MARCH 2015
VOLUME 13
#2
EMBEDDED-COMPUTING.COM

Embedded COMPUTING DESIGN

Connecting Silicon, Software, and Strategies for Intelligent Systems

SMART ENERGY
PG. 28

BUILDING A SMARTER "SMART HOME" ON ZIGBEE 3.0

PG. 23

PLUS

SOFTWARE

SOFTWARE-DEFINED NETWORKING – A Q&A WITH CISCO

PG. 20

IOT INSIDER

ENERGY HARVESTING IN WEARABLES

PG. 7

Annapolis Micro Systems

The FPGA Systems Performance Leader

WILDSTAR OpenVPX Ecosystem

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

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

1 to 40 Gbit Ethernet
SDR to FDR Infiniband

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

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

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

Chassis
4, 6 or 12 Slot
Up to 14G

Annapolis Micro Systems

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

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

Smart energy: Distributed localised electricity grids

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

You would be forgiven for imagining the national electricity grid as just that, one single nationwide lattice – as historically, that's not too far from the truth. Back in less connected, in fact often unconnected times, electricity was first provided to settlements by adding an extra branch on that sole, nationwide tree.

As this tree grew ever larger, quickly reaching colossal proportions, it became apparent that perhaps this single behemoth would never be the ideal solution. The rapid population expanse, the vastness of the area covered and the increased density of power requirements have all exerted pressure on what is now an aging infrastructure.

Beyond population density, the demand of those individuals and companies has also exponentially soared. Past decades have observed the rapid increase in electrically powered devices per capita combined with the electrification of historically combustible-fuelled transport and heating services – both massive consumers of energy themselves.

This decade has seen the definition and whirlwind proliferation of smart devices, particularly the well-publicised IoT revolution, in itself expected to see an expansion from 1.9 billion connected devices today to more than 9 billion as soon as 2018.

All of this needs power, with particular emphasis on reliability of that power, as we trust more and more of our lives to the 24/7 operation of these devices. The evidence-backed verdict is that peak demand will be well in excess of anything the current infrastructure was designed for, so what next?

Correlatively, the very propellant that has forced the hand of this infrastructure upgrade holds the key to its success – IoT devices powering smart, local energy grids.

Why local?

Localising energy grids dictates moving away from the nationwide model. Interesting parallels can be found in the analogous advantages of employing local area networks within your company versus each workstation connecting directly to the Internet.

There is a strong argument that this decade has also seen the terrorism threat worldwide rise significantly, with those intent on causing maximum disruption and devastation employing ever-sophisticated tools and techniques to achieve their iniquitous aims. An energy grid that isn't localised greatly increases the potential magnitude of blackouts in such an event. Local energy grids vastly reduce the extent of such disruption, whether caused purposefully or not.

With governments desperate to reduce energy import needs and the country's carbon footprint, it's easy to see the advantages localisation provides; generated electricity travelling lower distances means invariably lower wastage…

…and the opportunity for very short distances now exists from generator to consumer, with household solar generation at an all-time high due to falling costs and government financial support, alongside local renewable generation – in the UK this is predominantly wind farms.

Local government is also taking a keen interest, particularly in solar generation. An Idaho-based company, Solar Roadways (www.solarroadways.com), will soon be rolling out solar panel roads. This technology not only utilizes a massive surface area of "dead" space with huge energy generation potential, but even purports to offer the solution to forcing obsolescence of fossil fuelled vehicles, via a very local electric vehicle recharging facility, directly beneath you! Though replacing the UK's 245,000 miles of road may take a little time!

Why smart?

Embedded intelligence within localised energy grids empowers the grid to react logically to demand. My favorite example is during a typical England international soccer game, the half-time break provokes a 1,500 megawatt surge brought by 600,000 kettles being switched on simultaneously!

Smart energy grids offer even more, being able to intelligently analyze usage patterns across an unimaginable sample size of users and over time; it essentially learns with a fresh injection of usage statistics every day to better manage energy distribution more efficiency, bringing down consumer costs and reducing carbon footprints.

Identifying the source of an underground water leak, particularly before losing thousands upon thousands of gallons is notoriously difficult and, whilst not so extreme, electricity grid maintenance and repair still suffers with this "blind" approach.

A smart energy grid employing peer-to-peer IoT devices can identify and report maintenance and servicing needs before they cause any outage through electrical attribute monitoring – and describe exactly where the fault lies and what it is, reducing investigative costs, thus, hopefully, enabling energy companies to pass on those savings to the consumer. ECD

Embedded COMPUTING DESIGN

MARCH 2015
VOLUME 13
#2

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

23

Departments

Silicon

Software

Strategies

Special Features

APP EXTRAS

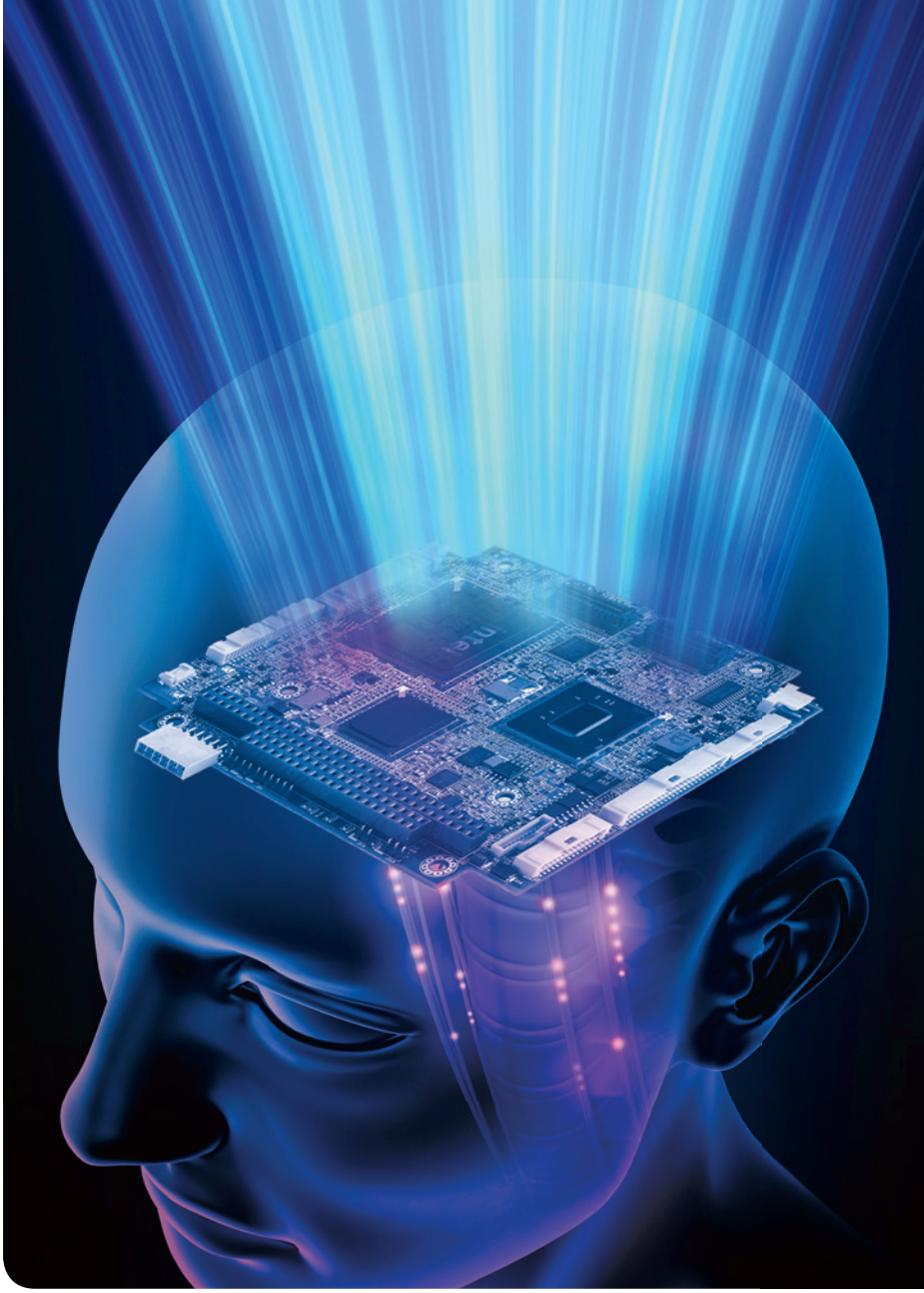
Download the Embedded Computing Design app:
iTunes: itun.es/iS67MQ
Kindle Fire: opsy.st/kindlefireamaz

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

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

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

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



Thinking beyond the board

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

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

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

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

WinSystems®
An Employee-Owned Company

ADVERTISER INDEX

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

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

OpenSystems media®

2015 OpenSystems Media ®

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

ENVIROINK
The inks used to print the body of this publication contain a minimum of 20% by weight, renewable resources.

Embedded COMPUTING DESIGN

OpenSystems media®

ECD Editorial/Creative Staff

Rich Nass, Brand Director
rnass@opensystemsmedia.com

Curt Schwaderer, Editorial Director
cschwaderer@opensystemsmedia.com

Monique DeVoe, Managing Editor
mdevoe@opensystemsmedia.com

Brandon Lewis, Assistant Managing Editor
blewis@opensystemsmedia.com

Rory Dear, Technical Contributor
rdear@opensystemsmedia.com

David Diomede, Creative Services Director
ddiomede@opensystemsmedia.com

Konrad Witte, Senior Web Developer
kwitte@opensystemsmedia.com

Sales Group

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

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

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

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

Shannon Alo-Mendosa, Strategic Account Manager
shannona@opensystemsmedia.com
978-501-9116

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

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

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

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

Reprints and PDFs

republish@opensystemsmedia.com

EMEA

Rory Dear, Technical Contributor
rdear@opensystemsmedia.com

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

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

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

OpenSystems Media Editorial/Creative Staff

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

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

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

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

Steph Sweet, Creative Director

Joann Toth, Senior Designer

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

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

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

Jennifer Hesse, Managing Editor
VITA Technologies

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

Corporate

opensystemsmedia.com

Patrick Hopper, Publisher
phopper@opensystemsmedia.com

Rosemary Kristoff, President
rkristoff@opensystemsmedia.com

John McHale, Executive Vice President
jmchale@opensystemsmedia.com

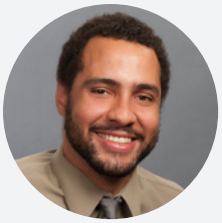
Rich Nass, Executive Vice President
rnass@opensystemsmedia.com

Wayne Kristoff, CTO

Emily Verhoeks, Financial Assistant

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

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



Cutting the cord – Energy harvesting in wearables

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

This past Christmas my girlfriend got me a Fitbit Flex. I didn't ask for one or even express interest in the devices because I saw them as little more than glorified pedometers, but I took the hidden message with a grain of salt and began dutifully using my new wearable.

Then a couple of weeks later at the Consumer Electronics Show I realized that I forgot to pack my Fitbit charger. On day 3 of the show, "The Little Fitbit That Could" finally couldn't, so I decided to make my way over to Fitbit's booth to see about getting some juice back into the band. But on my way there I started wondering, "Why can't a device that's so intimately involved with motion and the human body take advantage of piezoelectric, thermoelectric, or some other energy harvesting technology so I'm not always at the mercy of cords and power outlets?" So I asked.

Granted it was an impromptu stop by and none of Fitbit's technical representatives were available when I arrived, so I just asked a young lady working the booth. She responded that they were always open to new ideas, fished through a giant bag of spare USB chargers they had stashed under the counter, and sent me on my way.

Wearable energy harvesting – where are we now?

Given that wasn't much of an answer, I decided to ring up Robert Andosca, President and CEO of MicroGen Systems, a startup out of Rochester, NY that develops MEMS-based energy harvesting technology (microgensystems.co), for some insight.

According to Andosca, there are currently three viable technologies for energy harvesting in wearable devices – piezoelectric, solar, and thermoelectric. However, none of them is without its faults:

- **Piezoelectric –** Piezoelectric energy harvesting has become a popular method of gathering excess energy produced by motion, and when operating in resonance mode (when all parts of a system operate at the same frequency and from a fixed point in time) can generate about a milliwatt of free energy. But, because piezoelectric devices often operate in the 100s of hertz, whereas humans normally move at around 10, it's necessary to impulse them over time to prevent the output signal from decaying. In impulse mode, piezoelectric harvesters yield only about 20 percent of the energy produced in resonance mode (or a couple hundred microwatts), which is nearly an order of magnitude less than the 2.19 milliwatt output power of my Fitbit Flex.
- **Solar cells –** A solar cell roughly 1 $in.^2$, or about the size of a watch face, can create 3 milliwatts of energy in direct sunlight. Unfortunately for wearables (and many other solar-powered devices), when not in direct sunlight that power production drops off significantly. The average person gets about 5 minutes a day of straight sunshine, and indoors, for example, solar cells harvest less than 20 microwatts of power. All things considered, this amounts in a typical daily output of 50-100 microwatts for solar cells of that size, which is only a fraction of the 675 microwatts required to energize Nike+ SportBands.
- **Thermoelectric –** Thermal energy harvesting is another intriguing technology for wearables, as heat generated by the human body can potentially provide milliwatts of power – given that a 30-degree temperature differential is maintained between the skin and its surroundings. It's possible to achieve this in thermoelectric systems, but maintaining this T in dynamic environments necessitates heat sinks and cooling fins to insulate energy harvesters can quickly balloon to the size of a few golf balls. Although they can be scaled down, with the size, goes the power.

