Embedded Memories Destined for IoT Seek Security/Power Management Balance

Smart Meters Embrace IoT Role

Europe’s Take on the IoT

www.EmbeddedSystemsEngineering.com
Resolving the Technical and Business Challenges of Getting Connected to the Internet of Things

Two full days of keynotes, training sessions and panel discussions. Topics covered include:

- Understanding and managing security-related issues
- Designing ultra-low power IoT nodes
- Exploring connectivity protocols and industry standards
- Harnessing the data explosion – the evolution of hubs and cloud
- Utilizing software development environments for M2M applications
- Making money with the Internet of Things
- How IoT technology will effect business and product development
- The future of what IoT will bring

Plan now. Come to the Internet of Things Developers Conference 2015!

IoT-devcon.com
Introducing Zilog’s Z8 Encore! XP F6482 Series of Flash Microcontrollers!

Based on Zilog’s advanced 8-bit eZ8 CPU core, these MCUs support 1.8 V to 3.6 V low-voltage operation with extremely low Active, Halt, and Stop Mode currents.

**FEATURES:**
- 24MHz eZ8 CPU core
- 16KB, 32KB, 60KB or 64KB Flash memory
- 2KB or 3.75KB internal RAM
- Two Enhanced Serial Peripheral Interface (SPI) controllers
- 16-bit controller which supports Master/Slave modes
- Watchdog Timer (WDT)
- 32-, 44-, 64-, and 80-pin packages
- -40°C to +85°C (extended) operating temperature range
- And many more!

**APPLICATIONS:**
- Battery Powered Sensors
- Wired/Wireless Keypads
- PIR Motion Detection
- Lighting Control
- Safety and Security
- Utility Metering
- Digital Power Supervisory
- Hand Held Electronics
- Wireless Controller
- LCD Keypads

The **F6482 Series Development Kit** is a complete development solution containing the following tools:

- F6482 Series Development Board
- USB SmartCable (for connecting the PC to the F6482 Series Development Board)
- USB A to Mini B cable
- RS-232 interface module

For more information about the F6482 Series, or to download product collateral and software, please visit [www.zilog.com](http://www.zilog.com).
4-in-1 Systems in these “Shoebox” Network Appliances

These two system examples showcase the incredible functionality that’s—ahem!—shoehorned into pre-packaged embedded systems.

Chris A. Ciufo, Editor

Within two weeks of each other, two pre-packaged embedded systems press releases rang the “Ah-ha!” bell. Both were deceptive, in a good way, because the products listed offered more functionality than what you’d first expect. The QNAP vNAS TVS-x63+ and Elma D50G-1 are perfect examples of how pre-packaged “shoebox” embedded systems offer high-density, cutting-edge technology.

QNAP VNAS STORAGE WITH PC

What strikes me about QNAP’s Turbo vNAS TVS-x63+ isn’t how much I wish my SOHO/SMB had this multi-slot network attached storage (NAS) box to replace my USB external drives: any good NAS would do that. Instead, this 10GigE NAS uses AMD’s 2.4 GHz quad core Embedded G-Series SoC (“Steppe Eagle”) with hardware encryption and ATI Radeon GPU plus I/O all on the same die. It’s a highly integrated x86 SoC with gaming-quality HD 8000 series GPU that AMD announced in 2013, promised in Q4 2014 and is delivering on-time: a neat feat for such a complex 32-bit SoC.

AMD says its 32-bit Jaguar CPU core outperforms Intel’s Bay Trail Atom with embedded graphics engine at video jobs such as 1080p source transcoding to 720p or 4K down conversion to 1080p. The “prosumer” (mid-range price point) QNAP vNAS stores lots of files, can act as a full-featured server functions at 400 MB/s throughput plus 256-bit AES for secure network recording and playback. The G-series APU can also handle server functions at 400 MB/s throughput plus 256-bit AES for secure network recording and playback. With this much processing and I/O, QNAP’s vNAS stores up to 192 TB of what’s now actionable and viewable data.

ELMA’S FIRST COTS SYSTEM

Elma Electronic’s S50G-1 “Complete Vehicular Mission System” is its first COTS-based catalog embedded system, complete with CPU, I/O, software and Wi-Fi antennae. But the company’s S50G-1 “Complete Vehicular Mission System” is the company’s first COTS-based catalog embedded system, complete with CPU, I/O, software and even Wi-Fi antennae. Designed for -40 °C to +85 °C passive cooling in high shock/vibration vehicles, the rugged shoebox is a complete mission computer that can be equipped with CANbus and Cisco IOS routing software. In this configuration, the box becomes a mobile ad hoc battlefield network router, alleviating the need for a tactical operations center (TOC) trailer or mombo (aka heavy) 19-inch rack in a HMMWV.

Inside the box is a Type 6 COM Express carrier and Intel Haswell (4th Gen) Core i5 SBC (rumored to be from ADLINK), miniPCIe modules (presumably for the radios and CANbus) and PMC/XMC I/O. In this three-card stack the cards are equipped with PCIe stack-through connectors à la PCIe/104. Cisco’s certified IOS routing software is available, shrinking an enterprise wiring closet down to this small Elma box.

While we’ve written extensively about Intel’s 4th Gen CPUs, ADLINK’s COM Express boards, Cisco’s IOS (and 5915 hardware) and Elma’s metal-bending expertise, putting all four under one shell is new. We’re thrilled to see Elma Electronic become a provider of prepackaged rugged shoeboxes.
500+ Million People rely on Toradex everyday

Free Premium Support  Local Warehouses

ARM® Computer on Modules: Small Size. Big Performance!

Powered by: • NVIDIA® Tegra™ • Freescale® Vybrid™ / i.MX 6 • Marvell® PXA

Apolis

Colibri

Starting from $75

Starting from $24

High Performance  Low Power  Fast Boot  Direct Support  Extensive Ecosystem  Long Lifecycle
In this issue

Contents

Embedded Systems Engineering

Features

Is My Holodeck Ready? Digital Signage Looks to Optical Phased Array
By Allen Marks, Advanced Innovative Solutions 6

Hardware/Software Planets Align with Hardware Emulation
By Lauro Rizzatti, Verification Consultant 10

Departments

From the Editor 2

Iot & M2M

Europe’s Take on the IoT
By Caroline Hayes, Senior Editor 12

Vendor Spotlight: VDC Research on ADLINK [Advertorial]
By ADLINK Technology Inc. 14

Making the Transition to 4G LTE [Advertorial]
By Symmetry Electronics Corp. 16

Cover Story
Embedded Memories Destined for IoT
Seek Security/Power Management Balance
By Bernd Stamme, Kilopass Technology 18

The IoT and RTOS Reinvention
By Thom Denholm, Datalight 20

Reconfigurable Image Sensors Make Imagination the only Limit for Innovative IoT Use
By Shawn Maloney, Forza Silicon and Kambiz Khalilian, Lattice Semiconductor 23

Product Showcases

Boards & Modules
 Wired, Wireless, Hybrid
GainSpan Corporation 25

Smart Energy

Secure Smart Meters Enable Smart Choices
By Jesus Teijeiro, Atmel 27

Smarter Energy: Meters Embrace Their Critical IoT Role
By Olivier Monnier, Texas Instruments, Inc. 30

It’s Smart to Communicate
By Caroline Hayes, Senior Editor 31

Product Showcases

Boards & Modules
 Network/Communication
Zilog, Inc. 33

Embedded Security

Deep Verification Defends Embedded Components’ Safety and Security
By David Kelf, OneSpin Solutions 34

Security and the IoT: A Q&A with Rambus
By Anne Fisher, Managing Editor 36

Virtual Prototyping and the IoT: A Q&A with Carbon Design Systems
By Anne Fisher, Managing Editor 38

IP-centric LTE Spotlights Security Risks: Devices, Access, Core Elements and Services
By Robin Kent, Adax 39

Attend the 2015 Internet of Things Developers Conference! www.iot-devcon.com

Internet of Things Developers Conference
May 6-7, 2015 — Hotel Regency — Santa Clara, CA

February 2015
Zilog’s Z8051 Product Family

Advantages:
- High-Performance, Low-Cost Architecture
- Industry-Standard 8051-Compatible Core
- Industry-Wide Popularity
- Numerous Third-Party Tools Available
- Zilog’s Continuing Commitment to Supporting Our Customers

Meet the members of Zilog’s Z8051 Product Family:

<table>
<thead>
<tr>
<th>Model</th>
<th>Flash Memory</th>
<th>RAM Memory</th>
<th>Package Size</th>
<th>Pin Count</th>
<th>Package Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z51F0410HCX</td>
<td>4KB Flash</td>
<td>256 bytes RAM</td>
<td>10 pin SSOP</td>
<td>LF</td>
<td></td>
</tr>
<tr>
<td>Z51F0811RFX</td>
<td>8KB Flash</td>
<td>512 bytes RAM</td>
<td>16-pin TSSOP</td>
<td>LF</td>
<td></td>
</tr>
<tr>
<td>Z51F3220SKX</td>
<td>LCD, 32KB Flash</td>
<td>1K bytes RAM</td>
<td>32-pin SOP</td>
<td>LF</td>
<td></td>
</tr>
<tr>
<td>Z51F3221ARX</td>
<td>LCD, 32KB Flash</td>
<td>1.25K bytes RAM</td>
<td>64-pin LQFP</td>
<td>LF</td>
<td></td>
</tr>
<tr>
<td>Z51F6412ARX</td>
<td>64KB Flash</td>
<td>3.25K bytes RAM</td>
<td>80-pin LQFP</td>
<td>LF</td>
<td></td>
</tr>
<tr>
<td>Z51F6412ATX</td>
<td>64KB Flash</td>
<td>3.25K bytes RAM</td>
<td>80-pin LQFP</td>
<td>LF</td>
<td></td>
</tr>
</tbody>
</table>

These powerful microcontrollers provide a highly flexible and cost-effective solution to many embedded control applications, including:

- Electronic Locks
- Keyless Entry Systems
- Battery Management
- LED Lighting Control
- Motor Control
- Digital Clocks/Watches

And much more … your design possibilities are endless!

For more information about our Z8051 Product Family, please visit www.zilog.com.
Is My Holodeck Ready? Digital Signage Looks to Optical Phased Array

Light projection and display technology developments are already revolutionizing digital signage and POS along with our smartphones and tablets, now Optical Phased Array (OPA) technology could take us closer to making a Holodeck or “cloaking” device science fact, not fiction.

By Allen Marks, Advanced Innovative Solutions

New technology on the horizon, Optical Phased Array (OPA), will revolutionize how we communicate and display information, and may be just the thing to bring a Holodeck and/or ‘cloaking’ device to a store near you....

The developments that could lead to a Holodeck are part of an extraordinary evolution taking place right now in light projection and display technology. Historically, the first projectors used a bright light source to illuminate an image (either directly through a translucent film or reflected off a surface) and then used optical lenses to magnify and focus the image on a target screen.

Milestones along the way have included:

- Cathode Ray Tube—scans and illuminates a phosphor with an x-y Matrix of elements creating an image that is directly viewed
- Light beams—reflected or refracted by mirrors and lenses to display the image on a surface
- Direct viewable flat screens—made up of a matrix of microscopic pixel elements
- Variations of single-gun and 3-gun projectors, LCD projects and displays, and TI’s DLP technology
- The latest new iteration, the Optical Phased Array (OPA) display/projector

Along the way, display technology has evolved from simple light sources to complex light sources, which utilize miniature phosphors, LEDs, LCDs, and lasers. All of this required sophisticated engineering involving mechanical and optical principals and devices to simulate and achieve the desired image. Now this has been transcended by a trend that uses physical devices and technologies evolving to the use of semiconductors.

Scientists at Caltech, MIT, Ghent University (and others) report the design and demonstration of light-bending silicon chips that have projected simple images (like triangles, letters and smiley faces) in infrared red using Optical Phased Arrays. Note: More on this in a moment...

