successful system verification and validation.

Attack scenario testing: This can include a black-box approach, pitting experienced reverse engineers with state-of-the-art attack tools against a system in a deployed setting to reveal vulnerabilities that cannot otherwise be found during most other evaluation exercises.

Side-channel analysis and mitigation: Side-channel attacks like DPA are currently the most practical method for compromising cryptography implementations. It is important to perform measurable, objective, and repeatable testing for resistance to side-channel attacks for applications where adversaries have the ability to observe side channels (i.e., power draw, timing, electromagnetic emanations) during on-device cryptographic operations.

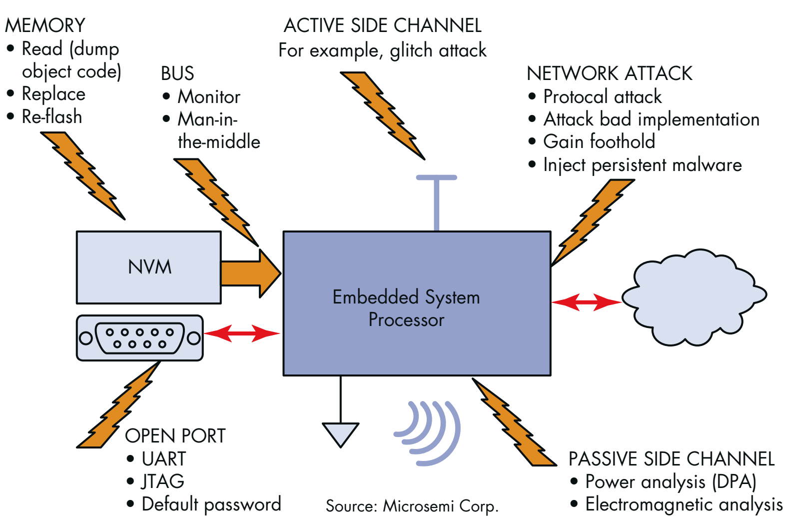
TYPICAL THREATS TO EMBEDDED SYSTEMS

The following are common attacks on embedded systems that should be considered during the architecture and design implementation engineering phases (*Fig. 1*).

Network attacks: Though fielded systems are subject to new threats, all of the existing battery of network attacks still apply, too. Ideally, all network communication is authenticated and encrypted using well-established protocols such as TLS. A public key infrastructure (PKI) can be used by both remote endpoint devices (clients) and servers to ensure that only communications from properly enrolled systems are accepted by the parties to the communication. A strong hardware root of trust can provide this secure "identity" for the system, providing unique-per-device keys linked to the hardware and certified in the user's PKI.

Active side-channel attacks: The most common active attack is to use voltage glitches on the power supply of the processor to cause an "interesting" malfunction at a critical juncture in the execution of the embedded program. For example, the infamous attack on the Sony Playstation, which started a chain of events that allegedly cost Sony $1 billion before it all played out, started as a glitch attack. It allowed the hacker to enter a privileged processor state where he could then dump all of the code, whereupon a cryptographic implementation flaw was found. Game over!

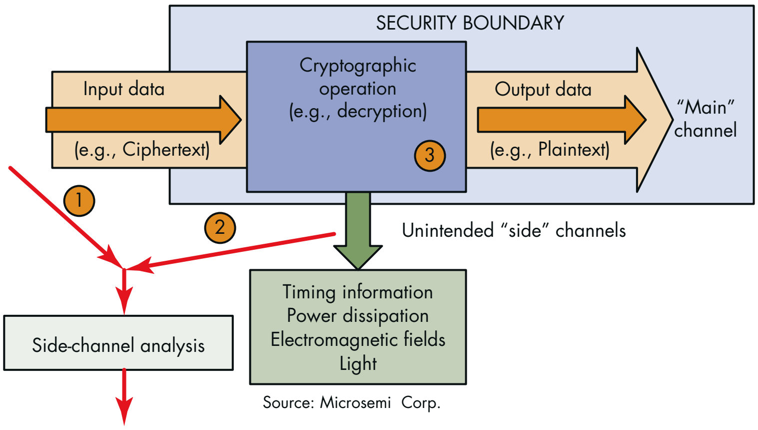
Memory and bus attacks: If the hardware is physically available and insufficiently protected, it may be possible just to read the contents of memory directly from an external programmable read-only memory (PROM) or external RAM memory chip, or by probing the connecting bus. It is generally good practice, and not that difficult, to encrypt and authenticate all static data, such as firmware stored in PROMs. Lack of memory encryption in a smart electric meter design was reportedly a critical factor that led to an estimated $400 million annual loss by a power company.



1. Examples of some of the most common attacks on embedded systems.

Another example is the so-called Cold Boot Attack, where the memory (a bank of SDRAM chips, for example), is chilled, quickly removed, and read on another system controlled by the attacker. The cold chips hold remnants of the data even during the short interval where they are unpowered. Thus, it is best not to store critical secrets such as cryptographic keys in off-chip memory. In cases where higher levels of security are justified, external volatile memory can be encrypted.

Some memory attacks can be performed remotely, such as with the Heartbleed bug introduced in a 2011 OpenSSL update that at its peak allowed remote reading of RAM working memory in an estimated half million secure web servers worldwide. The Heart-



2. Side-channel analysis such as DPA or DEMA is used to extract secret keys from an unprotected processor or FPGA.

bleed bug was discovered and announced publicly by Google and independently by Codenomicon in April 2014. Technologies such as whitebox cryptography can be brought to bear on this type of memory attack.

Reflashing, or changing the contents of memory, either remotely or with physical access can, in what is called a "persistent" attack, bypass any software-based security. Since the malware is installed in non-volatile boot-up memory, even resetting the system does not clear away the malware.

It is important to boot the embedded processor securely by verifying the authenticity of all code in rewritable memory, or code loaded from off-chip, including the very first such word executed. Therefore, any changes to the memory are detected and an appropriate action is subsequently taken. An independent hardware-based root of trust can be used to build a secure boot solution.