The problem, as you can see, is that we, as consumers (and therefore the companies that manufacture our consumer devices), want wearables that are infinitely small, infinitely cheap, and infinitely powerful. For instance, Andosca explained to me that the current Samsung Galaxy smart watches incorporate piezoelectric energy harvesting technology that is currently 10 mm (L) x 10 mm (W) x 3 mm (D). In their next-generation devices, Samsung is looking at cutting those dimensions basically in half, to 5 mm x 5 mm x 2 mm, necessitating a 2x improvement in harvesting capabilities just to maintain the status quo in that form factor.

Wearables and the energy harvesting fashion police

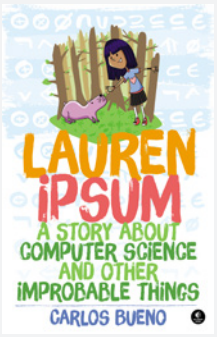
Keep in mind that throughout this article when referring to the power consumption of specific wearables, I have been referring to the power draw of the entire wearable system. The sensors on devices like Fitbit typically only require a few microwatts of power, which is a low enough draw to be accommodated by any of the previously mentioned technologies. Where the real snag in wearable devices (and IoT devices in general) comes in is connectivity. Every time a Bluetooth, Wi-Fi, ZigBee, or other SoC pings the network to transmit data, an exponential amount more power is used than when sensors themselves are simply taking readings.

All of this comes down then to a question of batteries and system design. Simply put, if wearables were designed from the ground up with the complete system in mind (including the resonance, sunlight capture, temperature differential, etc. of humans that make up part of a wearable system), you could minimize the challenges of trying to turn smartphones into armbands, and potentially lose the battery altogether. A good place to start would be calculating the power consumption of your wireless chip and your transmission frequency (especially the frequency of your transmissions), comparing it with the energy generated by your harvesting technology, and going from there. Aside from this, and barring the advent of cold fusion or an innovation in materials, energy harvesting technology will remain a way to extend, rather than eliminate, batteries for the foreseeable future.

And with that, right on cue, my Fitbit died. Again. ECD

COMMUNITY OUTREACH

A fantastic adventure into programming



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

Simple coding projects and DIY/maker boards can be a fun, practical way to introduce the art and science of engineering to kids, but a new book called "Lauren Ipsum, A Story About Computer Science and Other Improbable Things" by Carlos Bueno (nostarch.com/laurenipsum) makes an introduction to computational thinking into a fantastical adventure story for budding engineers.

Readers follow Lauren "Laurie" Ipsum as she goes on an Alice in Wonderland-style adventure into Userland. She begins her journey chased by frightening "Jargon" creatures until she's lost – a familiar feeling for many beginners in the real world of STEM (science, technology, engineering, and math). But she meets some helpful and not-so-helpful characters inspired by programming concepts that help her learn new thinking skills to find her way home. Pros will probably get a kick out of the punny nature of names and attributes of these characters and pick up on the common programming challenges she's about to face.

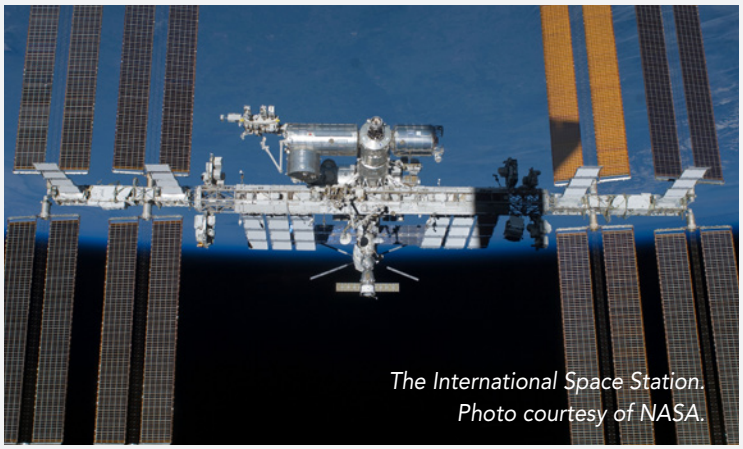
Laurie learns logic methods and how to apply them to solve challenges like the traveling salesman problem, designs algorithms to draw shapes, and analyzes security measures like timing attacks. I particularly enjoyed when Laurie had to be clever to get around the complicated "Byzantine Process" in Byzantium, and learned to work smart, not hard from Bruto Fuerza's follies. And I might find it hard to resist imagining turtles executing code instructions from now on...

The in-story challenges can be a bit wild, but they provide a fun approach to learning and emphasize creativity and imagination – important traits for today's professional engineers and programmers who need to create new ideas for increasingly complex design challenges. A field guide in the back of the book draws connections between the wacky characters and real scientists, computer science concepts, and other real-world things, and calls on the reader to think up solutions to some additional challenges. ECD

DIY in space

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

It's been an exciting time for space exploration. Philae landed on Comet 67P, the Orion mission is working to develop reusable spacecraft, and SpaceX and Virgin Galactic are rapidly developing private and commercial space technology.



The International Space Station. Photo courtesy of NASA.

I was also intrigued about NASA's recent embrace of 3D printing at the International Space Station (ISS) – which can potentially shorten the time for replacement tool/part delivery down to hours from months! – bringing space travel beyond even the commercial realm and into that of DIY. Printed part specs are strict due to the critical nature of aerospace projects, but makers can be a part of the ISS and space exploration in another way: through the Astro Pi (astro-pi.org) challenge.

Education Resource Engineer Dave Honess from the Raspberry Pi Foundation (raspberrypi.org) announced late last year a partnership with the European Space Agency (ESA) and British ESA Astronaut Tim Peake to send Raspberry Pis to the ISS. Primary and secondary school children in the UK can enter a competition to develop code for two Raspberry Pis connected to the sensor-loaded Astro Pi boards that will be flown to the ISS as part of Peake's six-month mission. They'll be deployed around the ISS to collect data in orbit and send that data back to Earth to the winning teams.

Projects are split up into five themes: spacecraft sensors, satellite imaging, space measurements, data fusion, and space radiation. Primary school students are tasked with developing an idea for an experiment or application that can be conducted by the Astro Pi on the ISS. Two winners will get the opportunity to have their ideas interpreted and coded by the Raspberry Pi Foundation. Secondary school students are split into three age categories where the best 50 submissions in each will win a Raspberry Pi and Astro Pi to use to implement their idea. The top two teams who developed code based on their concept will have their code prepared for the mission by the Raspberry Pi Foundation. The secondary school winning teams will also have Raspberry Pi and Astro Pi boards sent to their entire classes. The competition officially opened in January, and the idea phase closes April 3.

The European Space Education Resource Office for the UK (ESERO-UK) is developing teaching resources with the Raspberry Pi foundation that help STEM teachers explain how to use the Astro Pi board/sensors and write code for it, and link the Astro Pi to other curriculum areas (The resources are available through the National STEM Centre at opsy.st/AstroPiResources). The UK Space Agency is supporting further outreach activities around the mission to inspire more interest in STEM fields. I think this is a pretty exciting project to get students into DIY and making, and in turn engineering.

Though you and I aren't UK students (though if you are one working on an Astro Pi project I'd love to hear from you!), we can get our hands on the Astro Pi and related resources and at least pretend like we're developing for the ISS. At press time the Astro Pi hardware attached on top (HAT) board wasn't yet available for purchase, but it was expected to be available in February 2015 for around £30 at swag.raspberrypi.org. On Tim Peake's mission the Astro Pi will be used with the Raspberry Pi 1 B+, though it's also compatible with the Raspberry Pi 1 A+, 2 B+, and 2.

Until space exploration is in reach of everyone, space isn't likely the destination for most of our projects, but the features of the Astro Pi aren't just useful for space. Any sensing and data collection heavy project could find use in the Astro Pi HAT. Its sensors include a gyroscope, accelerometer, magnetometer, temperature sensor, barometric pressure sensor, and humidity sensor. Other features include visible light or infared (Pi NoIR) cameras, five-button joystick, 8x8 RGB LED matrix display, additional function push buttons, and real-time clock with backup battery (See details at astro-pi.org/hardware).

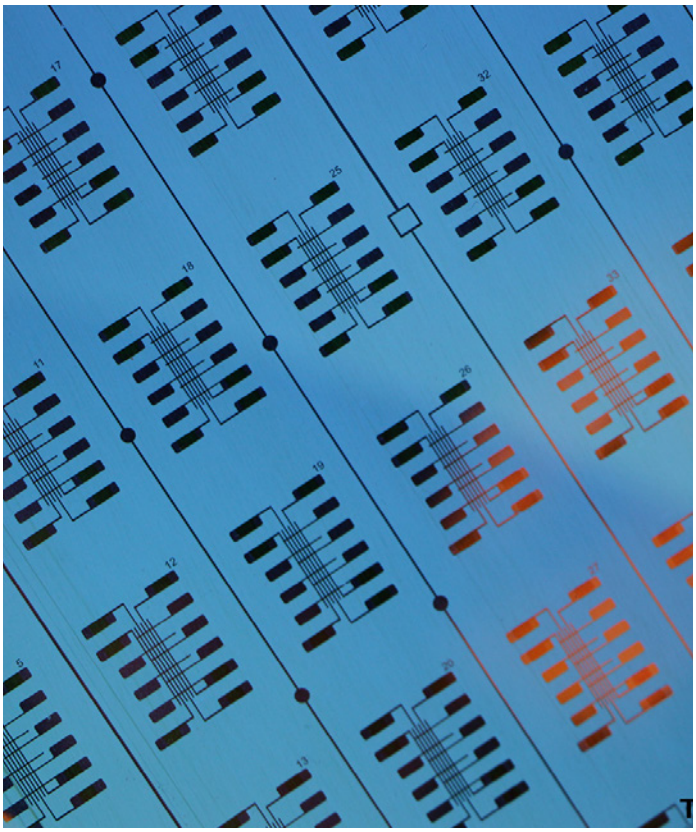
It'll be interesting to follow the progress of the challenge and see what ideas students come up with and how they'll be implemented. If it's a successful challenge, I hope to see it spread to other countries so students and space enthusiasts of all ages can have a shot at sending their projects to space. ECD

Printed electronics embed intelligence – Everywhere

By Matthew Bright

As the Internet of Things (IoT) moves from hype to action it has become clear that ubiquitous and intelligent sensing and data transmission to and from embedded systems are but two elements that must be addressed. Quickly.

To date, this proliferation of intelligent sensing has been hampered by the cost, weight, size, form factor, and power consumption of electronic system components and boards that are manufactured using conventional techniques. However, new advances in printed electronics have extended the sensing and data capture reach of embedded systems far beyond what we have known, while also incorporating much-needed security features. Coupled with the development of smart algorithms that emphasize the use of small data sets to make presentation and analysis of acquired data more efficient and actionable, the promise of the IoT paradigm shift in embedded computing is primed for fulfillment.



So far industry has done admirably leveraging highly integrated, PC board-based embedded systems and low-power techniques to reduce the cost and improve the efficiency of IoT systems. Now we have reached a critical juncture in that the next level of actionable intelligence in the IoT requires scaling intelligent sensory inputs from tens, hundreds, or thousands of nodes to millions or even billions. Though numbers vary, IDC predicts an installed base of over 28 billion endpoints by 2020, all of which need to maintain an acceptable level of cost, efficiency, and security. As the reach of affordable electronic intelligence further expands to include high-volume consumer goods, the number of connected objects could easily reach the trillion units predicted by IBM.

As the number of forecasted endpoints rises, the pressure has shifted to algorithm developers to find ways of filtering the type and amount of data collected in order to reduce the amount of time and processing power required to gather usable information (Figure 1). This has led to much research in data stream analysis, which, for example, prescribes that instead of sensors constantly reporting their states and creating terabytes of data to be processed and stored, algorithms are used that set predetermined pressure and temperature ranges so that alerts are only sent when these limits are surpassed. As a result, network and system processing, as well as storage overhead, can be reduced, improving overall efficiency [1,2].

This focus on smaller data sets, combined with the opportunity for sensing nodes to penetrate new applications and markets – such as labels, disposable healthcare, pharmaceuticals, consumer goods, supply chain, and product security – has created a pull for innovative manufacturing and sensing technologies like printed electronics. Using such techniques with a flexible, low-power processing solution can help designers add intelligence to their embedded systems, both wired and wirelessly, at low cost.