Phased Array Optics is actually the use of nanometer Spatial Light Modulators built for general manipulation of light. This new technology can support ‘single-point and scan,’ ‘multi-point and scan,’ and ‘matrix array scan.’ It is not only capable of steering light, but also capable of modulating light color and brightness!

Although the concept of such “phased arrays” of antennas (in which the peaks and troughs of a wave from each antenna are combined to send the signal in a particular direction) goes back to the early 20th century for radio waves, these optical wavelengths are so much smaller than radio wavelengths, the devices have to be fabricated with very high accuracy, at nanometer scales.

CURRENT ENVIRONMENT

Traditional projectors, like those used to project a film or classroom lecture notes, pass light through an image, using lenses to map each point of the picture to corresponding, yet expanded, points on a large screen. But now, this is possible by steering light through a mash-up of coherent laser light and sophisticated semiconductor technology.

The engineering challenge has always been to replace a mechanical or electro/optical-mechanical device with a semiconductor solution. In the evolution of semiconductor technologies, there have been many instances of physical devices being replaced with solid-state devices, as:

- Vacuum tubes and relays became transistors
- Large multi-component amplifiers became single integrated circuits
- Movies evolved from film to CRTs to projectors to LCD/LED displays
- Computer systems became single board and single chip computers
- LEDs (light sources) from quantum effects rather than Joule heating
• Light Valves LCDs that open and close ‘optical valves,’ not plumbing

• Digital micro-mirrors that reflect, without motors or actuators

OPA is a technology on the cutting edge. It has been theorized and demonstrated in laboratories. Current OPA technology has demonstrated the ability to create static images and a few small matrices of dynamic images. As the technology progresses, manufacturers can now be created to create very large and efficient devices capable of projecting on, or covering very large surfaces (such as what a holodeck would require).

The OPA device will revolutionize the projector industry. The chips will be a few square millimeters, as opposed to the bulky projectors that use large and expensive lenses, hot light sources, prisms, and mirrors, along with moving parts. But with OPA all that can now be created in a single semiconductor substrate with NO moving parts!

WHAT IS OPA?

To understand Optical Phased Arrays, we first need to understand phased array optics (PAO). PAO is the technology of controlling the phase of light waves transmitted or reflected from a two-dimensional surface by means of adjustable surface elements. It is the optical analogue of ‘phased array radar.’ By dynamically controlling the optical properties of a surface on a microscopic scale, it is possible to steer the direction of light beams, or the view direction of sensors, without any moving parts.

Hardware associated with beam steering applications is commonly called an OPA. Phased array beam steering has been used for optical switching and multiplexing in optoelectronic devices, and for aiming laser beams on a macroscopic scale for many years. Complicated patterns of phase variation can be used to produce diffractive optical elements, such as dynamic virtual lenses, used for beam focusing or splitting, in addition to directional aiming. Dynamic phase variation can also produce real-time holograms.

An OPA is a ‘solid-state’ device capable of altering the phase and amplitude of light on scales smaller than a wavelength over large areas of addressable control, and will be capable of 3D imaging without ANY of the undesirable effects of current 3D technologies such as diffraction, which causes blurring, ghosting, or false images.

WORK AT CALTECH

Ali Hajimiri, Thomas G. Myers Professor of Electrical Engineering, in concert with other researchers at the California Institute of Technology (Caltech) laboratory has successfully fabricated a 64 by 64 optical phased array. Each array is 3 micrometers on a side, or covering 4096-element array constitutes a single semiconductor pixel element, which is manipulated to draw an image, sourced by laser light!

If two waves are coherent in the direction of propagation—meaning that the peaks and troughs of one wave are exactly aligned with those of the second wave—the waves combine, resulting in one wave, or a beam with twice the amplitude and four times the energy as the initial wave, moving in the direction of the coherent waves. The elements in the researchers’ chips have been made to manipulate the coherent light slightly out of phase, producing interference patterns.

WORK AT MIT

In another development, at the Photonic Microsystems Group at MIT, Jie Sun, a graduate student, and Michael Watts, an associate professor of electrical engineering, working with silicon, have successfully fabricated a 64 by 64 optical-phased array. Each array is 3 micrometers long, 2.8 μm wide, and 0.22 μm thick and fits in a 0.33-square-millimeter area. The 4096-element array constitutes a single pixel element, which is manipulated to draw an image, sourced by laser light!

The challenge will be in building and controlling arrays in a sufficiently large area to build a holographic display. Imagine that such a device, a square meter in size, would contain 4 trillion pixels.
The MIT example uses fixed phase shifts to produce its images of the MIT logo. The individual elements are not turned on and off as the pixels are in a LCD or LED, but rather all of the elements emit light, and the interference of the individual phase-shifted beams produces a detailed image.

HOW THE OPA WORKS

An OPA provides the ability to change the direction of the light beam by simply changing the relative timing of light waves. By using a series 'light pipes,' called phase shifters, the OPA chip slows down or speeds up the timing of the waves, enabling it to control the direction of the light beam. As mentioned earlier, two light waves are coherent in the direction of propagation if the peaks and troughs of one wave are exactly aligned with those of the second wave. Coherent waves combine in amplitude, so instead of two separate waves, there is now one beam with twice the amplitude and four times the energy as the initial wave, moving in the direction of the coherent waves.

The process starts with an image, sent from a computer and converted into multiple electrical signals of various currents. This is achieved by applying stronger or weaker currents to the light within the phase shifter, which changes the number of electrons within each light path, which, in turn, changes the timing of the light wave in that path. The synchronized 'timed light' is delivered through tiny array elements within a grid on the chip, with each element projecting light. The grid coherently combines each element of the array in the air to form a single beam and a spot on the screen! The images are formed in 2D because the signal is phase-shifted in both the X and Y directions. The out-of-phase light waves interfere with one another, reinforcing each other in some directions but annihilating each other in others. The result is a light source that doesn't move, but can project a beam in any direction.

As the electronic signal rapidly steers the beam left, right, up, and down, the light acts as a very fast pen, drawing an image made of light on the projection surface. Because the direction of the light beam is controlled electronically, not mechanically, it quickly draws a line image. Since the light draws many times per second, the eye sees the process as a single image instead of a moving light beam. This beam is electronically controlled, and moves extremely fast on a projected surface, which gives the impression that the image is projected as a whole, when in reality an individual point of light is moving so fast your eyes can't tell the difference.

Steering a beam of light like a pen is not new. There are many laser projectors used in entertainment that use single, discrete laser diodes, and mirrors to draw very bright images. But these devices are very large, bulky, and slow; and will not be as effective as an OPA will be. The beauty of the new OPA technology is that these chips are small, can be made at a very low cost and have all the components integrated into one semiconductor device. Once that is a possibility, imagine an array of OPA emitters arranged in a large matrix—a matrix so large, it can cover a 10' x 10' wall.

“Computer, turn the Holodeck on!” (Application and Use Cases)

Nothing in science fiction books or movies will be beyond the reach of science and engineering. If it can be thought of by man, or invented for a movie, it someday may become a reality. OPA will make this science fantasy a reality.

For example, OPA will have a very large impact on mobile devices, especially on cell phones, because the technology is small, requires no moving parts, no mirrors, no lenses, and it can easily be fabricated in a multilevel semiconductor device.

A smartphone will naturally evolve into a mobile projector. Imagine giving a presentation that is projected on a conference room wall via your cell phone! Instead of a group crowding around to get a glimpse of an image on a cell phone—to view pictures, Tweets, YouTube videos, Facebook or other messages—it will have the capability to be shared with a whole room of people simultaneously. Your smartphone or tablet will be capable of projecting a bright, clear image onto a wall or a big screen, where there aren’t any displays or projectors.

When dealing with portable projection devices the challenges to overcome have been power and lumens. This technology solves the power problem based on the use of solid-state lasers in the same way the inexpensive laser pointers that produce an incredibly bright light use just three button batteries. The laser light source is just another layer in the layout of the semiconductor substrate. The entire package is likely to be integrated into a mobile phone, without adding any thickness.

... AND NOW “HOW TO BUILD A HOLODECK”

With the potential of creating 2D displays of any size, the idea of both 2D and 3D imaging stirs the imagination. Corning has presented a lot of ideas in its vision of
the future of glass. But Corning hasn’t yet addressed the semiconductor technology behind the glass. OPA is a technology that does.

First, imagine that all flat surfaces will become adaptive displays, becoming whatever 2D or 3D image you desire. Walls and windows made of OPA substrates will give the gift of virtual reality, window shades will be open or closed based on polarization. There will be direct 3D viewing on surfaces as well as 3D imaging projected into free space.

Real world applications will include the flexibility of adaptive environments such as cave and immersive technologies, as well as simulators, virtual games and virtual reality, virtual travel, and virtual collaboration spaces.

Another unique area of application will be invisibility or cloaking. (Klingons aren’t the only ones…) Invisibility can be simulated by having an object project whatever image is behind the object. This may only work when looking straight on, but I’ve got a hunch more is possible.

This all requires very high-resolution and extremely realistic imaging, especially in 3D. Such high-resolution arrays would permit three-dimensional image displays with no unwanted orders of diffraction, including invisibility cloak or optical camouflage. Using ‘e-textiles,’ the invisibility cloak can become a reality.

One final application example of OPA is the presentation of three-dimensional scenery indistinguishable from real life. Not a hologram, but rather 3D similar to the Star Trek Holodeck. A multiplexed OPA could act as a window into any 3D world that can be imagined, so real that it would be difficult to distinguish the image from reality.

This would make the Holodeck a reality. First with “holo” surfaces, then two walls, three walls, then six walls, and eventually, it will be similar to the AlloSphere. The AlloSphere is a display technology at the University of California, Santa Barbara (UCSB) that allows images to be displayed on the inside surface of a dome. It uses multiple digital projectors to synchronize and stabilize the image on the dome’s surface. In conjunction with 3D glasses, the images can be seen in 3D. By using this new technology, the AlloSphere can be 3D without the aid of glasses.

However, reality will set in when “moving” in this 3D simulation, since there is nothing to alert you before running into one of the walls. That’s something they will still have to work on.

[Editor’s Note: Allen Marks serves on the Digital Signage Expo Advisory Board and will be available at Digital Signage Expo 2015 on Tuesday, March 10 and Wednesday, March 11 at the Las Vegas Convention Center to discuss this topic. For more information about DSE or to register for this or any other educational seminar or workshop and learn about digital signage go to www.dse2015.com]

Allen Marks is the Principal Investigator at Advanced Innovation Solutions, a technology consulting firm. He is a consultant at Advanced Innovative Solutions and ITAV. He also provides IT leadership and technical support to several non-profit organizations, YMCA and several LAUSD schools. He is actively involved with the Boy Scouts of America (Troop 927, Thunderbird District, and LAAC) as a district commissioner and as an Eagle Scout Mentor. Marks has been a con-

tributor, advisor and board member for the Wireless Internet for Mobile Enterprise Consortium (WINMEC) at UCLA for seven years and to Frost and Sullivan’s Mobile and Wireless Enterprise for two years. He has served on the advisory board for the Digital Signage Expo (DSE) since 2010.

REFERENCES


http://www.caltech.edu/news/bending-light-tiny-chip-42252
http://www.phase-array.com/
http://www.allosphere.ucsb.edu
Hardware/Software Planets Align with Hardware Emulation

Hardware emulation that includes a hardware debugging environment can lower SoC development expense, as groups once as different as Mars and Venus team up.

By Lauro Rizzatti, Verification Consultant

It wasn’t all that long ago when hardware engineers and embedded software developers saw no common ground. It was all but the semiconductor world’s version of “Men are from Mars, Women are from Venus.”

While they may have been the same gender, worked for the same company and attended the same college in the same university, these developers and engineers were planets apart. Hardware and software groups were managed separately and worked in isolation, using different tools and methodologies. They spoke different languages, worked in different areas and didn’t understand the interactions between the two disciplines. Worse yet, neither was able to comprehend their debugging domains. They wasted valuable project time traveling between the two planets to identify and fix problems. Talk about wasted time travel!