Open ports: There really aren't many good excuses for leaving open ports on your system, yet these attacks remain one of the most common successful embedded-system attacks. An open port may consist of, for example, a UART connection left available for easily hooking up a terminal monitor. Unfortunately, this is equally convenient for the hacker. Most software password-protection schemes used to prevent logging in via the terminal are just a speed bump to a good hacker.

Another common mistake is to use a single factory password to protect privileged access to the system or a device in it. These have a way of turning up in hacker internet blogs, giving worldwide access to your entire product line free for the asking. A related problem is where users don't change the default password when they configure the system for themselves.

A secure FPGA can protect debug and other factory test ports from hackers at the hardware level while still providing access to authorized personnel. The access keys can be secured against extraction by the FPGA, providing much better protection than is possible with software alone.

Passive side-channel attack: Simple power analysis (SPA) and DPA, and their EM equivalents (SEMA and DEMA) can extract secret keys used in a processor or FPGA, if suitable countermeasures are not implemented (*Fig. 2*).

In a "differential" side-channel analysis, the adversary monitors available inputs or outputs of the system (e.g., encrypted communications), and at the same time also monitors the selected side channel, such as the instantaneous power consumption or electromagnetic (EM) emissions, while the key is being used. Then, with the application of some straightforward statistical post-processing, it learns the secret value of the key that was used during the calculations. In a "simple" analysis, step one (monitoring the ciphertext) is not even required as the key can be extracted from just the side-channel information with little or no statistical post-processing required.

SPA and DPA countermeasures are typically found in smart-card ICs with very large minimum-purchase quantities, but not in a standard 32-bit flash-based microcontroller. FPGAs are available with licensed DPA countermeasures that have been certified as effective by an independent third-party laboratory, and include a DPA patent license that allows the user to implement DPA-resistant cryptography running on them without requiring any additional legal work or royalty payments.

FIGHTING BACK

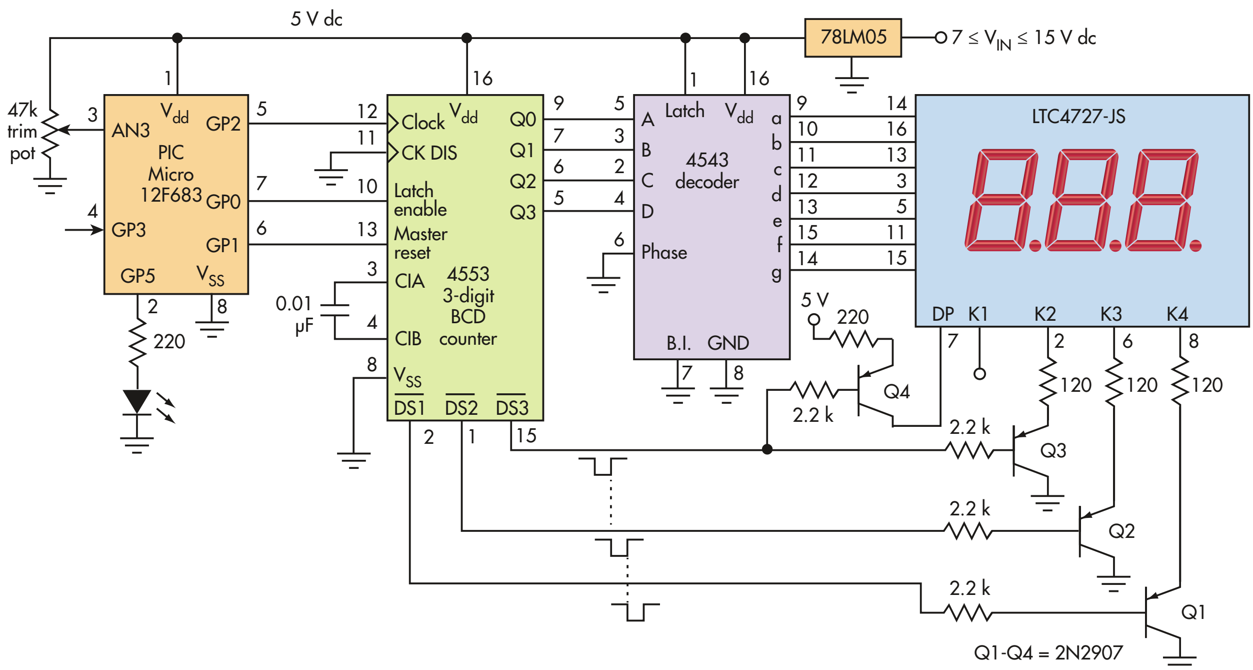
Secrets are essential to securing the IoT. In this and other hyperconnected system environments, it takes more to keep up with the bad guys than a fixed factory password and software patches. It is not enough to simply include a crypto accelerator—it must include DPA countermeasures. External assessments as part of a risk-based, multi-layered strategy built from the ground up are essential.

The latest SoC FPGAs embed microcontrollers and security features such as true hardware-based random-number generators and secure key storage so the SoC FPGA can be used to provide a hardware root of trust to an external processor, ensuring it boots securely from the first word of code loaded from off-chip memory. The secret keys and public key certificates pre-installed in the FPGAs and SoC FPGAs from some manufacturers can provide the basis for a strong identification of a networked IoT endpoint, ensuring that no communications can be spoofed. This provides the foundation for a layered technology approach, ensuring the highest protection against cyber threats. ed

RICHARD NEWELL serves as senior principal product architect at Microsemi and plays a key role in planning the security features for the current and future generations of flash-based FPGAs and SoC FPGAs.