The new foundations of printable electronics

Printed electronics have evolved substantially from the early implementations of basic conductive copper or silver traces printed on hard (and later flexible) substrates to which conventional electronic components were attached. Now, thanks to advances in materials science, printed electronics incorporates a wide variety of capabilities, from roll-to-roll memories to printable thin film transistor (TFT) logic and even wireless communications.

One recently commercialized core building block in printed electronics is printed memory. The printed memory works on the principle that when a voltage is applied to a ferroelectric polymer material the dipoles within the polymer layer align in one of two directions, depending on whether the voltage is applied to the top or bottom electrode. When voltage is removed, the material remains in the same state and can be read as a one or a zero, making it equivalent to a non-volatile memory (NVM) cell, but at lower cost and available in a thin, flexible self-adhesive label (Figure 2).

But while memory has many applications, printed systems also require logic. There are at least two options here. First, a collaboration including Xerox Palo Alto Research Center (PARC) and Thin Film Electronics ASA resulted in printable TFT transistors. Second, a hybrid printed manufacturing process called printed dopant polysilicon (PDPS) has been developed to address RF and other applications that require high-performance transistors, which we'll explore further.

The PDPS process, which enables NFC barcode and sensor-based NFC smart label products, enables the design of printable, high-frequency RF circuits for printed systems connected to smartphones using NFC. The addition of NFC capability has opened up a new spectrum of smartphone-centric applications, some of which are only just starting to take shape.

In Thin Film ASA's Smart Label, memory, logic, and NFC are combined with a temperature sensor and low-profile batteries to warn of temperature deviations outside factory-set limits. While the flexible substrate allows it to adapt to curved surfaces, the sensor can be set with threshold detection as low as -2 °C and as high as +30 °C. The completely self-contained system requires no external power or wiring, with the underlying sensor platform serving as a base for other future sensing mechanisms, such as timing, humidity, or even blood oxygen counts (Figure 3).

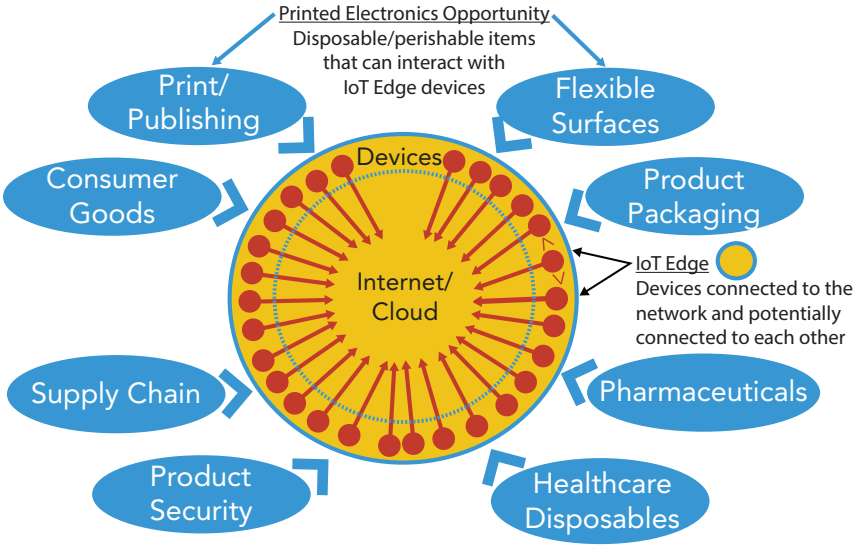


Figure 1 New data sources will add exponentially to the intelligence of networks, but will require new algorithms to decrease the burden of data processing.

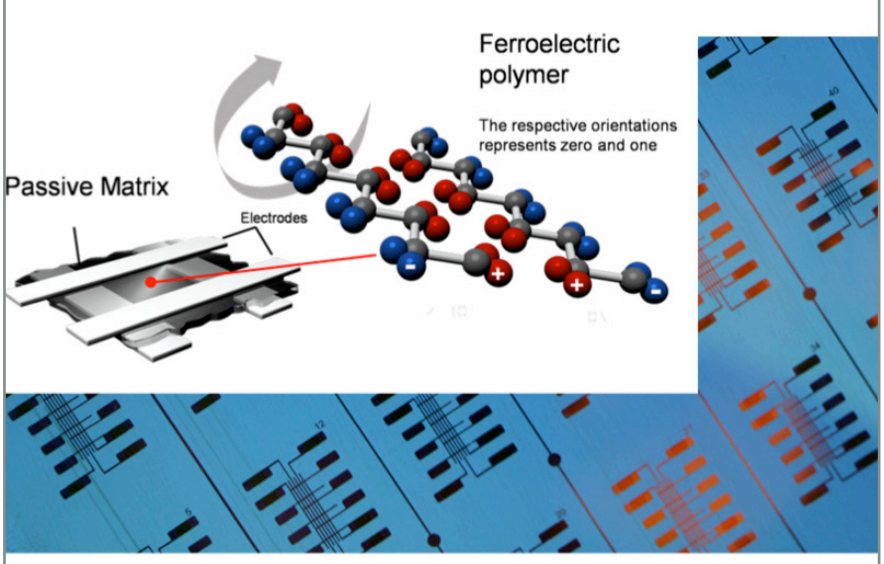


Figure 2 Thin Film Electronics ASA's EN71-3 certified memory based on a ferroelectric film sandwiched between two electrodes forms a roll-to-roll printable alternative to EEPROMs. Standard 20-bit memory can store over 1 million combinations, with 16-, 25-, and 36-bit formats also available, the latter of which can store more than 68 billion states.

IoT security assured

While printable electronics have the ability to penetrate deep into the IoT, designers need to be assured of the security features of the technology in order bring it to next-generation system designs.

In the case of printed memories, this assurance comes at three levels. Firstly, the basic makeup of ferroelectric materials in printed memory produces a distinct signature that can only come from a genuine part. Second, this characteristic signature can only be read through physical contact with a reader. Finally, the memory itself is not IP addressable, thereby preventing external intrusion.

In the case of NFC tags and smart labels, security is provided by the short-range readability of NFC tags (integrated read-only memories that cannot be electrically modified), and the fact that the NFC interface is also not IP addressable.

Development and getting connected

As with any new technology, getting started right is critical. Support must be in place to ensure a rapid and painless development process, so to streamline development with printed memories in "smart consumables" and brand protection applications designers can start with a basic kit comprising memory labels and a corresponding memory interface IC (in bare die or packaged form) that reads and writes to the printable memory (Figure 4). Code support is also available for integration with the host microcontroller.

For NFC-based applications, connecting a smart label or node to the cloud must be simple. Support here comes in the form of the EVRYTHNG Active Digital Identity platform.

EVRYTHNG handles the assigning of a unique digital identity to each physical product. The cloud-based Software-as-a-Service (SaaS) platform can connect and manage all types of intelligent items, from a connected washing machine to an NFC-enabled sensor label based on printed electronics. The EVRYTHNG engine manages a dynamic profile for each item and enables interactivity through a uniquely addressable API. This makes the product or device always accessible, manageable, and intelligent.

Figure 3 Coupling printable memory, logic, and NFC with a sensor enables the development of affordable, low-power, disposable, intelligent sensing nodes that add system intelligence. In this case, such a system integrates a simple temperature sensor into a smart label that wirelessly uploads temperature excursion data from a smartphone to the cloud when predefined limits are breached, allowing sensitive vaccines and perishable foods to be monitored and tracked.

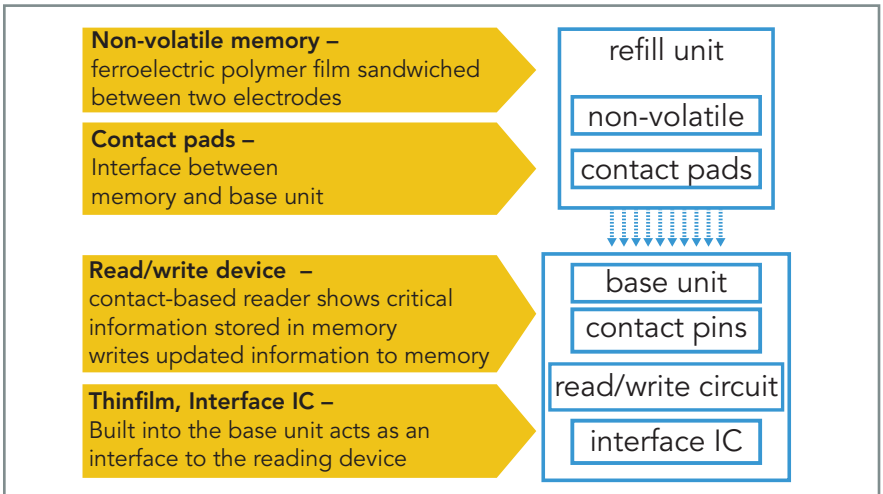


Figure 4 To get started on development, a printed electronics dev kit is provided with a memory interface IC for reading and writing to the printed memory over physical contact pins. Shown here is a consumable label being read.

The printed electronics differentiator

Now, embedded developers are free to develop highly scalable systems that take advantage of the step increase in the number of IoT nodes by adding cost-effective, efficient technology to better service their end customers.

Matthew Bright is the director of product and technical marketing at Thin Film Electronics ASA.

Thin Film Electronics ASA
www.thinfilm.no
@ThinfilmMemory
linkedin.com/company/thin-film-electronics
blog.thinfilm.no/

References:
[1] Data Streaming Algorithms for High-Quality Clustering
www.cis.upenn.edu/~sudipto/mypapers/stream_icde.pdf
[2] Mining Data Streams
infolab.stanford.edu/~ullman/mmds/ch4.pdf

Bluetooth Low Energy brings power-efficient communications to wearables

By Richa Dham and Pushek Madaan

Wearable devices cross a wide range of applications, including healthcare, sports fitness, gaming, lifestyle, industrial, and military. They monitor various parts of the body including the eyes (smart glasses), neck (necklace or collar headphones), hands (gloves), wrists (activity monitors and sleep sensors), feet (smart socks and shoes), and specialized areas, such as is required for tracking devices or motion sensors. Wearable devices are commonly equipped with sensors, a processor, storage, connectivity link (for uploading data and downloading updates), display, and battery. Figure 1, page 15 shows the block diagram for a typical activity monitor.

Wearables introduce several designs factors that must be considered and may differ from other types of embedded devices. Because these devices are worn, size and weight are crucial. Average battery life is important as well, given that wearables must operate on limited battery power. For consumer-based applications, low cost is essential. The type of processor required and amount of storage required depends upon the use cases the wearable device must support. For example, motion sensors provide a continuous data stream that must be transferred; in contrast, an activity monitor collects data continuously, processes it to identify what activity is currently being performed, and then logs this metadata for later downloading.

Low-power communication

How wearable devices communicate has a major impact on key design factors. OEMs have a number of communication protocols available for use in wearables. Well-established standards like Bluetooth Classic, ZigBee, and Wi-Fi have strong market penetration, but were not designed with low power as their primary design consideration. As a result, many OEMs have turned to proprietary protocols to achieve the necessary energy efficiency. However, proprietary protocols can limit the flexibility and market reach of wearables since they have restricted interoperability to only devices supporting the same proprietary protocol.

To meet the requirements of wearable devices and other low power applications, the Bluetooth Special Interest Group has developed Bluetooth Low Energy (BLE). BLE focuses on achieving the lowest power for short-range communications. BLE operates in the 2.4 GHz ISM band that Bluetooth Classic uses, enabling devices to leverage existing Bluetooth radio technology to keep costs down.

BLE offers bandwidth of 1 Mbps, which is more than sufficient for most wearable applications. Typically, wearable applications also need to provide state information rather than having to log large amounts of data between transfers.

To minimize power consumption, the BLE architecture has been optimized at each layer:

- **PHY layer –** Increasing the PHY modulation index reduces transmit and receive current
- **Link layer –** Quick reconnections reduce overall transmit time
- **Controller layer –** A more intelligent controller handles tasks such as establishing the connection and ignoring duplication packets. Offloading the host processor in this way enables the processor to remain in standby or sleep mode longer
- **Protocol layer –** Connection setup time for exchanging data is reduced to a few ms. The protocol is also optimized to burst small blocks of data at regular intervals. This allows the host processor to maximize the time it can spend in standby or sleep mode when information is not being transmitted
- **Broadcaster mode –** Wearable devices can operate in broadcaster mode only, eliminating the need for devices to undergo a connection procedure
- **Robust architecture –** BLE supports Adaptive Frequency hopping with a 32-bit CRC to ensure more reliable transmissions

The ultra low power consumption of BLE makes it ideal for wearable devices. Its efficiency keeps battery size down, which reduces device cost, size, and weight.