That had to change as embedded design got more complex. At the same time, there was increasing emphasis on verifying that the systems’ embedded software and hardware would work together as the specification described. Change did come about as individual hardware and software groups became one project team and began verifying simultaneously the hardware and software portions of a system-on-chip (SoC) design—practicing what’s now known as hardware/software co-verification.

**NO TIME TO WAIT FOR WORKING SILICON**

The change happened with the move to hardware emulation and I credit it for aligning two disparate design planets. The hardware-assisted verification tool is able to find any kind of design bug—save analog since emulation requires a digital representation of the design—and can trace bugs across the software and the hardware platform.

It was an inevitable change, however, because the earlier that software development can begin, the more likely the embedded hardware will succeed. Programming software for embedded design can take longer than the chip design, and with unyielding time-to-market pressures project teams can’t wait for working silicon before starting software development.

An SoC design is rife with complexity. It includes embedded microprocessors, running operating systems, drivers and numerous applications with several millions of lines of code. The chip is comprised of logic blocks to accelerate processing of data, such as digital signal processing, image processing or packet identification and routing. The chip connects to peripherals and physical interfaces appropriate to its target application. Verifying each hardware block and validating the embedded software impose specific requirements on the tools and methodologies.

As for executing a vast amount of embedded software, the chip processor requires speed as billions...
of cycles are needed to obtain meaningful results. Embedded software development mandates the use of software debuggers. Logic blocks need accurate simulation with access to waveforms. Peripherals require accurate simulation as well to verify the interaction between device drivers and peripherals and the efficient transfer of data in and out of the chip.

In the past, hardware developers relied on hardware description language (HDL) simulators, great for hardware debug in the early stages of the design cycle when the design is at the block level. They haven’t kept pace and now run way too slowly on designs of tens or hundreds of million gates. Hardware emulation can handle designs of several hundreds of million gates or even a couple billion gates and provide the desired level of accuracy, speed and visibility.

Embedded software developers validated their code using instruction-set simulators (ISSs) that are not cycle-accurate and don’t support interfaces to custom register transfer level (RTL) blocks.

Transactors have eliminated much of these challenges and made hardware/software co-verification possible. By raising the level of abstraction of peripheral interfaces from the cycle/bit-level to the transaction level, transactors can simplify the description of data exchange between an SoC and its peripherals.

Hardware transactors are a viable alternative to the traditional in circuit emulation (ICE) driven by a target system. Unlike ICE, hardware transactors benefit from being controlled by software, which allows for a flexible and adaptable verification environment, impossible in ICE. They eliminate speed adapters, remove all hardware dependencies and run verification of corner cases at the same speed of execution of ICE, if not faster.

But transactors come with a string attached. They need a testbench in place of a target system. This was the case until Mentor Graphics introduced VirtuaLAB. VirtuaLAB is an innovation based on transactors that replaces the physical target system with a functionally equivalent virtual target system, i.e., a software implementation of ICE applications. Unlike hardware-verification testbenches that are not understood by software developers, VirtuaLAB allows for creating user scenarios and environments well understood by software designers.

Furthermore, VirtuaLAB supports multiple concurrent users without the massive burden of ICE hardware that such deployment would entail. Think of 20 software engineers accessing concurrently their DUTs, where each design would need its own target system and a set of ICE speed adapters. With VirtuaLAB, software-based virtual ICE target systems and interfaces would replace a bulky and impractical hardware setup.

With this approach, project teams can use hardware emulation remotely. Hardware emulation as a remote resource for R&D groups residing all over the globe is a trend welcomed by project teams. Emulation design data centers filled with emulation enter-

prise servers and a centralized team of experts can support a multitude of users in different geographies and time zones. The servers can manage any combination of small and large designs, up to more than one billion gates.

Hardware emulation includes a hardware debugging environment, which performs at close to the speed of a software development board and can be controlled in software. It’s also a software development environment that maximizes flexibility, analysis and reuse. It reduces the cost of developing SoCs and the two formerly disparate planets are able to work together with relative ease to debug SoC designs.

While it didn’t take a best-selling book to highlight the differences between hardware developers and embedded software designers, it seemed impossible that their two planets would ever orbit near each other. That changed with the accessibility of hardware emulation.

Dr. Lauro Rizzatti is a verification consultant. He was formerly general manager of EVE-USA and its vice president of marketing before Synopsys’ acquisition of EVE. Previously, he held positions in management, product marketing, technical marketing and engineering. He can be reached at lauro@rizzatti.com
Europe’s Take on the IoT

With 30 billion connected devices expected within five years and spanning automotive, consumer, medical, industrial, smart energy, wearables and more, the Internet of Things (IoT) may already be part of our vernacular, but it is certainly not standing still.

In Europe, companies are embracing the Internet of Things. As well as being the home of ARM, Europe is also the base for STMicroelectronics, among the first companies to boost connectivity and capability by adopting the ARM® Cortex®-M7 (Figure 1) in its goal for connected, smart devices. Imagination Technologies also offers an example of an enterprise anticipating the demands of the IoT, aka the Internet’s ‘third wave,’ with a low-power architecture.

At last year’s Embedded World conference in Nuremberg, Germany, countless booths declared support for the IoT’s many roles: Home automation, with lights and heating on when the home-owner chooses; factory automation, for efficient operation and communication across the plant floor; smart vehicles that protect, entertain and inform driver and passengers alike; and consumer health technology that will tell you, and anyone in your network, how many calories you have consumed and burned in a day or any other updates.

At Embedded World 2015 anticipation will increase again, as the level of connectivity and the volume of data around the IoT rise. This article looks at the industrial and consumer slant with which European companies are approaching the IoT.

ONTTO INTERNET 2025

The IoT has been described as the third phase of the Internet. Simona Jankowski, senior equity research analyst, Global Investment Research, Goldman Sachs, describes the three waves of the Internet: from a fixed desktop access, in the 1990s, linking one billion users; to the second wave of using mobile devices at the turn of the century to access the Internet, used by two billion users; and culminating with a tsunami wave of the IoT, connecting 20 to 30 billion devices to the Internet over the next 10 years.

For STMicroelectronics, the IoT is ubiquitous. Executive vice president and president of the company’s Greater China and South Asia region, Francois Guibert, describes the company’s IoT strategy as augmenting everyday objects to make them smart and connected. “STMicroelectronics sees the IoT as the next step in the natural progression of ‘smart’ features in electronic devices,” he said at the IoT Forum, Computex, in Taipei, Taiwan last year. He spoke of “products and technologies that include integrated smart systems with multiple sensors, processing and communication technologies.”

Laurent Vera, EMEA marketing director, STMicroelectronics, agrees. Adding a microcontroller to a connected device, a smartwatch, for example, he tells Embedded Systems Engineering, will mean that users can add new features by updating the firmware after the product enters the market.

Considering the infrastructure, energy meters, home automation and industrial, Vera also believes that the company’s adoption of the ARM® Cortex®-M7 in its STM32 F7 series of microcontrollers (Figure 2) will allow updates and upgrades to be made easily. The first microcontroller in the series is able to operate up to 105°C, with later F7 models expected to have a maximum operating temperature of 125°C for industrial applications. The low power consumption will also be significant here, says Vera, as utility meters rely on battery-based communications. Exploiting
the deep-sleep RAM and quick wake-up modes will keep information dynamic, he adds.

Connection to the network pushes the performance of the connected products, says Vera, with smart meters that have increased memory and data demands.

**POWER CONCERNS**

Consumer uses for the IoT require low-power operation. UK-based Imagination Technologies keeps that in mind as it focuses its Ensigma Series4 low-power ‘Whisper’ radio processing units (RPUs) on IoT-connected devices, including wearables (Figure 3).

Released last summer, Imagination’s baseband core can be integrated into SoCs and chipsets and configured to support a licensee’s requirements. And the company’s Universal Communications Core (UCC) programmable radio technology allows consumer products to use multi-standard basebands. By employing several low-power, 32-bit Meta processors, the RPU is scalable as well as efficient, as tasks can be implemented here rather than on application processors.

Another European company, Nordic Semiconductor, uses Bluetooth to communicate with the Cloud in its IoT strategy. At CES 2015, it introduced the nRF51 IoT Software Development Kit. The IPv6-ready IP suite (Figure 4) enables Bluetooth Smart to be used in cloud-connected networks for home, industrial and business automation.

The software development kit follows the company’s strength in RF processor technology and extends IP addressing to the connected device. Based on open standards, the kit includes IP support, transport layers and Message Queuing Telemetry Transport (MQTT) application layers as well as application examples.

At the beginning of last year, the company introduced the first ARM mbed development platform for Bluetooth

Smart applications, the nRF51822-mKIT. Aimed at developers creating wirelessly connected sensors around the IoT, the platform integrates an ARM® Cortex®-M0 CPU core and a Bluetooth v4.1-compliant, 2.4 GHz multiprotocol radio on a single chip.

**NOTES**

Caroline Hayes has been a journalist, covering the electronics sector for over 20 years. She has worked on many titles, most recently the pan-European magazine, EPN. Now a freelance journalist, she contributors news, features, interviews and profiles for electronics journals in Europe and the US.
ADLINK TECHNOLOGY INC.
HQ: 9F, No.166 Jian Yi Road | Zhonghe District New Taipei City 235, Taiwan
Founded: 1995
Funding/Key Investors: ADLINK Technology is a public company listed as 6166 on TAIEX
Number of Employees: 1,456
Contact: www.adlinktech.com
info@adlinktech.com

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

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

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

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

PRODUCT PORTFOLIO AND TECHNICAL CAPABILITIES
While ADLINK has a long-standing history within the telecommunication & networking industries supplying ATCA-based solutions equipped with the latest Intel platforms, the company is far from being a typical board supplier from the Asia-Pacific region. The company continues to build support for more of the IoT solution stack (which includes connected hardware, application software, middleware, and cloud services), particularly around software/middleware, to serve as a one-stop-shop for most end users.

The company’s traditional data acquisition hardware and software products (and expertise) facilitate one of the major pain points for deploying IoT-driven big data applications – collecting and managing progressively more data from a growing continuum of devices. Further, ADLINK’s software solutions, which at the moment principally enable monitoring control and active management applications, are a starting point for which OEMs can add their own big data analytics or application software on top. ADLINK will offer progressively more flexibility and variety with its embedded software offerings as the company plans to integrate and partner with more third-party solutions, with cloud management being a major point of focus.

ADLINK’s Smart Embedded Management Agent (SEMA), which comes supported by the majority of board and system products equipped with a board management controller, enables monitoring and collection of systems performance and status information from the embedded hardware. The SEMA-cloud solution pushes system data to the data center server through any kind of TCP/IP connection – ultimately enabling easier access to data and analytics through any commercial cloud portal. ADLINK selected Gemalto in May 2014 as their partner to complete the cloud integration, enabling remote system monitoring and real-time maintenance for connected devices using SEMA via a secure web-based dashboard.
ADLINK also offers industrial mobile computing products such as Smart Panels, rugged tablets, and handheld mobile computers supporting Android and Windows operating systems. The company’s COM products span a variety of architectures such as COM Express, SMARC, Qseven, and ETX. By supplying a flexible product portfolio for OEMs to easily augment their designs with a variety of peripherals and functionality, OEMs can focus on differentiating their products and reducing time-to-market. The company also supplies a variety of other embedded computing products such as slot SBCs and carriers, ATCA boards, CompactPCI boards, VPX blades, embedded flash storage, chassis, and more.

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

The company’s OEM/ODM engineering team is capable of customizing a variety of embedded hardware including system boards, mechanics enclosures, system or carrier boards for modules, and other essential components such as power supplies, DC modules, touch controllers, and more. ADLINK’s growing engineering services business is a product of the company’s rich expertise with single-board design, COM carrier board design and integration, system design & system integration, fanless designs, and extreme temperature and rugged systems (IP65, EN50155, Mil-Std-810G). ADLINK’s OEM/ODM engineering team is further supported by rich investments in R&D and test equipment; the company recently spent more than $1 million in pre- and post-route simulation tools and measurement hardware.