Versatile Voltage-to-Pulse Train Converter Supports Sensor Data I/O

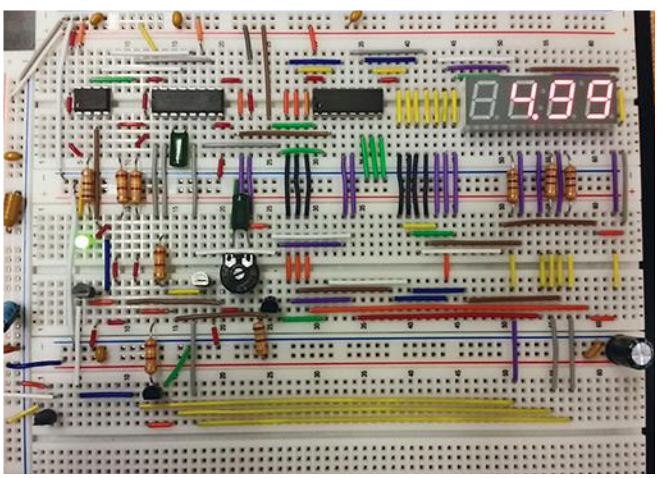
RICARDO JIMÉNEZ, and JUAN C. ÁNGELES | Imperial Valley College



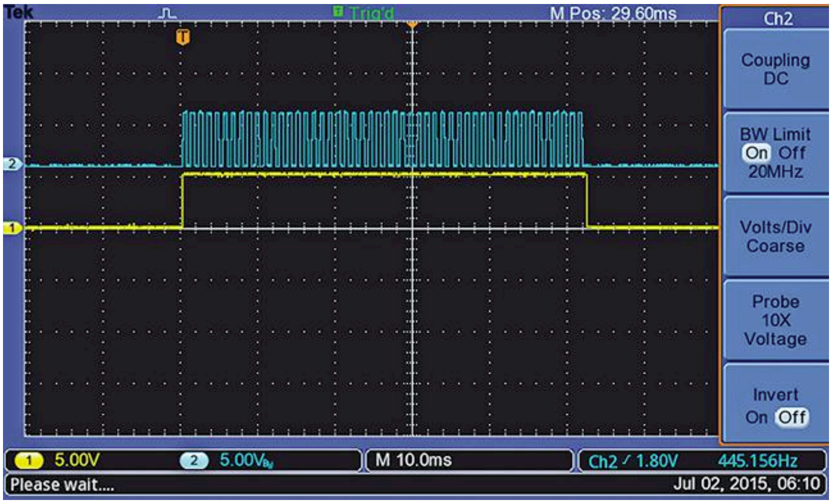
1. In the voltage-to-pulse train-converter design, the train on GP2 is proportional to the sensed voltage on AN3; a counter detects the pulse train, which is then decoded and multiplexed to a common-cathode LED display.

WHEN THE NEED ARISES to convert voltage readings from an analog sensor into a pulse train, a low-end microcontroller offers a versatile solution. The design in *Fig. 1* uses an 8-pin PIC 12F683 to provide a pulse train that's proportional to the sensed input voltage. This is useful, for example, when transforming a sensor signal into a format that's compatible with a basic digital or GPIO input. The output operating range spans between 0 to 500 pulses for an input voltage of 0 to 5.00 V dc.

An input voltage (V_{IN}) of 1.25 V dc, for example, will generate a pulse train

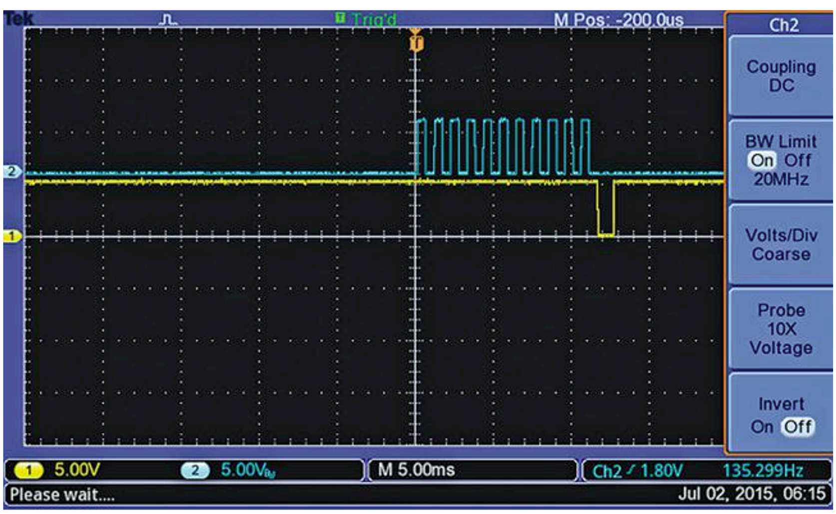


2. Due to absence of layout-critical wiring or RF issues, the circuit was assembled and tested on a standard prototyping board.



3. The timing diagram shows a pulse train being generated; the yellow pulse stays high during the pulse train transmission.

4. The Latch and Reset pulses generated by the microcontroller at the end of a pulse train are used to store a reading and clear the counter, respectively.



5. For a reading of 0.11 V dc, the MCU generates 11 pulses, which are then followed by a Latch pulse to store the reading.

(Pt) of 125, which is defined by the equation:

$$Pt = V_{IN} \times 100$$

where V_{IN} is in volts, decimals, and hundredths. In this design, each pulse has a period of 1 ms with a 50% duty cycle. The refresh time (Rt) is given by:

$$Rt = V_{IN} \text{ x } 1 \text{ ms} + 50 \text{ ms delay}$$

The longest refresh time of 0.499 seconds (plus 50-ms delay) occurs for a 4.99-V reading, while the shortest one of 51 ms corresponds to an input voltage of 0.01 V. The 50-ms delay added to all readings is needed to avoid a flickering display.

In the circuit, an analog input voltage delivered by a 47-kΩ trimming potentiometer is applied to the microcontroller's analog Input (AN3). The internal analog-to-digital converter (ADC) is configured to 8 bits, providing a precision of ±19.60 mV, with a resolution of 100 mV.

To test the MCU program, the circuit includes a 3-digit BCD counter using an MC14553 (www.onsemi.com) to count the pulse train. The train is latched in the counter and decoded with a CD4543 to drive a four-digit multiplexed LED Display (Lite-On Inc. LTC-4727JR) via three switching transistors. *Figure 2* shows the actual circuit assembled in a prototyping board.

To generate a pulse train on GP2 proportional to the input voltage, the algorithm takes a voltage reading and makes a conversion to decimal with the LSB constant equal to 19.60. It then gets its equivalent in digital format for the units, decimals, and hundredths, using the instructions DIG3, DIG2, and DIG1, respectively. The DIG1 value is stored in variable "units" to create a loop that generates that number of pulses. Similarly, the DIG2 value is multiplied by 10 and stored in a variable called "decimals" to generate the tens of pulses. Finally, the DIG3 value is stored in the variable called "units," which is multiplied by 100 to generate the hundreds of pulses required for the reading.