While Bluetooth Low Energy is based on Bluetooth technology, it is not compatible with the standard Bluetooth radio. However, dual mode radios are available that support both Bluetooth Classic and BLE. Dual mode devices, known as Bluetooth Smart Ready hosts, eliminate

the need for a dongle, as is required when using proprietary protocols. The readily availability of BLE Smart Ready hosts in smart phones gives consumers a simple and cost-effective way to connect to wearable devices.

A complex, full-package design

Communications is only one part of a wearable architecture. Among other components, these devices must also have:

- Analog front end to process raw sensor signals
- Digital signal processing capabilities to filter out noise and provide advanced post-processing
- Storage
- Processor for high-level system functions
- Battery charger

Figure 2 details an optical heart rate monitor implemented as a wristband. This type of device uses an LED to illuminate tissue and the reflect signal, measured by a photodiode, carries information about changes in blood volume. A trans-impedance amplifier converts the photodiode current to a voltage, which is converted by an ADC into a digital signal. This digital signal needs filtering to remove DC offset and high frequency noise before heartbeats can be detected. This information is passed to the BLE controller for transmission. Optionally, the heart rate can be computed by the wearable device before transmission.

Multiple discrete components complicate system design. Each additional component also increases power consumption,

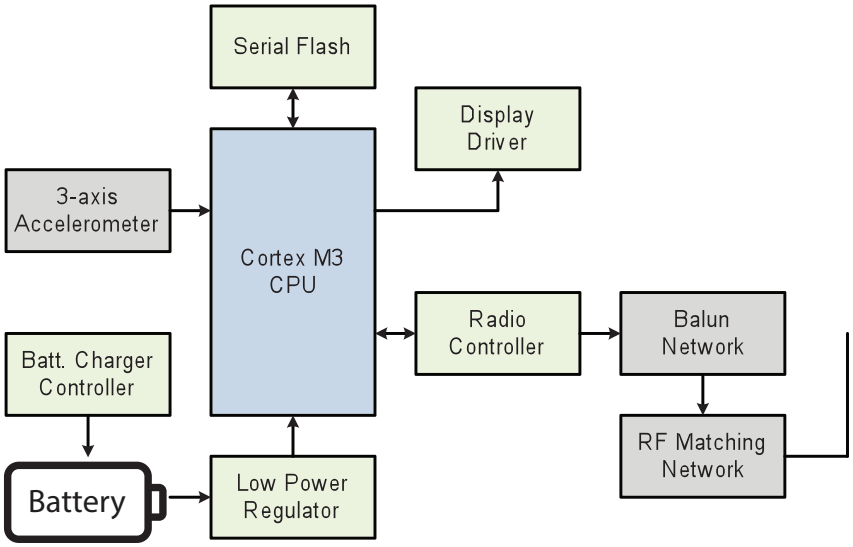


Figure 1 Block diagram for wearable activity monitor.

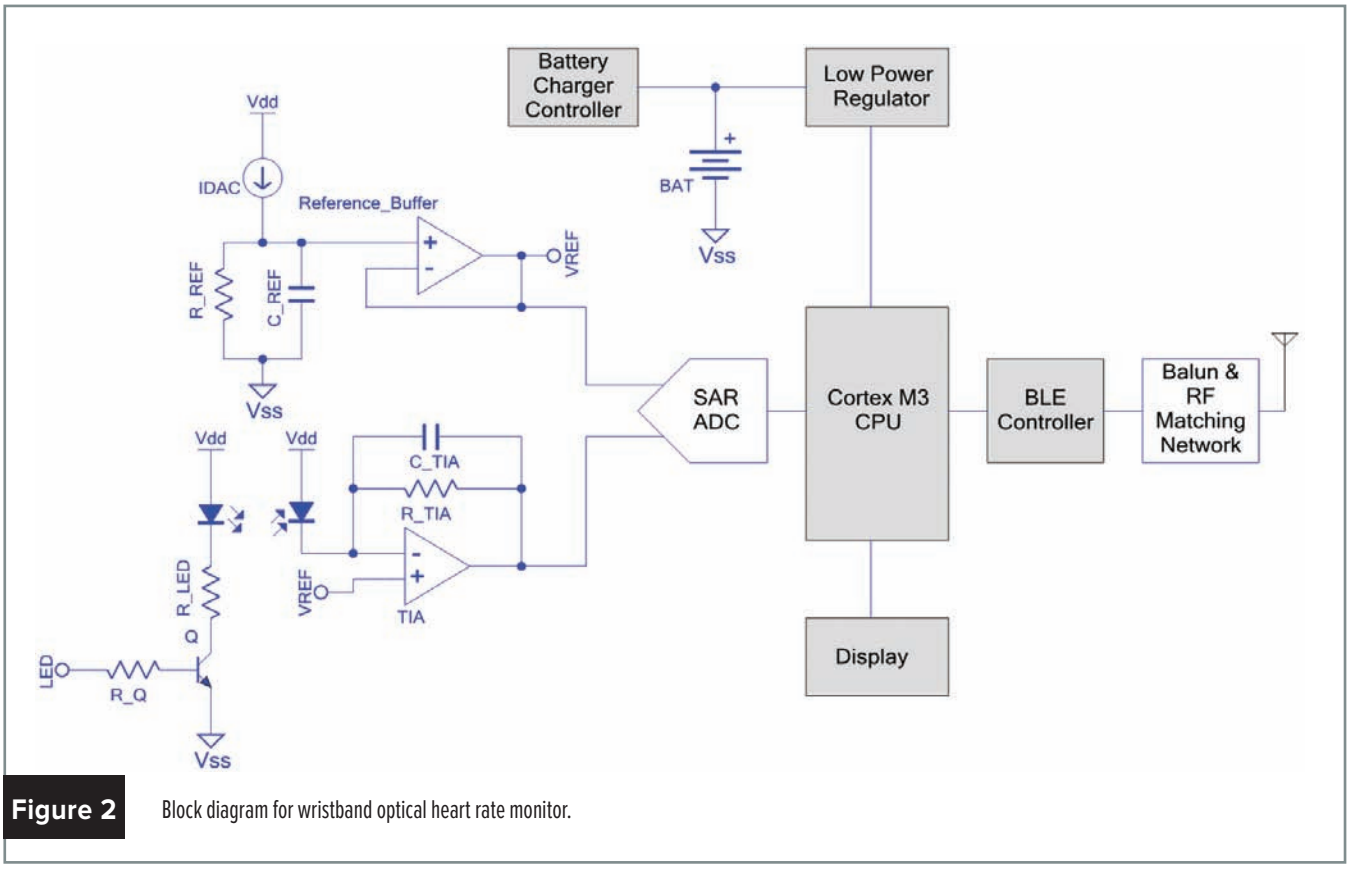


Figure 2 Block diagram for wristband optical heart rate monitor.

system size, and cost. To minimize these factors, OEMs can utilize a system-on-chip (SoC) architecture that integrates a controller with the necessary analog and digital components. The PSoC BLE from Cypress, for example, has been designed to meet the strict requirements of the wearable market. It integrates a 40 MHz Cortex M0 CPU with configurable analog and digital resources and has a built-in BLE subsystem.

Figure 3 shows the implementation of a heart rate monitor using a PSoC BLE. For the analog front end, four unconfigured opamps, two low power comparators, one high-speed SAR ADC, and a dedicated capacitive sensing block enable advanced touch-based user interfaces. For digital processing, two serial communication blocks can be used to support I2C, UART, and SPI interfaces. The processor also has four 16-bit hardware timer counter pulse width modulators and four universal digital blocks for implementing digital logic in hardware similar to how logic is implementing in an FPGA.

For this application, the only external components required outside of the controller are a few passive components, a transistor for driving the LED, and those required for RF matching. One advantage of having the other components integrated is greater control over system power. For example, developers can turn disable the analog front when it is not in use.

The ready availability of Bluetooth Smart Ready in smart phones, tablets, and other portable devices makes Bluetooth Low Energy an excellent choice as the communication protocol in wearable applications. With SoC-based BLE controllers, OEMs can minimize power consumption, device size, and system cost, making their wearable designs even more attractive and competitive.

Richa Dham is a Product Apps Manager for the PSD division at Cypress Semiconductor.

Pushek Madaan is a Senior Application Engineer at Cypress Semiconductor India Pvt. Ltd.

Cypress Semiconductor

- www.cypress.com
- @cypresssemi
- linkedin.com/company/cypress-semiconductor
- youtube.com/user/cypresssemi

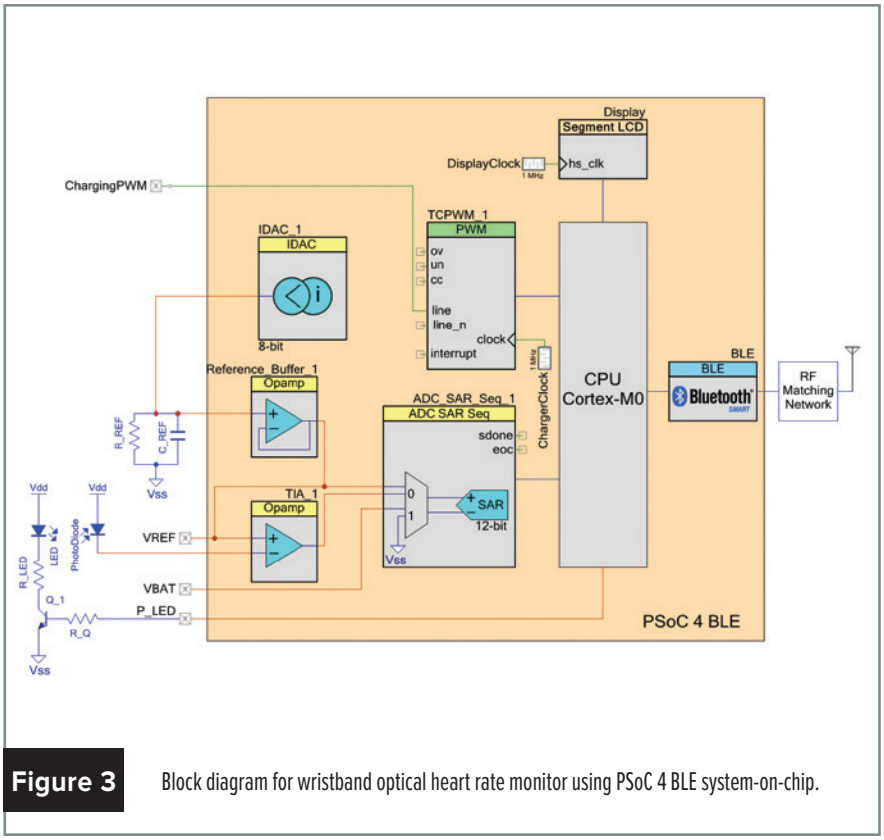


Figure 3 Block diagram for wristband optical heart rate monitor using PSoC 4 BLE system-on-chip.

Q&A

SECURITY INCREASINGLY CRITICAL AS IOT BLURS LINES BETWEEN ENTERPRISE AND EMBEDDED

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

The Internet of Things (IoT) has caught the attention of every industry on the planet. The notion of smart sensors deployed everywhere that source important information promises to transform and inform for greater efficiency, profitability, and situational awareness.

The line between embedded and enterprise has historically been fairly clear – client and server firmly rooted within the enterprise technology while a myriad of "black box" processors, platforms, and software made up the embedded space.

The emergence of IoT blurs the line between enterprise and embedded. And with it comes an entirely new area of security and what it means to "secure the enterprise." Enterprise IT departments are waking up to the fact that traditional security perimeters are increasingly vulnerable as IoT becomes intertwined with daily enterprise life. Embedded systems developers can no longer assume their system is sitting safely out of reach of the hackers.

In this month's column, we'll hear from the enterprise and the embedded side – both surprisingly aligned with their understanding of the implications of IoT and increased security for these systems within the enterprise.

Recent examples

For an example of problems that may arise as a result of IoT and the enterprise, look no further than the Target breach from 2014. This breach came in through the HVAC system via stolen credentials from a heating and cooling company[1]. From the HVAC launching point, hackers gained access into the payment system network and acquired credit card information.

Another example, perhaps more ominous, involved a German steel mill where the hackers were able to control a blast furnace so that it could not properly be shut down, causing "massive" damage[2].

Karl Volkman
CTO
SRV Network

Alan Grau
President and Co-founder
Icon Labs

Point/counterpoint: The participants

Karl Volkman is the CTO of SRV Network and has been in enterprise IT for 33 years. SRV Network is a managed services provider for mid-size firms. They do outsourcing from desktop through purchasing to planning. I was fascinated by reading some comments from Karl relating to the IoT influence and security issues within the enterprise and I wanted to pursue this further with him.

Alan Grau is the President and Co-founder of Icon Labs. Alan has been engaged with embedded systems development since 1991 first with Bell Laboratories and Motorola before starting Icon Labs. Icon Labs is focused on a variety of security aspects and solutions for embedded systems and IoT and there may be no better authority on practical embedded security than Alan. Companies like McAfee, Intel, and ARM have all worked with Alan on a variety of security related embedded projects.