COMPETITIVE POSITIONING
ADLINK is a market share leader in a variety of embedded hardware markets such as embedded motherboards, SBCs, COMs, and embedded integrated computer systems. Combined with its data acquisition experience, products, and resources, the company is able to satisfy a broad range of IoT requirements while remaining versatile to changes in the embedded hardware market. This versatility, and need to continue building out its product mix, will be required. A number of ADLINK’s home embedded markets, including those for ATCA blades and PC/104 family modules, will see meager growth through 2017. However, the company will be propelled by its more lucrative box PCs and strong market share within the COMs market, which the company continues to build and which has remained strong since the acquisition of Ampro in 2008. The acquisitions of embedded PC systems providers LiPPERT Embedded Computers and PENTA in recent years will also help drive revenues in high-growth markets like medical devices and industrial automation, and new markets (for ADLINK) such as food & beverage.

The industrial automation, medical, and transportation markets present the greatest near-term opportunities for ADLINK, as the company's embedded products and rugged devices are suitable for a variety of field applications within these industries. Further, the company’s data acquisition experience will help ADLINK absorb some share from larger competitors such as Advantech and Kontron in these markets and the instrumentation sector, all of which require progressively greater data management to accommodate IoT data streams.
WHY THE TRANSITION TO 4G LTE?
AT&T will be shutting down the 2G GSM network on January 1, 2017, forcing the machine-to-machine (M2M) industry to begin transitioning to 2G CDMA, 3G HSPA, or 4G LTE networks. This represents a major challenge for the M2M industry, as it will entail the replacement of devices, new contracts with network carriers, and time and cost of major system-wide changes. At first glance it may seem like the GSM carriers just don’t want to keep supporting the old 2G networks, so you may be wondering why that is. The answer is quite simple: they are running out of frequencies. Each carrier in the US is only allotted a certain band of the cellular frequency spectrum, and with the high data rate demands of 4G it uses many more frequency bands than the previous 2G and 3G standards. So if some of these frequencies are reserved for “2G only” signals, then they don’t have enough bandwidth left for the 4G network. This part is the stick, the carrot part of the 4G transition is because the 4G protocol is much more efficient at combining both voice and data. With 2G and 3G, voice and data travels across different paths in the network, so there is no way to share capacity between these two paths. However with 4G, both voice and data are sent across the same path in the network, so carriers can easily optimize their networks to get the best possible utilization of their bandwidth.

BENEFITS OF 4G LTE
Increased speed is the obvious benefit of 4G LTE when transitioning from 2G or 3G networks. However, the evolution of 4G LTE is not all about speed. 4G LTE also has the benefit of reduced latency for time-critical applications. Recent and upcoming releases focus on lower power consumption, lower complexities, and lower costs. They also provide support for new connections and channels.

WHAT THIS MEANS FOR THE M2M INDUSTRY
The transition to 4G LTE will require a significant up-front investment, but it will pay off with increased connection speeds and improved coverage. 4G LTE coverage is being rapidly deployed around the country, as well as around the world. Globally, there are over 300 4G LTE networks available, deployed in 100 countries. AT&T recently completed a significant upgrade of their domestic 4G LTE network, and Verizon offers 4G LTE coverage to a vast majority of the United States. Multi-band devices are becoming increasingly prevalent, allowing for devices that will work with more than one carrier.

4G LTE ANTENNA CONSIDERATIONS
4G LTE presents additional difficulties for the designer when it comes to antenna selection. LTE modules typically have fallback to 3G and sometimes even 2G, so the antenna has to have good performance over a very wide range of frequencies. A common misconception is that the wider the antenna’s spectrum, the better the antenna. Unfortunately, the wider the antenna’s spectrum is, the more noise you let in to your receiver which degrades the receive signal quality. In this case bigger is not always better. With most 2G and 3G modules, it was possible to use only one antenna, even if the module had an RX diversity port. However, with LTE, many carriers have a hard requirement on having two antennas. This increases the cost and size of the design.

4G LTE CERTIFICATION
Certification is an expensive part of the cellular design cycle, and even more so with 4G LTE. Certification costs are based on the number of tests that have to be performed by a lab in order to prove compliance, and for 4G LTE the number of tests are increased from 2G and 3G. With more frequencies there is also a larger chance of interference from active components on the PCB, such as microprocessor clock and data lines. It is therefore more likely that you will have to tweak your design and do repeat testing during the certification step.

SYMMETRY’S 4G LTE SOLUTIONS
Having a strong technical partner is a necessity for completing your 4G design on time and budget. Symmetry Electronics can help simplify the migration process through a comprehensive product offering and extensive technical support. Symmetry’s expertise in wireless designs is invaluable for customers trying to simplify the migration process. Our Technical Marketing Engineers and our field sales team are primarily engineers by trade and go through extensive factory and in-house product training so they can provide phone and email support for specific technologies, hands-on experience with development kits, and detailed design support with schematic and design reviews. They are able to provide guidance and support through all phases of the design cycle.

Symmetry offers replacements for existing 2G GSM design-ins. Multitech offers a number of M2M products covering 2G CDMA, 3G HSPA, and/or 4G LTE, including the embedded SocketModem Cell, the embedded SocketModem iCell, the MultiConnect® rCell 100 Series, the MultiConnect® Cell 100 Series, and the QuickCarrier™ USB-D dongle.
Symmetry also offers exclusive custom Telit IN-A-BOX kits for 3G HSPA and 4G LTE connectivity. These kits are designed to make cellular M2M design easier by providing development kits based on the Telit CE910, DE910, HE910 and GE864-GPS M2M modules. Each kit includes everything required to begin a cellular design for a variety of applications: a Telit EVK2, a Telit Interface Board, software development introduction tools, cellular antenna(s), power supply, and the Getting Started Guide and documentation.

Call Symmetry Electronics at (310) 536-6190 for technical guidance and all the latest M2M connectivity devices.
Embedded Memories Destined for IoT Seek Security/Power Management Balance

Low-power designs that also stand guard against passive, semi-invasive and invasive attacks are evolving to protect the IoT devices found in automotive, wearables, medical, industrial and consumer applications.

By Bernd Stamme, Kilopass Technology

As the number of connected devices increases, so do such security risks as malicious software and reverse engineering. At the same time as risks and the rapid adoption of the IoT are gaining attention for security, power management is gaining its fair share of attention, with wireless devices proliferating and consumers continuing to push for more apps and longer battery life.

Embedded memories destined for IoT devices have multiple requirements including low power with instant-on, a small silicon footprint and programmable non-volatile code storage. Most important, they must be highly secure to protect software intellectual property (IP) and prevent hacking.

Non-volatile memory (NVM) currently is found in many forms, such as embedded flash, electrical fuses, multi-time programmable (MTP) and one-time programmable (OTP). These on-chip designs are low-power, configurable, reduce costs, improve performance and enable secure storage and operation.

PROTECTION AT THE MOST VULNERABLE LAYER

One antifuse OTP technology is an embedded non-volatile memory noted for its security, low-active and standby power (Figure 1). It supports all the proposed requirements for IoT device memory. It cannot be hacked using passive, semi-invasive or invasive methods because of a strong layer of protection at the most vulnerable physical layer. Its bit cell does not store a charge, which means there is no physical evidence of the state of the non-volatile memory bit cell. Instead, the bit determines an initial “0” or programmed “1” through the process of sensing current, not voltage.

Passive hacking techniques using current profiles to determine word patterns are unsuccessful. An intruder cannot determine the pattern of the word being read because the bit cell current for “0s” and “1s” is much smaller than the current required for sensing or operating the peripheral circuits in order to read the memory. Invasive techniques, including backside attacks or scanning electron microscopy (SEM) passive voltage contrast, are unsuccessful because it is difficult to isolate the bit cell since it is connected in a cross point array. Moreover, it is nearly impossible to determine which bit is programmed because it is difficult to locate the oxide breakdown using chemical etching or mechanical polishing and by looking at a cross section or top view.

The highest level of security relies on physical security since this is the most vulnerable layer of security in any system. Information programmed into a bit cell provides a high degree of physical security. That is, it cannot be determined through conventional non-invasive, semi-invasive or invasive attacks. This means that system-on-chip (SoC) designers can integrate NVM storage for data protection that will make their system.

Figure 1: An embedded NVM memory IP is used in a variety of chips for secure storage.
impenetrable to all but organizations not constrained by normal funding or time considerations.

A security lock register, bit or memory based on floating-gate NVM technology is inherently vulnerable to an attack from one of the standard methods. Antifuse memory technology offers superior security because it is practically impossible to reverse engineer. The secure antifuse bit cell is implemented for standard logic CMOS process. It also includes a lock feature that assures that the memory is locked and cannot be over-written or further modified by hackers or competitors.

Security risks are unwanted aspects of a connected world. More and more IoT-enabled devices include embedded NVM IP because it reduces the vulnerability of such devices. Low-power and configurable, IoT-enabled devices with embedded NVM IP offer secure storage and operation, reduce costs and improve performance.

Bernd Stamme is vice president of Field Applications Engineering at Kilopass Technology. He has more than 20 years of experience in the IP and semiconductor industry. Prior to Kilopass, he was the director of IP Technology at SiRF Technology, managing the licensing and successful integration of third-party IP into SiRF’s GPS chip sets. Before SiRF, he held management positions in LSI Logic’s CoreWare organization and worked on high-speed SerDes IP, communication interfaces and processor cores. Bernd holds a Dipl.-Ing. degree in Electrical Engineering from FH Bielefeld in Germany.

Your Internet of Things (IoT) needs reliable building blocks. We have them.

RTD Embedded Technologies, Inc. designs and manufactures a complete suite of robust, scalable board-level and system-level IoT solutions. Our comprehensive products give developers the tools they need to link valuable data to the people who need it. Whether it’s off-the-shelf or completely custom – for your embedded IoT needs, RTD is a one-stop shop. Visit www.rtd.com to learn more.
The IoT and RTOS Reinvention

A heads up on some of the changes in a new modular operating system environment.

By Thom Denholm, Datalight

Wind River is positioning VxWorks 7 as the reinvented “Internet of Things” RTOS. For targets, the company has identified a broad spectrum of devices, from edge devices (using a super tiny microkernel) to aggregators, gateways and controllers, and finally reaching all the way to cloud storage. The RTOS environment in each of these devices is slightly different, but connectivity and communication are shared goals.

Datalight products have been supported on Wind River’s VxWorks environment for over a decade, including sole support for flash memory through its license of Datalight’s FlashFX Pro. As Wind River has advanced its operating system, Datalight has enhanced our products to support the latest releases. We also continue to support legacy versions as far back as VxWorks 5.5, which has a large customer base. As we finish up our integration into the VxWorks 7.0 environment, here’s a heads up on some of the changes in Wind River’s new modular operating system environment.

Key aspects that Wind River is focused on include modularity, scalability, security and safety. The VxWorks 7 design feature that enables customers to run safe and non-safe applications on the same device extends to application updates, allowing an update without recertification. In full support of these updates, Datalight’s Reliance Nitro protects all system and application changes from power interruption, preventing a bricked device or factory return.

DISTRIBUTION MODEL EMULATES IOT APPROACH

One of the most significant changes from our perspective is a new distribution model for third-party components—the VxWorks 7 Marketplace. The idea, according to Wind River, is to provide customers with an “Internet of Things” approach—a one-stop shop for in-house and OEM additions to the environment. As with many marketplaces in the physical world, this shop opened before all the shelves were complete, and only BSPs were available earlier in the year. Since releasing VxWorks 7.0, Wind River has made some changes to the build process for Datalight and other OEM vendors. We expect those required changes to be delivered in the Marketplace through a build package dependency, which should be seamless to our customers.

Third-party components are designed to be completely modular, and the core RTOS API should remain unchanged for three years. This enables patches and updates where required, without a corresponding full release of VxWorks. This three-year window will cover a lot of updates to hardware drivers—from USB to Bluetooth to other sensors. Hardware manufacturers are also quickly delivering security changes at the media level, and this plan will allow Wind River to keep current without locking out older components and applications.