In this way, for example, a voltage reading of 2.54 V will be composed of 4, then 50, and then 200 pulses, to get a total of 254 pulses with a period of 1 ms. Therefore, it takes approximately 254 ms to transmit this pulse train. If one of the digits is equal to zero, the program skips that loop. *Figure 3* shows a pulse train with its corresponding output generated by GP5.

Once the pulse train is finished, a 1-ms latch (active low) pulse on GP0 is transmitted to store that reading in the MC14553's internal latches. Then a second (active high) 1-ms pulse on GP1 is generated to clear the counter to all zeroes (*Fig. 4*). The latch in the CD4543 decoder is set to transparent mode. Output GP5 is used to indicate when the MCU is transmitting the pulse train.

Three PNP transistors 2N2907 (Q1 to Q3), which continuously scan the data to the LED display, are controlled by the MC14553 counter. Transistor Q4 activates the decimal point, providing a 5-V pulse only when /DS1 is pulsed low. *Figure 5* shows the 11 pulses generated for a voltage reading of 0.11 V dc, and the latch pulse generated at the end of the pulse train.

For higher-precision applications (such as 4.88 mV per LSB), you can configure the ADC to 10 bits. In this case, the output-signal period might be reduced to 0.5 ms to avoid having longer delays when the input voltage is at maximum. In such a case, a 1.000-V dc reading would generate 1000 pulses. For battery-operated applications, a numerical liquid-crystal display is recommended, which requires using three CD4543 decoders.

RICARDO JIMÉNEZ is an adjunct professor in Electronics at Imperial Valley College, Imperial, Calif. He can be reached at ricardo.jimenez@imperial.edu .

JUAN C. ÁNGELES is pursuing his associate degree in math and science at Imperial Valley College.

LabVIEW Files Implement Simple Chess Simulation

GUDA VAMSI KRISHNA | SASTRA UNIVERSITY, Thanjavur, Tamilnadu, India

THIS DESIGN DESCRIBES a novel implementation of a brainstorming game in LabVIEW virtual instrument (VI) files. The innovative approach can trigger ideas for designers in the field of robotics, since the graphical menu-driven program has been instrumental in tracing the composition of various elements. The program is a simple implementation of the game "chess," and can be played with two (human) players in the LabVIEW background.

The program has nine VIs, of which eight are sub-VIs used in "VI chess" (posted online as LabVIEW LLB files). The VIs are simply split up the way we play the game in real life. They provide the following basic functions, as each one's name indicates:

- possible_moves.vi and moves.vi can do possible moves of each piece
- type_of_place.vi can change the color of the box
- type_of_piece.vi can change of color of the selected piece
- initial_board.vi can initialize the positions of the pieces and the squares
- move_from_to.vi can move the piece from one position to the other position
- which_piece.vi can decide which piece to move next
- enable_square.vi can enable the square
- clicked.vi can check what happens when clicking a piece
- Chess vi is the virtual instrument program for entire game of chess

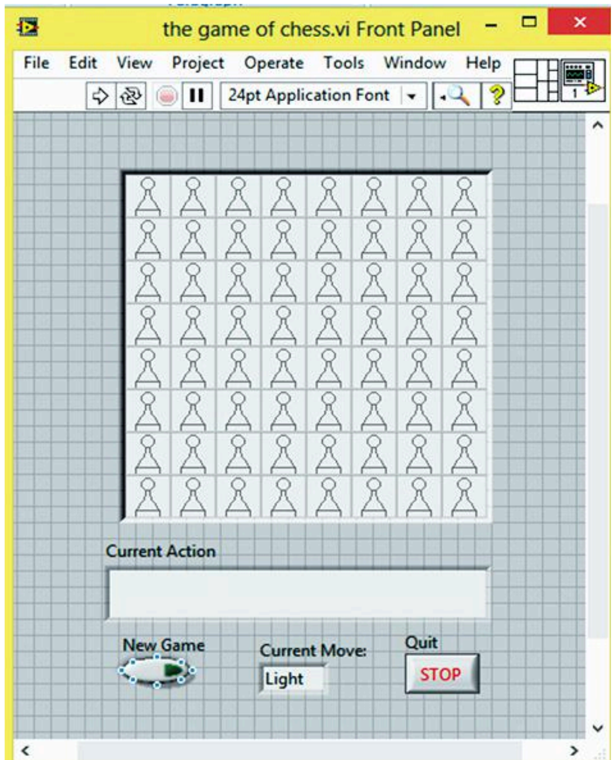
These VIs are combined in a single VI called the game of chess. This basic 8 × 8 matrix initializes these VIs, with a front panel shown in *Fig. 1*. In some cases, two VIs perform the same action to counter-check whether the action is properly simulated or not. The initial_board.vi resets the position of the board, the type of place, and piece, to ensure that only a specified square and pieces are placed on the board according to the existing conditions. Moves.vi defines each piece's move, and other possible moves, and takes care of the moves of a particular piece at a particular instant in the game. Move_from_to.vi gives the recent move made by the player at the particular instant.

Figure 2 shows the functional blocks and palette diagram. The game starts by pressing the button 'New Game' and the coins are set in the appropriate positions using the sub VI (initial_board.vi). The “Current Move” text field shows whose turn it is to move, and the “Current Action” text field shows the movement action (example: queen from e6 to e1).