I asked Karl and Alan questions about cyber security in an attempt to find out how closely aligned the enterprise IT side is with the embedded development side of IoT.

Q How do you define cyber security as it relates to the IoT?

VOLKMAN: To me, cyber security is about protecting technology. In the past, this might be information, but with the advent of enterprise uses of IoT, it's everything. This extends the protection

to authorized access and use. Things that have made headlines today have been information breaches like financial data. Other considerations involve taking down web sites by flooding Internet connections. With IoT there is a new dimension involving hacker control of an IoT device and the consequences if it occurs.

Anything that sits on the network is prone to an attack or unauthorized control. For example, smart lighting seems fairly low risk. But depending on the situation, unauthorized control of lighting systems could facilitate in a crime or possible accident or injury.

The Target breach is an example where IoT was used to gain entrance into enterprise information. Anything that has specialized software that controls embedded devices could be at risk.

Sometimes the entity that gets compromised isn't the actual embedded device per se – it's some kind of gateway system that leads to the enterprise network with sensitive information or the mission critical IoT network. From there, the attacker can use that device as the launching point for other malicious behavior.

There is a social aspect to cyber security as well. People leave passwords in obvious locations or choose passwords poorly. Social media can provide information on people, passwords they might choose, and where they work. This human interface and social aspect should also be considered within the scope of cyber security.

GRAU: From the IoT perspective, security means allowing only authorized users in and keeping bad guys out. One dimension of cyber security that's often overlooked is preventing accidental breaches or misconfiguration. A recent study mentioned 70 percent of cyber incidents are internal and of those internal incidents, over 70 percent of those were accidental. Whether accidental or malicious, they stem from the same problems and require the same kinds of capabilities.

Comprehensive cyber security needs to start with secure boot, download authentication, and code signing as a foundation. Other required components are secure communication, authentication, and security management. The unique thing about cyber security as it relates to IoT is not the problem being solved but that these security solutions often require a specialized implementation or at least some amount of unique customization for the environment.

Q What are the IoT security trends and market drivers?

VOLKMAN: I believe there is an emerging realization that there is no one magical thing I can deploy that will protect me. There has always been investment in "safe perimeter" capabilities like firewalls and intrusion detection. This isn't enough and investments must include things that will quickly tell me when I'm being attacked. We need to understand that as IoT integrates with the enterprise, attacks will happen and focus needs to shift to early notification when things are attacked or compromised. IoT systems need to be designed to minimize damage resulting from a security breach. So security strategies must include capabilities for fast identification and notification of possible breaches.

The interaction between embedded systems and controls is becoming broad and automated. Breaching of these systems has the potential for far greater negative impact. For example, auto infotainment system connectivity with smart phones and in-car Wi-Fi represent potential gateways to the power train and other critical systems within the auto. Perimeters are important, but action needs to be taken to minimize damage if vulnerabilities are exploited.

GRAU: Time to market pressures have and will always be with us. Within the IoT world (or any emerging embedded industry), the trend is to quickly develop, rush the solution to market, and leave security considerations for later. Maybe the initial deployment involves simple password based authentication and/or SSL/SSH access. But this isn't enough. Most IoT devices don't have a well thought out security strategy. The current trend is to not do much at this point. Fortune 500 companies that lead their market space tend to address security more. These companies tend to have decent security perimeters already and understand the need to augment security.

Another promising trend is industry organizations forming around security issues. The ISA/IEC 62443 standards for industrial control security are an important step toward progress and companies are working to achieve compliance. This moves the ball forward and provides a means to ensure a consistent way of measuring security. But it's also important to understand compliance doesn't equal secure. Compliance by itself is a big step forward, but not enough. Significant thought, design, and implementation must occur in order to understand how your IoT solution might be attacked and what kinds of things need to be protected to minimize damage if it is compromised.

Q Who is investing and why?

VOLKMAN: Larger companies are investing, but smaller organizations recognize the need and don't know what measures to take and risk assessments can cost a lot of money. Today, IT departments understand what a desktop computer network and server farm is, and which elements may be attacked and how. Perimeters and detection systems can be deployed. But the addition of machine-to-machine (M2M) or IoT environments have points of attack that aren't well understood because they are black boxes with little or no documentation.

Companies deploying M2M and/or IoT are asking what they need to be concerned about. There is growing awareness that all the devices on the network need to be addressed with respect to security. One of the biggest problems right now is these individual devices don't have any kind of security software protection built-in. If there is, it's not exposed in a way enterprise IT can incorporate it into their security strategy. There hasn't been any consistent "this is how you address security for this kind of device."

Money continues to be spent on perimeter solutions. Conversations start around "what's the worst that can happen," then assessing and prioritizing security solutions to deal with the biggest threats is a good first step.

Every company is different. Most corporate leaders have fears or heard of issues where companies are hit this way or that way. They listen to news reports, which can be informative, but they may be missing the point. It's critical to determine which security breaches are most problematic for your specific business and how to protect against those. Addressing security isn't cookie-cutter – you have to address them based on your unique circumstance.

One thing I think the industry could benefit from is the notion of a fail-safe. When a system does get compromised, is it possible for the IoT device to be put into a "safe" mode and send a notification that compromise has happened. This involves building something into the device itself.

In my opinion, the best security strategy involves:

1. Protecting against the "known bad"
2. Identifying things that are "outside the norm"
3. Building in fail-safe operation and notification in the event the system is compromised

GRAU: In this new combined enterprise/M2M/IoT world, people are using a traditional mindset. They establish perimeters within perimeters, which puts tons of money into Cisco's pockets. The trouble is these perimeters don't address these new IoT/M2M vulnerabilities. These are embedded devices that most traditional network IT companies do not understand with little or no built-in security or interfaces for security management.

Industrial control companies are starting to invest in more secure solutions and the big players are investing, but not the lower tiers. Of course there are companies like ours (Icon Labs) that are completely focused on embedded security and are actively developing software and toolkits for IoT developers to leverage. Silicon manufacturers are starting to incorporate security aspects like ARM's trust zone feature to enable security, but there still has to be software that uses it.

> "There is a real need for embedded IoT and M2M solutions to grow up when it comes to security."

Larger companies understand that embedded system compromise stems from download execution, and gaining control of the embedded device. So things like secure boot software, and secure software validation between the embedded operating system and application becomes an important security feature. All these linkages must be maintained to have a good level of security. Then focus switches to manageability. Can the system integrate with a remote policy and security information and event management (SIEM) systems within the enterprise that allows anomaly detection. It's all these additional security aspects around the introduction of M2M and IoT where we at Icon Labs are focused.

Most embedded devices sit somewhere on a network with a remote access interface. If a hacker starts probing and runs a dictionary attack, they could potentially do that for days or weeks without anyone noticing, as opposed to a desktop environment where the user would notice slow response or lots of warnings and report this to IT.

Embedded devices typically don't distinguish these kinds of attacks and the lack of visibility for the administrator can be a huge problem. If there are no controls on modifying the configuration of an embedded device, a hacker that spends weeks running attacks can finally breach the device and potentially change configuration without anyone noticing. Smart devices need to be smart about security. Immediate notification should be sent in cases where login attempts or communications with the device is outside the bounds of normal. There needs to be more refinement in the area of detection. For example, attempts to change firmware or configuration without proper credentials should be blocked and a notification created for early warning. But the vast majority of these IoT devices don't expose any kind of security interface for administrators to utilize.

Aligned security approaches and goals

Both experts from the enterprise and embedded IoT spaces had the same key take-aways without ever talking to one another:

1. Security must go beyond perimeters
2. IoT and M2M devices must have interfaces for fast detection and notification of possible breaches
3. IoT and M2M devices themselves must have a comprehensive security plan within the device

It appears the enterprise and IoT security experts are aligned. There is a real need for embedded IoT and M2M solutions to grow up when it comes to security. Without action with respect to IoT security, the results could be far more devastating than getting some credit card information.

References

[1] "Target Hackers Broke in Via HVAC Company" http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[2] "Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever" http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

Q&A

SOFTWARE-DEFINED NETWORKING – A VIEW FROM THE TOP

Jeff Reed
VP/GM – Enterprise Infrastructure and Solutions Group, Cisco

Out of the loosely understood concepts of several years ago, Software-Defined Networking (SDN) has evolved into a framework that will usher in the next network paradigm. This interview with Jeff Reed, Vice President, Enterprise Infrastructure Solutions Group, Cisco, looks at what policy-driven networking means to the networking giant, as well as SDN's implications on network equipment vendors the world over.

Q What's Cisco's SDN strategy?

When we look at SDN at Cisco, we see it as a key enabler to simplifying and automating a network. I look at SDN doing that in a few ways. One is the ability to treat the network as a system. If you think about today's networks that are made up of all of these components, the beauty of SDN is the use of a controller in the environment that allows you to look at the network as a whole. That dramatically simplifies things for IT organizations and applications – basically anything that's interacting with the network either because they're trying to manage the network or because they need resources from the network. That's a common theme around SDN.

One thing that's specific to Cisco is our focus around using policy as a way to interface with that network as a system. And when I talk about policy, really what I'm talking about is moving from the "how" network interfacing of today, where specific configurations on devices for features like QoS, access control, etc., are enabled by talking in the language of the interface on a specific box. What Cisco's doing with our strategy around Application Centric Infrastructure (ACI) is moving that interface to a "what" interface (Figure 1). So you just tell the network what you want – "I want to prioritize application A over applications B and C," or "I want to allow all of the folks in the engineering department to have access to these resources" – and the ACI controller takes that intent and basically translates it into the changes that need to happen across the network infrastructure to make it possible. It's hugely important because it

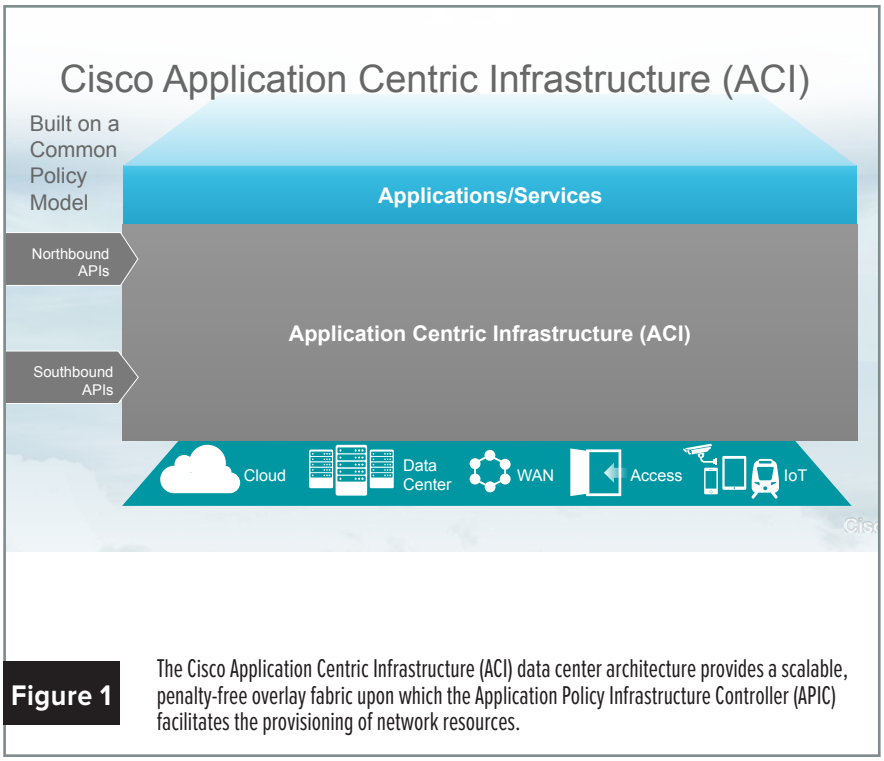


Figure 1 The Cisco Application Centric Infrastructure (ACI) data center architecture provides a scalable, penalty-free overlay fabric upon which the Application Policy Infrastructure Controller (APIC) facilitates the provisioning of network resources.

really changes the nature of how all of the things that rely upon the network potentially interface with the network, and really simplifies and automates it.

One analogy I like to use is thinking about how we used to take care of cars 30 years ago – you'd pop open the hood and really tune low-level components of the car like the timing belt, etc. Now when you think about how modern cars have evolved, I can just go in and flip the sport mode switch on my transmission and the car behaves differently. That's the "what" in that I want the car to behave in a specific manner instead of having to go under the hood and change all the underlying pieces. You just interface with the car very simply as a system, and you're off and running. So it's really key to how we think about the network evolving, and what it enables is third-party applications being able to interface with the network much more simply because instead of having to know all the specific details of what's going on, they can just tell the network what they want and then the network provides that.

Q In terms of the controller, are Cisco SDN controllers based on OpenFlow, homegrown, or something else?