In VxWorks 7, the Datalight product build is considerably simpler. All source editing, building and debugging can be done in the VxWorks IDE. Processor build and environment are based on the BSP, and that information is now delivered to the installed package. The software developer would still want to customize the configuration files for Reliance Nitro and FlashFX Tera, especially when selecting a NAND flash part and controller. As always, unlocking the full feature set of Datalight products will still be done via a license key obtained from Datalight.

MORE RAPID INTEGRATION

Our most recent release of FlashFX Tera for VxWorks 7 will be delivered with our NAND flash simulation project as the default media storage. Customers can now bring up our solution with a block device immediately, which should allow faster integration and scalability. Following that, the full suite of provided tools and tests will allow rapid debugging and optimization of the customer’s hardware/software design.

Wind River has also made the claim to prevent malicious code in the development phase, though we’re not sure exactly what that means. What we do know is that security measures are available throughout the device, from boot time (untrusted binaries are prevented from executing) to run time and power down (no access to onboard data when the device is at rest). Root certificates and signed applications in the process and kernel space help with the former; encryption and digital signature verification (through X.509) with the latter. Security and user management also ties in nicely with Datalight’s file system offering, providing user authorization...
Nürnberg, Germany
February 24 – 26, 2015

embedded world 2015
Exhibition & Conference
... it’s a smarter world

THE gathering for the embedded community!
The world’s largest event for embedded technologies brings together all the players in the embedded sector for a productive conversation.
Make sure you are there when contacts and networks are being cemented on the international level and new trends are being set.

Media partners

elektroniknet.de
computer-automation.de
energie-und-technik.de
MEDIZIN-elektronik.DE
Markt&Technik
DESIGN & ELEKTRONIK

Trade fair organizer
NürnbergMesse GmbH
Tel +49 (0) 911 86 06-49 12
visitorservice@nurnbergmesse.de

Congress organizer
WEKA FACHMEDIEN GmbH
Tel +49 (0) 89 2 55 56-13 49
info@embedded-world.eu
through a full suite of customized attributes, in a fashion similar to recent Linux offerings.

More and more low-end hardware and media have built in security options. Allowing the RTOS and file system to utilize these features will reduce core CPU usage, resulting in a savings in power and an overall reduction in user perceived latency. One example close to our hearts is eMMC, which has this sort of protection available in the firmware.

One key market for secure devices is medical, and we believe this sector’s demands can be well served by a set of offerings from Wind River and Datalight that spans the time and space partitioning scheduler to cryptography libraries and extends from Wind River’s secure sockets to the complete protection from power interruption Datalight software offers. The reasons noted here are why we at Datalight are excited about this new Wind River release, and we’re convinced the protected boot, signed images and other security options are exactly where embedded devices need to be. Modularizing the kernel means fewer “complete system” upgrades and more flexibility for OEMs and BSPs. We’re pleased to continue supporting Wind River VxWorks with our reliable data storage products.

Thom Denholm is a technical product manager at Datalight. He is an embedded software engineer with more than 20 years of experience, combining a strong focus on operating system and file system internals with a knowledge of modern flash devices. Thom holds a BS in Mathematics and Computer Science from Gonzaga University. His love for solving difficult technical problems has served him well in his fifteen years with Datalight. In his spare time, he works as a professional baseball umpire and an Internet librarian. Though he has lived in and around Seattle all his life, he has never had a cup of coffee.
Reconfigurable Image Sensors Make Imagination the only Limit for Innovative IoT Use

The improvements in image sensors in the key areas of resolution, power and pixel low light performance evidenced in today’s camera phone products can be leveraged for an array of IoT devices.

By Shawn Maloney, Forza Silicon and Kambiz Khalilian, Lattice Semiconductor

With an estimated 13 billion electronic devices already connected to the Internet, interest in the potential explosive growth of the Internet of Things (IoT) market has greatly increased and attracted a large amount of technology investment. While initial product applications have incorporated a number of sensor technologies, the limitations of unintelligent sensor technology have hamstrung efforts to provide real-time information such as images and video.

Image sensor technology allows IoT devices to become smarter and provide real-time data. Improvements in image sensors in the key areas of resolution, power and pixel low light performance evidenced in today’s camera phone products can be leveraged for an array of IoT devices. In the case of IoT devices, however, there is an additional need for image processing at the point of image capture (“edge”) in order to ensure quick and accurate “decision making” by these smart devices. Image processing at the sensor also enables improved video performance (faster frame rates, HDR video, etc.) Finally, the ability to field reconfigure these smart devices by adding more functionality and correcting system errors without the need for product recalls is invaluable to both the customer and manufacturer of connected devices.

While the technology building blocks necessary to integrate imaging capabilities into smart devices have been available, a low-cost, integrated way to meet the size and power constraints of most IoT devices has not.

BEYOND SMOKE DETECTION

By leveraging the technology advances made at Forza Silicon at the sensor level, through more than 10 years of custom design experience, with similar advances made in programmable logic design at Lattice Semiconductor, a successful “proof of concept” platform has been developed. Leveraging parallel technology developments in the area of image sensor packaging using 3D stacking, Forza Silicon has demonstrated an Internet-connected smoke detector device (Figure 1) with the enhanced ability to monitor room condition, transmit an alert to the homeowner’s smartphone and stream real-time video of the actual event. This application was chosen to both validate the ability to incorporate these types of functions in a small-profile, low-cost, integrated device as well as the ability to field update the device remotely for additional capabilities or firmware changes without the need for replacement of the physical product. In addition, the reconfigurable capability of this same device means it can be programmed for other product applications and feature sets.

The possibilities for novel uses of imaging in IoT devices is expanded drastically by enhancing the image sensor’s timing and control logic with a programmable logic device. With Forza Silicon’s reconfigurable architecture, customer algorithms can control pixel integration and readout in non-standard, unique ways. For example, instead of being forced into a frame-based readout of sequential rows, as is typically the case in standard image sensors, the reconfigurable system can read rows in any arbitrary sequence, and react immediately to the latest pixel data by adjusting the readout sequence (Figure 2). Pixel integration time can also

Figure 1. An Internet-connected smoke detector device.
be adjusted on the fly, as determined by the customer algorithm. The FPGA’s configurable I/Os also allow flexibility to choose the best embedded processor, microcontroller or application processors for the IoT application. These examples only scratch the surface of how the full flexibility of this reconfigurable image sensor will be harnessed for future IoT devices, as the FPGA community can only guess at the diverse applications opened up by programmable logic itself.

Lattice’s MachXO/2/3 architecture complements the Forza Silicon image sensor. The MachXO families have driven down the size, power and cost of small FPGAs to the point where high-volume IoT applications can now incorporate FPGAs. The goal of this architecture is to balance capability and value for image sensor based applications. By meeting the technology challenges of the IoT market, the reconfigurable image sensor provides an optimal solution for additional markets such as automotive, surveillance and industrial applications where the implementation of image sensors and the need for enhanced image processing at the point of capture is critical.

Shawn Maloney is Executive Vice President of Business & Product Strategy at Forza Silicon. He has over 30 years of strategic sales and marketing experience in the imaging semiconductor industry and played a leading role in the introduction of two breakthrough technologies (CMOS image sensors and MEMS) into the mobile imaging market.

Kambiz Khalilian is marketing director at Lattice Semiconductor, responsible for driving strategy for the company’s cost-effective and flexible industrial and automotive solutions, which address the market’s need to interface with new image sensors and display technologies and process ever increasing image resolutions and frame-rates. For over the past two decades, he has worked in the technology field developing his expertise in video solutions, serving in various product marketing and engineering roles.
GainSpan Corporation

GS2011M Low Power, High Speed 802.11 b/g/n Module

The GS2011M module provides a quick, easy, and cost effective way for device and appliance manufacturers to add Wi-Fi connectivity to their products. The module provides a high speed serial interface connection to an embedded design built on an 8/16/32-bit microcontroller, achieving up to 40 Mbps throughput over an SDIO interface. The GS2011M is an ideal solution for organizations with limited Wi-Fi or RF expertise or for those seeking faster time to market, as it reduces RF design time and removes the burden of testing and certification. The module is IEEE 802.11b/g/n compliant, and meets worldwide regulatory and Wi-Fi Alliance certification requirements. The module includes two analog to digital converter (ADC) pins for connecting energy measurement and other sensors. It runs the full Wi-Fi and TCP/IP networking stacks on module, completely offloading the host microcontroller. The module supports a complete suite of security protocols, also without tasking the host microcontroller, including WPA/WPA2-Enterprise and Personal security modes, legacy WEP encryption, and upper layer security protocols such as TLS/SS and HTTPs. Alternatively, it can be run self-contained without a host. For ease of provisioning, the module can be set up simply and easily from a smartphone or laptop through the innovative Limited AP mode or with Wi-Fi Protected Setup (WPS). The GS2011M has extended range with industry leading receiver sensitivity and is available with the u.FL connector to add an external antenna for max performance or a ceramic chip antenna for performance and convenience while saving space.

FEATURES & BENEFITS

- Adds low power, high speed Wi-Fi and Internet connectivity to any device with a microcontroller and serial host interface
- Certified module reduces development time, testing and certification, accelerating time to market
- Easy upgrade path: footprint and pin compatible to GS1011M and GS1500M modules
- Full offload solution minimizes load on host processor
- Ultra low power consumption through dynamic power management modes:
  - Standby
  - Sleep
  - Deep Sleep

TECHNICAL SPECS

- IEEE 802.11 b/g/n connectivity with PHY rates up to 72 Mbps
- Limited AP, Wi-Fi Direct with concurrent mode, WPS 2.0
- UART, SPI, SDIO interface to microcontroller.
  Throughput (typical): 40 Mbps on SDIO, 30 Mbps on SPI (master), 12 Mbps on SPI (slave) , and 1 Mbps on UART
- Extensive networking stack and services
- Security: 802.11i, WPA/2–Personal and Enterprise, legacy WEP, TLS

APPLICATION AREA

The GainSpan GS2011M module is easily designed into embedded systems, allowing customers to develop a broad array of devices and appliances that connect to other local devices or the Internet over Wi-Fi. Applications include healthcare and fitness, smart energy, industrial controls, commercial building automation, and consumer electronics.

AVAILABILITY

Sampling now with production slated later this year
WE DESIGNED THIS WEBSITE FOR YOU...

- Complete Coverage of 30+ Key Embedded Technologies
- Valuable Company and Product Information
- Opinions and Insight

www.eecatalog.com
Secure Smart Meters Enable Smart Choices

In small subscriber areas where using data concentrators on the smart grid is like taking a sledgehammer to crack a nut, gateways cannot only save costs, but also offer the flexibility of managing different networks from the same data center.

Low-cost embedded processors and increasingly ubiquitous data networks have made it possible to revolutionize energy metering. By enabling two-way communication between residences and utility companies, connected meters with embedded processors can record and transmit usage data to a power company’s data center for use in billing and customer service. These new “smart” meters can also help customers make intelligent choices to save energy and reduce their gas and electric bills. Benefits for both power companies and their customers explain why utilities are rolling out these communication-enabled meters on a massive scale in countries across the world. However, enabling this two-way communication presents networking and security challenges.

One approach to safeguarding networked metering applications involves embedded SoCs that incorporate features such as advanced security engines and robust data encryption.

Ordinary to Smart

Having intelligence and connectivity built into the meter is not enough to reliably connect smart meters. Achieving reliable connectivity requires advanced networking technologies linking meters with the utilities. Devices such as data concentrators, routers, communications hubs and gateways are essential to connect meters to the backbone of the system. This connectivity, along with embedded processing, is what converts an ordinary meter into a smart meter.