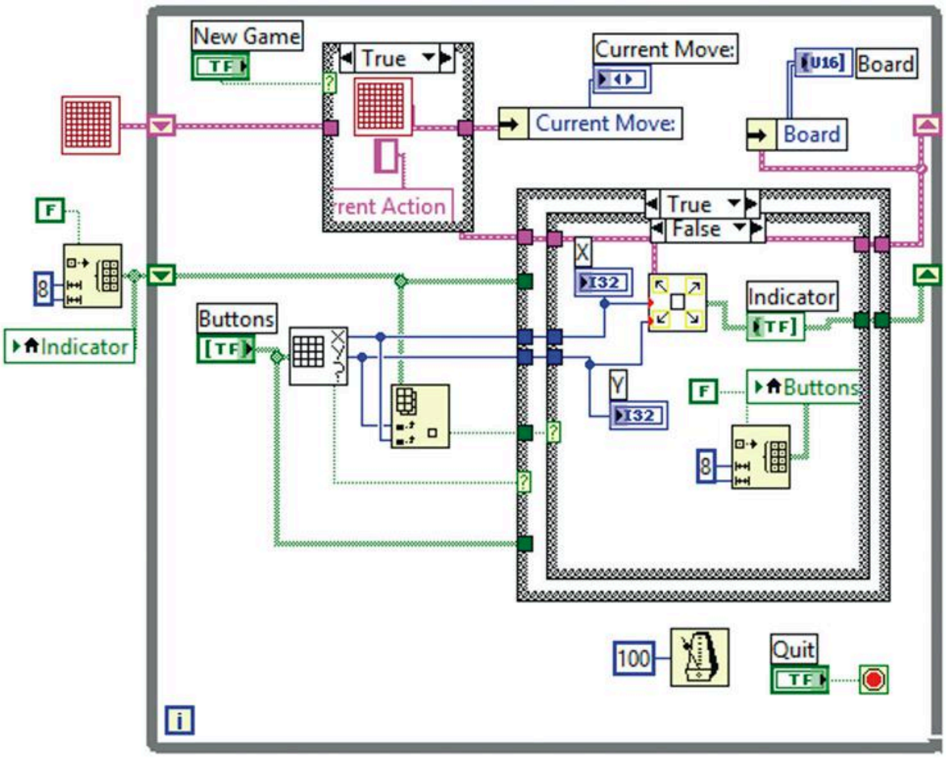
The board is designed using the array initialization, and the coins are placed in their default position. When the coin is moved, sub VI highlights only those positions that are valid for the coin to be moved; it doesn’t accept invalid positions. Once the move is made, the “current move” text field changes and shows which player has to move. Each sub VI decides the color of the coin and the square, and possible steps of the coin from each of its locations.

The quadrants are set after the initialization of the matrix. Each time the information from a coin is taken or moved, the previous and the present quadrant values are taken, as seen in the function palette diagram. Variables X and Y are the present coordinates of the coin on the board; then the future coordinates (the places it can move) are decided.

If the square already has a coin in it, it will be replaced by the new coin. The same concept is used for killing or removing any coins. A player can move any coin even if the king is in check, while the screen shows the king is in check in the text field. Even though this program is simulating a game, it can trigger creative and intelligent thinking in humans, and



1. The front-panel diagram of the LabVIEW Chess Game virtual-instrument program shows the basic 8 × 8 matrix in which these VIs are initialized.

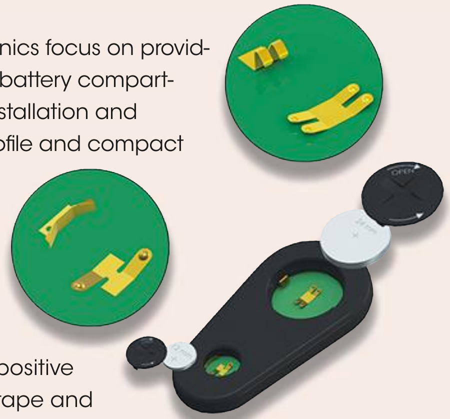


2. A function-palette diagram of the program shows the relationship between blocks and their interactions.

can promote the development of additional user-friendly and widely acceptable simulations for many applications, including robotics.

GUDA VAMSI KRISHNA is a third-year student in the Department of Electronics and Communications Engineering, SASTRA University, Thanjavur, Tamilnadu, India. His research interests are in the areas of embedded design, virtual instrumentation programs, and analog designs. He can be reached at vkvamsi355@gmail.com.

SMT Coin-Cell Contacts Provide Design Versatility

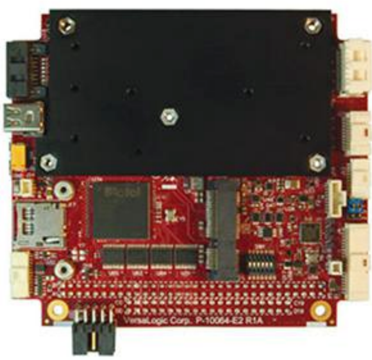


THE LATEST SMT ENCLOSURE COIN-CELL CONTACTS from Keystone Electronics focus on providing design versatility for more dependable connections in self-contained battery compartments. Requiring minimal board space, the new contacts boast simple installation and removal of a coin-cell battery within a battery enclosure. Their ultra-low profile and compact design is suited for small hand-held controls, key fobs, personal medical devices, digital timers, and other industrial and consumer applications. Manufactured from gold-plated stainless steel, the contacts offer low contact resistance. The spring tension adjusts to all cell height variations for dependable connectivity of coin cells with diameters from 12 mm and larger with heights from 1.2 to 7.7 mm.

Positive and negative battery contacts are available in the series. For positive contact use with 12 to 23 mm coin cells select Catalog #120 (120TR on tape and reel), for 16 to 30 mm coin cells select catalog #110 (110TR), or for 20 to 24 mm coin cells choose catalog #122 (122TR). The matching negative contacts are also available: for 12 to 16 mm coin cells select catalog #118 (118TR on tape and reel), and for 16 to 30 mm coin cells select catalog #112 (112TR).

KEYSTONE ELECTRONICS

www.keyelco.com



PC/104-Plus SBC Integrates Bay Trail Processor

VERSALOGIC IS NOW SHIPPING BayCat, a rugged PC/104-Plus SBC based on Intel's Bay Trail processor. BayCat combines high performance, low power consumption, enhanced security and small size, and is available in three performance levels: single-, dual-, and quad-core models. An on-board TPM security chip can be used to lock out unauthorized hardware and software access, and on-board hardware acceleration is available for encode/decode of H.264, MVC, VP8, VC1/WMV9 and other standards.