I'll use myself as an example to start. I was working in the campus and branch environment, and though the switches that we and other vendors provide support OpenFlow, a lot of those boxes were built years ago. Just the way that switches work, and particularly how the networking ASICs on those boxes work, they can do OpenFlow but it's not the most efficient way to make changes on the network.

The way that OpenFlow works is basically a rule set where you match against a set of rules, and if you have a match you perform an action. That's essentially how the protocol works on the controller function and the data pipeline. In networking, ASICs have been very highly tuned to enable switching with the most speed, the lowest power consumption, and the least amount of cost. These ASICs are pre-programmed to do certain things as part of the pipeline, so they don't naturally enable this generic match and action requirement of OpenFlow. If you look at a lot of the OpenFlow implementations on the switches that customers have been purchasing, they've all been done in CPU software, and there's a real scale limitation to doing things at the software CPU layer versus in the network ASIC itself. So when you look at most of my customer's environments, OpenFlow capabilities would dramatically limit the performance of their network infrastructure.

What Cisco did was look at how we could enable ACI – the principles of a policy-based network as a system – while taking advantage of the interfaces that those products have today to allow them to run at full line rate. It's not super sexy. We use CLI, we use SNMP, we use almost any interface, and that's one of the beauties of our strategy. In a lot of senses we're pretty agnostic in terms of what the protocol is between the controller and the device. We want to enable the use case and the value that ACI can provide, and we don't want to necessarily require that customers have to change out their networking infrastructure, particularly in the branch and campus environment. How we can deliver policy-based networking to an environment in a way that they can take advantage of the purchases they've already made.

We've got a lot of different capabilities in terms of the protocols we work with, but with that said, we're also working on new protocols. An exciting example there is one called OpFlex. We talked about these policy-driven networks, and the idea behind OpFlex is that it's basically a policy protocol between the controller and the switch. So, without OpFlex, the controller needs to essentially determine the policy to prioritize an application, and then figure out what it needs to do from a configuration perspective on each of the appropriate devices on the network to deliver against that policy. What OpFlex does is actually allow us to talk policy language to the devices, making the controllers work a lot less and the devices do more of the policy implementation locally.

In general the protocol process is still relatively early in the maturity cycle, so I think you'll see a lot of interesting developments on the protocol side that Cisco and other vendors are participating in.

Q When do you see SDN technology really hitting critical mass, and does Cisco plan to evolve with that progression?

We're close. We already have north of 200 customers that have deployed ACI, and I think that in this calendar year that number is going to increase dramatically. By the end of this calendar year you'll see critical mass adoption of what we're doing with respect to ACI, so it's coming and it's coming quickly, and we're getting really great feedback.

In terms of how that's changing Cisco, one of the key things that we focused on with ACI has been driven by the fact that SDN was such an abstract concept to customers. The, "I kind of understand what you're talking about, but what does that give me?" So what we're doing is looking at how to apply SDN and ACI to specific use cases.

Let me give an example. We have a capability in our routing infrastructure to do more intelligent path selection. So if you're in a branch environment, the idea is to use cheaper broadband Internet links to connect branches because what we're able to do with our technology is, even though they may be less reliable, take a couple of those links based on policies set with ACI and intelligently determine what link to send the appropriate traffic over. With secure encryption on top of that, I can provide a very robust, high bandwidth, potentially lower cost branch connectivity solution, and we call this Intelligent WAN (IWAN), which provides software defined routing services. We've had the building blocks for IWAN in our infrastructure for quite a while, but what we're doing with ACI is enabling the adoption of IWAN, as part of our SD WAN strategy, much more easily. Customers can come in and set these application-level policies at the controller level, and then the controller takes those policies and enables IWAN across the branch routing infrastructure. So what you'll see is more and more of our development resources working to integrate what we're doing with SDN

and ACI with the underlying functionality in the network infrastructure to be able to go out and provide these broader level business capabilities.

The beauty of this is that as a standalone capability, SDN is interesting, but it's more, "I can deliver much better application performance to users in the branch than I did before," or "I can automate the remediation of a security vulnerability because with just a couple of REST API calls my Sourcefire security solution can quarantine a user that has malware or is acting suspiciously." There are all of these interesting use cases that, once you get to policy-based networking, become much easier than they've been in the past. In the next five years you'll see a whole set of things that Cisco does, but also other third parties like Citrix and Lancope, that can take advantage of the network and policy-based abstraction to get the network to do more and more creative and useful things for businesses.

Q Do you see SDN threatening Cisco's dominance in network equipment, and does it force the sale of commoditized hardware?

No, and here's why. I actually think that SDN will play into the end-to-end capabilities that Cisco brings. If you think about having the network behave in the manner I described, so much of it cuts all the way across the network. All the way from the user like myself, connected wirelessly in a branch or campus environment, all the way through the network to the application that's sitting in the data center or the cloud that I'm getting access to. Those are the types of use cases that I'm seeing customers ask for, and Cisco, because of the breadth of our capabilities in the market is uniquely positioned to enable that end-to-end capability. That's one.

The second one is that I was one of the founders of our SDN strategy in the campus and branch environment, and what drove me to look at SDN was that the complexity of networks was making it harder for customers to take advantage of the functionality and capabilities in network hardware. So, I'll go back to my car analogy. If you have an underpowered engine, it's only going to go so fast. Really what I see with ACI is the fact that it's allowing customers to take advantage of the capabilities in underlying infrastructure, and because customers can now take advantage of the underlying infrastructure it will become, in many ways, increasingly important in segments of our solution.

Cisco Systems, Inc.
- www.cisco.com
- @Cisco
- linkedin.com/company/1063
- facebook.com/Cisco
- plus.google.com/+CiscoSystems/posts
- youtube.com/Cisco
- blogs.cisco.com/getyourbuildon

Building a smarter "smart home" on ZigBee 3.0

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

No longer just gizmos and gadgets for the wealthy, devices for the smart home are fast becoming the purview of the every man. Estimates project that within the next 10 years the average household will consist of 100 connected devices, networking everything from lights and motion sensors to thermostats and smoke detectors.

But simply Internet-enabling appliances does not a smart home make. Data analysis will be the differentiator in realizing the benefits of truly "smart" homes, which requires an underlying communications infrastructure capable of data reporting within the power, cost, and usability constraints of a consumer home environment. To this end, ZigBee 3.0 offers improved interoperability to help put the "smart" into smart home.

With every passing day it seems more and more otherwise-mundane household items are being outfitted with connectivity. From refrigerators and washing machines to toasters and light bulbs, appliances of all kinds are being networked and marketed as elements of the impending smart home.

While the smart home architectures of tomorrow will indeed be comprised of numerous networked devices, however, simply Internet-enabling a door lock or light switch doesn't make it inherently "smart." The key to the smart home is harnessing data based on behavior and usage patterns, and using that intelligence to autonomously improve the residents' quality of life. But when comparing today's smart homes with those of the future that operate independently and behind the scenes, Paul O'Donovan, Principal Research Analyst of the Semiconductor Group at Gartner (www.gartner.com) says it's "similar to where the mobile phone was in the 1990s to where it is now – functional, but by no means smart."

"Basically, there is little or no computing or learning going on in the systems available today," O'Donovan says. "There is some limited decision making, such as turning off heating or lights when the home owner leaves the building, but otherwise there is little 'processing' of the data locally or in the cloud."

"The smart home is still in its infancy," says Ryan Maley, Director of Strategic Marketing at the ZigBee Alliance (www.zigbee.org). "There are many products available and these are well deployed extending comfort and efficiency for home owners. However, these products tend to be single-purpose applications such as lighting, security, or energy efficiency.

These installations probably reflect where the homeowner has interest or where there is some easily understood value. However, the smart home should be much more.

"As more devices are connected, consumers will see more value than simply extending control of their home to mobile devices," Maley continues. "The smart home should be optimizing efficiency and making decisions for us automatically rather than simply allowing us turn things on and off via a mobile device instead of a light switch. As more everyday objects are connected and become smart, many new interesting applications may arise, such as balancing the needs of lighting and energy management by opening window coverings instead of turning on a light when we enter a room."

To enable analytics for new smart home applications and services such as energy management, embedded software development companies like DSR (www.dsr-company.com) design architectures that amass sensor data from connected devices (Figure 1). In addition, new technologies and techniques are emerging that will add value and make home automation more transparent to the end user, says Genie Peshkova, Vice President of Operations at DSR.

"Consumers expect the smart home to be truly smart – don't ask me about things that you can determine, learn my behavior and adapt," Peshkova says. "Don't unnecessarily disturb me, but do let me know when something is wrong or out of the ordinary. The idea is for the smart home to fit perfectly into the consumer's lifestyle, adapt to his or her likes or dislikes, simplify life, add convenience, and provide much needed security and peace of mind.

"Without analytics and data intelligence, smart home systems cannot learn, intelligently respond, and truly adapt to the

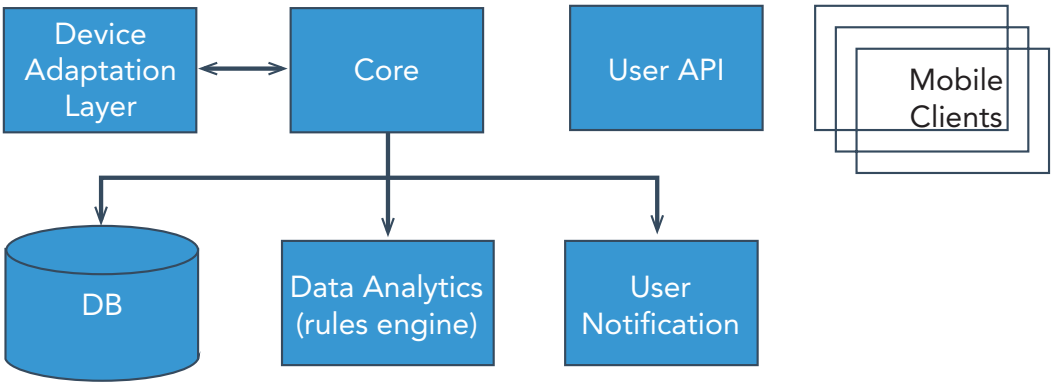


Figure 1 Companies like DSR integrate embedded devices with smart home analytics architectures such as this to enable new applications and services for the smart home.

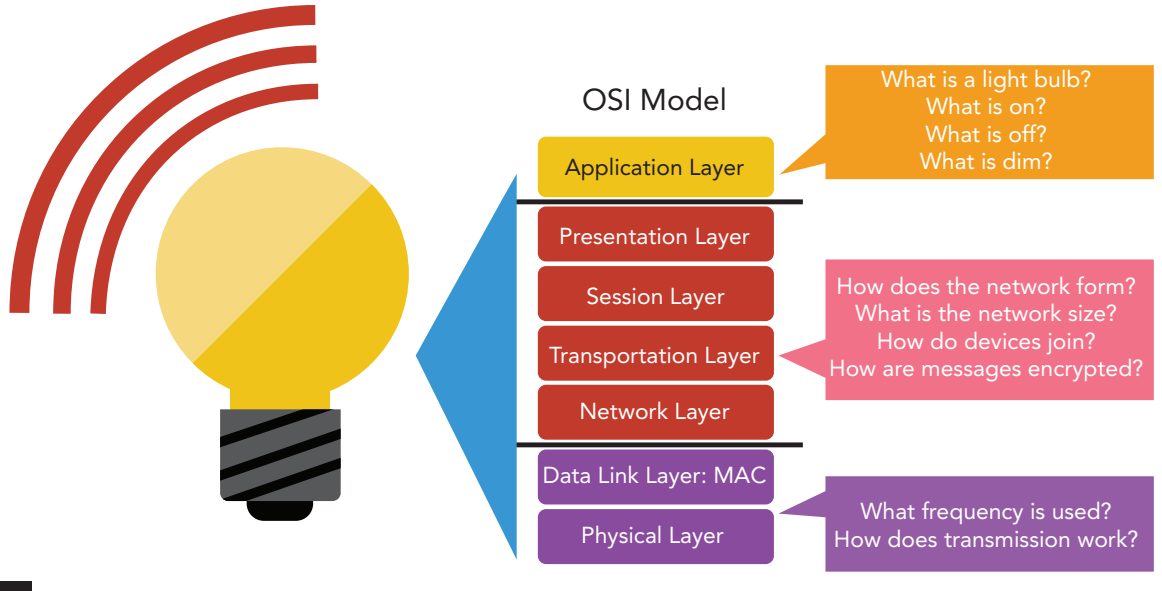


Figure 2 Unlike interoperability at the network layer, application-level standardization can define operational, reporting, and other information to make device-level data exchange more transparent in the smart home. Image courtesy the ZigBee Alliance.

consumer," she continues. "As the smart home market continues to grow, data will become a more and more powerful component of the equation. We are working in collaboration with partners that provide behavior analysis engines, content analysis, and voice control – a large degree of automation for the user's lifestyle, social preferences, behavior analysis, and prediction, a lot of which already exists but will become even more sophisticated. Pulling all these together will lead to providing a truly smart solution that will deliver a lot of value to the consumer."