The use and location of these devices on the smart grid differs from country to country. It depends on local regulations, whether it’s an electricity, gas or water meter, and in the case of electricity meters, the architecture of the power distribution network. In the United Kingdom, for example, a communication hub helps gas and electricity meters talk among each other and home displays through ZigBee (Figure 1), sending the information to the backbone system through a Global System for Mobile Communications/General Packet Radio Service (GSM/GPRS) modem.

Data concentrators or gateways are preferred for electricity meters, although this depends on region, power distribution network topology, the level of subscriber concentration and the quality of the networking infrastructure.

In countries like Italy, France, Portugal and Spain, data concentrators have been used on a massive scale. They read and store meter information using the narrow power line signal for last-mile communication, and GPRS wireless or Ethernet for upstream communication.

The Argument for Gateways

The level of concentration at the secondary substation is between 200-300 subscribers in big cities. Doing data
concentration with or without low voltage supervision works best. A data concentrator is divided into two main components. One component pulls in the data from the meters and stores this information in a database with a complex and powerful web interface. The second component is the communication interface with network coordination capabilities. The PoweRline Intelligent Metering Evolution (PRIME) standard calls this the base node (Figure 2). The application layer of the data concentrator has an embedded Distribution Line Messaging Specification/Companion Specification for Energy Metering (DLMS/COSEM) client, which interrogates the meters using the software stack’s encryption capabilities. Usually the data concentrator includes a 3-phase low-voltage supervisor for energy balance and remote supervision. The base node is the part of the data concentrator that builds and keeps the meter network stable, providing a transparent channel to the application layer to talk with each meter.

Utilities must deal with a percentage of areas where the number of subscribers is very low—anything between 5-50. In these situations, a data concentrator scaled to manage hundreds of devices is not optimum. Here a gateway, which simplifies installation and offers a cost advantage over a traditional data concentrator, is a better value proposition.

The gateway is a pure communication device. Low-voltage supervision is usually not required. Another important difference: Unlike with a traditional data concentrator, it’s not necessary to store data on the device. The memory only has to store the communication protocols. The application layer can host the DLMS/COSEM client into the central data server, saving license costs and allowing management of different networks from the same data center. You should secure information downstream and upstream with commonly used security and encryption algorithms such as RSA, DSA, AES, SHA, ECC, etc.

Anti-tampering features are also important to detect and avoid illegal access to the equipment.

A good example of gateway utilization is the PRIME standard smart metering network (Figure 3). A PRIME gateway comprises a PRIME base node that manages everything related to power line communication (PLC) networking, a GPRS/GSM modem and an Ethernet interface.

A smart metering architecture based on gateways opens a world of possibilities as the smart grid evolves. The advantages are lower costs in low-subscriber density areas, as well as in the operation and maintenance of the network. The gateway concept allows the integration of different telecommunication technologies over PLC enabled smart meters. This improves the performance of the entire network.

Jesus Teijeiro is director of business development for Smart Energy products at Atmel Corporation. He has an electrical engineering background and more than 18 years experience in the semiconductor industry. He has worked for semiconductor distributors Arrow Electronics and EBV Elektronics, and semiconductor companies including National Semiconductor, Fairchild, Fujitsu, Cypress and ADD Semiconductors.
Zilog offers a wide selection of lens and pyroelectric sensor bundled options to fit your application needs.
Smarter Energy: Meters Embrace Their Critical IoT Role

The IoT will extend the connected benefits of the smart grid.

By Olivier Monnier, Texas Instruments, Inc.

The global focus on energy and water management and conservation is leading to a smart grid that involves more than distribution, automation and monitoring by utility providers. Management systems for in-home and in-building use will help consumers monitor their own usage and adjust behaviors. These systems will eventually regulate automatically by operating during off-peak energy hours, and they will connect to sensors to monitor occupancy, lighting conditions and more. Through the IoT, consumers, manufacturers and utility providers will uncover new ways to manage devices and ultimately conserve resources and save money.

STEP ONE: TWO-WAY COMMUNICATION

Millions of meters are already connected today, and the connected grid momentum is growing. However, to obtain its maximum potential, the first step for the smart grid is to transition from mechanical meters to smart electronic meters in order to establish two-way communication between the meter and utility providers.

The adoption rate of smart electrical meters in the US is close to 50 percent, with millions of electrical meters deployed today in the field, connected to the grid and regularly communicating data. Essentially, electrical meters are extending their functions from an energy-measuring device to a two-way communication system.

Modern e-meters must meet certain criteria to play such a critical role in the smart grid and IoT. First, meters need to report energy consumption information from houses and buildings back to the utilities. In the US, the appropriate solution is low-power RF (LPRF) communication using a Sub-1 GHz mesh network. However, depending on the country and the nature of the grid, a wireless solution might not be the best choice. For example, Spain and France employ wired orthogonal frequency-division multiplexing (OFDM) power line communication (PLC) technologies. No one connectivity solution fits all deployments. Making the IoT real requires a larger portfolio that can go from wired to wireless and sometimes combine the two.

METERS AS IOT SENSORS

Second, the meter needs to deliver useful power consumption information into the home through an in-home display or a gateway. Armed with this information, consumers can adapt energy behavior and lower utility bills. The US and UK use the ZigBee standard in combination with the Smart Energy application profile. Other countries such as Japan are evaluating Sub-1 GHz RF or PLC solutions for greater reach or a combination implementation with both hybrid RF and PLC. In essence, electrical meters are becoming smart sensors for the IoT that communicate both ways, inside and outside homes and buildings, connected to each other in a mesh network while reporting essential energy data to utilities.

Additionally, a smart meter needs to support advanced functions like dynamic pricing, demand response, remote connect and disconnect, network security, over-the-air downloads and post-installation upgrades, so utility providers don’t have to send out technicians to each meter. Wirelessly connected meters can also help providers with predictive maintenance and remote diagnostics to further reduce technician deployments and downtime.

Connecting devices together in buildings and homes is one of the next steps to reach the full benefits of the smart grid. Many innovative solutions and convenient applications are already offered to consumers with more on the horizon. The introduction of dedicated home energy gateways, smart-hub, or energy management systems will greatly accelerate connected grid and IoT benefits for consumers. In parallel, the massive wave of smartphones and tablets is helping accelerate the adoption of communication standards and technologies like Bluetooth Smart, for instance, connecting even more devices every day. Additionally, innovations in sensors, analog power components, microcontrollers, processors and wireless connectivity semiconductors are delivering more energy savings and features through lower power consumption, improved performance and programmability.

Olivier Monnier is director of marketing, Wireless Connectivity Solutions, Texas Instruments, Inc.
It’s Smart to Communicate

The smart grid is a way for consumers to monitor and save energy and for utility companies to prepare and meet periods of demand, improve efficiency and maintain a reliable, secure supply. Caroline Hayes looks at measures to ensure that the communications between user and utility company are maintained.

The connected energy ecosystem is made up of smart meters that send and receive data to the utility company as well as inform the user of the levels of energy being used. This bi-directional communication between home, or office, networks and the power grid creates a reliable and sustainable energy supply. Communicating with devices in the network can allow information, such as a temperature drop, meaning more energy is required, to be relayed and acted upon. It is a consumer convenience but also a management system.

Two bodies are striving to bring interoperability to the smart energy world. The ZigBee Alliance, the WiFi Alliance, the Home Plug Alliance and Bluetooth Special Interest Group are promoting the Smart Energy Profile 2.0. The Wi-SUN Alliance is defining the specification for field area network communications.

SMART ENERGY PROFILE 2.0

The Smart Energy Profile (SEP) 2.0 addresses the fact that multiple manufacturers design smart energy systems, all of which have to operate and communicate securely within a network. The profile addresses communication, connectivity and data sharing. It is a multi-layer protocol, built on top of an Internet Protocol (IP) stack (see Figure 1). The application layer includes Transmission Control Protocol / Internet Protocol (TCP/IP) for transport and network functions.

The profile’s guidelines address how properties of devices that are on the smart energy network communicate, for example metering or pricing systems, using Transmission Control Protocol /User Datagram Protocol (TCP/UDP) and IP-based networking for interoperability.

The profile requires a TCP/IP stack with UDP support, IPv6 services, including multicast Domain Name service (mDNS) and (Domain Name Service Discovery (DNS-SD). These are commonly used protocols meant to make SEP 2.0 devices easy to find on a local network via a computer, tablet or smartphone.

The use of TCP/IP makes it Media Access Control (MAC) and physical layer (PHY) agnostic. It also requires security implementations such as Secure Sockets Layer/Transport Layer Security Protocols (SSL/TLS)

The Profile is also based on a client-server Representational State Transfer (REST) architecture that deploys web services over HTTP. It accesses servers to read, write, create and delete operations for client devices, such as meter reading, or for resources for events that demand a response, such as a temperature drop.

Figure 1: Smart Energy Profile (SEP) 2.0 provides a framework for communication, connectivity and information sharing in the smart energy ecosystem.

so that data is securely transmitted. Security is critical to both user and provider, as consumer information has to be protected, and the utility network has to be secure from attack.

The Profile’s resource (or function) representations are compatible with the IEC’s Common Information Model (CIM) and use an XML-based protocol, using HTTP.
The always-on nature of the smart energy network means that microcontroller developers aiming to position devices into smart metering devices not only have to ensure low energy consumption, but also support for a barrage of protocols in its stack. Most recently, in January, this year, Atmel has released the latest additions to its SmartConnect wireless combo SoC, the WILC3000 and WINC 3400. Both combine WiFi 802.11n and low-energy Bluetooth Smart technology; the WINC3400 network controller has an on-chip stack with TCP, UDP, DHCP (Dynamic Host Configuration Protocol), ARP, HPPT, SSL and DNS.

**FIELD AREA NETWORK SPECIFICATION**

January also saw the release of a feature-complete version of the Wi-SUN Alliance’s specification for field area network communications (Figure 2). The association is promoted by Analog Devices, Cisco, Omron, Murata, National Institute of Information and Communications Technology (NICT), Silverspring Networks, Osaki, Renesas and ProCubed.

The specification enables interoperable and secure IPv6 communications over an IEEE 802.15.4-based wireless mesh, involving devices on the network such as Advanced Metering Infrastructure (AMI) and networked municipal lighting in smart cities.

Although many of the companies in the Alliance are Japanese, the IEEE 802.15.4g is an international standard, making the specification applicable in North America, Japan, Brazil, Australia, Asia Pacific, India, Europe, the Middle East and South Africa.

The principle is that the mesh-enabled field area network provides secure and cost-effective connectivity and sound coverage in a variety of environments, from dense, urban areas to rural regions, without a great deal of costly, additional infrastructure.

The specification includes an 802.1g PHY, frequency hopping and network discovery or join and protocol dispatch function. There is also an IPv6 protocol suite, with 6LoWPAN, address management, RPL routing and both unicast and multi-cast forwarding. The standards-based, multi-layer security specification includes authentication, authorization and encryption.

Early last year, the Alliance collaborated with the HomePlug Alliance to work towards enabling hybrid smart grid networks that support both wireless (i.e., RF) and wired (i.e., power line) connectivity. The agreement encourages Alliance members to share specifications for MAC and transport layer profiles for interoperability of IP-based smart grid applications. Phil Beecher, Wi-SUN Alliance Chairman, talked of it being the start of “hybrid connectivity for utility networks.”

While the specifications for PHY and MAC layers address the authentication and certification issues for networked devices, the MAC layer differs depending on the application—for example home automation or a smart meter.

Caroline Hayes has been a journalist, covering the electronics sector for over 20 years. She has worked on many titles, most recently the pan-European magazine, EPN. Now a freelance journalist, she contributes news, features, interviews and profiles for electronics journals in Europe and the US.
Zilog, Inc.

Zilog’s World of Reference Designs

Zilog’s World of Reference Designs allow you to accelerate your next design with a head start. Zilog has combined the technical innovation of our product portfolio with optimized designs, an extensive pool of software, and the tools and resources needed to quickly get your product to market. Our reference design solutions ship complete with hardware and software, and all of the documentation you need is available free for download, which helps expand the design potential for all engineers, including engineering students. Our reference designs give you access to a wealth of new potential.