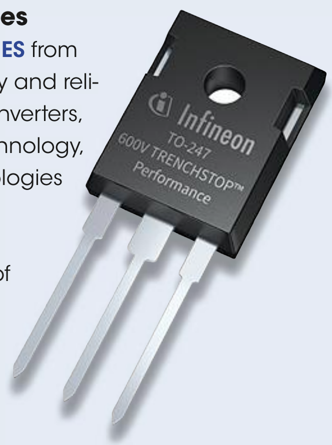
The fanless SBC's I/O connectivity includes dual GbE ports, one USB 3.0 port, four USB 2.0 ports, two serial ports (RS-232/422/485), I2C interface, 24 digital I/O lines, SATA 3 Gb/s interface, mini PCIe socket with mSATA capability, and a microSD socket. A Gen 7 HD graphics engine is capable of supporting up to two 1080p video streams.

All three BayCat models are designed and tested for industrial temperature operation. They are equipped with latching connectors and meet MIL-STD-202G specifications to withstand high impact and vibration. The BayCat SBC (part number VL-EPM-31) is in stock with prices starting at $694 each/OEM quantities.

VERSALOGIC

www.versalogic.com

IGBT Enhances Efficiency for Home Appliances



A NEW 600 V TRENCHSTOP PERFORMANCE IGBT SERIES from Infineon Technologies provides high energy efficiency and reliability for applications like air conditioning, solar PV inverters, drives, and UPS. Based on Infineon's TRENCHSTOP technology, the discrete IGBT is optimized for hard-switching topologies working at frequencies of up to 30 kHz.

As a plug-and-play replacement to the predecessor TRENCHSTOP IGBT, the new IGBT yields reduced losses of 7% at a switching frequency of 8 kHz. An unmatched 11% lower total loss is delivered for a switching frequency of 15 kHz. The performance IGBT contributes to more energy efficient power consumption, lower diode recovery losses, higher reliability and longer operational lifetime of the application. Other features include low speed dV/dt switching (<5V/ns), 5us SC rating, and low EMI. The 600 V TRENCHSTOP Performance IGBT is available now.

INFINEON TECHNOLOGIES

www.infineon.com

Portable Scopes Deliver Functionality of Six Instruments

PICO TECHNOLOGY'S NEW PICOSCOPE 2000A and 2000B Series two-channel, four-channel, and mixed-signal models have the functionality of an oscilloscope plus a logic analyzer (on MSO models), spectrum analyzer, function generator, arbitrary waveform generator, and serial bus analyzer with support for 15 protocols included as standard. They are USB-powered and come in an ultra-portable package that can be transported in a laptop bag.

PicoScope 2000A 2- and 4-channel models are designed for technicians, trainers, students, and hobbyists doing fault-finding on signals up to 25 MHz. The PicoScope 2205A MSO has two analog-plus 16 digital channels for viewing and making measurements on digital or mixed technology designs.

PicoScope 2000B Series models are equipped with deep buffer memory from 32 M to 128 M samples with bandwidths of 50, 70, or 100 MHz supported at sampling speeds to 1 GS/s, and hardware acceleration to deliver over 80,000 waveforms per second update rates. Like A models, they are available in 2- and 4-channels, plus 2+16 channel MSO versions.

Powered via USB interface, 2000 Series models connect to host PC or tablet and are controlled with PicoScope 6 software. The PicoScope 2000A and 2000B Series models are available now with prices ranging from $129 to $1,235.

PICO TECHNOLOGY

www.picotech.com

ATRs and Specialty Enclosures Are Conduction-Cooled

PIXUS TECHNOLOGIES' NEW CONDUCTION-COOLED CHASSIS are available in the ATR format or in specialty SFF designs. Specialty enclosure formats are available for both OpenVPX and MicroTCA architectures. The conduction-cooled ATRs come in standard 1/2 and 3/4 sizes for 3U or 6U boards. There are also options for the MicroTCA.3 hardened form factor as well as heat-exchanged versions. The enclosures are designed to meet MIL-STD-704, MIL-STD-810G, and MIL-STD-461. Off-the-shelf power interface boards are available to incorporate VITA 62 or PICMG 2.9 power supplies.

For specialty designs, Pixus also offers application-specific conduction-cooled solutions. The company provides rugged 19-in. rack-mount enclosures in multiple backplane architectures including OpenVPX, MicroTCA, AdvancedTCA, and legacy CompactPCI/VME.

PIXUS TECHNOLOGIES

http://pixustechnologies.com

32 GB ULP DDR4 Modules Feature PC4-2400 Interface

VIRTIUM'S NEW MEMORY MODULES provide 32 GB densities in the smallest ultra-low profile RDIMM and Mini-RDIMM form-factors. Featuring the PC4-2400 interface, these new memory modules dramatically enhance embedded systems through their high capacity and performance. Target applications for the ULP RDIMM and Mini-RDIMM modules include ATCA height-restricted blade servers, 1U rack designs, SBCs, mezzanine cards and designs with space constraints. The ULP memory modules are sized at 17.78 mm, compared to standard low-profile modules' 18.75 mm size.

The RDIMM and Mini-RDIMM memory modules deliver high performance PC4-2400 solutions, the longest product availability, and as with all Virtrium DDR products, the new high-capacity RDIMM and Mini-RDIMM solutions boast significant power savings, in addition to bandwidth twice that of DDR3. Industrial temperature rated at -40°C to + 85°C, the memory modules also offer optional conformal coating, and extreme-temperature, accelerated-burn-in for zero-downtime applications. The high-capacity ULP DDR4 modules are expected to be available in early May 2016.

VIRTIUM

www.virtium.com

Power-Entry Module Designed for Protection Class II

THE KMF POWER-ENTRY MODULE from Schurter, designed for use in protection class II double-insulated applications, provides high functionality in a compact package, just like the module for use in protection class I. The new version is designed for medical equipment used at home.