But at the network application layer underlying this infrastructure, interoperability challenges still exist that limit the potential of the connected home.

Application-level interoperability and the fight for the smart home – ZigBee 3.0

Though architectures such as those depicted in Figure 1 generally abstract the application layer through a gateway or router that connects sensors directly to the cloud, application-level interoperability is still key for the many subdomains and devices that make up a fully outfitted smart home. For instance, while standardization at the network-level allows for commonality around packet forwarding, interoperability at the application layer establishes consistent rules for exchanging data between devices (Figure 2). As a point of reference, the latter is similar to how HTML is used across the Internet.

Given this, and the low-power, low-cost, and ease-of-use requirements of consumers, wireless mesh networking technologies have gained prominence as a scalable way of integrating products into the smart home. However, with widespread incompatibility between vendor devices and numerous networking technologies all competing for an emerging market, settling on any one connectivity solution has become a struggle for industry and consumers alike, O'Donovan says.

"Multiple networking technologies clearly complicates the picture for the consumer and slows manufacturer attempts to unify around one or more compatible systems," he explains (Figure 3). "There is little cohesion in the market. Despite efforts to deploy mesh networking by some players as a way to offer a whole home/system solution, there is scant interoperability between most manufacturers."

"There are a number of options vying for the home automation market, with X10 probably known best because it has been

A Selection of Enabling Technologies

Technology	Frequency / License	Target Application	Standards Body	Max Data Rate	Comments
ZigBee	2.4 GHz / Unlicensed in Most Countries	Industrial/Home Automation	IEEE and ZigBee Alliance	0.25 Mbps	› Mesh network › Large ecosystem support
Z-Wave	900 MHz / Licensed	Home Automation	Proprietary	0.04 Mbps	› Short range and low data rate limit smart home usage › Problematic frequency band (cellular interference) Large ecosystem support
Wi-Fi	2.4 GHz, 3.6 GHz, 5 GHz / Country Dependent	Home Networking	IEEE and Wi-Fi Alliance	54 Mbps (802.11a/g), 300 Mbps - 600 Mbps (802.11n)	› High power consumption › Large installed base Does not require separate gateway
Bluetooth Low Energy	2.4 GHz / Unlicensed	Accessories	IEEE and Bluetooth SIG	1 Mbps	› Low cost, low energy consumption › Short-range limits smart home usage
ONE NET	868 MHz, 915 MHz / Unlicensed	Wireless Personal Area Networks	Open Source	0.23 Mbps	› Small installed base › Limited ecosystem support
DECT ULE	1.7 GHz - 1.9 GHz / Licensed	Cordless Phones and Data	ETSI	1 Mbps	› Very low power consumptioin, long battery life › Large installed base, low cost › Does not require separate gateway

Figure 3 The large number of networking technologies available for the smart home has made cohesion around any one of them difficult. Data courtesy Gartner.

around a long time, although ZigBee and Z-Wave are now recognized as the way forward," O'Donovan continues. My prediction is that the winner will always be a widely available, standards-based solution, and in that case ZigBee should dominate."

Though ZigBee has gained traction since being conceived in the late '90s, much of its success and market adoption came as a result of "application profiles" that tailored the technology to certain vertical markets. While these helped ZigBee penetrate new areas and use cases, they also impaired the ability of devices based on different profiles to interoperate seamlessly, which, as mentioned, is a critical consideration in full-blow smart home deployments.

However, in late 2014 the ZigBee Alliance announced the release of ZigBee 3.0, a new standard that unifies the previous ZigBee PRO-based application standards to enable interoperability between home automation, energy management, lighting, appliances, security, health care monitoring, and other smart home devices (Figure 4). Based on the IEEE 802.15.4 standard, ZigBee devices were previously compatible at lower levels of the network, but the advent of ZigBee 3.0 promotes interoperability at the application layer as well to alleviate some of the challenges of device-level interoperability.

"Certainly, interoperability is a key concern because consumers must have easy-to-use and easy-to-connect devices that simply work together," Maley says. "ZigBee 3.0 will allow a wider range of devices to seamlessly interoperate. ZigBee has always provided interoperability among the various domains (lighting, health care), but ZigBee 3.0 will permit a wider variety of devices to connect together, which should simplify the choice for product developers and consumers alike.

"The ZigBee Certified program can help by insuring interoperability between certified devices regardless of the manufacturer," he adds.

With ZigBee 3.0, all of the traditional characteristics of ZigBee devices are maintained, such as the self-healing capabilities associated with mesh networks and power consumption several orders of magnitude less than Wi-Fi, as well as features such as Green Power that support battery-less energy harvesting devices. This last point on power is also a crucial one for the smart home, on the one hand because improved efficiency in one area shouldn't come at the expense of inefficiency in another, and on the other hand the prospect of changing batteries for a house full of connected devices on a regular basis is simply a non starter in the consumer world.

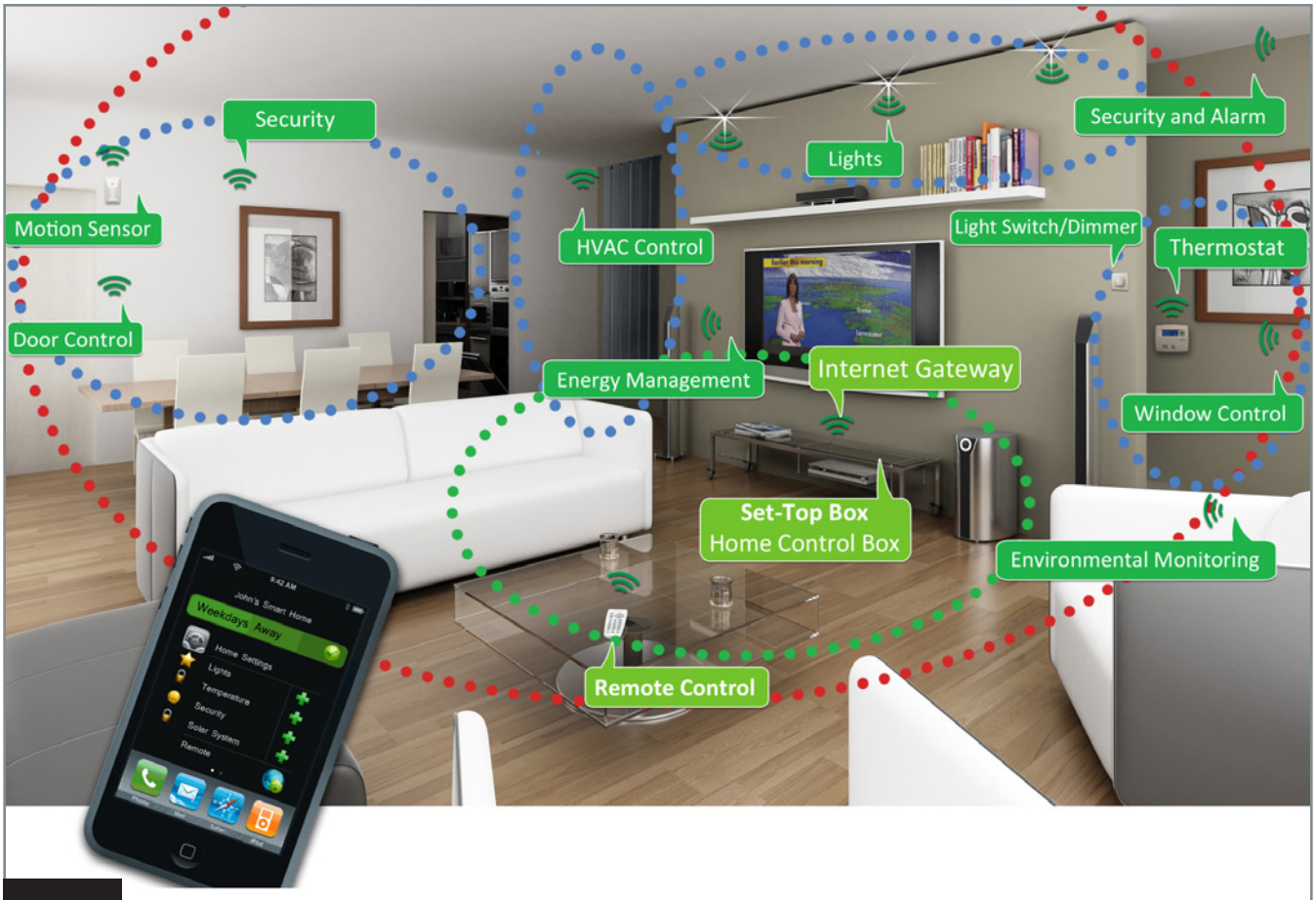


Figure 4 ZigBee 3.0 unifies the various application profiles defined in ZigBee PRO to improve device-level interoperability for the smart home.

Cost and the "killer app"

As intriguing as application-level standardization is for the advancement of the smart home, architectures that make beneficial decisions based on behavior and efficiency being embraced by the broad market is a question of cost and consumer demand. As O'Donovan notes, "costs are important if you have to pay $1,500 for new lighting that will only save you $50 in energy costs. There has to be a compelling reason to buy into the smart home concept."

On the heels of recent discussions in the California legislature related to regulating the standby power requirements for set-top boxes[1], Cees Links, Founder and CEO of leading ZigBee chipset and module vendor GreenPeak Technologies (www.greanpeak.com), believes an answer to both is on the horizon (Figure 5).

"Volumes drive down cost, lower costs drive up volume," Links says. "The only question is, "What does it take to kick-start the process? The killer app. From a GreenPeak perspective, we see the killer app as having ZigBee in the set-top box and remote control," Links continues. "First of all, consumers have a better user experience with ZigBee compared to IR, but [because of the power benefits] operators see a drop in service cost – one out of four service calls to operators is actually about the battery in the remote control being dead. So with ZigBee in the remote control the cable operator wins twice: reducing service calls and cost. Plus, with ZigBee in every set-top box it allows the subscriber to connect other sensors or applications with the set-top box, enabling incremental services.

For Links, full-fledged adoption of the smart home and its accompanying technologies will progress in the same way that Wi-Fi technology did, with roughly 10 years of cost reductions and cultural breakthroughs before reaching the nearly universal acceptance it enjoys today. Along with progressive reductions in the cost of the technology and success educating the population, however, the achievements of Wi-Fi are largely based in joint industry collaboration around the standard that eventually benefitted all parties involved.

"Cost and culture are the two major constraints," Links says. "Assuming that the cost will decrease with the volume increase, the key will be getting people comfortable with living in a smart home. That means there need to be guarantees that the system is secure, that the system is not infringing on privacy, etc. But to a large extent this is not technology, but a marketing challenge that needs to be resolved in the coming years.

"Also, the industry needs to come together on a set of standards to ensure interoperability and ease of use for the end user. It was the international adoption of 802.11 that truly enabled the eventual market success of Wi-Fi. The industry needs to learn from the Wi-Fi history. The big tech companies need to stop building tech silos designed to fight for market share, and instead realize the more the sectors work together to ensure interoperability, partnership, and customer ease of use, the more successful all tech companies will be," he continues. "With the ZigBee 3.0 unified communication standard in place, smart home applications should not be more costly or complex for the end user than a smartphone. This is when the smart home becomes reality for both vendors and consumers." ECD

CES 2015 Announcement - GP691 Chip and Module

- New chip - GP691 with full ZigBee PRO support
  - Green Peak GP691 communication chip optimized for the Smart Home
  - Optimized for advanced yet low cost ZigBee PRO applications
    - Supports all ZigBee application profiles
      - Smart Energy, ZHA 1.2 and ZLL 1.0
      - Also support ZigBee Green Power
    - 248k Flash and 16k RAM memory- 40-pin footprint
    - 2.4 GHz radio with worldwide approval
  - Also available in module version (GPM6000)
    - Small size (25x17x2.5mm), can easily be integrated
    - Pre-certified with additional Power Stage/Amplifier (+20 dB)
    - Integrated antenna with connector for second antenna (diversity)
  - Differentiation
    - Full home coverage enabling ease of installation
    - Most efficient power consumption for both transmit and receive
    - Patented Antenna Diversity enables superior range and WiFi/Bluetooth interference rejection
  - Ready to support ZigBee 3.0 and Thread

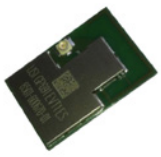


Figure 5 The GreenPeak Technologies' GP691 communications chip and GPM6000 support the ZigBee 3.0 standard and are well-suited for deployment in the smart home.