Zilog has many technologically innovative reference designs that include boards, modules, and even educational platforms. The Zilog Educational Platform is designed to offer a comprehensive educational advantage to students who are pursuing a degree in the electronics and computer sciences. It is an electronics development system for learning and teaching at the university level.

One of Zilog’s most recent motion detection reference designs is the ZMOTION AC Load Controller Design Module, which demonstrates how to use Zilog’s ZMOTION MCU in a passive infrared-based motion detector to control power to an AC load in applications such as lighting and HVAC systems. Our new Microstepper Motor reference design offers a complete and easy to use platform, and drives a unipolar stepper motor using the Z8F1680 MCU’s onboard analog comparators.

Zilog has a considerable selection of reference designs, helping to expand the potential for all.

FEATURES & BENEFITS

◆ Mini-Z USB Design Board provides a reference design to incorporate USB host and peripheral functionality with Zilog’s portfolio of Mini-Z modules; the design also incorporates a Secure Digital (SD) card
◆ World of Sensors Design Board is an easy-to-use platform, and includes a world of sensing technology with which you can easily experiment, including seven different sensors, each on different peripherals
◆ ZMOTION AC Load Controller Design Module uses the 8-pin Z8FS040 MCU to intelligently control a mechanical relay, and provides user adjustments for motion sensitivity, delay time, and ambient light level
◆ Microstepper Motor Design Board drives a unipolar stepper motor using the Z8F1680 MCU’s onboard analog comparators for one-shot feedback current limiting, and is optimized for microstepper motor control

APPLICATION AREAS

Consumer electronics, industrial, communications/networking, medical, military/aerospace, security, wireless/mobile.

AVAILABILITY

Available for purchase from the Zilog Store at www.zilog.com/Store.
Deep Verification Defends Embedded Components’ Safety and Security

Automotive, defense and power generation are among the applications where rigorous verification using updated approaches is making a difference.

By David Kelf, OneSpin Solutions

Safety and security have become a paramount concern in a number of embedded design applications. Engineering segments such as automotive, defense, aeronautical and power generation require failsafe components that cannot be disrupted through accidental or malicious action, and often must demonstrate adherence to government or industry standards.

These designs include additional, often complex, design structures that must be rigorously verified. This verification process must itself be proven to meet exacting coverage standards that specify the testing of all alternative operational possibilities.

The verification of safety and security features often involves new techniques. They might include, for example, the insertion of faults without actually changing design code, the analysis of design signaling to ensure no leakage of secure data, the testing of redundant systems and many other scenarios unique to these systems. This verification process must be performed at a component and system level to ensure complete validation.

FAR FROM SIMPLE

For instance, meeting safety standards, such as the automotive ISO 26262 standard, requires the inclusion of redundant structures for key functionality so that a fault during operation would be detected and the failing section switched out in favor of a correctly working structure. In order to meet this requirement, Triple Modular Redundancy (TMR) is used. TMR involves three components performing the same function. An arbiter unit checks that all three produce the same result. If one produces a different result from the other two, then the output of the two correctly operating devices is used, and an alarm raised.

The verification of this unit is not simple. First, all units must be exercised for EVERY possible fault condition that might occur. Second, a fault must be injected into the units without changing the design code, thereby not rendering the verification exercise void. Finally, surrounding components (e.g., the arbiter itself) must be exhaustively checked at the same time as the critical parts to ensure compliance of the entire system.

This could potentially be accomplished with simulation. However, simulation tends to consider a design situation state-by-state, relying on test vectors to ensure that all states are tested. This is further compounded by the insertion of faults. A simulation “force” operation may be used to change a state without changing the design, but an exhaustive fault set would have to be used for every test vector to ensure a full test. The resulting testbench and fault list would be enormous and would in no way be guaranteed to be exhaustive.

ASKING QUESTIONS

Formal Verification is becoming popular as a mechanism to ensure exhaustive testing. The nature of the technology essentially allows a user to “ask a question” about the design, and the tool then tests for every possible state the design can enter to answer the question. This can include the full range of possible faults as well. A basic question could be one such as “for every possible input and for every possible fault condition, will the arbiter always discover a failing item?” With the appropriate coverage tools, this can be proven to exhaustively test a design. The design could include embedded software operating on a hardware platform, and still be proven to achieve the same verification result.

Another example is the use of error correction codes to recover an internal fault. In some applications, as illustration, the corruption of a memory bit can lead to unwanted effects, and this might be cured with the use of an error correction system. Depending on the error severity to be handled, the correction algorithm might be a simple check to a full correction solution such as a Viterbi correction algorithm.

Data being written into the memory is coded using a Viterbi coder and then decoded on a read. An error occurring in the memory will be corrected...
automatically. However, to verify this system, any kind of error in the memory must be tested, which requires faults to be injected. Similar to the TMR solution, the formal engine allows for this level of exhaustive analysis.

Security systems in an embedded design are sometimes related to Safety systems in that they also require special design structures to be included, and specialist verification solutions to be employed in their testing.

A well-known security methodology is ARM’s TrustZone®. TrustZone allows for a “secure region” in the hardware of a device, and provides for the creation of a virtual environment for related secure software to operate. In this scenario, there should be no ability for part of the hardware or software in the system outside these protected regions to read or write data inside the regions, unless through a specific secure channel.

These regions need to be tested to ensure that no “leakage” of secure data or malicious access can occur. Formal techniques allow for an exhaustive check to be applied, which essentially examines all the states a system can achieve and for any one of those states, to check that leakage cannot occur. To provide an exhaustive verification environment for this functionality using simulation or by running the design in the final FPGA device, tests would have to be created that methodically check each input against each state of the system while looking for insecure access. Such a system would require many hours of effort, and it would be hard to ensure total coverage.

Formal verification is being used in a greater number of applications, especially those that require exacting standards of thorough verification. Safety and Security are two excellent examples of scenarios that simply must be fully verified, and proof provided that every operational possibility has been checked. It is clear that more applications of the technology will emerge in the areas of Safety Critical and Ultra Secure designs.

Author. David Kelf heads OneSpin’s marketing efforts and serves as vice president of marketing. Previously, he was president and CEO of Sigmatix, Inc. He worked in sales and marketing at Cadence Design Systems, and was responsible for the Verilog and VHDL verification product line. As vice president of marketing at Co-Design Automation and then Synopsys, Kelf oversaw the successful introduction and growth of the SystemVerilog language, before running marketing for Novas Software, which became Springsoft (now Synopsys). He holds a Master of Science degree in Microelectronics and an MBA from Boston University.
Security and the IoT: A Q&A with Rambus

Thoughts on IoT semiconductor growth and how addressing security concerns is paramount.

By Anne Fisher, Managing Editor

Editor’s note: Our thanks to Steve Woo, vice president, Enterprise Solutions Technology and distinguished inventor at Rambus, who recently offered his insights on a number of questions.

EECatalog: Steve, you have what you call a cautious take on IoT semiconductor market growth, can you elaborate?

Steve Woo, Rambus: One of the things that was really encouraging that I saw at CES is the tremendous progress in terms of IoT devices and interoperability. A couple of years ago there were a lot of people looking at interesting ideas and technology, but what you began to realize is that in most of those cases the technology itself wasn’t the challenge (and don’t get me wrong, there are individual challenges), but you did get the feeling, “maybe that isn’t the hardest part of all of this—maybe the hardest thing that has come to light over the last couple of years is that the challenges are going to be in interoperability.”

We need standards and methods that people have agreed upon to have these devices interoperate. And we also have to work on some other technical things like power and security. What was interesting at CES this year is all of those topics got a lot of attention—as more than others—it is the kind of thing you would expect to happen as an industry starts to try to work together and go from the crawling stage to the walking stage.

A recent Gartner report projected growth in the semiconductor industry, and I think [growth of that caliber] is definitely possible if you examine industries that are looking for ways to connect a lot of devices together.

It is definitely the case that the automobile industry is looking at a lot more technology in cars. And it’s also the case that there is a lot more discussion about home automation and wearable devices. So it is definitely possible for us to see the growth [the Gartner report] predicted, but I think there are some issues that need to get addressed.

One of the things that came up a few times at CES this year is: the technology making the devices is very doable in many cases, but the real issue is: do you have a reasonable business model that allows you to stay in business with these devices—that is a tougher challenge, and the reason why you tend to see a number of companies coming in and out of the market so quickly for wearables and IoT devices. The market’s not mature, and the business models are unproven at this point [although] there are undoubtedly some that will work very well.

[However] if you’ve got established markets and you’re trying to overlay or inject IoT-type devices into the markets, it seems like an easier path than it is to generate a whole new business model where you are not going to try to tap into an existing revenue stream.

Another challenge is power. People are saying, “gosh, I don’t want to have to take off my device every day to recharge it.” For other types of devices, like beacons, the goal is to provide enough power so that the device can stay in the field for years and be powered by something like a watch battery. Two areas where there are challenges in meeting power limitations are communication and on-chip storage. Moving data on and off a device takes power, and the power can be prohibitive if lots of data is moving to and from the device over long distances. Storing data on-chip can also be a challenge, as persistent storage is needed that doesn’t require a lot of power to store and retrieve the data.

Fortunately, the industry has been busy addressing these and other challenges in recent years. Bluetooth LE addresses communication challenges by optimizing power for short-range communication with other devices

People have come to the realization that security is a goal that needs to be treated as a ‘first class design parameter’,....”
the IoT devices and/or the communication hubs that sit between the IoT devices and data centers.

**EECatalog:** What do architects and chip designers need to do in order to improve chip and system security?

**Woo, Rambus:** When you start having things like automated homes and automated cars, what you are also doing is offering more ports and entryways into the system, and every one of those has to be secured. If not done correctly, then that just means that there are more opportunities to get into chips and systems.

People have come to the realization that security is a goal that needs to be treated as a ‘first class design parameter,’ which means that it needs to be thought about during the definition phase for an architecture and a product.

**EECatalog:** What is the advantage of building security into silicon?

**Woo, Rambus:** There are definitely levels of security that you can provide, and in part it’s about the types of tradeoffs one is willing to accept. Some systems choose to do everything in software because it’s relatively easy to deploy and to layer on top of existing systems. The problem is that software-only protection can be hacked, and we’ve seen numerous cases of that in the past year alone. This goes back to the point about treating security as a first-class design parameter—legacy systems often weren’t designed with software security in mind, so the system doesn’t enable software to do the best job possible for securing the system.

Our view is that having a hardware root of trust integrated into the silicon enables the highest levels of security. The key issue is that from the moment power is applied to the system or device, the first thing that comes up is the hardware, and at this point the chip or system can be attacked. Solutions exist that use hardware as a basis for security, but having that hardware integrated into the silicon increases the security of the silicon and system.

Having features built into that hardware, we believe, is the best way to secure the hardware. Again, there are tradeoffs to be made, and in some cases people will be willing to live with lower levels of security provided by software-only solutions. But as you begin to interconnect more and more devices, some are inevitably going to want higher levels of security, so providing hardware security and a hardware root of trust is going to be very important going forward.

You might have a device where you say, “I really need it to be secure for the next five years. One of the nice things about that is that if you think about adding hardware elements or something like that and they are in silicon, Moore’s Law has done a great job of naturally cost reducing any kind of hardware element that you put into a system. One way to secure the interaction of two communicating devices is to provide hardware elements in both of those devices that each device can use to authenticate the other. Moore’s Law enables these devices to include this functionality at reduced cost over time, and/or to provide more complex authentication mechanisms over time.

**EECatalog:** What led to the development of your hardware root of trust offering, CryptoManager?

**Woo, Rambus:** We are excited about the CryptoManager platform. On the surface it provides some very interesting capabilities, but when you dig a little deeper and you look at how devices are used you begin to realize that the elements that are contained within Crypto Manager actually offer a very powerful tool kit that allows you to do things that are beyond what you might think about initially.