The module provides double insulation between energized components and exposed parts. This reinforced insulation is tested with a voltage of 4,000 Vdc between the energized conductor and the neutral conductor relative to the mounting panel. The class II version without ground pin is according to IEC 60320-1, style C18. The KMF line switch is available with a 2-pole line switch and a 1- or 2-pole fuse holder. For medical applications, an extra-safe fuse holder is available that can only be opened with the aid of a tool. The EMC filter is obtainable in medical and low leakage, M5 versions. Current ratings range from 1-10 A at 250 Vac.

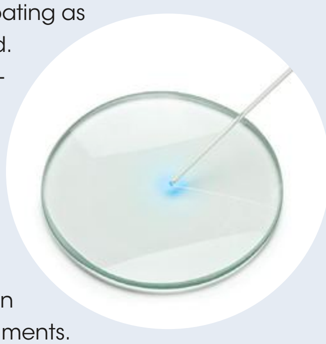
The KMF class I and class II are ENEC, cURus and CCC approved. They are suited for use in equipment according to IEC 60950 and IEC 60601-1. The class II version is particularly suited for use in home medical equipment according to IEC 60601-1-11.

SCHURTER

www.schurter.com

UV-Cured Epoxy Bonds with Metals/Glass/Plastics

UV-8504E CATIONIC EPOXY from EpoxySet is formulated for bonding, sealing and coating metals, glass and most plastics including ultem, ABS and polycarbonates. Boasting strong bonds, the clear system can be used as a water protective coating as well as a structural bond.



With an elastic modulus of about 300,000 psi and a glass transition temperature of 125°C, the UV-cured epoxy is suited for temperature cycling applications from -55°C to 200°C even in high humidity environments. The epoxy also demonstrates a 1.57 cured refractive index that makes the clear system useful in a number of optical applications. The UV-8504E cationic epoxy's low viscosity boasts easy application and a tack free cure that is capable of being accomplished in 15 seconds.

EPOXYSET

www.epoxysetinc.com

Rugged Mobile Edge IoT Gateway Runs Multiple Apps

TRAX-2 IS OCTAGON SYSTEMS' rugged mobile edge gateway for the IoT. An application-ready design provides the ability to run multiple applications on one platform, and its low profile facilitates ease of installation in a variety of vehicles. The in-vehicle computer is designed for integrating software applications and wireless technologies including safety, fleet management, communication, asset management, maintenance, and dispatching. Potential markets for the new platform include: small mines and quarries, freight hauling, emergency vehicles, construction, harsh industrial environment, and fleet management.

Key features of the TRAX-2 mobile edge gateway include: a 1.33 GHz Intel E3825 dual-core 64-bit processor; 4 GB DDR3L-1066 MHz of memory; DirectX 11, OpenGL 3.0, OpenCL 1.2, and up to 1920 x 1200 (WUXGA) resolution; an open architecture with Windows 7, 10, and Linux compatibility; removable storage up to 256 GB; Dual CAN Bus, GbE, serial, digital, USB, audio I/O and video; and an optional 10-in. sunlight-readable display with integrated touchscreen.

OCTAGON SYSTEMS

www.octagonsystems.com

For more information on products or services visit our website www.electronicdesign.com, menu item Reader Service. The advertisers index is prepared as an extra service. *Electronic Design* does not assume any liability for omissions or errors.

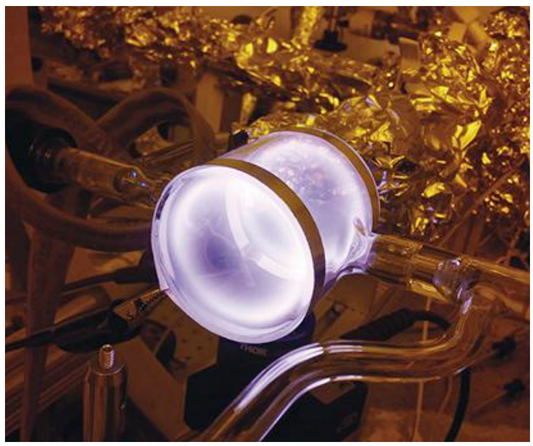
BILL WONG | Embedded/Systems/Software Editor
bill.wong@penton.com

For Ghostbusting Technicalities, WHO YA GONNA CALL?

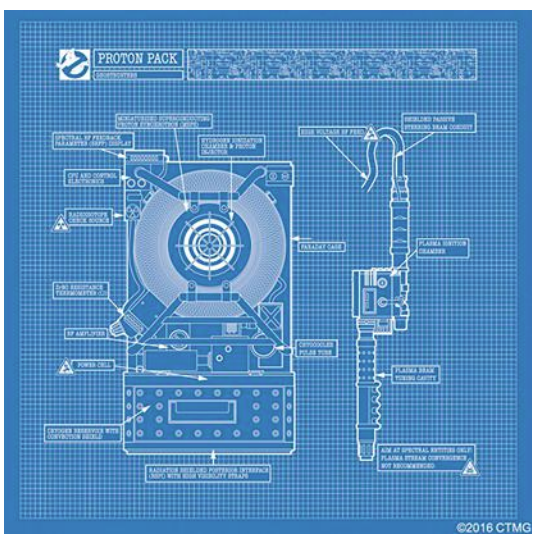
The makers of the new *Ghostbusters* movie turned to an MIT post-doc to help create an up-to-date proton pack for the big-budget reboot.

The new *Ghostbusters* movie has a lot of changes, including some new hardware designed by senior postdoctoral associate Dr. James Maxwell at MIT's Laboratory of Nuclear Science. It seems that polarizing helium 3 gas using magnetic field gradients has a little in common with possible ghostbusting technology. His MIT lab (*Fig. 1*) caught the eye of director Paul Feig, who tasked Maxwell to create a new, up-to-date proton pack (*Fig. 2*) for the female ghostbusting crew. Feig wanted a real particle physicist to help design the props to be used in the film. It is not the first time a movie has been updated with an eye toward realism (see *"RoboCop Returns With An Eye On Realism"* on electronicdesign.com).

The new ghostbuster backpack uses a synchrotron instead of a cyclotron. Both are particle accelerators used in particle physic experiments. The difference is that a cyclotron uses a constant magnetic field and electric field frequency in a cylindrical or spherical chamber with a particle that spirals outward from the center, gaining speed, whereas a synchrotron uses a torus-shared tube and varies both fields to accelerate the particles. Normally a synchrotron is used in large installations like the large hadron collider (LHC) at CERN.