References

[1] National Cable & Telecommunications Association. "Amendment No. 1 to the Voluntary Agreement for Ongoing Improvement to the Energy Efficiency of Set-Top Boxes." https://www.ncta.com/sites/prod/files/VOLUNTARY-AGREEMENT-ENERGY-EFFICIENCY-OF-SET-TOP-BOXES.pdf

Developing exemplary smart cities for a smarter world

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

As cities grow and the world barrels toward urbanization, it's important to stay smart about city planning. It's estimated that $10 trillion in investments will be needed for urban infrastructure by 2025. The Institute of Electrical and Electronics Engineers (IEEE) is working to help municipalities address urbanization and integrate technology to create smart cities in its Smart Cities Initiative (SCI).

"IEEE SCI works to bring together technology, government, and society in order to foster the creation of sustainable environments that reduce environmental impacts and offer citizens a higher quality of life," says Gilles Betis, Chair of the IEEE SCI. "In working with our first round of cities, we will garner actionable knowledge that's not just technology based, but that also demonstrates how to best build effective collaboration and cohesion amongst all parties involved in smart initiatives. The lessons learned will be applicable across a wide range of cities striving to create a functioning smart city."

Building the first smart city

Guadalajara, Mexico is the first of 10 planned municipalities participating in the IEEE SCI, which launched in March 2014, followed by Wuxi, China, and Trento, Italy. The IEEE initiative enables these cities to collaborate with each other and world-renowned smart city builders and experts in addition to drawing on a pool of knowledge from IEEE volunteers.

The culture-rich, historic city center of Guadalajara with surrounding universities and a high-tech community has a lot to offer, and the city's size – 1.5 million inhabitants and 2.7 million in the metro area – and projected growth make it a good target for the SCI.

"City leaders and Mexican government officials have been fully supportive of the project, and they see it as a test bed to develop best practices and a pool of talent that can be used in cities throughout Mexico," Betis says.

Guadalajara has already started the Ciudad Creativa Digital (CCD) campaign to drive the smart city transformation and become a global center of digital media creation. To create a Smart City of Guadalajara, city and national leaders are embracing IoT, smart grid, e-health, augmented reality, and other technologies to improve and revolutionize the city.

"For Guadalajara, we hope our support of the CCD will assist in the creation of a high-quality, socially integrated urban environment that attracts employers in advertising, gaming, movies, television, and related fields," Betis says. "It is hoped this project will generate more than 20,000 high-tech jobs, stimulate many millions of dollars of investment in the state of Jalisco, and raise Guadalajara to another level of competition. According to ProMéxico, a government agency that seeks to strengthen Mexico's role in the international economy, the project will generate US $10 billion of investment in Guadalajara over the next 5 to 10 years."

A smart grid for a smart base

Of all the systems at play in an urban environment, Betis says improving the energy sector is key to avoid straining the underlying infrastructure and supporting new smart initiatives.

"All supporting systems are ultimately tied to creating a smart grid and realizing the benefits it brings about," Betis says. "Smart cities can only exist with the support of smart grids in a symbiotic way where they share electronics, telecommunications, and information technologies to leverage smart initiatives across all the other areas involved in developing a smart city."

One example of how the smart grid can help city infrastructure as a whole can be seen through water utilities.

"Water utilities are typically one of the largest consumers of energy in a city," Betis says, "yet savings can be achieved by coordinating with the electric utility and shifting water pumping to non-peak hours. The water utility reduces its energy consumption and lowers its costs while, at the same time, lessening the demand on the electric utility so that it can provide for more critical and less flexible functions (such as hospitals) to maintain an uninterrupted energy supply."

In addition to other utilities, transportation can gain from a citywide smart grid by interactively managing electric trains' power consumption through better acceleration and braking while still staying on schedule. Building owners and the public can also benefit by participating in demand response programs that lower energy consumption and increase their utilities' efficiency.

Engineering a smart city

Smart grids are just getting started out in the real world, and embedded engineers have an important role in making efficient systems for smart cities.

"Embedded engineering plays a key role by allowing for modernization of power systems through self-healing designs, automation, remote monitoring and control, and the establishment of microgrids," Betis says. "Once these things are accomplished within a smart grid, other municipal systems benefit as well. So, embedded engineering and, for that matter, a wide span of Internet of Things (IoT) technologies are essential for smart grids to deliver resilient energy while improving efficiencies and enabling coordination between city infrastructure and operators. Energy, water, transportation, public health and safety, and other aspects of a smart city will rely to a great extent on embedded and IoT technologies to manage and support the smooth operation of critical infrastructure."

Though development in IoT and smart grid technology is advancing, there are still many engineering challenges ahead on the road to creating smart cities.

"One of the key challenge areas for core technology development and ongoing research will be energy storage," Betis says. "This is really important because overcoming these hurdles will allow for the storage of distributed energy sources, something that has been an issue up until now. For example, with windmills people have pointed out that excess energy is often wasted because there is no means to sell it, store it, or inject it into the grid. Advancements in large energy storage mechanisms, as well as increased individual low-scale storage capabilities, will open a lot of different options for how energy can be used and shared within a smart city. Additionally, having a stable system is essential for energy storage and the technical complexities of these systems rely on embedded technologies. Such a system needs to be carefully assessed and built out using accepted standards."

The IEEE Standards Association (IEEE-SA) is providing a platform for global, open development of standards to aid in the success and scalability of smart cities, with current work on creating an IoT architectural framework for cross-domain interaction, interoperability, and compatibility. ECD

For more coverage on smart energy visit embedded-computing.com/topics/smart-energy

MORE ON... Smart Energy

BLOG
GreenPeak and ZigBee open doors to the smart home
By Brandon Lewis, Assistant Managing Editor
opsy.st/GreenPeakZigBee

BLOG
Let them drink beer, or try ultrasonic meters
By David Andeen, Maxim Integrated
opsy.st/UltrasonicMeters

ARTICLE
Greener power requires smarter grids
By Markus Staeblein and Kripa Venkat, Texas Instruments
opsy.st/GreenerPowerTI

ARTICLE
Integrating wired and wireless outdoor lighting control in smart cities
By Sanjay Manney and Vijay Dhingra, Echelon Corporation
opsy.st/LightingControlEchelon

E-CAST
Five ways the Industrial Internet will change the oil and gas industry
Presented by RTI
opsy.st/IndIntOilGas

Fanless thin client for industrial applications

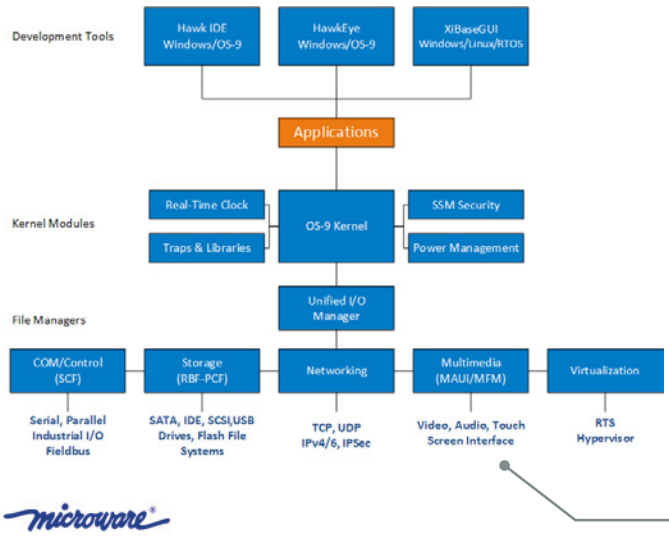
The ML210G-10-TR from Logic Supply combines a custom-engineered, hardened fanless enclosure with an industrially focused I/O to create a unique thin client hardware solution. Certified by leading thin client management software provider ACP to be ThinManager-Ready, the system comes pre-installed with ACP-enabled BIOS to provide an economical and reliable virtualization solution. The thin client supports system shadowing, MultiSession, dual display, and integration with Cirtrix and VMware, and has been designed to reduce downtime and simplify installation and maintenance. Featuring an Intel J1900 Celeron processor, the system uses less than 20 watts total while still providing power needed for advanced industrial applications. The ML210G-10-TR is designed to thrive in harsh environments. The fanless and ventless enclosure prevents damage from dust and other airborne contaminants while advanced fanless cooling enables the system to reliably operate in temperatures ranging from 0 °C to 50 °C.

Logic Supply | www.logicsupply.com
embedded-computing.com/p372596

Touch panel PC for smart building management

The LYNC-708 Touch Panel PC is designed for smart building management and helps manage security, energy, parking and other smart systems. The PC is powered by an Intel Atom N2600 processor and features an 8" touch screen with a flexible modular design that can be integrated into office buildings, commercial complexes, and school campuses. The LYNC-708 lowers management costs by integrating a building system and its equipment and by providing a platform for monitoring and control. Building systems and equipment are integrated in one place, including surveillance, ventilation, air conditioning, fire detectors and alarm, lighting, parking deck systems, elevators and escalators, and various energy management systems.

ARBOR Technology | us.arborsolution.com
embedded-computing.com/p372597



Real-time operating system available for Raspberry Pi

Microware LP announced that the OS-9 real-time operating system has been ported and is running on the Raspberry Pi board. OS-9 is an embedded real-time operating system with a Linux API and modular architecture – all components are implemented as separate code modules with CRCs that provides the ability to dynamically download and upgrade kernel components without requiring downtime. The CRC also provides added security against software threats. OS-9 also provides a variety of connectivity, device, and graphics I/O along with a Java virtual machine.

Microware LP | www.microware.com
embedded-computing.com/p372598

Embedded TechCon™

#EmbeddedTechCon

June 9-10, 2015

Moscone Center
San Francisco, CA

David **Kleidermacher**
Chief Security Officer,
BlackBerry

Jean **Labrosse**
Founder/President/
CEO, Micrium

Bill **Gatliff**
Renowned
Industry Expert

RC **Cofer**
Field Applications
Engineer, Avnet

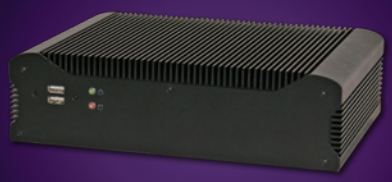
Embedded TechCon, designed to educate today's design engineers in the most critical embedded product and technologies, will be held at the Moscone Center in San Francisco, Calif., on June 9-10, 2015. The live event extends OpenSystems Media's current online educational program, Embedded University. The classes, which will be taught by leading industry experts, will cover key embedded topics like IoT, automotive, and security, while drawing from the industry's roots with topics like firmware development, debugging, and open source hardware and software.

CLASSES, SPEAKERS, SCHEDULES, AND MORE AT:

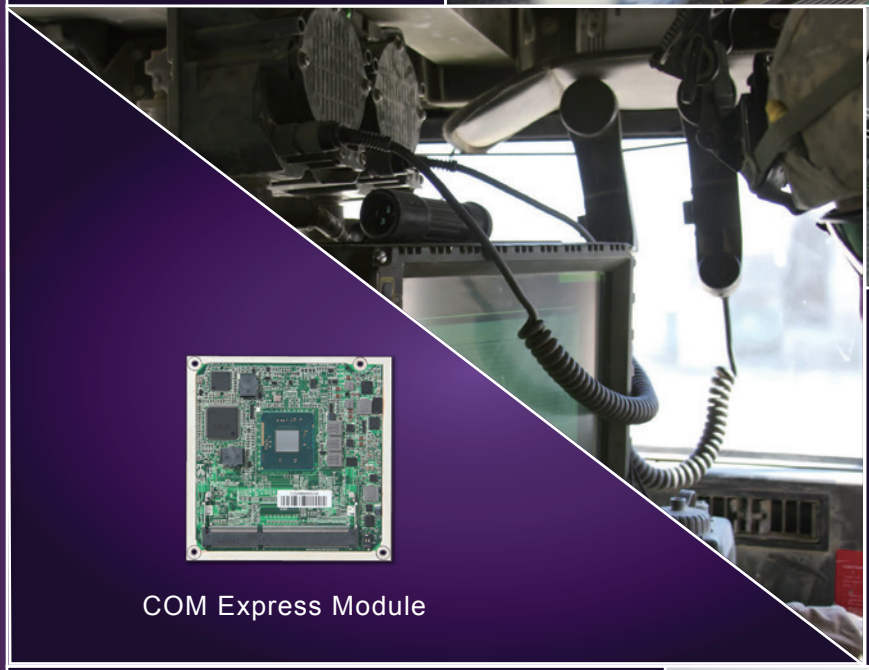
embeddedtechcon.com

Portwell Empowers Intelligent Solutions

Mini-ITX

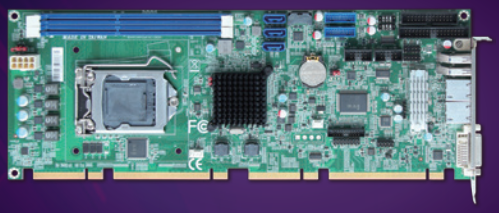


Small Form Factor System



COM Express Module

Network Security Appliance



PICMG SBC

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

Portwell

intel IoT Solutions Alliance Premier