One of the things that CryptoManager has is a hardware root of trust that provides a secure foundation for connected communication. This core allows you to very securely enable and disable features and functionality in the chip that core sits in, and secures the chip throughout the lifecycle from manufacturing through deployment and end of life. The secure core acts like a vault door, where unless you know the combination and can open the vault door, you cannot gain access to anything inside the vault.

CryptoManager is a platform that allows us, using that core, to secure a semiconductor device throughout the device lifecycle, and to enable and disable features by managing keys that can lock and unlock functionality. One thing that CryptoManager enables is that as the silicon travels from facility to facility—for example, from fab to wafer cutting to die packaging to testing packaged die to fabrication to integration into a device like a phone—is to ensure that the semiconductor device itself has manufacturer-specific keys put in there that no one else can get to or manufacturer-specific capabilities enabled or disabled.

A great example is managing access to the JTAG port of a chip. During device test, you need access to the JTAG port. The problem with JTAG and other debug ports is that it is almost like having the master keys to the house. [Via debug ports] you can get deep access to many areas of a chip, and once the device is in the field you may not want people to get access to some or all of these areas.

What CryptoManager can do is enable/disable access to things like debug ports. For example, you can turn on the debug port only when the device is being debugged, and once it leaves the factory you can turn off that port so no one else can get through there.

What that also means is that once the device leaves, say, the phone manufacturing facility and gets deployed into the field, you can actually enable and disable features in the silicon itself, so that you can now think about new kinds of business models where carriers can enable and disable features on the phone. Or you could enable or disable certain kinds of content to be played on that phone so you get this interesting way of looking at new revenue models and usage models—and it all relies on the same CryptoManager platform and toolkit that manages keys to enable and disable functionality.
Virtual Prototyping and the IoT: A Q&A with Carbon Design Systems

A designer of high-performance verification and system integration products highlights the virtual prototyping/IoT relationship and explains the more prominent part pre-built virtual prototypes now play.

By Anne Fisher, Managing Editor

Editor’s note: Our thanks Bill Neifert, chief technology officer of Carbon Design Systems and a Carbon co-founder who recently offered his insights on a number of questions.

**EECatalog:** How much embedded design activity are you seeing for IoT?

**Bill Neifert, Carbon Design Systems:** IoT is an intriguing space since exactly what this means varies from source to source. Regardless though, the fundamental premise of IoT is taking a device and placing it on the Internet. While this seems simple enough at first, it introduces substantial design complexity along with a lot of additional potential. Any device connected to the Internet needs to be able to interact securely, which requires a good amount of design effort and proper design practices. In addition, since connected features are seen as a means for differentiation, it’s common for the connected capabilities to be leveraged to integrate other features such as remote controllability and notification. All of this complexity drives a need for additional embedded development.

**EECatalog:** How can IoT designers take advantage of virtual prototyping, especially when security is a consideration?

**Neifert, Carbon Design Systems:** Virtual prototypes add value to IoT development in multiple ways. Since IoT devices typically are more consumer-focused, time to market is often a key way to differentiate. Virtual prototypes are able to pull in design schedules by parallelizing the hardware and software design efforts. In addition, since security plays a big role in IoT, accurate virtual prototypes can help ensure that all of the system’s corner cases have been validated early in the design.

**EECatalog:** What trends are you seeing that will affect embedded designers in 2015?

**Neifert, Carbon Design Systems:** The primary trend that will continue to affect embedded designers in 2015 is the mass migration of designs to the ARM architecture. ARM has long been the dominant player in the mobile space. In the past few years though, it has achieved significant penetration into other market verticals. We’ve seen strong adoption of ARM processors in a number of areas, winning design starts away from both internal offerings as well as other processor IP vendors. We’re seeing this trend reflected in our own customer base. A year ago, the majority of our virtual prototypes were used in SoC designs focused on the mobile space. While mobile is still a widely used application, in just the past 12 months, we’ve seen new ARM-based design starts in servers, base-stations, storage, sensors and industrial applications. In many cases, this is the first time that the design team is using ARM IP. If you’re an embedded designer and your current project isn’t using an ARM processor, there’s a good chance that you’ll use one on your next project.

**EECatalog:** How has virtual prototyping changed the way in which embedded designers work?

**Neifert, Carbon Design Systems:** In the past few years, multicore designs have become far more prevalent. Although this puts a lot more power into the hands of the designer, it also introduces substantial complexity from both the hardware and software design perspective. Virtual prototypes empower designers with the tools to handle this complexity. Accurate virtual prototypes enable architects to ensure that the performance goals of the chips used to drive embedded designs are being met. Validation and verification engineers are leveraging virtual prototypes to ensure that the interactions between system software and the hardware being designed are correct. Finally, firmware and software engineers are able to leverage the early availability, speed and visibility of virtual prototypes to design software earlier and debug problems that would take much longer to isolate in real hardware. There’s no way for real silicon or even hardware prototypes to match the visibility and debuggability, which is standard in a virtual prototype.

Recently, pre-built virtual prototypes such as Carbon Performance Analysis Kits (CPAKs) have been playing a much larger role in the embedded design process. These pre-validated systems come complete with all of the hardware and software models needed to be productive. Designers are typically up and running within minutes of download. The system serves as a great starting point to accurately model the performance of the embedded design long before it is built. Since pre-built virtual prototypes support both 100 percent accurate execution as well as 100 MIPS performance, they can be used by all of the design teams in an embedded design. They enable embedded designers to spend less time creating a virtual prototype and more time using that virtual prototype to be productive.
IP-centric LTE Spotlights Security Risks: Devices, Access, Core Elements and Services

As LTE is deployed worldwide, seamless communications amongst all forms of devices and access methods to the All-IP LTE core are advancing daily. There are now more new services, at higher speeds, and with greater reliability than ever before. These advances bring new revenue opportunities but also new and advanced security threats to the IoT, for example.

By Robin Kent, Adax

Historically, carrier-grade telecom networks have had an excellent record for user and network security, however, today's communications infrastructure is more vulnerable than its predecessors. The Internet is becoming an integral part of all communications. With corporate network security breaches everywhere affecting millions of users, networks must address security at all levels.

Attacks can come in many different shapes and sizes; user malware, fraudulent calls, spam, viruses, data and identity theft, and denial of service, to name a few examples. The rise in security threats is partly due to the growing deployment of carrier Wi-Fi access infrastructures and small cells in public areas, offices and homes and will increase exponentially with M2M.

ABI Research predicts that by 2016, half of all small-cell security gateway revenue will come from the enterprise space, reflecting greater exposure to risk and much greater loss potential. Each enterprise site is an IP access point to the network that could potentially be used as an entry point by attackers and hackers. Operators and enterprises need to take steps to ensure their networks are safe, while continuing to respond to the relentless demand for the ubiquitous coverage and faster data speeds both home and enterprise customers expect.

These new security risks are being exposed by the move to the IP-centric LTE architecture. The deployment of LTE is a primary driver behind the security risks as the LTE architecture is much flatter and more IP-centric than 3G, meaning there are fewer steps to access the core network. With 3G, the Radio Network Controller (RNC) controls all access to the base stations meaning that potential hackers can’t get close to the core network. In LTE, IP backhaul is mandatory but the RNC node is eliminated, giving a potential attacker a straighter path to the core network.

Operators recognize that IPsec tunnels will be required at every cell site connected to an insecure network for the purpose of authentication and encryption. See Figure 1.

WHAT’S NO LONGER TRUE ABOUT SECURITY

Operators must be prepared to meet every threat. Security gateways and firewalls have been the go-to device for IP, but not all such devices are configured or priced appropriately to need. To meet today’s threats, no single

Figure 1. A recognized need for authentication and encryption involves IPsec tunnels to deal with connections to insecure networks.
device can be the right fit for all circumstances. Operators need to address security as a multi-level problem. IPsec encryption and authentication provides the most basic layer of user and network security.

LTE IP backhaul creates a major risk, potentially exposing both the control and user data plane to attacks. TDM protocols such as SS7 and end-to-end authentication and encryption in 2G and 3G networks have meant that, historically, wire line and mobile networks have been inherently secure. However, LTE does not benefit from this mandatory protection. Until recently, the growth of IP in telecoms networks has tended to be in the core network, and therefore was secure, as it was far enough away from the user and edge of the network to be protected by traditional security methods. This is no longer true. Protection is imperative at the edge of the core; access protection that only a security gateway can provide. To keep the network running smoothly and safely, the least amount of protocol filtering or packet inspection at this point the better.

**CORE NODE IPSEC AND PROTOCOL FILTERING**

Protecting access to the core network is not enough in LTE networks. As shown in Figure 1, there is a direct path from the eNodeB or small cell directly into the network. If secure access to the core is breached, there are innumerable signaling and bearer paths between core network elements to exploit unless protected internally. Connection protection can be achieved with an embedded IPsec security gateway in each node. This provides encryption of all control and data plane traffic. An advanced security gateway within the core provides checkpoints to ensure that only truly authorized traffic is passing through the network.

**SPOTTING HIDDEN THREATS**

Network security starts with the mobile user and ends up affecting core services. Operators and vendors alike must ensure the highest levels of device security and educate users to protect themselves. Even if encryption is embedded on the device, applications must make use of it, and of course the device itself must be secured by the use of multi-factor authentication. At the end of the day, even the most secure network cannot protect against bad data packets it may receive from compromised devices. In that case, the network must have protection at the receiving end of the connection. Security within the network, especially at data centers and service nodes, must be addressed by security applications with DPI capabilities to identify hidden threats in packet streams and prevent attacks on these essential network services.

Once the network is protected, end-to-end, there can be no performance bottlenecks in terms of throughput and latency. Security cannot simply be effective; it must also be highly efficient.

Operators must choose high-throughput, right-featured, flexible security solutions to ensure their competitive advantage. Only then can they continue to build out their networks to reach more users while also protecting them, and enabling them to take advantage of the growth opportunities available in the expanding ultra-broadband mobile market.

Robin Kent is Director of European Operations at Adax Europe. For many years, Robin held senior positions within established equipment manufacturers, software houses and integrators in the telecom, wide area network, and office automation markets. He joined Adax in 1994 to establish the Adax business unit in Europe. He has overseen the company’s successful transition from an OEM technology supplier to a customer-focused provider of high-quality, high-performance telecommunications products to network equipment providers and VAS companies throughout EMEA and India.
Go With The Best In Motor Control!

Zilog Motor Control Solutions

• Wide range of microcontrollers for your Motor Control applications
• Highly-optimized instruction set that achieves higher performance per clock cycle, with less code space and lower overhead than competing architectures
• World-class development environment for ease of implementation

BLD Universal and Brushed DC Motor Control
- Z8 Encore! F083A Series (28-Pin)
- 3-Phase/Single-Phase AC Induction and PMSM Motor Control
  - Permanent Magnet Synchronous Motors
  - Z16FM C Series Motor Control

Stepper Motor Control
- Z8 Encore! XP F1680 Series (28-Pin)
- BLDC Sensor and Sensorless Motor Control
  - Z8FM C16100 Series Motor Control

The Right Choice for Your Motor Control Needs

For more information, please visit www.zilog.com.
We simplify the use of embedded technology

FAST AND COMPACT
conga-TC97
- COM Express Compact Type 6 module
- Dual-core 5th generation Intel® Core™ i7 processors
- 3x DisplayPort 1.2, up to 4k resolution
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

HIGH END PERFORMANCE
conga-TS87
- COM Express Basic Type 6 module
- Quad-core 4th generation Intel® Core™ i7 processors
- 3x DisplayPort 1.2, up to 4k resolution
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

POWERFUL AND SMALL
conga-MA3/conga-MA3E
- COM Express Mini Type 10 module
- Intel® Atom™ and Intel® Celeron® processors
- Gen 7 Intel® HD graphics
- Extended temperature range option

HIGH PERFORMANCE QSEVEN
conga-QA3
- Qseven module
- Intel® Atom™ and Intel® Celeron® processors
- Gen 7 Intel® HD graphics
- Extended temperature range option

Find more details at: www.congatec.us