1. Dr. Maxwell's lab experiments included polarizing helium 3 gas using magnetic field gradients.



2. The new Ghostbuster's backpack uses a synchrotron instead of a cyclotron.

Super-conducting magnets are used in the unit to keep the size down, so it needed cyrocooler and helium to keep the magnets cold. It would take some technical leaps to really build one, but that is what movie magic is for.

Dr. Maxwell started the design by writing a mock abstract for the proton pack that included jargon of his own creation. This went through various design iterations before the final one was created for the ghostbusting crew. Dr. Maxwell was also involved with the design of some of the other movie props.

Isolating weird phenomenon, be it conventional particles or spectral particles, requires taking a different view of the problem. In real life, high-energy beams are used to explore particle interactions. Scattering experiments can generate secondary particles that can be tracked and analyzed.

You will have to check out the movie to see the new, all-female team, but keep an eye out for the hardware now that you know its design heritage. *Ghostbusters* opens nationwide on July 15. ed

WE'RE THE MANUFACTURER YOUR COMPETITION WANTS KEPT SECRET.

Companies large and small leverage our rapid manufacturing services when speed-to-market is critical and on-demand parts are needed beyond launch. We've been told it's their supply chain secret weapon. But you didn't hear it from us.

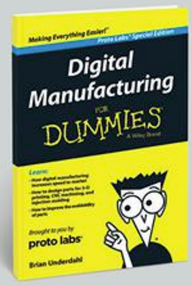
CUSTOM PROTOTYPES AND LOW-VOLUME PRODUCTION FOR THOSE WHO NEED PARTS TOMORROW.

proto labs®

Real Parts. Really Fast.™

3D PRINTING | CNC MACHINING | INJECTION MOLDING

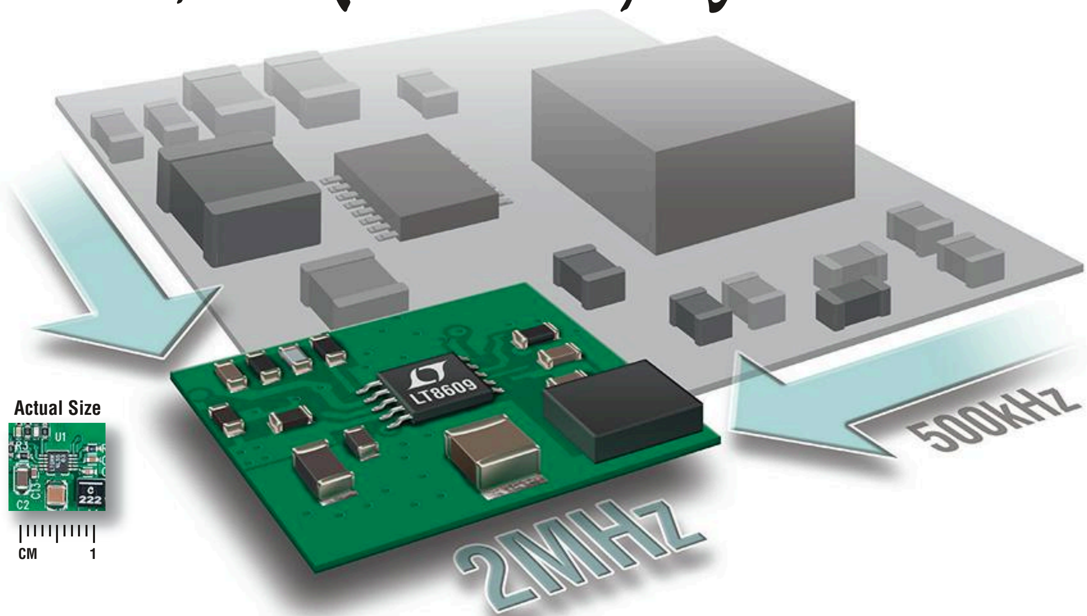
ISO 9001: 2008 Certified | ITAR Registered | 2016 Proto Labs, Inc.



FREE BOOK

Request your Digital Manufacturing for Dummies book at **go.protolabs.com/ED6DJ.**

93% Efficient at 2MHz
42V, 2A (3A Peak) Sync Buck



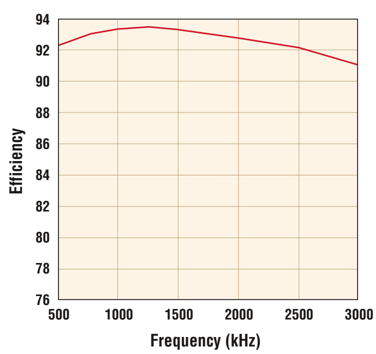
Faster, Smaller, Quieter

The LT®8609 combines high efficiency and high switching frequencies to deliver a very compact synchronous step-down 2A (3A peak) solution. It offers 93% efficiency switching at 2MHz stepping $12V_{IN}$ down to $5V_{OUT}$, offering a very small solution footprint while keeping switching noise out of critical frequency bands. Spread spectrum frequency modulation reduces EMI concerns. The LT8609 delivers 2A of continuous output current and can deliver 3A peak load for up to 1 second offering a tiny solution for applications ranging from automotive power systems to GSM modems. Its Burst Mode® operation only requires 2.5µA of quiescent current extending battery life.

Features

- Wide Input Voltage Range: 3.0V to 42V
- Ultralow Quiescent Current <2.5µA
- High Efficiency 2MHz Synchronous Operation 93%
- 2A Maximum Continuous Output, 3A Peak Transient Output
- Spread Spectrum Frequency Modulation for Low EMI
- Fast Minimum Switch-On Time: 45ns
- Adjustable and Synchronizable: 200kHz to 2.2MHz
- Thermally Enhanced MSOP-10 Package

$12V_{IN}$ to $5V_{OUT}$ @ 1A I_{OUT}
Efficiency vs Switching Frequency



Info & Free Samples

www.linear.com/product/LT8609

1-800-4-LINEAR

LINEAR TECHNOLOGY